LIVRE BLANC 2026

DEEP AUTHENTICITY©

TABLE DES MATIÈRES GÉNÉRALE

Architecture définitive des huit volumes

Note éditoriale. Cette table générale présente l’architecture intellectuelle du Livre Blanc 2026. La pagination définitive sera intégrée lors de l’assemblage du Document Maître final, afin qu’elle corresponde exactement aux pages de la version consolidée.

TRILOGIE DE LA VÉRITÉ

- **3 QR Codes — vérité du produit physique**
- **Empreinte Cryptographique Native — sésame de l’information et des médias**
- **QR Code Dynamique — sésame du document vérifiable**

VOLUME I — VISION ET FONDEMENTS

• Chapitre 1 — Nouveau paradigme : de la confiance déclarative à la vérité vérifiable
• Chapitre 2 — Infrastructure universelle de vérité : physique, numérique et administratif
• Chapitre 3 — Architecture fondamentale des 3 QR Codes
• Chapitre 4 — Passeport Numérique Universel
• Chapitre 5 — AP Core : noyau technologique
• Chapitre 6 — Architecture générale des modules
• Chapitre 7 — Domaine physique
• Chapitre 8 — Domaine numérique
• Chapitre 9 — Domaine administratif et QR Code Dynamique documentaire
• Chapitre 10 — Architecture des données et interopérabilité
• Chapitre 11 — Identités, rôles, droits et gouvernance des accès
• Chapitre 12 — Preuve, provenance, intégrité et temporalité
• Chapitre 13 — Architecture de confiance et fédération
• Chapitre 14 — Écosystème Deep Authenticity©
• Chapitre 15 — Jumeaux numériques : principes fondateurs
• Chapitre 16 — Simulation Institutionnelle Profonde© : principes fondateurs
• Chapitre 17 — Tableaux de bord et intelligence institutionnelle
• Chapitre 18 — Résilience, continuité et souveraineté
• Chapitre 19 — Trajectoire stratégique et déploiement
• Chapitre 20 — Synthèse et conclusion du Volume I

VOLUME II — ARCHITECTURE TECHNOLOGIQUE ET CYBERSÉCURITÉ

• Architecture détaillée : AP Core — AP Ledger — AP Cloud — AP Shield
• Bases de données — API — cryptographie — signature cryptographique native
• Empreinte Cryptographique Native — IA/CNN — IoT/NFC
• Fonctionnement Online/Offline — ERP — identités et droits
• Cybersécurité — haute disponibilité — résilience — déploiement
• Conclusion générale du Volume II

VOLUME III — ÉCOSYSTÈME ÉCONOMIQUE, COMMERCIAL ET FINANCIER

• Chapitre 1 — Producteur : identité économique et tableau de bord
• Chapitre 2 — Revendeur : fenêtre professionnelle et stock authentifié
• Chapitre 3 — Vente, acquisition et continuité commerciale
• Chapitre 4 — Premier acquéreur et propriété numérique
• Chapitre 5 — Seconde Main : marché authentifié
• Chapitre 6 — Transfert numérique sécurisé de propriété
• Chapitre 7 — Propriété : registre et relations patrimoniales
• Chapitre 8 — AP Business

• Chapitre 9 — Recherche commerciale et localisation du revendeur
• Chapitre 10 — Artisans, agriculteurs, créateurs et PME
• Chapitre 11 — AP Finance
• Chapitre 12 — AP Pay
• Chapitre 13 — AP Pay et paiements transfrontaliers
• Chapitre 14 — Traçabilité économique : produit, transaction et propriété
• Chapitre 15 — SaaS : modèle de services et abonnements
• Chapitre 16 — Licences, propriété intellectuelle et gouvernance
• Chapitre 17 — Royalties : gouvernance et audit
• Chapitre 18 — Modèle économique consolidé : création de valeur et soutenabilité
• Chapitre 19 — Tableaux de bord économiques et commerciaux
• Chapitre 20 — Intelligence économique prédictive
• Chapitre 21 — Valeur économique des données agrégées
• Chapitre 22 — Souveraineté économique et commerciale
• Chapitre 23 — Corridors commerciaux de confiance
• Chapitre 24 — Création de valeur pour les acteurs et effets de réseau
• Chapitre 25 — Stratégie d’adoption économique
• Chapitre 26 — Conclusion stratégique : de la confiance à l’économie vérifiable

VOLUME IV — APPLICATIONS SECTORIELLES

- Déclinaisons sectorielles : industrie, artisanat, agriculture, élevage, pharmacie et santé
- Luxe, alimentation, automobile, pièces détachées, art et création
- Propriété intellectuelle, transport, logistique, billetterie et seconde main
- Applications étendues : éducation, Smart City, Water, Government, Defense et autres domaines structurés dans le volume

VOLUME V — DEEP AUTHENTICITY© : DONNÉES, IA ET INTELLIGENCE SYSTÉMIQUE

- Chapitre 1 — Architecture des données, IA et intelligence systémique
- Chapitre 2 — Données internes et externes
- Chapitre 3 — Analyse statistique et intelligence des tendances
- Chapitre 4 — Détection d’anomalies
- Chapitre 5 — Watch System©
- Chapitre 6 — Signaux faibles et détection précoce
- Chapitre 7 — Tableaux de bord économiques et sociaux prévisionnels
- Chapitre 8 — Pénuries et tensions
- Chapitre 9 — Surplus et capacités excédentaires
- Chapitre 10 — Disparités
- Chapitre 11 — Cartographie Dynamique©
- Chapitre 12 — Intelligence prédictive
- Chapitre 13 — Intelligence systémique intersectorielle
- Chapitre 14 — Simulation, scénarios et stress tests
- Chapitre 15 — IA décisionnelle assistive
- Chapitre 16 — Gouvernance, souveraineté et sécurité des données et des modèles IA
- Chapitre 17 — Deep Authenticity© appliqué aux données et aux modèles IA
- Chapitre 18 — AP Ledger et mémoire analytique
- Chapitre 19 — Centre d’intelligence systémique
- Chapitre 20 — Synthèse générale, critères d’acceptation et clôture du Volume V

VOLUME VI — JUMEAU NUMÉRIQUE NATIONAL ET SIMULATION INSTITUTIONNELLE PROFONDE

• Chapitre 1 — Fondements et architecture du Jumeau Numérique National©
• Chapitre 2 — Identité, état, événements et synchronisation
• Chapitre 3 — Jumeau Numérique du Produit
• Chapitre 4 — Jumeau Numérique de l'Entreprise
• Chapitre 5 — Jumeau Numérique du Secteur
• Chapitre 6 — Jumeau Numérique du Territoire
• Chapitre 7 — Jumeau Numérique National©
• Chapitre 8 — Jumeau Numérique Institutionnel
• Chapitre 9 — Modélisation multisectorielle et multi-institutionnelle
• Chapitre 10 — Scénarios et branches de simulation
• Chapitre 11 — Simulation Institutionnelle Profonde©
• Chapitre 12 — Comparaison des décisions
• Chapitre 13 — Passage de la simulation à la décision autorisée
• Chapitre 14 — Exécution réelle et chaîne de mise en œuvre
• Chapitre 15 — Monitoring continu : simulation, décision, exécution et réel
• Chapitre 16 — Apprentissage, recalibrage et amélioration continue
• Chapitre 17 — Gouvernance, sécurité et souveraineté du Jumeau Numérique National©
• Chapitre 18 — Résilience, continuité nationale et modes dégradés
• Chapitre 19 — Centre National de Simulation et d'Intelligence Institutionnelle
• Chapitre 20 — Synthèse, architecture intégrée et conclusion du Volume VI

VOLUME VII — GOUVERNANCE, SOUVERAINETÉ ET DÉPLOIEMENT INTERNATIONAL

• Gouvernance de Deep Authenticity©
• Souveraineté numérique et économique
• Protection des données et souveraineté informationnelle
• Résilience nationale et dépendances stratégiques
• AP Global Secure Trade Program — AP-Certified™ — normalisation
• Corridors de Confiance — coopération entre États
• Diplomatie technologique et déploiement international

VOLUME VIII — STRATÉGIE MONDIALE, IMPACT ET VISION 2040–2050

• Stratégie mondiale et infrastructure universelle de vérité
• Impact économique mondial
• Impact social et humain
• Lutte mondiale contre la contrefaçon
• Commerce éthique et confiance internationale

• Scénarios d’adoption internationale
• Risques géopolitiques, gouvernance et résilience
• Vision civilisationnelle 2040–2050
• Feuille de route 2026–2050 et conclusion prospective

LOGIQUE GÉNÉRALE DE LA COLLECTION

- Volume I — Comprendre le paradigme
- Volume II — Comprendre son fonctionnement technologique
- Volume III — Comprendre son économie
- Volume IV — Comprendre ses applications sectorielles
- Volume V — Comprendre son intelligence systémique
- Volume VI — Comprendre sa capacité institutionnelle de simulation
- Volume VII — Comprendre sa gouvernance et son déploiement mondial
- Volume VIII — Comprendre sa portée mondiale et prospective

Principe transversal. La Trilogie de la Vérité accompagne désormais la lecture des huit volumes : les 3 QR Codes pour le monde physique, l'Empreinte Cryptographique Native pour le monde numérique et le QR Code Dynamique pour le monde documentaire et administratif.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

BLOC D’OUVERTURE CONSOLIDÉ

Édition intégrant le Passeport Numérique Universel

LIVRE BLANC 2026

DEEP AUTHENTICITY©

PRÉFACE GÉNÉRALE DÉFINITIVE — VERSION MISE À JOUR

Une infrastructure universelle de vérité pour le physique, le numérique et l'administratif

« La confiance ne doit plus dépendre seulement de ce qui est affirmé, mais de ce qui peut être vérifié. »

Préface

Nous entrons dans une époque où la capacité de produire, copier, transformer et diffuser dépasse progressivement la capacité humaine à vérifier. Un produit peut être imité. Une image peut être modifiée. Une voix peut être synthétisée. Un document peut être reproduit. Une identité peut être usurpée. Une information peut circuler à l'échelle mondiale avant que son origine ne soit établie.

Face à cette transformation, la question centrale n'est plus seulement de disposer de davantage d' informations. Elle devient : pouvons-nous établir d'où vient un élément, s'il a été altéré, quel est son statut, qui en répond et quelles preuves permettent de lui faire confiance ? C'est à cette question que répond la vision de Deep Authenticity©.

Une infrastructure universelle de vérité

Deep Authenticity© est conçue comme une infrastructure universelle de vérité couvrant trois domaines fondamentaux : le monde physique, le monde numérique et le monde administratif. Son ambition n'est pas de créer une autorité mondiale qui déciderait seule de ce qui est vrai, mais de fournir une infrastructure permettant d'établir plus rigoureusement ce qui peut être prouvé : origine, intégrité, émission, statut, transfert, certification, modification ou révocation.

La Trilogie de la Vérité

Trois mécanismes fondamentaux constituent les sésames complémentaires de Deep Authenticity©. Les 3 QR Codes — Consommateur, Revendeur/Professionnel et Contrôle/Douanes — constituent le cœur du mécanisme anti-contrefaçon d'Authenticity Plus© pour le produit physique. VERT signifie original ; JAUNE signifie original mais déjà vérifié ou vendu ; ROUGE signifie contrefait ou code inexistant dans le système Authenticity Plus©.

L'Empreinte Cryptographique Native constitue le sésame de l'information et des médias. Le QR Code Dynamique constitue le sésame du document vérifiable. Cette Trilogie relie vérité du produit, vérité de l'information et vérité du document.

Le Passeport Numérique Universel — la continuité de la vérité

La vérification ponctuelle ne suffit pas. Un élément authentique aujourd'hui doit pouvoir conserver une continuité de confiance demain. Le Passeport Numérique Universel constitue cette mémoire persistante. Il ne remplace pas la Trilogie de la Vérité : il prolonge dans le temps la preuve établie par les mécanismes natifs.

Dans le domaine physique, la première activation légitime du QR Code Consommateur protégé par le film à gratter déclenche le Passeport Numérique Universel du produit et permet son rattachement initial au premier propriétaire selon les règles applicables. L'authenticité devient alors le point de départ d'une histoire vérifiable : acquisition, propriété, maintenance, rappel, transfert, seconde main et fin de vie.

La formule doctrinale est désormais centrale : « L'authenticité établit la vérité à l'instant de la vérification. Le Passeport Numérique Universel donne à cette vérité une continuité dans le temps. »

De la preuve à l'architecture

AP Core orchestre les relations et les états. AP Ledger peut ancrer les preuves critiques. AP Cloud apporte l'infrastructure de service. AP Shield protège l'écosystème. Les signatures cryptographiques, l'IA, les CNN, l'IoT, le NFC, les modes Online/Offline, les API et les ERP constituent des couches complémentaires : elles étendent la confiance sans remplacer les mécanismes fondamentaux.

Souveraineté et interopérabilité

Une infrastructure universelle crédible ne peut signifier centralisation absolue. Les États, institutions et organisations doivent pouvoir conserver leurs données sensibles, leurs clés, leurs compétences et leurs décisions. Les Nœuds Souverains Nationaux préservent cette maîtrise ; les Corridors de Confiance rendent possible l'échange de preuves nécessaires entre juridictions.

Une infrastructure au service de l'humain

La technologie ne doit pas devenir l'arbitre absolu de la société. Une preuve cryptographique ne décide pas seule de la valeur scientifique, morale, politique ou historique d'un contenu. Une IA ne doit pas transformer une probabilité en culpabilité. Un tableau de bord éclaire une décision sans supprimer la responsabilité humaine. Deep Authenticity© doit rester fondée sur la proportionnalité, la confidentialité, l'auditabilité, la réversibilité, l'explicabilité et le recours.

Une vision civilisationnelle

À son niveau conceptuel le plus élevé, Deep Authenticity© peut être décrite comme le système d'exploitation de la civilisation moderne. Cette expression ne signifie pas qu'elle gouvernerait la civilisation. Elle exprime l'ambition de fournir une couche commune de provenance, d'intégrité, d'identité persistante et de confiance entre les systèmes physiques, numériques et administratifs.

Le sens de ce Livre Blanc

Ce Livre Blanc 2026 présente une architecture, une doctrine et une trajectoire. Il ne prétend pas que toutes les fonctions décrites sont déjà déployées ni que la technologie peut résoudre seule les problèmes de confiance du monde. Il définit un cadre à éprouver par l'ingénierie, les pilotes, la cybersécurité, le droit, l'économie, les institutions et l'expérience réelle des utilisateurs.

Son ambition est de faire passer la société d'une logique où l'on demande principalement « puis-je croire cet élément ? » à une logique où l'on peut demander « quelles preuves me permettent de le vérifier, quelle est son identité et quelle est son histoire vérifiable ? ».

C'est dans cet esprit que s'ouvre le Livre Blanc 2026.

Saïd *Smaallah*
Créateur de Deep Authenticity©

CHAPITRE FONDATEUR SPÉCIAL

LE PASSEPORT NUMÉRIQUE UNIVERSEL

Identité persistante — preuve — propriété — cycle de vie — continuité de la vérité

1. Statut doctrinal du Passeport Numérique Universel

Le Passeport Numérique Universel constitue l'un des piliers structurants du paradigme Authenticity Plus© / Deep Authenticity©. Il ne doit pas être présenté comme une fonctionnalité accessoire, ni comme un simple dossier numérique associé à un produit. Il est la continuité numérique de l'identité vérifiable d'un objet, d'un actif, d'un contenu, d'un document, d'un titre ou d'un droit, selon le domaine concerné et le cadre juridique applicable.

L'authentification répond à une question immédiate : « ce qui est présenté est-il authentique ? ». Le Passeport Numérique Universel répond à une question plus large : «quelle est l'identité vérifiable de cet élément, quelle est son histoire et quel est son état actuel ? ».

La doctrine peut ainsi être résumée par une formule centrale : « L'authenticité établit la vérité à l' instant de la vérification. Le Passeport Numérique Universel donne à cette vérité une continuité dans le temps. »

2. Une identité numérique persistante

Le Passeport Numérique Universel est conçu comme une identité numérique persistante, évolutive et vérifiable. Il accompagne l'élément auquel il est rattaché pendant son cycle de vie et organise les événements autorisés qui modifient son état.

Il ne remplace pas nécessairement les registres, bases de données ou systèmes souverains existants. Il peut agir comme une couche de continuité et de preuve reliant des informations distribuées, sous le contrôle des acteurs compétents et selon des droits d'accès définis.

3. Le domaine physique : naissance du passeport du produit

Dans le domaine physique, l'architecture fondamentale demeure celle des trois QR Codes fonctionnellement distincts d'Authenticity Plus© : QR consommateur, QR revendeur/professionnel et QR contrôle/douanes. Cette architecture reste le mécanisme anti-contrefaçon fondateur.

Le Passeport Numérique Universel complète cette architecture sans s'y substituer. Lors de la première activation légitime du QR Code consommateur protégé par le film à gratter, le système peut déclencher l'activation du passeport numérique du produit et établir son rattachement initial à son premier propriétaire, conformément aux règles de la plateforme et aux droits applicables.

Cette étape transforme le produit authentifié en objet doté d'une continuité numérique vérifiable.

4. Le film à gratter comme événement d'activation

Le film à gratter du QR Code consommateur possède une fonction stratégique : il protège l'accès initial au mécanisme destiné au consommateur et matérialise un événement irréversible ou fortement contrôlé de première activation.

L’enlèvement du film, suivi de la vérification légitime, ne doit donc pas être compris comme un simple geste de lecture d’un QR Code. Dans l’architecture proposée, il peut constituer l’événement qui ouvre le Passeport Numérique Universel du produit, inscrit son entrée dans le cycle de propriété et permet la création de la relation initiale entre le produit et son premier détenteur légitime.

5. La mémoire vérifiable du cycle de vie

Le Passeport Numérique Universel a vocation à conserver ou référencer, selon les autorisations et les exigences de minimisation des données, les événements essentiels du cycle de vie : identité et origine, statut d’authenticité, première activation, changements de propriété, interventions techniques, maintenance, rappels, garanties, certification, seconde main, événements logistiques pertinents et fin de vie.

Il ne s’agit pas de tout centraliser. Le passeport doit pouvoir pointer vers des preuves, statuts ou registres distribués, et restituer uniquement les informations nécessaires à l’acteur autorisé.

6. Propriété et transfert numérique sécurisé

L’un des rôles majeurs du Passeport Numérique Universel est de permettre la continuité entre l’ authenticité du produit et son histoire de propriété. Le transfert numérique sécurisé de propriété permet de faire évoluer le titulaire reconnu dans le système sans rompre la chaîne de preuve.

Cette fonction devient particulièrement importante pour la revente, la seconde main, les biens de valeur, les équipements professionnels et tous les actifs pour lesquels l’origine et la succession des détenteurs peuvent avoir une importance économique, contractuelle ou réglementaire.

7. Articulation avec les statuts de vérification

Pour les produits physiques, l’interprétation utilisateur des trois QR Codes reste stricte : VERT signifie original ; JAUNE signifie original mais déjà vérifié ou vendu ; ROUGE signifie contrefait ou code inexistant dans le système Authenticity Plus©.

Le Passeport Numérique Universel ne remplace pas ces statuts. Il leur donne un contexte temporel et historique. La couleur répond à l’état de la vérification ; le passeport explique l’identité persistante et les événements autorisés qui ont conduit à l’état actuel.

8. AP Core comme moteur d’orchestration

AP Core constitue le noyau technologique chargé d’orchestrer les relations entre identifiants, preuves, droits d’accès, événements, statuts et services de la plateforme. Le Passeport Numérique Universel s’ appuie sur ce noyau pour conserver une cohérence entre les différentes couches de Deep Authenticity©.

Le passeport doit être conçu comme un objet logique gouverné : chaque événement doit être attribuable, horodatable, contrôlable et, lorsque nécessaire, vérifiable cryptographiquement. Les données sensibles doivent rester soumises à des règles de confidentialité, de proportionnalité et de souveraineté.

9. Extension aux trois domaines de la vérité

Le principe du Passeport Numérique Universel s’inscrit dans les trois domaines fondamentaux de Deep Authenticity©.

Dans le physique, il accompagne les objets et produits authentifiés, avec les trois QR Codes comme architecture anti-contrefaçon fondatrice.

Dans le numérique, il peut organiser la continuité d'identité d'un contenu, logiciel, média ou actif de propriété intellectuelle autour de son empreinte cryptographique native, de ses versions, de ses droits et de sa provenance.

Dans l'administratif, il peut relier l'identité persistante d'un document, d'un titre ou d'un droit à son QR Code Dynamique documentaire et à l'état vivant reconnu par l'autorité ou le registre compétent.

Ces déclinaisons doivent respecter la nature propre de chaque domaine et ne doivent pas être confondues avec un mécanisme unique appliqué indistinctement.

10. Passeport et Nœuds Souverains Nationaux

Dans une architecture internationale, les Nœuds Souverains Nationaux peuvent jouer un rôle essentiel pour préserver la maîtrise nationale des données, des registres et des règles d'accès. Le Passeport Numérique Universel n'implique donc pas la création d'une base mondiale unique concentrant toutes les informations.

La logique recherchée est celle d'une fédération de preuves et de statuts : Deep Authenticity© fournit une infrastructure d'interopérabilité et de vérification, tandis que les États, autorités et organismes compétents conservent la maîtrise des données et décisions qui relèvent de leur souveraineté.

11. Un passeport évolutif plutôt qu'un certificat statique

Un certificat traditionnel décrit généralement un état à un moment donné. Le Passeport Numérique Universel est conçu pour évoluer. Il peut recevoir de nouveaux événements, changer de statut, enregistrer un transfert, signaler une révocation, une maintenance ou une fin de validité, tout en préservant la continuité de l'identité de référence.

Cette caractéristique est fondamentale : le paradigme ne consiste plus seulement à produire une preuve initiale, mais à maintenir une relation vérifiable entre identité, état et histoire.

12. Valeur économique et institutionnelle

À l'échelle économique, le Passeport Numérique Universel peut réduire les ruptures d'information entre producteur, distributeur, consommateur, marché de seconde main, assureur, réparateur et autorité de contrôle. Il peut faciliter la traçabilité, la confiance commerciale et la valorisation des produits dont l' histoire est vérifiable.

À l'échelle institutionnelle, les informations agrégées et dûment gouvernées peuvent contribuer aux tableaux de bord, aux mécanismes d'alerte, aux jumeaux numériques et aux capacités de simulation de Deep Authenticity©, sans transformer le passeport individuel en instrument de surveillance généralisée.

13. Principe de minimisation et contrôle des accès

Universalité ne signifie pas visibilité universelle. Le Passeport Numérique Universel doit distinguer les informations publiques, professionnelles, réglementaires et privées. Chaque catégorie d'acteur ne doit accéder qu'aux informations nécessaires à sa fonction et autorisées par le cadre applicable.

Cette séparation est indispensable pour concilier vérifiabilité, protection des données, secret commercial, sécurité et souveraineté.

14. Formule fondatrice

Le principe général peut être formulé ainsi :

« Tout objet, contenu, document, titre ou actif vérifiable susceptible de créer, transmettre ou représenter une valeur doit pouvoir disposer d'une identité numérique persistante, vérifiable et évolutive : son Passeport Numérique Universel. »

Cette formule donne au passeport sa véritable place : non pas une fonction parmi d'autres, mais l' instrument de continuité qui relie la preuve initiale à l'histoire future de l'élément vérifié.

15. Position dans l'architecture générale de Deep Authenticity©

Le Passeport Numérique Universel doit désormais apparaître explicitement dans l'architecture doctrinale du Livre Blanc. La hiérarchie peut être lue ainsi : les mécanismes natifs de vérité établissent la preuve dans chaque domaine ; AP Core orchestre cette preuve ; le Passeport Numérique Universel lui donne une continuité d'identité et de cycle de vie ; les modules spécialisés exploitent cette continuité ; les tableaux de bord, jumeaux numériques et simulations utilisent ensuite les informations autorisées et agrégées.

Dans cette architecture, le Passeport Numérique Universel constitue le pont entre l'authentification ponctuelle et la confiance durable.

16. Conclusion stratégique

Deep Authenticity© vise une infrastructure universelle de vérité. Une telle infrastructure ne peut se limiter à dire si un élément est authentique au moment où il est contrôlé. Elle doit pouvoir maintenir, dans le respect des droits et des souverainetés, la continuité de son identité, de son état et de son histoire.

Le Passeport Numérique Universel remplit précisément cette fonction. Il transforme une preuve isolée en continuité vérifiable.

Pour le produit physique, cette continuité naît de l'architecture fondatrice des trois QR Codes et prend une dimension particulière lors de l'activation légitime du QR Code consommateur protégé par le film à gratter. Pour le numérique et l'administratif, elle s'adapte aux mécanismes natifs propres à ces domaines.

Le Passeport Numérique Universel doit ainsi être considéré comme l'un des fondements majeurs permettant à Authenticity Plus© / Deep Authenticity© de passer de l'authentification d'un instant à une infrastructure de confiance dans le temps.

TABLE GÉNÉRALE DES MATIÈRES

LIVRE BLANC 2026 — DEEP AUTHENTICITY©

ARCHITECTURE GÉNÉRALE EN HUIT VOLUMES

OUVERTURE GÉNÉRALE

Couverture officielle — Droits d'auteur et propriété intellectuelle — Page institutionnelle et doctrinale — Préface générale mise à jour — Trilogie de la Vérité — Chapitre fondateur spécial : Le Passeport Numérique Universel — Table générale des matières — Introduction générale mise à jour.

CHAPITRE FONDATEUR SPÉCIAL — LE PASSEPORT NUMÉRIQUE UNIVERSEL

Position doctrinale : après la Trilogie de la Vérité et avant l'entrée dans les huit volumes. Le Passeport Numérique Universel assure la continuité d'identité, de preuve, de propriété et de cycle de vie des éléments vérifiables de Authenticity Plus© / Deep Authenticity©.

VOLUME I — FONDATIONS, VISION ET ARCHITECTURE GÉNÉRALE

Fondements du paradigme — architecture générale — mécanismes natifs — Passeport Numérique Universel renforcé — AP Core — principes structurants.

VOLUME II — INFRASTRUCTURE TECHNOLOGIQUE, SÉCURITÉ ET PREUVE

AP Core — AP Ledger — AP Cloud — AP Shield — cryptographie — IoT/NFC — Online/Offline — API/ERP — continuité technologique du Passeport Numérique Universel.

VOLUME III — ÉCOSYSTÈME ÉCONOMIQUE, COMMERCIAL ET FINANCIER

Producteur — Revendeur — premier propriétaire — transfert sécurisé — seconde main — AP Business — AP Finance — AP Pay — continuité économique du Passeport Numérique Universel.

VOLUME IV — APPLICATIONS SECTORIELLES

Industrie — artisanat — agriculture — pharmacie — santé — luxe — automobile — alimentation — art — propriété intellectuelle — documents — transport — billetterie — seconde main — extensions sectorielles du Passeport.

VOLUME V — DONNÉES, IA ET INTELLIGENCE SYSTÉMIQUE

Événements vérifiables — agrégation — Watch Systems — signaux faibles — tableaux de bord — IA — prévision — séparation entre faits, statistiques, prédictions et simulations.

VOLUME VI — JUMEAU NUMÉRIQUE NATIONAL ET SIMULATION INSTITUTIONNELLE PROFONDE

Passeport = continuité du réel — Jumeau Numérique = représentation structurée — Simulation Institutionnelle Profonde = exploration des futurs possibles — monitoring continu.

VOLUME VII — GOUVERNANCE, SOUVERAINETÉ ET CONFIANCE INTERINSTITUTIONNELLE

Nœuds Souverains Nationaux — Corridors de Confiance — fédération — gouvernance des identités et des clés — audit — protection des données — continuité transfrontalière.

VOLUME VIII — VISION MONDIALE ET TRAJECTOIRE CIVILISATIONNELLE

Interopérabilité mondiale — résilience — économie circulaire — continuité générationnelle — mémoire vérifiable de la valeur — Deep Authenticity© comme système d'exploitation de la civilisation moderne.

CLÔTURE GÉNÉRALE

Conclusion générale mise à jour — Vision du créateur — principes de déploiement — page institutionnelle finale.

NOTE ÉDITORIALE

Cette table générale constitue la structure de navigation définitive du Livre Blanc 2026 après réintégration du Passeport Numérique Universel. Les intitulés détaillés des chapitres et sous-chapitres demeurent dans les sommaires propres aux huit Documents Maîtres Consolidés.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

INTRODUCTION GÉNÉRALE DÉFINITIVE — VERSION MISE À JOUR

De l'authentification du produit à une infrastructure universelle de vérité et de continuité

1. Le point de départ : rendre l'authenticité vérifiable

Authenticity Plus© est né d'une exigence fondamentale : permettre à un produit physique de démontrer son authenticité et de conserver une continuité de confiance au cours de son cycle de vie. L'architecture des trois QR Codes fonctionnellement distincts — Consommateur, Revendeur/Professionnel et Contrôle/Douanes — demeure le mécanisme fondateur de lutte contre la contrefaçon.

2. Du produit au Passeport Numérique Universel

Le QR Code Consommateur protégé par un film à gratter introduit l'événement décisif de première activation. Lors de sa première activation légitime, il déclenche le Passeport Numérique Universel du produit et permet, selon les règles applicables, son rattachement au premier propriétaire. Le Passeport devient la continuité numérique de l'identité vérifiée : création, distribution, acquisition, propriété, transfert, maintenance, seconde main, rappel et fin de vie.

3. Une sémantique universelle

Dans le domaine physique, l'interprétation utilisateur reste stable : VERT signifie original ; JAUNE signifie original mais déjà vérifié ou vendu ; ROUGE signifie contrefait ou code inexistant dans le système Authenticity Plus©.

4. Le changement d'échelle : Deep Authenticity©

Deep Authenticity© élargit la question initiale à la provenance, l'intégrité, le statut et la continuité de ce sur quoi une société fonde sa confiance. Elle couvre trois domaines : physique, numérique et administratif.

5. La Trilogie de la Vérité

Le physique repose sur les 3 QR Codes d'Authenticity Plus©. Le numérique repose sur l'Empreinte Cryptographique Native. L'administratif repose sur le QR Code Dynamique. Cette Trilogie de la Vérité constitue le socle transversal du Livre Blanc 2026.

6. Le Passeport comme quatrième articulation transversale

Le Passeport Numérique Universel n'est pas un quatrième mécanisme natif de vérité : il est l' articulation de continuité qui prolonge les trois mécanismes dans le temps. Son principe est universel, tandis que sa preuve source reste propre à chaque domaine. Il relie identité persistante, provenance, statut, événements, propriété ou droits lorsque pertinents, et cycle de vie.

7. Une infrastructure fédérée

La vocation universelle de Deep Authenticity© n'implique pas une concentration mondiale des données. Les Nœuds Souverains Nationaux permettent à chaque pays de conserver sous sa gouvernance les éléments critiques relevant de sa souveraineté. Les Corridors de Confiance permettent l'interopérabilité entre juridictions.

8. De la preuve à l'intelligence systémique

Les événements vérifiables et gouvernés issus des passeports peuvent, sous forme appropriée et souvent agrégée, alimenter tableaux de bord, Watch Systems, intelligence prédictive, cartographies, Jumeaux Numériques et Simulation Institutionnelle Profonde. Faits, agrégats, prédictions et simulations doivent rester explicitement distingués.

9. Une architecture économique, sectorielle et institutionnelle

Le Livre Blanc examine la manière dont l'infrastructure accompagne producteurs, artisans, agriculteurs, créateurs, revendeurs, consommateurs, entreprises, administrations, États et organisations. AP Business, AP Finance, AP Pay, AP Ledger, AP Cloud, AP Shield, AP Léger et les autres modules constituent des couches spécialisées autour du noyau de confiance.

10. La logique des huit volumes

Les huit volumes suivent une progression volontaire : fondements ; infrastructure technologique ; écosystème économique ; applications sectorielles ; données et intelligence ; Jumeau Numérique et Simulation Institutionnelle Profonde ; gouvernance et souveraineté ; stratégie mondiale et vision civilisationnelle. Le Passeport Numérique Universel traverse désormais ces huit niveaux comme infrastructure de continuité.

11. Une ambition accompagnée de limites

Le Livre Blanc décrit une architecture, une doctrine et une trajectoire. Il ne signifie pas que toutes les fonctions exposées sont déjà déployées, ni qu'une technologie puisse garantir à elle seule la vérité d' une déclaration ou la légitimité d'une décision. La valeur recherchée réside dans la vérifiabilité, l' attribution, la traçabilité, l'auditabilité et la responsabilité.

12. Une vision civilisationnelle

À son niveau conceptuel le plus élevé, Deep Authenticity© peut être envisagé comme le système d' exploitation de la civilisation moderne : une couche commune de vérification, de provenance, d' identité persistante, de continuité et de confiance entre les systèmes physiques, numériques et administratifs.

13. Objet du Livre Blanc 2026

Le Livre Blanc 2026 formalise cette architecture dans un corpus cohérent, distingue ses mécanismes fondamentaux de ses couches complémentaires, examine ses applications, ses conditions de souveraineté, ses limites, ses modèles de déploiement et ses perspectives. Le Passeport Numérique Universel y occupe désormais explicitement sa place de pilier transversal de continuité.

AUTHENTIFIER — PROUVER — ACTIVER LE PASSEPORT — TRACER — TRANSFÉRER — RELIER — COMPRENDRE — ANTICIPER — SIMULER — DÉCIDER — MESURER — APPRENDRE

Une continuité de confiance entre le physique, le numérique et l'administratif.

Livre Blanc 2026 — Authenticity Plus© / Deep Authenticity© — Document Maître Définitif

VOLUME I — VISION ET FONDEMENTS

CHAPITRE 1 — LE NOUVEAU PARADIGME DE LA VÉRITÉ VÉRIFIABLE

PARADIGME — PREUVE — CONFIANCE — AUTHENTICITÉ — PROVENANCE — RESPONSABILITÉ — INTEROPÉRABILITÉ — SOUVERAINETÉ

1. Objet du chapitre

Ce chapitre établit le fondement intellectuel du Livre Blanc 2026. Deep Authenticity© part d'un constat : dans une civilisation où les objets, contenus, documents, identités et transactions circulent à une vitesse croissante, la confiance ne peut plus reposer uniquement sur l'apparence, la déclaration ou la réputation. Elle doit pouvoir être soutenue, lorsque l'enjeu le justifie, par une preuve vérifiable.

2. La crise contemporaine de la confiance

La numérisation a démultiplié la capacité de produire, copier, modifier et diffuser. Un produit peut imiter l'original ; un contenu peut être synthétique ; un document peut être falsifié ; une identité peut être usurpée. La difficulté centrale n'est donc plus seulement d'accéder à l'information, mais d'établir son origine, son intégrité, son statut et la responsabilité de ceux qui l'émettent.

3. De la confiance déclarative à la confiance vérifiable

Le paradigme proposé ne supprime pas la confiance humaine. Il la complète par une infrastructure permettant de vérifier certaines affirmations critiques. Une preuve vérifiable doit pouvoir répondre à des questions simples : qui a émis l'élément ? à quoi est-il relié ? a-t-il été modifié ? quel est son statut actuel ? quelle autorité ou organisation répond de l'information présentée ?

4. La preuve n'est pas la vérité absolue

Deep Authenticity© ne prétend pas déterminer une vérité philosophique, scientifique, politique ou morale universelle. Elle organise la vérifiabilité d'éléments précis. Une signature peut établir l'origine d' un document sans garantir que toutes ses affirmations sont exactes. Cette distinction entre preuve, authenticité, intégrité et vérité factuelle constitue une limite fondamentale du système.

5. Les trois domaines de Deep Authenticity©

L'infrastructure englobe trois domaines fondamentaux. Le physique couvre les objets et produits. Le numérique couvre logiciels, médias, contenus et propriété intellectuelle. L'administratif couvre documents, identités et titres de propriété. Deep Authenticity© vise à relier ces trois mondes par une grammaire commune de provenance, de statut, de droits et de preuve.

6. Le domaine physique et Authenticity Plus©

Dans le domaine physique, Authenticity Plus© constitue la fondation anti-contrefaçon. Son architecture repose sur trois QR codes fonctionnellement distincts : un QR consommateur, un QR revendeur/professionnel et un QR contrôle/douanes. Les autres technologies — IA, IoT, cryptographie, traçabilité et analytique — sont des couches complémentaires.

7. La sémantique fondamentale VERT / JAUNE / ROUGE

La lecture utilisateur doit rester immédiate : VERT signifie original ; JAUNE signifie original mais déjà vérifié ou vendu ; ROUGE signifie contrefaçon ou code inexistant dans le système Authenticity Plus©.

Cette sémantique simple constitue l'interface visible d'un mécanisme de contrôle plus profond et doit rester stable dans les futurs modules.

8. Le Passeport Numérique Universel

Le paradigme se prolonge par un Passeport Numérique Universel capable d'accompagner un produit, un actif, un contenu ou un élément vérifiable à travers son cycle de vie. Il peut référencer identité, provenance, événements, certifications, propriété et statuts selon les droits d'accès. Universalité signifie interopérabilité, non centralisation de toutes les données.

9. AP Core : le noyau de confiance

AP Core peut être compris comme le noyau orchestrant les identités, preuves, événements, droits, règles de vérification et interfaces entre modules. Son rôle est de garantir une cohérence transversale sans obliger chaque secteur à utiliser exactement les mêmes processus. Le noyau doit rester modulaire, auditable et interopérable.

10. Les modules comme extensions spécialisées

Autour du noyau, les modules répondent à des besoins spécialisés : sécurité, ledger, cloud, entreprise, paiement, santé, billetterie, certification, modes allégés et autres applications sectorielles. Le principe architectural est important : les modules étendent la capacité de Deep Authenticity© ; ils ne doivent pas brouiller son fondement de preuve et d'authentification.

11. De la traçabilité à la continuité de preuve

La traçabilité traditionnelle décrit un parcours. Deep Authenticity© vise une continuité de preuve : chaque événement important peut être relié à une identité, un moment, un acteur habilité et un statut. Cette continuité peut soutenir contrôle, transfert de propriété, rappel, seconde main, certification et analyse de chaînes de valeur.

12. Le rôle de l'intelligence artificielle

L'IA peut détecter des anomalies, analyser des images, comparer des comportements ou identifier des signaux faibles. Elle reste une couche d'assistance. Une probabilité produite par un modèle ne doit pas être confondue avec une preuve cryptographique, une certification, une décision administrative ou le statut déterminé par l'architecture fondamentale d'Authenticity Plus©.

13. Jumeaux numériques : représenter pour comprendre

Les jumeaux numériques permettent de représenter un produit, une entreprise, un secteur, un territoire ou une institution à partir de données structurées. Lorsqu'ils sont alimentés par des informations suffisamment fiables, ils peuvent faciliter la compréhension des flux, dépendances, anomalies, capacités et évolutions dans le temps.

14. Simulation Institutionnelle Profonde

La Simulation Institutionnelle Profonde étend cette logique à l'exploration de décisions. Elle peut permettre de tester des scénarios, d'estimer des conséquences et d'organiser un monitoring continu après mise en œuvre. Elle ne remplace pas la décision politique : elle fournit un environnement d'aide à la décision dont les hypothèses et incertitudes doivent rester visibles.

15. Résilience comme condition de confiance

Une infrastructure de vérité vérifiable doit continuer à fonctionner dans un monde imparfait : pannes, coupures de réseau, cyberattaques, crises géopolitiques et changements technologiques. La

résilience exige redondance, modes dégradés, sauvegardes, migration cryptographique, procédures de reprise et capacité à préserver la mémoire probante.

16. Souveraineté comme principe d'architecture

Deep Authenticity© ne doit pas exiger que les États ou institutions abandonnent leurs données à une base mondiale unique. Une architecture fédérée peut permettre aux informations sensibles de rester sous contrôle souverain tout en échangeant les preuves nécessaires. L'interopérabilité doit relier les souverainetés, non les dissoudre.

17. De l'authentification à l'infrastructure de vérité

Le changement de paradigme consiste à passer d'une solution centrée sur l'authentification d'un produit à une infrastructure capable de relier plusieurs formes de preuve. Authenticity Plus© reste la racine du domaine physique ; Deep Authenticity© généralise la logique de vérifiabilité aux mondes numérique et administratif.

18. Une infrastructure au service des acteurs

Producteurs, consommateurs, entreprises, administrations, douanes, créateurs et citoyens n'ont pas les mêmes besoins. Le système doit donc distribuer les droits et informations selon les fonctions. La confiance vérifiable ne signifie pas que chacun voit tout ; elle signifie que chacun peut vérifier ce qu'il est légitimement autorisé et appelé à vérifier.

19. Le système d'exploitation de la civilisation moderne

Dans sa formulation conceptuelle la plus élevée, Deep Authenticity© peut être décrite comme « le système d'exploitation de la civilisation moderne ». L'expression désigne une couche commune permettant aux objets, contenus, documents, droits et institutions d'établir des relations vérifiables. Elle ne désigne ni un gouvernement mondial ni une autorité absolue de vérité.

20. Critères d'acceptation et conclusion

Le nouveau paradigme est cohérent si la preuve reste distincte du jugement ; si les trois domaines physique, numérique et administratif sont clairement définis ; si Authenticity Plus© et ses trois QR codes restent la fondation du domaine physique ; si le Passeport Numérique Universel organise la continuité sans centralisation excessive ; si l'IA reste complémentaire ; si les jumeaux numériques et la simulation restent des outils d'aide ; et si résilience, souveraineté, droits et interopérabilité sont intégrés dès l'origine.

Deep Authenticity© ne part donc pas de l'idée que tout doit être contrôlé. Elle part de l'idée que ce qui engage fortement la confiance devrait pouvoir être accompagné d'une preuve dont la provenance, la portée et la responsabilité sont compréhensibles.

Ce principe constitue le point de départ du Volume I et de l'ensemble du Livre Blanc 2026.

Le Chapitre 2 développera Deep Authenticity© comme infrastructure universelle de vérité et précisera l'architecture des trois domaines fondamentaux.

Note de cadrage institutionnel

Les notions de « vérité vérifiable », d'« infrastructure universelle de vérité » et de « système d' exploitation de la civilisation moderne » constituent le cadre conceptuel propre à Deep Authenticity©.

Elles décrivent une ambition architecturale et prospective ; elles ne constituent ni une norme internationale reconnue ni une délégation d'autorité juridique, scientifique ou politique.

VOLUME I — VISION ET FONDEMENTS

CHAPITRE 2 — DEEP AUTHENTICITY© : INFRASTRUCTURE UNIVERSELLE DE VÉRITÉ ET ARCHITECTURE DES TROIS DOMAINES

INFRASTRUCTURE — PHYSIQUE — NUMÉRIQUE — ADMINISTRATIF — PREUVE — PROVENANCE — INTÉGRITÉ — INTEROPÉRABILITÉ — SOUVERAINETÉ — CONTINUITÉ

1. Objet du chapitre

Ce chapitre définit Deep Authenticity© comme une infrastructure universelle de vérité vérifiable organisée autour de trois domaines fondamentaux : le physique, le numérique et l'administratif. L' objectif n'est pas de fusionner ces mondes dans une base unique, mais de leur fournir une architecture commune permettant d'établir provenance, intégrité, statut, droits et responsabilité.

2. Pourquoi une infrastructure universelle

La civilisation moderne utilise des systèmes spécialisés pour les produits, les contenus, les identités, les documents et les droits. Leur fragmentation crée des ruptures de confiance : une preuve valable dans un système devient parfois difficile à interpréter dans un autre. Deep Authenticity© vise à créer une couche d'interopérabilité de la preuve entre ces environnements.

3. Premier domaine — le physique

Le domaine physique comprend objets, produits, matières, équipements et actifs tangibles. Son problème central est de relier de manière fiable l'objet réel à son identité numérique, puis de préserver cette relation pendant production, distribution, vente, transfert, contrôle, maintenance, seconde main et fin de vie.

4. Authenticity Plus© : fondation du domaine physique

Authenticity Plus© constitue le mécanisme anti-contrefaçon fondamental de ce domaine. Son architecture repose sur trois QR codes fonctionnellement distincts : consommateur, revendeur/professionnel et contrôle/douanes. Cette séparation distribue les fonctions de vérification selon les acteurs et réduit la dépendance à un point de contrôle unique.

5. Les trois statuts fondamentaux

La lecture des QR codes conserve une sémantique définitive : VERT signifie original ; JAUNE signifie original mais déjà vérifié ou vendu ; ROUGE signifie contrefaçon ou code inexistant dans le système Authenticity Plus©. Les informations complémentaires peuvent varier selon les secteurs, mais cette interprétation centrale doit rester stable.

6. Deuxième domaine — le numérique

Le domaine numérique comprend logiciels, médias, contenus, créations, données publiées et propriété intellectuelle. Son défi principal est la provenance : déterminer quelle source a émis un élément, si son intégrité a été préservée, quelles transformations sont documentées et quels droits ou licences lui sont associés.

7. Signature cryptographique native des contenus

Deep Authenticity© peut associer aux contenus des mécanismes de signature cryptographique native, d'horodatage, de versionnement et de provenance. Ces mécanismes permettent d'établir des faits sur l'origine ou l'intégrité d'un contenu. Ils ne doivent jamais être présentés comme une garantie automatique de la véracité de toutes les affirmations qu'il contient.

8. Troisième domaine — l'administratif

Le domaine administratif comprend documents, identités, certificats, autorisations, diplômes, actes et titres de propriété. La fonction de Deep Authenticity© est de permettre la vérification de l'émetteur, du statut, de l'intégrité et de la continuité de ces éléments sans se substituer aux autorités qui leur donnent leur valeur juridique.

9. Les registres souverains restent souverains

Un registre foncier, un registre d'état civil ou une base administrative nationale ne doit pas être absorbé automatiquement par Deep Authenticity©. L'infrastructure peut vérifier ou transporter des preuves émises par ces systèmes tout en laissant les données sources, compétences et décisions sous le contrôle des autorités compétentes.

10. La grammaire commune des trois domaines

Malgré leurs différences, les trois domaines peuvent partager des primitives : identité de l'émetteur, identifiant de l'élément, signature, horodatage, provenance, statut, droits, événements et preuve d' intégrité. Cette grammaire commune permet l'interopérabilité sans imposer un modèle métier identique à tous les secteurs.

11. AP Core comme couche d'orchestration

AP Core assure la cohérence entre ces primitives et les modules spécialisés. Il peut gérer identités, événements, politiques d'accès, vérifications, relations entre preuves et interfaces d'intégration. Il constitue un noyau transversal, tandis que les données métier peuvent rester distribuées dans les systèmes compétents.

12. Le Passeport Numérique Universel comme continuité

Le Passeport Numérique Universel fournit une continuité logique entre l'élément vérifié et les preuves autorisées qui l'accompagnent. Pour un produit, il peut relier origine, cycle de vie et propriété ; pour un contenu, provenance et versions ; pour un document, émetteur, statut et historique de validité.

13. Relations entre physique et numérique

Un objet physique peut être relié à des documents numériques, logiciels embarqués, certificats ou contenus de maintenance. Deep Authenticity© permet de vérifier ces relations sans confondre les objets eux-mêmes. Une preuve numérique doit toujours préciser à quel objet, version ou événement physique elle se rapporte.

14. Relations entre physique et administratif

Produits et actifs peuvent dépendre d'autorisations, certificats, contrôles douaniers, titres ou décisions administratives. L'infrastructure peut relier ces éléments afin qu'un acteur habilité puisse vérifier non seulement l'identité du produit, mais aussi certains statuts institutionnels pertinents.

15. Relations entre numérique et administratif

Un document administratif peut être entièrement numérique ; un logiciel peut nécessiter une autorisation ; une œuvre numérique peut porter des droits de propriété intellectuelle. La couche commune permet de relier identité, autorité, signature, droits et versions tout en respectant les régimes juridiques propres à chaque élément.

16. Architecture fédérée et souveraineté

L'universalité de Deep Authenticity© doit être compatible avec la souveraineté. Les preuves peuvent être échangées entre systèmes fédérés sans imposer la centralisation des données. Les États, institutions et entreprises conservent leurs systèmes, tandis que les mécanismes communs permettent d'établir une compréhension vérifiable entre eux.

17. Interopérabilité avec l'existant

Deep Authenticity© doit pouvoir s'intégrer aux ERP, systèmes douaniers, registres, plateformes industrielles, solutions IoT et services numériques existants par API et standards adaptés. La stratégie consiste à ajouter une couche de confiance plutôt qu'à exiger le remplacement systématique des infrastructures déjà opérationnelles.

18. Sécurité, confidentialité et proportionnalité

Une infrastructure transversale augmente la valeur des relations entre données ; elle doit donc limiter les corrélations inutiles. Les droits d'accès, la minimisation, la segmentation, le chiffrement, l'audit et la séparation des fonctions doivent empêcher que l'interopérabilité devienne une transparence totale ou une surveillance universelle.

19. Deep Authenticity© comme architecture intégrée

Les trois domaines forment ensemble une architecture cohérente : Authenticity Plus© protège l' identité du produit physique ; les mécanismes de provenance protègent l'origine et l'intégrité numériques ; les mécanismes administratifs relient les preuves aux autorités et droits. AP Core et le Passeport Numérique Universel assurent leur continuité logique.

20. Critères d'acceptation et conclusion

L'architecture des trois domaines est cohérente si chacun conserve ses règles propres ; si Authenticity Plus© et ses trois QR codes restent la fondation du physique ; si la provenance numérique reste distincte de la vérité factuelle ; si les autorités administratives conservent leurs compétences ; si AP Core orchestre sans centraliser inutilement ; si le Passeport Numérique Universel relie les preuves de manière proportionnée ; et si l'interopérabilité respecte souveraineté, sécurité et réversibilité.

Deep Authenticity© devient ainsi une infrastructure universelle non parce qu'elle possède toutes les données, mais parce qu'elle fournit une architecture commune permettant à des mondes différents de comprendre et de vérifier leurs relations.

Le Chapitre 3 développera en profondeur l'architecture fondamentale des trois QR codes d' Authenticity Plus©, leur séparation fonctionnelle, leur sécurité et leur rôle dans la chaîne mondiale d' authentification.

Note de cadrage institutionnel

Les expressions « infrastructure universelle de vérité » et « architecture des trois domaines » désignent le cadre conceptuel de Deep Authenticity©. Elles n'impliquent ni centralisation mondiale obligatoire, ni reconnaissance juridique automatique, ni substitution aux registres, autorités ou standards existants.

VOLUME I — VISION ET FONDEMENTS

CHAPITRE 3 — AUTHENTICITY PLUS© : ARCHITECTURE FONDAMENTALE DES TROIS QR CODES

3 QR CODES — CONSOMMATEUR — REVENDEUR — CONTRÔLE — DOUANES — AUTHENTIFICATION — ANTI-CONTREFAÇON — STATUTS — TRAÇABILITÉ — PROPRIÉTÉ

1. Objet du chapitre

Ce chapitre définit l'architecture anti-contrefaçon fondamentale d'Authenticity Plus© dans le domaine physique. Elle repose sur trois QR codes fonctionnellement distincts, associés à une unité de produit et destinés respectivement au consommateur, au revendeur/professionnel et au contrôle/douanes. Cette architecture constitue le mécanisme central autour duquel les autres capacités de Deep Authenticity© viennent se greffer.

2. Pourquoi trois QR codes

Un seul point de vérification ne répond pas aux mêmes besoins tout au long de la chaîne. Le consommateur, le professionnel et l'autorité de contrôle disposent de responsabilités, d'informations et de droits différents. La séparation en trois QR codes permet de distribuer les fonctions, de limiter les accès et de créer plusieurs niveaux de contrôle autour du même produit.

3. Le QR Consommateur

Le QR Consommateur permet à l'acheteur ou à l'utilisateur final d'interroger Authenticity Plus© afin de vérifier l'existence et le statut du produit. Il constitue l'interface publique de confiance. Les informations affichées doivent être compréhensibles, proportionnées et limitées à ce qui est utile à la vérification et au Passeport Numérique Universel.

4. Le QR Revendeur / Professionnel

Le QR Revendeur / Professionnel est destiné aux acteurs habilités de la chaîne commerciale. Il peut servir à intégrer le produit dans l'environnement du revendeur, confirmer certaines opérations, accompagner la vente et alimenter la continuité de traçabilité. Ses droits sont distincts de ceux du consommateur afin de protéger les fonctions professionnelles.

5. Le QR Contrôle / Douanes

Le QR Contrôle / Douanes est destiné aux agents et autorités habilités. Il permet un niveau de vérification adapté aux contrôles officiels, avec authentification de l'agent ou mécanisme d' autorisation lorsque nécessaire. Son existence renforce la capacité de contrôle sans exposer au public les informations ou fonctions réservées.

6. Séparation fonctionnelle

Les trois QR codes sont liés au même produit mais ne sont pas interchangeables. Chacun représente une fonction et un niveau d'accès. Cette séparation permet d'appliquer le principe du moindre privilège :

chaque acteur accède uniquement aux opérations et informations correspondant à son rôle dans le système.

7. Protection physique et couche à gratter

Selon la configuration du produit et le niveau de risque, les QR codes sensibles peuvent être protégés par une couche ou un élément à gratter afin de limiter leur consultation ou copie avant le moment légitime de vérification. La protection physique complète la sécurité numérique en introduisant un indice d'accès ou d'utilisation.

8. Les statuts VERT, JAUNE et ROUGE

La sémantique utilisateur est définitive : VERT signifie original ; JAUNE signifie original mais déjà vérifié ou vendu ; ROUGE signifie contrefaçon ou code inexistant dans le système Authenticity Plus©. Ces statuts doivent rester simples et cohérents quels que soient le secteur, l'interface ou le module complémentaire.

9. Le statut comme état du système

Le résultat d'une vérification ne doit pas être compris comme une information imprimée dans le QR lui-même. Le code sert à identifier ou à adresser une preuve dans Authenticity Plus© ; le système évalue alors l'état enregistré, les règles applicables et les événements pertinents avant de restituer le statut autorisé.

10. Première vérification et changement d'état

Lorsqu'une règle sectorielle prévoit qu'une première vérification ou une vente modifie le statut, l'événement est enregistré afin que les vérifications suivantes puissent refléter cette évolution. Le passage éventuel de VERT à JAUNE devient ainsi un signal anti-réutilisation : une copie d'un code déjà utilisé ne se comporte plus comme un code jamais vérifié.

11. Détection des codes inexistants

Lorsqu'un identifiant présenté ne correspond à aucun code valide enregistré dans Authenticity Plus©, le système restitue le statut ROUGE. Cette distinction est fondamentale : l'apparence graphique d'un QR ne constitue jamais une preuve d'existence dans l'infrastructure.

12. Détection des anomalies d'usage

Des scans incompatibles avec l'historique attendu — répétitions anormales, géographies incohérentes, séquences impossibles ou comportements atypiques — peuvent alimenter des mécanismes complémentaires d'analyse. Ces signaux renforcent l'investigation mais doivent rester distincts du mécanisme fondamental de vérification des codes.

13. Lien avec le Passeport Numérique Universel

Les QR codes constituent des points d'accès au Passeport Numérique Universel du produit selon le rôle de l'utilisateur. Le passeport peut référencer provenance, fabricant, lot, certifications, événements, propriété ou maintenance. Chaque acteur ne reçoit que les informations correspondant à ses droits et à la finalité de la consultation.

14. Transfert numérique sécurisé de propriété

L'architecture peut accompagner un transfert numérique de propriété lorsque le produit et le cadre d'usage le prévoient. La vente ou la cession peut être enregistrée comme événement, avec

authentification des parties et règles de validation. Cette continuité renforce les usages de seconde main et la lutte contre la réintroduction frauduleuse.

15. Fenêtre Revendeur et visibilité commerciale

Le QR professionnel peut contribuer à l'intégration du produit dans la Fenêtre Revendeur d'Authenticity Plus©. Lorsqu'un produit est correctement enregistré chez un professionnel, les services autorisés peuvent aider le consommateur à identifier un revendeur disposant du produit, sans exposer inutilement des informations internes.

16. Contrôle douanier et coopération institutionnelle

Le troisième QR permet d'adapter Authenticity Plus© aux contrôles de frontières, inspections et opérations institutionnelles. Les autorités peuvent disposer de données ou de fonctions supplémentaires selon leurs habilitations. L'objectif est de renforcer la capacité de vérification officielle tout en conservant une séparation nette avec les usages commerciaux et publics.

17. Sécurité cryptographique et AP Core

AP Core orchestre l'identité des codes, les droits, événements et règles de vérification. Des mécanismes cryptographiques peuvent protéger les échanges, signatures, jetons d'accès et preuves critiques. La cryptographie renforce les trois QR codes ; elle ne remplace pas leur séparation fonctionnelle, qui demeure le principe architectural fondamental.

18. Compléments IA, IoT et AP Ledger

L'IA peut détecter des anomalies ; l'IoT ou le NFC peuvent renforcer le lien avec certains produits ; AP Ledger peut ancrer des événements probants. Ces capacités sont complémentaires. L'identité anti-contrefaçon du domaine physique doit rester compréhensible même lorsqu'un produit n'utilise pas toutes ces technologies supplémentaires.

19. Distinction avec le QR Code Dynamique documentaire

L'architecture des trois QR codes d'Authenticity Plus© concerne le domaine physique. Elle doit être distinguée du QR Code Dynamique documentaire de Deep Authenticity©, utilisé dans le domaine administratif pour interroger l'état vivant d'un document — validité, version, expiration, révocation ou remplacement. Les deux mécanismes appartiennent à la même infrastructure de vérité vérifiable mais répondent à des logiques fonctionnelles différentes.

20. Critères d'acceptation et conclusion

LIVRE BLANC 2026 — DEEP AUTHENTICITY©

VOLUME I — VISION ET FONDEMENTS

CHAPITRE 4 — LE PASSEPORT NUMÉRIQUE UNIVERSEL

Identité persistante — propriété — cycle de vie — continuité de la vérité

1. Objet et statut fondateur

Le Passeport Numérique Universel constitue l'un des piliers structurants de Authenticity Plus© / Deep Authenticity©. L'architecture générale du Livre Blanc place déjà le Passeport Numérique Universel parmi les fondements du Volume I, aux côtés des trois QR Codes et d'AP Core. La présente version renforce cette position doctrinale.

Le Passeport Numérique Universel n'est pas un simple dossier numérique. Il représente la continuité numérique de l'identité vérifiable d'un élément au cours du temps. L'authentification établit une vérité à un instant donné ; le Passeport Numérique Universel organise la persistance de cette identité, de son état et de son histoire vérifiable.

2. La chaîne fondatrice du paradigme

Dans le Volume I, la logique doit être lue comme une chaîne continue : infrastructure universelle de vérité → mécanismes natifs de vérité → architecture des trois QR Codes pour le domaine physique → Passeport Numérique Universel → AP Core → domaines et modules → intelligence systémique, jumeaux numériques et simulation.

Cette hiérarchie évite deux confusions : le Passeport Numérique Universel ne remplace pas le mécanisme anti-contrefaçon des trois QR Codes ; inversement, les QR Codes ne résument pas toute la vie numérique du produit. Les premiers établissent et protègent l'accès à la preuve ; le passeport assure la continuité de l'identité vérifiée.

3. Naissance de l'identité numérique du produit

Dans le domaine physique, le producteur crée l'identité numérique du produit et les éléments nécessaires à son inscription dans Authenticity Plus©. Le produit reçoit l'architecture des trois QR Codes fonctionnellement distincts : consommateur, revendeur/professionnel et contrôle/douanes.

Cette architecture demeure le mécanisme anti-contrefaçon fondateur du domaine physique. Le Passeport Numérique Universel vient prolonger cette fondation en donnant au produit une mémoire numérique persistante et évolutive.

4. Le QR consommateur sous film à gratter : porte d'activation

Le QR Code consommateur protégé par un film à gratter possède une fonction déterminante. Le retrait du film, suivi d'une première vérification légitime, constitue l'événement d'activation du Passeport Numérique Universel du produit.

Cette opération ne doit pas être décrite comme un simple scan. Elle marque le passage d'un produit mis en circulation à un produit dont l'identité numérique entre dans une relation active avec son premier propriétaire légitime.

5. Rattachement au premier propriétaire

Lors de cette première activation légitime, le Passeport Numérique Universel peut être rattaché au premier propriétaire selon les règles d'identité, de consentement, de confidentialité et de droit applicables.

Le rattachement crée un point de départ vérifiable pour l'histoire de propriété. Il permet ensuite de distinguer l'identité permanente du produit de l'identité successive de ses détenteurs. Le produit reste le même ; son propriétaire peut changer.

6. Séquence opérationnelle de référence

La séquence fondatrice du domaine physique est la suivante :

Fabrication → création de l'identité numérique → génération et association des trois QR Codes → mise en circulation → retrait du film à gratter du QR consommateur → première vérification légitime → activation du Passeport Numérique Universel → rattachement au premier propriétaire → événements de cycle de vie → transfert sécurisé de propriété → seconde main → clôture ou fin de vie.

Cette séquence doit devenir une référence transversale du Livre Blanc 2026.

7. Mémoire vérifiable du cycle de vie

Le Passeport Numérique Universel conserve ou référence, selon les droits d'accès, les événements utiles à l'histoire du produit : origine, fabrication, authenticité, première activation, propriété, garanties, certifications, maintenance, réparations, rappels, changements de statut, transferts, seconde main et fin de vie.

La vocation du passeport n'est pas de centraliser indistinctement toutes les données. Il organise une continuité vérifiable et peut relier des preuves distribuées, des registres, des systèmes industriels ou administratifs et des services autorisés.

8. Transfert sécurisé de propriété

Le transfert de propriété constitue une fonction majeure du Passeport Numérique Universel. Lorsqu'un produit est cédé, le système doit permettre le passage contrôlé du statut de propriétaire d'un titulaire au suivant sans rompre l'histoire vérifiable du produit.

Cette continuité donne une base structurante à la seconde main : l'acheteur ne reçoit pas seulement un objet ; il peut recevoir, selon les règles applicables, la continuité vérifiable de son identité numérique et de son historique autorisé.

9. Articulation avec VERT, JAUNE et ROUGE

Pour les trois QR Codes du domaine physique, la signification utilisateur demeure impérative : VERT signifie original ; JAUNE signifie original mais déjà vérifié ou vendu ; ROUGE signifie contrefait ou code inexistant dans le système Authenticity Plus©.

Le Passeport Numérique Universel ne modifie pas cette règle. Il donne au statut instantané un contexte historique : identité du produit, activation, événements et chaîne de propriété autorisée.

10. AP Core et le Passeport Numérique Universel

AP Core orchestre les identités, preuves, statuts, événements, droits et relations nécessaires au fonctionnement du Passeport Numérique Universel. Il assure la cohérence entre la preuve initiale et les événements ultérieurs sans confondre donnée, preuve et décision.

Le passeport devient ainsi un objet logique gouverné : ses événements importants doivent pouvoir être attribués, horodatés, contrôlés et, lorsque nécessaire, protégés ou vérifiés cryptographiquement.

11. Extension à la Trilogie de la Vérité

Le principe de continuité du Passeport Numérique Universel s'étend aux trois domaines de Deep Authenticity©, avec des mécanismes natifs distincts.

Dans le physique, il s'articule avec les trois QR Codes. Dans le numérique, il peut accompagner l' Empreinte Cryptographique Native, les versions, la provenance et les droits d'un contenu ou actif

numérique. Dans l'administratif, il peut s'articuler avec le QR Code Dynamique documentaire et l'état vivant reconnu par l'autorité ou le registre compétent.

L'universalité réside dans le principe de continuité d'identité ; elle n'impose pas un mécanisme technique identique aux trois domaines.

12. Interopérabilité et souveraineté

Le Passeport Numérique Universel doit pouvoir fonctionner dans une architecture fédérée. Il n'exige pas une base mondiale unique. Les données peuvent demeurer auprès des producteurs, institutions, registres et Nœuds Souverains Nationaux compétents tandis que Deep Authenticity© assure l' interopérabilité des preuves et statuts autorisés.

Cette conception permet de rechercher une portée universelle sans effacer la souveraineté des États ni la responsabilité des autorités compétentes.

13. Du produit au système de confiance

Le Passeport Numérique Universel transforme la relation au produit. Avant lui, la vérification peut rester un événement ponctuel. Avec lui, l'authenticité devient le point de départ d'une histoire numérique vérifiable.

Cette histoire peut alimenter, sous forme autorisée et éventuellement agrégée, les services de traçabilité, les tableaux de bord, les mécanismes d'alerte, les jumeaux numériques et les capacités de simulation de Deep Authenticity©.

14. Principe doctrinal

La doctrine du Volume I doit désormais être formulée sans ambiguïté :

« L'authenticité établit la vérité à l'instant de la vérification. Le Passeport Numérique Universel donne à cette vérité une continuité dans le temps. »

Et son principe universel :

« Tout objet, contenu, document, titre ou actif vérifiable susceptible de créer, transmettre ou représenter une valeur doit pouvoir disposer d'une identité numérique persistante, vérifiable et évolutive : son Passeport Numérique Universel. »

15. Conclusion

Le Passeport Numérique Universel est le pont entre l'authentification et la continuité. Dans le domaine physique, son activation par le QR consommateur protégé par le film à gratter et son rattachement au premier propriétaire donnent une portée nouvelle à l'architecture des trois QR Codes.

Authentifier établit la vérité. Le Passeport Numérique Universel conserve son identité. La traçabilité construit son histoire. Le transfert assure sa continuité. Deep Authenticity© rend cette continuité vérifiable dans le temps.

À partir de ce chapitre, le Passeport Numérique Universel doit être traité dans les volumes suivants comme une infrastructure transversale d'identité et de cycle de vie, et non comme une fonctionnalité secondaire.

Note éditoriale — Ce chapitre constitue la version renforcée définitive du Passeport Numérique Universel pour le Volume I. Le chapitre fondateur placé dans l'ouverture expose la doctrine générale ; le présent chapitre en fixe l'application aux fondements du Volume I.

Le Passeport Numérique Universel est cohérent si l'identité reste persistante ; si l'historique est distingué de l'état actuel ; si les droits d'accès sont différenciés ; si Authenticity Plus© reste la fondation du passeport physique ; si le QR Code Dynamique documentaire reflète l'état vivant des documents administratifs ; si les certifications conservent leur niveau d'assurance ; si AP Core orchestre sans centraliser inutilement ; et si interopérabilité, souveraineté, confidentialité et réversibilité sont préservées.

Le Passeport Numérique Universel transforme ainsi l'authentification ponctuelle en continuité de preuve. Il permet à un élément de conserver une histoire vérifiable à travers les systèmes, les acteurs et le temps.

Cette continuité constitue l'un des ponts fondamentaux entre les trois domaines de Deep Authenticity©.

Le Chapitre 5 développera AP Core : noyau technologique, orchestration des identités, preuves, événements, droits, API et interopérabilité.

Note de cadrage institutionnel

Le Passeport Numérique Universel est un concept architectural de Deep Authenticity©. Son contenu, sa valeur juridique, ses durées de conservation et ses mécanismes d'accès doivent être adaptés aux secteurs et juridictions concernés. Le QR Code Dynamique documentaire est explicitement distingué de l'architecture des trois QR codes d'Authenticity Plus© appliquée aux produits physiques.

VOLUME I — VISION ET FONDEMENTS

CHAPITRE 5 — AP CORE : NOYAU TECHNOLOGIQUE, ORCHESTRATION DES PREUVES ET INTEROPÉRABILITÉ

AP CORE — IDENTITÉS — PREUVES — ÉVÉNEMENTS — DROITS — API — INTEROPÉRABILITÉ — SÉCURITÉ — ORCHESTRATION — SOUVERAINETÉ

1. Objet du chapitre

Ce chapitre définit AP Core comme le noyau technologique transversal de Deep Authenticity©. Sa fonction est d'orchestrer identités, preuves, événements, statuts, droits et interfaces entre les trois domaines — physique, numérique et administratif — sans transformer l'infrastructure en base de données mondiale unique.

2. AP Core comme noyau d'orchestration

AP Core ne doit pas être compris comme un module métier supplémentaire. Il constitue la couche centrale qui applique les règles communes de vérification, relie les composants et distribue les

demandes vers les services compétents. Les modules sectoriels s'appuient sur ce noyau tout en conservant leurs logiques propres.

3. Gestion des identités techniques

AP Core doit pouvoir reconnaître les identités nécessaires au fonctionnement : produit, document, contenu, organisation, système, appareil ou acteur habilité. L'identité technique ne signifie pas nécessairement identité civile complète. Le niveau d'identification doit rester proportionné au risque et à la fonction.

4. Orchestration des preuves

Une preuve peut provenir d'Authenticity Plus©, d'une signature cryptographique, d'une certification, d' un registre souverain, d'un événement AP Ledger ou d'un système externe reconnu. AP Core relie ces preuves, conserve leur provenance et restitue leur portée sans les présenter comme équivalentes lorsqu'elles ont des niveaux d'assurance différents.

5. Orchestration des événements

Création, vérification, vente, transfert, certification, maintenance, révocation ou remplacement peuvent constituer des événements. AP Core applique les règles déterminant qui peut produire l'événement, quelles preuves sont nécessaires, quelles conséquences il entraîne et quels systèmes doivent être informés.

6. Moteur de statuts

Le noyau peut calculer ou restituer des statuts à partir des règles et événements autorisés. Dans Authenticity Plus©, il doit préserver la sémantique fondamentale : VERT — original ; JAUNE — original mais déjà vérifié ou vendu ; ROUGE — contrefaçon ou code inexistant dans le système Authenticity Plus©.

7. Les trois QR codes et AP Core

Les QR consommateur, revendeur/professionnel et contrôle/douanes constituent trois portes fonctionnelles du domaine physique. AP Core identifie le contexte de consultation, applique les droits correspondants et interroge l'état pertinent. Il renforce l'architecture des trois QR codes sans remplacer leur séparation fonctionnelle.

8. QR Code Dynamique documentaire

Dans le domaine administratif, AP Core joue un rôle essentiel pour le QR Code Dynamique documentaire. Lorsqu'un document est consulté, le noyau peut interroger son état vivant et restituer, selon les droits, sa validité, sa version, son expiration, sa révocation ou son remplacement. Ce mécanisme reste distinct des trois QR codes du produit physique.

9. Gestion des droits et habilitations

AP Core doit appliquer des politiques d'accès granulaires. Un consommateur, un revendeur, un producteur, un contrôleur, une administration ou un système automatisé ne disposent pas des mêmes droits. Les autorisations doivent être limitées dans leur portée, leur durée et leur finalité, avec traçabilité des opérations sensibles.

10. API et interfaces

Les API constituent l'un des principaux moyens d'intégrer Deep Authenticity© aux ERP, systèmes logistiques, registres, plateformes publiques, solutions IoT et applications tierces. Elles doivent

exposer des fonctions documentées, versionnées et sécurisées, tout en limitant les données retournées au strict nécessaire.

11. Interopérabilité par conception

L'interopérabilité ne consiste pas à imposer un logiciel unique. AP Core doit pouvoir utiliser des identifiants, formats et protocoles documentés permettant à plusieurs systèmes de comprendre une preuve ou un statut. Des adaptateurs peuvent relier des infrastructures anciennes sans obliger leur remplacement immédiat.

12. AP Core et Passeport Numérique Universel

Le Passeport Numérique Universel représente la continuité de l'élément ; AP Core orchestre les opérations qui le font évoluer. Lorsqu'un événement est validé, le noyau peut mettre à jour les références, droits ou statuts du passeport tout en laissant certaines données détaillées dans leurs systèmes sources.

13. AP Core et AP Ledger

AP Ledger peut recevoir l'ancrage de certains événements critiques, empreintes ou références probantes. AP Core décide, selon les politiques applicables, quels événements nécessitent cet ancrage et comment vérifier leur cohérence. Le ledger renforce l'auditabilité mais ne doit pas devenir le dépôt systématique de toutes les données.

14. AP Core et intelligence artificielle

Les moteurs d'IA peuvent fournir à AP Core des scores d'anomalie, classifications ou alertes. Ces résultats doivent être identifiés comme analyses algorithmiques. AP Core ne doit pas transformer automatiquement une probabilité en preuve définitive lorsqu'une validation humaine, cryptographique ou institutionnelle est requise.

15. AP Core et IoT

Capteurs, NFC, puces ou équipements connectés peuvent transmettre des événements liés à certains produits ou infrastructures. AP Core doit vérifier l'identité de la source, l'intégrité du message et l' autorisation de l'événement avant de l'intégrer au cycle de preuve. L'IoT reste une extension selon les secteurs.

16. Sécurité du noyau

Parce qu'AP Core relie des fonctions critiques, sa sécurité doit intégrer séparation des privilèges, chiffrement, authentification forte, journalisation, gestion des secrets, segmentation, supervision et procédures de réponse aux incidents. Les composants critiques doivent éviter les dépendances uniques lorsque le niveau de risque le justifie.

17. Résilience et modes dégradés

AP Core doit prévoir les conséquences d'une perte de réseau, d'un service externe indisponible ou d' une panne régionale. Certaines vérifications peuvent être temporairement limitées ou fonctionner en mode dégradé lorsque des preuves préalablement sécurisées le permettent. Le système doit indiquer clairement lorsqu'une vérification n'est pas complète ou temps réel.

18. Souveraineté et déploiement fédéré

AP Core doit pouvoir être déployé dans des architectures où les États, institutions ou organisations conservent leurs données sensibles et certaines fonctions localement. La fédération permet l'échange

de preuves entre noyaux ou systèmes compatibles sans créer une dépendance obligatoire à une infrastructure centrale mondiale.

19. Gouvernance et évolution d'AP Core

Les règles, API, mécanismes cryptographiques et modèles de preuve évolueront. AP Core doit donc être versionné, documenté, auditable et réversible. Les changements critiques doivent préserver la capacité d'interpréter les preuves historiques et permettre des migrations sans rupture arbitraire des droits ou des statuts.

20. Critères d'acceptation et conclusion

AP Core est cohérent si son rôle reste celui d'un noyau d'orchestration ; si les identités et droits sont proportionnés ; si les preuves conservent leur provenance et leur niveau d'assurance ; si les trois QR codes d'Authenticity Plus© restent la fondation du domaine physique ; si le QR Code Dynamique documentaire permet la vérification de l'état vivant des documents ; si les API favorisent l' interopérabilité ; si AP Ledger, IA et IoT restent des couches complémentaires ; et si sécurité, résilience, souveraineté et réversibilité sont intégrées dès la conception.

AP Core constitue ainsi le moteur de cohérence de Deep Authenticity© : il ne possède pas nécessairement toutes les données, mais il sait quelles preuves interroger, quelles règles appliquer, quels droits respecter et comment relier les événements entre systèmes.

Cette fonction d'orchestration permet à Deep Authenticity© de passerd'une collection de modules à une infrastructure intégrée de vérité vérifiable.

Le Chapitre 6 développera l'architecture générale des modules de Deep Authenticity© et leur articulation autour d'AP Core.

Note de cadrage institutionnel

AP Core est présenté ici comme l'architecture logique centrale de Deep Authenticity©. Les choix définitifs de protocoles, standards, mécanismes cryptographiques, modèles de déploiement et API devront être précisés lors de la conception technique, des audits de sécurité et des intégrations sectorielles.

VOLUME I — VISION ET FONDEMENTS

CHAPITRE 6 — ARCHITECTURE GÉNÉRALE DES MODULES DE DEEP AUTHENTICITY©

MODULES — AP CORE — AP LEDGER — AP CLOUD — AP SHIELD — AP BUSINESS — AP PAY — AP HEALTH — BILLETTERIE — CERTIFICATION — ÉCOSYSTÈME

1. Objet du chapitre

Ce chapitre présente l'architecture générale des modules de Deep Authenticity© et leur articulation autour d'AP Core. L'objectif est de construire un écosystème modulaire dans lequel chaque

composant répond à une fonction spécialisée tout en partageant une même logique de preuve, d'identité, de droits, d'interopérabilité et de souveraineté.

2. Une architecture modulaire plutôt qu'un système monolithique

Deep Authenticity© ne doit pas devenir une application unique tentant d'exécuter toutes les fonctions. AP Core constitue le noyau commun ; les modules spécialisés peuvent être activés selon le secteur, l'organisation et le niveau de maturité. Cette modularité réduit la complexité, facilite les évolutions et limite les dépendances inutiles.

3. Authenticity Plus© : fondation opérationnelle du physique

Authenticity Plus© demeure le socle anti-contrefaçon du domaine physique avec ses trois QR codes fonctionnellement distincts : consommateur, revendeur/professionnel et contrôle/douanes. Les statuts restent VERT — original ; JAUNE — original mais déjà vérifié ou vendu ; ROUGE — contrefaçon ou code inexistant dans le système Authenticity Plus©.

4. AP Ledger : mémoire probante

AP Ledger peut ancrer certains événements, empreintes, changements de statut ou références critiques afin de renforcer leur auditabilité. Il n'a pas vocation à recevoir toutes les données de l'écosystème. Sa fonction est de préserver une mémoire probante sélectionnée, vérifiable et résistante à l'altération.

5. AP Cloud : infrastructure de services

AP Cloud regroupe les services nécessaires au fonctionnement distribué de la plateforme : hébergement, synchronisation, stockage autorisé, traitements et exposition sécurisée de services. Son architecture doit rester compatible avec des déploiements souverains, hybrides ou fédérés lorsque les données ne peuvent pas être centralisées.

6. AP Shield : sécurité transversale

AP Shield représente la couche de protection de l'écosystème : authentification, surveillance, gestion des menaces, politiques d'accès, détection d'anomalies, protection des interfaces et réponse aux incidents. Il complète la sécurité propre à chaque module et contribue à une posture cohérente à l'échelle de Deep Authenticity©.

7. AP Business : environnement économique

AP Business peut organiser les fonctions destinées aux producteurs, entreprises, distributeurs et professionnels : gestion des produits, visibilité commerciale, tableaux de bord, intégration des stocks, suivi des événements et interactions avec les services de vérification. Il constitue une interface entre la preuve et l'activité économique.

8. Fenêtre Revendeur

La Fenêtre Revendeur permet aux professionnels autorisés d'intégrer et gérer les produits liés à Authenticity Plus©. Elle peut contribuer à la visibilité des produits disponibles et permettre aux consommateurs de localiser des revendeurs disposant d'un produit recherché, selon les règles de confidentialité et de publication définies.

9. Seconde main et continuité de propriété

Une fenêtre dédiée aux produits d'occasion peut exploiter le Passeport Numérique Universel et le transfert sécurisé de propriété. Elle permet de préserver l'authenticité et l'historique pertinent lors de la

revente, tout en distinguant clairement la preuve d'authenticité, l'état matériel du produit et les responsabilités du vendeur.

10. AP Finance et AP Pay

Les fonctions financières peuvent prolonger la logique de preuve vers certains flux monétaires et règlements. AP Pay peut être conçu pour relier paiement, identité des parties, transaction autorisée et événement économique vérifiable. Toute mise en œuvre doit respecter les réglementations financières, les licences et les infrastructures de paiement applicables.

11. AP Health

AP Health peut organiser la continuité vérifiable de certaines informations de santé, prescriptions, actes ou parcours de soins selon les autorisations applicables. Il s'agit d'un domaine hautement sensible : confidentialité, consentement, sécurité, séparation des rôles et réglementation doivent primer sur toute ambition de centralisation.

12. AP Billetterie

AP Billetterie peut appliquer les principes d'identité et de statut aux titres d'accès pour transports, stades, cinémas, événements ou autres services. Un billet numérique peut disposer d'un statut vérifiable avant et après utilisation, réduisant certaines formes de duplication et facilitant les contrôles par smartphone ou terminal habilité.

13. AP-Certified™

AP-Certified™ peut constituer un cadre de certification lié à des exigences vérifiables. Il doit distinguer clairement la certification de l'authentification : un produit peut être authentique sans être certifié selon un référentiel particulier. Chaque certification doit indiquer son émetteur, sa portée, sa durée et ses critères.

14. AP Léger

AP Léger vise les organisations ou contextes disposant de capacités techniques limitées. Il doit fournir un accès simplifié aux fonctions essentielles sans supprimer les garanties fondamentales de sécurité et de preuve. Cette approche favorise l'inclusion des artisans, petites entreprises, producteurs et territoires moins équipés.

15. Modules d'analyse et tableaux de bord

Les données autorisées issues des modules peuvent alimenter des tableaux de bord destinés aux producteurs, entreprises ou institutions : volumes, anomalies, flux, stocks, rappels, expirations, tendances ou indicateurs territoriaux. Les agrégations doivent conserver une traçabilité suffisante vers les sources et leurs limites.

16. Jumeaux numériques

Les Jumeaux Numériques peuvent exploiter les données vérifiées provenant de plusieurs modules afin de représenter produits, entreprises, secteurs, territoires ou institutions. Ils constituent une couche d' analyse supérieure et non une source autonome de vérité. Leur fiabilité dépend directement de la qualité et de la fraîcheur des données sous-jacentes.

17. Simulation Institutionnelle Profonde

La Simulation Institutionnelle Profonde peut s'appuyer sur les jumeaux numériques et tableaux de bord pour explorer des scénarios de décision. Elle permet de comparer des hypothèses, anticiper

certains effets et organiser le monitoring après décision. Elle reste une fonction d'aide à la décision et ne remplace pas l'autorité institutionnelle.

18. Modules et trois domaines fondamentaux

Certains modules sont principalement physiques, d'autres numériques ou administratifs, mais AP Core permet leurs interactions. Le QR Code Dynamique documentaire appartient au domaine administratif et permet d'interroger l'état vivant d'un document ; il demeure distinct de l'architecture des trois QR codes d'Authenticity Plus© appliquée aux produits physiques.

19. Gouvernance de l'écosystème modulaire

Chaque module doit disposer d'un périmètre, de droits, d'API, de responsabilités et de critères de sécurité clairement définis. L'ajout d'un nouveau module ne doit pas modifier silencieusement les principes fondamentaux du système. AP Core, la gouvernance des versions et les audits assurent la cohérence de l'ensemble.

20. Critères d'acceptation et conclusion

L'architecture modulaire est cohérente si AP Core demeure le noyau d'orchestration ; si Authenticity Plus© reste la fondation du domaine physique ; si chaque module possède une fonction clairement délimitée ; si AP Ledger, AP Cloud et AP Shield assurent des fonctions transversales distinctes ; si les modules sectoriels peuvent évoluer indépendamment ; si AP Léger préserve l'accessibilité ; si Jumeaux Numériques et Simulation Institutionnelle Profonde restent des couches d'analyse ; et si souveraineté, sécurité, interopérabilité et réversibilité s'appliquent à tout l'écosystème.

Deep Authenticity© apparaît ainsi non comme une juxtaposition d'applications, mais comme une architecture modulaire cohérente organisée autour d'un noyau commun de vérité vérifiable.

Cette structure permet d'étendre progressivement la plateforme à de nouveaux secteurs sans perdre son identité fondamentale.

Le Chapitre 7 développera le domaine physique dans son ensemble : objets, produits, producteurs, distribution, contrôle, seconde main et continuité de traçabilité.

Note de cadrage institutionnel

La nomenclature et le périmètre des modules décrits dans ce chapitre constituent l'architecture fonctionnelle de référence du Livre Blanc 2026. Leur mise en œuvre technique, réglementaire et commerciale pourra être progressive et sectorielle. Aucun module spécialisé ne doit être interprété comme remplaçant AP Core ou l'architecture fondamentale des trois QR codes d'Authenticity Plus© dans le domaine physique.

VOLUME I — VISION ET FONDEMENTS

CHAPITRE 7 — LE DOMAINE PHYSIQUE : OBJETS, PRODUITS ET CONTINUITÉ DE TRAÇABILITÉ

PHYSIQUE — PRODUITS — 3 QR CODES — PRODUCTEURS — DISTRIBUTION — CONTRÔLE — SECONDE MAIN — PROPRIÉTÉ — TRAÇABILITÉ — PASSEPORT
Livre Blanc 2026 — Authenticity Plus© / Deep Authenticity© — Document Maître Définitif

1. Objet du chapitre

Ce chapitre définit le domaine physique de Deep Authenticity© : l'ensemble des objets, produits et actifs tangibles auxquels une identité numérique et une continuité de preuve peuvent être associées. Authenticity Plus© en constitue la fondation anti-contrefaçon, tandis que le Passeport Numérique Universel, AP Core et les modules complémentaires prolongent cette identité pendant tout le cycle de vie.

2. Relier l'objet réel à son identité numérique

Le premier défi consiste à établir une relation suffisamment robuste entre l'objet physique et son identité dans le système. Cette relation doit résister autant que possible à la copie, à la substitution et à la réutilisation frauduleuse. Les mécanismes physiques, numériques et organisationnels sont combinés selon le niveau de risque du produit.

3. Architecture fondamentale des trois QR codes

Authenticity Plus© repose sur trois QR codes fonctionnellement distincts : consommateur, revendeur/professionnel et contrôle/douanes. Ils sont associés au même produit mais remplissent des fonctions différentes. Cette architecture constitue le mécanisme central du domaine physique et ne doit pas être remplacée par les couches complémentaires.

4. Protection des codes et élément à gratter

Lorsque le cas d'usage le requiert, les QR codes sensibles peuvent être protégés par une couche à gratter ou un dispositif physique équivalent. Cette protection limite l'accès anticipé et peut fournir un indice d'utilisation. Elle complète la vérification numérique, sans être considérée seule comme une preuve d'authenticité.

5. Statuts VERT, JAUNE et ROUGE

La sémantique fondamentale demeure inchangée : VERT signifie original ; JAUNE signifie original mais déjà vérifié ou vendu ; ROUGE signifie contrefaçon ou code inexistant dans le système Authenticity Plus©. Cette lecture simple doit rester cohérente pour les utilisateurs, indépendamment du secteur ou de l'interface.

6. Producteurs et création de l'identité

Le producteur ou l'acteur habilité initialise l'identité du produit, ses références et les données nécessaires à son Passeport Numérique Universel. Les procédures d'émission doivent empêcher la création non autorisée de codes et assurer la traçabilité des lots, séries ou unités selon la granularité retenue.

7. Tableau de bord producteur

Le tableau de bord producteur peut regrouper activation des produits, volumes, statuts, zones de vérification, anomalies, stocks déclarés, rappels, certifications et indicateurs de distribution. Les graphiques et analyses doivent distinguer les données constatées des estimations ou alertes produites par les moteurs analytiques.

8. Distribution et chaîne logistique

Les événements logistiques autorisés peuvent enrichir la continuité de preuve : sortie d'usine, réception, transfert, stockage ou livraison. Deep Authenticity© n'a pas besoin de remplacer les

systèmes logistiques existants ; AP Core peut relier les événements pertinents provenant d'ERP ou d' autres plateformes.

9. Revendeur et environnement professionnel

Le QR Revendeur/Professionnel permet au commerçant habilité d'interagir avec le produit selon ses droits. Il peut contribuer à l'intégration du produit dans la Fenêtre Revendeur, à la gestion de certaines opérations commerciales et à la confirmation d'événements nécessaires à la continuité du cycle de vie.

10. Recherche du produit et proximité

Lorsqu'un revendeur choisit de rendre son stock ou sa disponibilité visible, les services d'Authenticity Plus© peuvent permettre au consommateur de rechercher un produit et d'identifier des points de vente pertinents, notamment selon la proximité. La visibilité commerciale reste distincte des informations internes du professionnel.

11. Vente et changement de statut

La vente ou la première vérification peut, selon les règles du produit, déclencher un changement d'état enregistré par AP Core. Le passage de VERT à JAUNE signale alors qu'un code authentique a déjà été vérifié ou que le produit a été vendu, contribuant à détecter certaines tentatives de réutilisation frauduleuse.

12. Transfert numérique sécurisé de propriété

Pour les biens concernés, Deep Authenticity© peut accompagner la cession par un transfert numérique sécurisé de propriété. Le Passeport Numérique Universel conserve la continuité de l'actif, tandis que les données personnelles des propriétaires restent protégées et accessibles uniquement selon les droits applicables.

13. Seconde main

La seconde main constitue un prolongement naturel de l'architecture. Un acheteur peut vérifier l' authenticité et certains éléments d'historique autorisés avant acquisition. Le système doit toutefois distinguer clairement authenticité, propriété, état matériel, garantie et qualité commerciale : une preuve d'authenticité ne certifie pas automatiquement l'état du bien.

14. Contrôle et douanes

Le QR Contrôle/Douanes fournit une porte de vérification réservée aux acteurs habilités. Il peut permettre l'accès à des informations ou fonctions de contrôle supplémentaires selon les accords et cadres applicables. Cette séparation protège les fonctions institutionnelles tout en maintenant la cohérence avec les vérifications consommateur et professionnel.

15. Rappels, non-conformités et maintenance

Le Passeport Numérique Universel peut relier un produit à un rappel, une campagne de maintenance, une révision ou une non-conformité. Les acteurs autorisés peuvent ainsi identifier les unités concernées et diffuser un statut ou une alerte adaptée sans remettre en cause l'authenticité intrinsèque du produit lorsqu'elle reste établie.

16. IoT, NFC et capteurs

Pour certains produits, une puce NFC, un capteur ou un dispositif IoT peut renforcer le lien entre l'objet et son identité, ou transmettre des événements supplémentaires. Ces technologies sont

complémentaires aux trois QR codes. Leur utilisation dépend du coût, du risque, de la durabilité et des contraintes du secteur.

17. Intelligence artificielle et détection d'anomalies

L'IA peut analyser images, comportements de scan, incohérences géographiques ou séquences atypiques afin de détecter des signaux de fraude. Elle augmente la capacité d'investigation mais ne doit pas remplacer les mécanismes fondamentaux de preuve. Les scores d'anomalie doivent rester identifiables comme résultats analytiques.

18. Du produit individuel au jumeau numérique

Les données vérifiées de nombreux produits peuvent alimenter des jumeaux numériques de chaînes, entreprises, secteurs ou territoires. Ces représentations peuvent aider à comprendre flux, stocks, anomalies, rappels ou pénuries. Leur fiabilité dépend de la couverture, de la fraîcheur et de la qualité des données sources.

19. Résilience, offline et souveraineté

Le domaine physique doit rester exploitable dans des contextes de connectivité variable. Des modes dégradés ou mécanismes hors ligne peuvent être prévus lorsque la sécurité le permet, avec resynchronisation contrôlée. Les données sensibles et fonctions institutionnelles doivent pouvoir être déployées selon des architectures souveraines ou fédérées.

20. Critères d'acceptation et conclusion

Le domaine physique est cohérent si le lien objet-identité est protégé ; si les trois QR codes restent la fondation anti-contrefaçon ; si VERT, JAUNE et ROUGE conservent leur signification ; si producteurs, revendeurs et contrôleurs disposent de fonctions distinctes ; si le Passeport Numérique Universel assure la continuité du cycle de vie ; si la propriété et la seconde main peuvent être traitées de manière sécurisée ; si IoT, IA et AP Ledger restent complémentaires ; et si résilience, confidentialité et souveraineté sont préservées.

Le domaine physique transforme ainsi chaque produit protégé en élément vérifiable d'un écosystème plus vaste : production, distribution, vente, propriété, contrôle, maintenance et seconde main peuvent être reliés par une continuité de preuve.

Authenticity Plus© demeure le point d'ancrage de cette architecture.

Le Chapitre 8 développera le domaine numérique : logiciels, médias, contenus, propriété intellectuelle, signatures cryptographiques natives et provenance.

Note de cadrage institutionnel

Le domaine physique décrit dans ce chapitre est fondé sur l'architecture des trois QR codes d' Authenticity Plus©. Le QR Code Dynamique documentaire relève du domaine administratif et ne doit pas être confondu avec ce mécanisme. Les fonctions IoT, NFC, IA, ledger et analyse sont complémentaires et leur adoption dépend des exigences propres à chaque secteur.

VOLUME I — VISION ET FONDEMENTS

CHAPITRE 8 — LE DOMAINE NUMÉRIQUE : CONTENUS, LOGICIELS, PROPRIÉTÉ INTELLECTUELLE ET PROVENANCE

NUMÉRIQUE — CONTENUS — LOGICIELS — MÉDIAS — PROPRIÉTÉ INTELLECTUELLE — SIGNATURE CRYPTOGRAPHIQUE NATIVE — PROVENANCE — INTÉGRITÉ — VERSION — PREUVE

1. Objet du chapitre

Ce chapitre définit le domaine numérique de Deep Authenticity© : logiciels, médias, créations, contenus et actifs de propriété intellectuelle dont l'origine, l'intégrité, la version et certains droits peuvent être rendus vérifiables. L'enjeu central est d'établir une chaîne de provenance suffisamment robuste dans un environnement où la copie et la transformation sont instantanées.

2. Le défi de l'authenticité numérique

Un fichier numérique peut être reproduit sans perte apparente, modifié puis redistribué à grande échelle. L'apparence ne permet donc pas toujours d'identifier l'origine. Deep Authenticity© vise à associer aux éléments numériques des preuves permettant de distinguer source déclarée, intégrité technique, historique documenté et droits associés.

3. Signature cryptographique native

La signature cryptographique native constitue un mécanisme majeur du domaine numérique. Lors de la création, publication ou validation d'un contenu, une signature peut être associée à l'élément ou à son empreinte afin de permettre ultérieurement la vérification de son origine et de son intégrité selon l'identité et les clés reconnues.

4. Ce que la signature prouve — et ne prouve pas

Une signature valide peut démontrer qu'un élément correspond à ce qu'une clé ou une identité reconnue a signé et qu'il n'a pas été altéré depuis l'opération couverte. Elle ne démontre pas automatiquement que toutes les affirmations du contenu sont vraies. Deep Authenticity© doit préserver explicitement cette distinction.

5. Provenance des contenus

La provenance peut relier création, publication, transformations, versions, signatures et sources. Pour une image, une vidéo, un texte ou un fichier audio, le système peut conserver les événements pertinents permettant de comprendre comment l'élément présenté se rattache à une source ou à une version antérieure.

6. Médias et contenus synthétiques

L'essor des contenus générés ou modifiés par intelligence artificielle augmente l'importance de la provenance. Deep Authenticity© ne doit pas prétendre détecter parfaitement tout contenu synthétique. Elle privilégie une approche positive : permettre aux sources reconnues de signer et documenter leurs contenus afin que leur provenance puisse être vérifiée.

7. Logiciels et composants

Pour les logiciels, la provenance peut relier éditeur, version, paquet, signature, dépendances et événements de publication. Un utilisateur ou système peut alors vérifier qu'un composant correspond à une version émise par une source reconnue. Les mécanismes doivent rester compatibles avec les chaînes de développement et de distribution existantes.

8. Propriété intellectuelle

Le domaine numérique peut relier une création à son auteur ou titulaire déclaré, à des dépôts, licences, contrats ou preuves d'antériorité. Deep Authenticity© facilite la continuité de preuve mais ne se substitue pas aux offices, tribunaux ou règles juridiques déterminant définitivement la propriété intellectuelle.

9. Versionnement

Un élément numérique évolue souvent. Le Passeport Numérique Universel peut relier plusieurs versions tout en identifiant laquelle est actuelle, obsolète, retirée ou remplacée. L'historique permet de comprendre les transformations sans présenter une ancienne version comme équivalente à la version officiellement reconnue.

10. Empreintes cryptographiques

Les empreintes permettent de représenter de manière compacte l'état d'un fichier ou ensemble de données. Elles peuvent être utilisées pour vérifier qu'un élément n'a pas changé. Leur sécurité dépend des algorithmes employés et doit pouvoir évoluer grâce à des stratégies de migration cryptographique.

11. AP Core et vérification numérique

AP Core orchestre les identités, signatures, versions, droits et événements liés aux contenus. Il peut interroger une source de preuve, vérifier la cohérence d'une signature, restituer un statut ou signaler qu'une preuve n'est plus valide. Il ne doit pas transformer une absence de preuve en accusation automatique de falsification.

12. Passeport Numérique Universel des contenus

Le Passeport Numérique Universel peut accompagner un contenu ou logiciel à travers ses versions, publications, licences et transformations documentées. Il fournit une continuité logique entre l'identité numérique de l'élément et les preuves accessibles selon les droits de l'utilisateur.

13. AP Ledger et ancrage probant

Certains événements critiques — publication, version majeure, attribution, certification ou retrait — peuvent être ancrés dans AP Ledger. L'objectif est de renforcer l'auditabilité de la chronologie. Les fichiers complets ou informations confidentielles n'ont pas à être inscrits dans le ledger lorsqu'une empreinte ou référence suffit.

14. Intelligence artificielle comme outil d'analyse

Des modèles d'IA peuvent rechercher incohérences, manipulations probables ou ressemblances avec des sources connues. Ces analyses constituent des signaux complémentaires. La provenance cryptographique, les signatures et les attestations identifiables doivent rester distinctes des conclusions probabilistes des modèles.

15. Droits, licences et autorisations

Le système peut associer à un contenu des informations vérifiables sur une licence, une autorisation d'utilisation ou certaines restrictions. Ces informations doivent préciser leur émetteur et leur portée. Deep Authenticity© facilite la vérification des droits déclarés mais ne crée pas, à elle seule, un droit juridique inexistant.

16. Protection des créateurs et petits producteurs numériques

Une infrastructure accessible peut permettre aux artistes, auteurs, développeurs, journalistes, chercheurs et petites organisations de disposer de mécanismes de provenance autrefois réservés aux grandes plateformes. AP Léger peut contribuer à réduire la complexité technique tout en maintenant les garanties essentielles.

17. Interopérabilité et standards ouverts

La provenance numérique acquiert une valeur mondiale seulement si plusieurs systèmes peuvent la comprendre. Deep Authenticity© doit donc favoriser formats documentés, API, signatures vérifiables et compatibilité avec des standards pertinents, afin que la preuve puisse survivre au changement de plateforme ou de fournisseur.

18. Confidentialité et divulgation sélective

Certains contenus, codes sources ou actifs intellectuels ne peuvent pas être exposés pour être vérifiés. Le système doit permettre, lorsque cela est techniquement approprié, de vérifier une empreinte, une signature ou un attribut sans révéler l'intégralité de l'information protégée.

19. Articulation avec les domaines physique et administratif

Un produit physique peut embarquer un logiciel signé ; un document administratif peut être numérique ; une œuvre peut être liée à un certificat ou à un titre. Deep Authenticity© relie ces preuves sans confondre leurs régimes. Le QR Code Dynamique documentaire reste un mécanisme administratif, tandis que les trois QR codes d'Authenticity Plus© restent la fondation du produit physique.

20. Critères d'acceptation et conclusion

Le domaine numérique est cohérent si la signature cryptographique native permet de vérifier origine et intégrité sans être présentée comme preuve automatique de vérité factuelle ; si la provenance conserve une chronologie intelligible ; si les versions sont distinguées ; si les droits et licences indiquent leur source ; si AP Core orchestre les preuves ; si AP Ledger reste sélectif ; si l'IA demeure une couche analytique ; et si confidentialité, interopérabilité et réversibilité sont préservées.

Deep Authenticity© apporte ainsi au monde numérique une capacité essentielle : ne plus demander seulement « que contient ce fichier ? », mais également « d'où vient-il, qui l'a signé, quelle version est-ce et quelles preuves accompagnent son histoire ? ».

Cette logique étend la vérité vérifiable au-delà des objets physiques et prépare son application aux documents, identités et titres.

Le Chapitre 9 développera le domaine administratif : documents, identité, certificats, titres de propriété et QR Code Dynamique documentaire.

Note de cadrage institutionnel

La provenance numérique et les signatures cryptographiques établissent des faits techniques sur l' origine, l'intégrité ou la chaîne de transformation. Elles ne doivent pas être assimilées à une certification générale de la véracité d'un contenu. La reconnaissance juridique des droits, signatures et preuves dépend des cadres applicables.

VOLUME I — VISION ET FONDEMENTS

CHAPITRE 9 — LE DOMAINE ADMINISTRATIF : DOCUMENTS, IDENTITÉ, TITRES ET QR CODE DYNAMIQUE DOCUMENTAIRE

ADMINISTRATIF — DOCUMENTS — IDENTITÉ — CERTIFICATS — TITRES DE PROPRIÉTÉ — QR CODE DYNAMIQUE — VALIDITÉ — RÉVOCATION — VERSION — SOUVERAINETÉ

1. Objet du chapitre

Ce chapitre définit le domaine administratif de Deep Authenticity© : documents, identités, certificats, autorisations, actes et titres dont l'authenticité, l'intégrité et surtout l'état actuel doivent pouvoir être vérifiés. Le QR Code Dynamique documentaire en constitue un mécanisme majeur, distinct de l' architecture des trois QR codes d'Authenticity Plus© appliquée aux produits physiques.

2. Le problème du document statique

Un document imprimé ou un fichier copié peut continuer à circuler longtemps après avoir expiré, été révoqué ou remplacé. Son apparence peut rester identique alors que sa valeur administrative a changé. Deep Authenticity© introduit une logique d'état vivant : la copie présentée devient un point d' accès à la situation actuelle reconnue par la source compétente.

3. Le QR Code Dynamique documentaire

Le QR Code Dynamique documentaire permet d'interroger l'état actuel d'un document dans l' environnement autorisé de Deep Authenticity©. Le code visible peut rester stable tandis que l' information retournée évolue : document valide, expiré, suspendu, révoqué, remplacé ou nouvelle version disponible. Le QR devient ainsi une porte vers un état numérique actualisable.

4. Une différence fondamentale avec un QR statique

Un QR statique peut simplement contenir une adresse ou une information figée. Le QR Code Dynamique documentaire doit être relié à un identifiant et à une source de statut contrôlée. La confiance ne provient donc pas du graphisme du QR, mais de la capacité du système à vérifier l' identité du document, son émetteur et son état courant.

5. Autorité émettrice

La valeur d'un document administratif provient de l'autorité ou de l'organisation compétente qui l' émet. Deep Authenticity© ne crée pas cette compétence. Elle fournit une infrastructure permettant à l' émetteur de rendre vérifiables l'origine, l'intégrité, la validité et les changements de statut du document.

6. Cycle de vie documentaire

Création, émission, activation, utilisation, renouvellement, modification, suspension, expiration, révocation, remplacement et archivage peuvent constituer des événements du cycle de vie. Le Passeport Numérique Universel documentaire relie ces événements afin que l'état actuel soit compréhensible sans effacer l'historique nécessaire à l'audit.

7. Versionnement et remplacement

Lorsqu'un document est corrigé ou remplacé, l'ancienne version peut demeurer physiquement en circulation. Le QR Code Dynamique doit pouvoir indiquer qu'elle n'est plus la version active et, lorsque

les droits le permettent, orienter vers la référence de la nouvelle version. Cette fonction réduit le risque d'utilisation involontaire ou frauduleuse de documents obsolètes.

8. Expiration

Pour les documents à durée limitée, le statut doit pouvoir évoluer automatiquement ou sur instruction de l'autorité compétente à l'échéance prévue. Une copie authentique mais expirée reste historiquement authentique ; elle ne doit cependant pas être présentée comme actuellement valide. Deep Authenticity© distingue donc authenticité et validité.

9. Révocation et suspension

Une autorité peut devoir suspendre ou révoquer un document avant son échéance. Le système doit permettre que cette décision soit reflétée rapidement dans l'état vérifiable. Les motifs détaillés peuvent rester confidentiels : le vérificateur peut n'avoir besoin que de savoir que le document n'est plus utilisable.

10. Certificats, diplômes et attestations

Diplômes, certificats professionnels, attestations et autorisations peuvent bénéficier d'une vérification directe de l'émetteur et du statut. Le mécanisme peut réduire certaines falsifications documentaires et simplifier les contrôles, tout en conservant les règles propres aux établissements, professions et juridictions.

11. Identité et documents d'identité

Dans le domaine de l'identité, Deep Authenticity© doit appliquer des exigences renforcées de confidentialité et de minimisation. Le système peut aider à vérifier qu'un justificatif ou attribut provient d'une autorité reconnue sans nécessairement révéler toutes les données personnelles qu'il contient. L'identité civile reste sous la compétence des autorités habilitées.

12. Titres de propriété et droits

Titres fonciers, certificats de propriété ou autres droits peuvent être reliés à des registres souverains et à des preuves vérifiables. Deep Authenticity© ne remplace pas le registre légal : elle peut fournir une couche permettant de vérifier qu'un document présenté correspond à un état ou à une référence reconnue par le registre compétent.

13. AP Core et orchestration documentaire

AP Core relie l'identifiant du document, l'émetteur, les droits, les signatures, les événements et le statut. Lors d'une consultation, il détermine quelles sources doivent être interrogées et quelles informations peuvent être retournées. Cette orchestration permet au QR dynamique de refléter l'état vivant sans contenir lui-même toutes les données.

14. Signature cryptographique et intégrité

Une signature cryptographique peut permettre de vérifier qu'un document ou une empreinte correspond à ce qui a été émis par une source reconnue. Combinée au statut dynamique, elle distingue deux questions : le document est-il bien celui qui a été émis ? et est-il encore actuellement valide ou applicable ?

15. Passeport Numérique Universel documentaire

Le passeport documentaire organise identité, émetteur, versions, statut, événements et preuves. Il peut être minimal pour un document simple ou plus riche pour un titre à longue durée de vie. Les

informations accessibles sont déterminées par la finalité et les droits, et non par une logique de transparence intégrale.

16. Vérification par le citoyen et le professionnel

Selon le document, un citoyen, une entreprise ou un professionnel peut scanner le QR Code Dynamique afin d'obtenir une confirmation compréhensible de son état. L'interface doit éviter d'exposer des données sensibles et permettre de distinguer clairement document reconnu, document non valide et impossibilité temporaire de vérifier.

17. Vérification institutionnelle

Les administrations, banques, notaires, établissements, employeurs ou autres acteurs habilités peuvent disposer de niveaux de vérification supplémentaires. Ces droits doivent être authentifiés, journalisés et limités à leur finalité. La capacité technique de consulter une donnée ne constitue jamais, à elle seule, une autorisation légitime.

18. Interopérabilité et registres souverains

Deep Authenticity© doit pouvoir interroger ou recevoir des preuves de registres nationaux et sectoriels sans exiger leur remplacement. Les États conservent la maîtrise de leurs registres, politiques et décisions. L'infrastructure apporte une couche d'interopérabilité permettant de vérifier certains statuts entre systèmes autorisés.

19. Distinction avec les trois QR codes d'Authenticity Plus©

Le QR Code Dynamique documentaire ne doit pas être confondu avec les trois QR codes du domaine physique. Authenticity Plus© utilise trois fonctions — consommateur, revendeur/professionnel et contrôle/douanes — autour d'un produit. Le domaine administratif utilise un QR documentaire dynamique pour interroger l'état vivant d'un document. Les deux architectures partagent AP Core et la logique de preuve, mais répondent à des besoins différents.

20. Critères d'acceptation et conclusion

Le domaine administratif est cohérent si l'autorité émettrice reste la source de compétence ; si authenticité et validité sont distinguées ; si le QR Code Dynamique documentaire reflète l'état vivant du document ; si expiration, révocation, suspension, remplacement et versionnement sont gérés ; si les titres restent reliés aux registres souverains ; si les droits d'accès sont proportionnés ; si AP Core orchestre sans centralisation excessive ; et si confidentialité, auditabilité, interopérabilité et recours sont préservés.

Deep Authenticity© transforme ainsi le document d'un objet statique en un élément vérifiable dont l'état peut évoluer sans que chaque copie physique doive être récupérée ou réimprimée.

Le QR Code Dynamique documentaire devient la passerelle entre le document présenté et la réalité administrative actuelle reconnue par sa source compétente.

Le Chapitre 10 développera l'architecture de données et l'interopérabilité : API, ERP, IoT, registres publics, standards et intégration aux infrastructures existantes.

Note de cadrage institutionnel

Le QR Code Dynamique documentaire constitue un mécanisme majeur du domaine administratif de Deep Authenticity©. Il est distinct des trois QR codes d'Authenticity Plus© du domaine physique. Sa valeur juridique et les statuts qu'il restitue dépendent de l'autorité émettrice, des registres compétents et du cadre juridique applicable.

VOLUME I — VISION ET FONDEMENTS

CHAPITRE 10 — ARCHITECTURE DE DONNÉES ET INTEROPÉRABILITÉ : API, ERP, IoT ET REGISTRES SOUVERAINS

DONNÉES — API — ERP — IOT — REGISTRES — STANDARDS — INTEROPÉRABILITÉ — FÉDÉRATION — SÉCURITÉ — SOUVERAINETÉ

1. Objet du chapitre

Ce chapitre définit l'architecture de données et d'interopérabilité de Deep Authenticity©. L'objectif est de permettre aux produits, contenus, documents, entreprises et institutions d'échanger des preuves vérifiables sans imposer le remplacement des systèmes existants ni la centralisation universelle des données.

2. Une architecture de relation plutôt que de concentration

Deep Authenticity© doit savoir relier des informations distribuées. Une donnée peut rester dans l'ERP d'un producteur, un registre public, une infrastructure souveraine ou un système sectoriel, tandis qu'AP Core conserve les références, droits et mécanismes nécessaires pour vérifier les éléments autorisés.

3. Modèle de données commun

L'interopérabilité nécessite une grammaire minimale commune : identifiant, type d'élément, émetteur, horodatage, statut, événement, preuve, droit et version. Chaque secteur peut enrichir ce modèle sans modifier la signification des primitives fondamentales utilisées par l'ensemble de l'infrastructure.

4. API comme couche d'intégration

Les API permettent aux systèmes externes d'interroger ou d'alimenter Deep Authenticity© selon des contrats documentés. Elles doivent être authentifiées, versionnées, limitées par droits et conçues pour éviter l'exposition excessive des données. Une API doit préciser ce qu'elle retourne, dans quel contexte et avec quel niveau d'assurance.

5. Intégration aux ERP

Les ERP des producteurs, distributeurs et entreprises peuvent fournir des événements liés à la production, aux lots, aux stocks, aux expéditions ou aux ventes. AP Core peut intégrer les événements nécessaires à la continuité de preuve sans reproduire l'intégralité de la gestion interne de l'entreprise.

6. Intégration logistique

Les systèmes de transport, entrepôts et chaînes logistiques peuvent transmettre des événements autorisés de réception, transfert ou livraison. La qualité de ces événements dépend de l'identité de la source et de la fiabilité du processus qui les produit. Deep Authenticity© doit conserver cette provenance.

7. IoT, NFC et systèmes embarqués

Les capteurs, puces NFC et dispositifs IoT peuvent enrichir le Passeport Numérique Universel avec des événements ou mesures. AP Core doit authentifier la source, vérifier l'intégrité des messages et appliquer les règles sectorielles avant d'accepter l'information comme élément de la continuité de preuve.

8. Registres publics et administratifs

Dans le domaine administratif, Deep Authenticity© peut interagir avec des registres d'état civil, fonciers, professionnels, éducatifs ou autres systèmes autorisés. Les registres restent sous la maîtrise de leurs autorités. L'infrastructure échange uniquement les références ou preuves nécessaires à la vérification légitime.

9. QR Code Dynamique documentaire et registres

Le QR Code Dynamique documentaire illustre cette architecture : le document présenté contient un point d'accès, tandis que son état vivant peut provenir d'un registre ou service souverain. Validité, expiration, révocation ou remplacement peuvent ainsi être vérifiés sans copier nécessairement toutes les données du registre dans Deep Authenticity©.

10. Les trois QR codes et les systèmes industriels

Dans le domaine physique, les trois QR codes d'Authenticity Plus© — consommateur, revendeur/professionnel et contrôle/douanes — utilisent AP Core pour interroger l'état du produit et les données autorisées. Leur architecture reste fondamentale même lorsque des ERP, IoT, NFC ou systèmes douaniers sont intégrés.

11. Standards et formats ouverts

L'infrastructure doit privilégier, lorsque cela est approprié, des standards documentés et largement interopérables. Les formats propriétaires peuvent être supportés par des adaptateurs, mais ne doivent pas devenir une dépendance irréversible. La portabilité des preuves est une condition de durabilité.

12. Identifiants et résolution

Un identifiant doit permettre de résoudre de manière fiable l'élément auquel une preuve se rapporte. Les stratégies d'identification peuvent varier selon les produits, documents et contenus, mais doivent limiter collisions, ambiguïtés et réutilisations frauduleuses. Les changements de systèmes ne doivent pas détruire l'historique.

13. Événements et synchronisation

Les systèmes distribués ne sont pas toujours synchronisés instantanément. L'architecture doit gérer horodatage, ordre des événements, duplications, reprises et conflits. Lorsque l'état n'est pas suffisamment récent pour une décision critique, l'interface doit signaler la limite plutôt que présenter une certitude artificielle.

14. Fonctionnement online et offline

Certaines vérifications peuvent devoir fonctionner avec une connectivité limitée. Des preuves préalablement sécurisées, caches contrôlés ou mécanismes hors ligne peuvent être utilisés selon le niveau de risque. La resynchronisation doit détecter les conflits et distinguer clairement une vérification locale d'une confirmation temps réel.

15. Sécurité des échanges

Les échanges entre systèmes doivent être protégés par authentification, chiffrement, signatures, gestion des clés, contrôle d'accès et journalisation selon le risque. Les API exposées publiquement doivent faire l'objet de limitations, supervision et protections contre les abus. Les secrets critiques ne doivent jamais être intégrés directement aux codes visibles.

16. Qualité et provenance des données

L'interopérabilité ne transforme pas automatiquement une donnée externe en donnée fiable. Chaque information doit conserver sa source, sa date, son niveau d'assurance et, lorsque pertinent, ses conditions de collecte. Les tableaux de bord et jumeaux numériques doivent pouvoir distinguer données vérifiées, déclarées, estimées et simulées.

17. Souveraineté et localisation

Les États et organisations peuvent imposer que certaines données restent dans une juridiction ou infrastructure déterminée. Deep Authenticity© doit supporter des architectures locales, souveraines, hybrides et fédérées. L'interopérabilité doit fonctionner par échange de preuves plutôt que par obligation de transférer toutes les données.

18. Architecture fédérée

Plusieurs instances ou infrastructures compatibles peuvent coopérer en échangeant des preuves selon des règles communes. Cette fédération limite le risque de point unique de défaillance et permet à différents acteurs de conserver leur autonomie. Les futures fédérations peuvent préparer les Corridors de Confiance© entre juridictions.

19. Réversibilité et évolution

Les API, protocoles, algorithmes et standards évolueront. L'architecture doit permettre migration, export, remplacement de composants et interprétation des preuves historiques. Aucun fournisseur, format ou technologie ne doit rendre impossible la continuité de l'infrastructure lorsque les besoins changent.

20. Critères d'acceptation et conclusion

L'architecture de données est cohérente si les données peuvent rester distribuées ; si AP Core orchestre les relations ; si les API sont documentées et sécurisées ; si les ERP et systèmes logistiques peuvent être intégrés sans remplacement obligatoire ; si IoT et NFC conservent leur provenance ; si les registres souverains restent sous contrôle des autorités ; si le QR Code Dynamique documentaire reflète leur état autorisé ; si les trois QR codes d'Authenticity Plus© restent la fondation physique ; et si standards ouverts, sécurité, qualité, offline, fédération et réversibilité sont prévus.

Deep Authenticity© ne cherche donc pas à posséder toutes les données du monde. Elle cherche à rendre vérifiables les relations essentielles entre des données, des éléments et des autorités distribués.

Cette architecture constitue la condition technique permettant à une infrastructure universelle de vérité de rester compatible avec la diversité des systèmes et la souveraineté des acteurs.

Le Chapitre 11 développera l'intelligence artificielle et la détection des anomalies : analyse d'images, comportements, signaux faibles et distinction fondamentale entre inférence et preuve.

Note de cadrage institutionnel

Les protocoles, standards et technologies précis d'intégration devront être sélectionnés en fonction des secteurs, juridictions et niveaux de risque. Le présent chapitre fixe les principes d'architecture : distribution des données, interopérabilité, sécurité, provenance, souveraineté et réversibilité.

VOLUME I — VISION ET FONDEMENTS

CHAPITRE 11 — INTELLIGENCE ARTIFICIELLE ET DÉTECTION DES ANOMALIES : DE L'INFÉRENCE À LA PREUVE

INTELLIGENCE ARTIFICIELLE — ANOMALIES — CNN — IMAGES — COMPORTEMENTS — SIGNAUX FAIBLES — RISQUE — EXPLICABILITÉ — PREUVE — CONTRÔLE HUMAIN

1. Objet du chapitre

Ce chapitre définit la place de l'intelligence artificielle dans Deep Authenticity©. L'IA constitue une couche d'analyse destinée à détecter anomalies, incohérences et signaux faibles dans les trois domaines de l'infrastructure. Elle renforce les mécanismes de vérification, mais ne doit jamais être confondue avec la preuve cryptographique, documentaire ou institutionnelle.

2. Une IA au service de la vérification

Deep Authenticity© n'utilise pas l'IA comme arbitre universel de l'authenticité. Les modèles peuvent analyser des données complexes et attirer l'attention sur des situations atypiques. La décision finale doit s'appuyer sur les preuves disponibles, les règles applicables et, lorsque nécessaire, une validation humaine ou institutionnelle.

3. Analyse d'images et CNN

Dans le domaine physique, des réseaux neuronaux convolutifs et autres modèles de vision peuvent analyser emballages, formes, textures, marquages ou caractéristiques visuelles. Ils peuvent comparer un produit observé à des références connues et produire un score d'anomalie. Ce score complète les trois QR codes d'Authenticity Plus© ; il ne les remplace pas.

4. Détection comportementale des scans

Les événements de vérification peuvent révéler des comportements atypiques : fréquence anormale, répétitions massives, séquences incompatibles ou utilisation simultanée d'un même identifiant. Des modèles peuvent analyser ces comportements afin de prioriser les investigations et renforcer la détection de réutilisations frauduleuses.

5. Analyse géographique et temporelle

Lorsqu'elle est juridiquement et techniquement justifiée, l'analyse peut rechercher des incohérences entre lieux, temps et parcours attendus. Un produit observé dans des contextes impossibles ou hautement improbables peut générer une alerte. La géolocalisation doit toutefois être minimisée et protégée afin d'éviter une surveillance disproportionnée.

6. Signaux faibles

Un signal faible est un indice qui, pris isolément, ne suffit pas à établir une fraude mais peut devenir significatif lorsqu'il est combiné à d'autres observations. Deep Authenticity© peut exploiter ces

signaux pour anticiper des schémas émergents de contrefaçon, de détournement, de falsification ou d'abus.

7. Détection dans le domaine numérique

Pour les contenus et logiciels, l'IA peut rechercher ressemblances, transformations probables, anomalies de métadonnées ou incohérences avec une chaîne de provenance. Les signatures cryptographiques natives et les preuves de provenance restent cependant les mécanismes privilégiés pour établir une origine ou une intégrité vérifiable.

8. Détection dans le domaine administratif

Dans le domaine documentaire, l'IA peut aider à identifier des altérations visuelles, incohérences de structure ou schémas de fraude. Le QR Code Dynamique documentaire et la source administrative compétente restent déterminants pour vérifier l'état vivant du document : validité, expiration, révocation, suspension ou remplacement.

9. IA et trois QR codes

Les trois QR codes d'Authenticity Plus© — consommateur, revendeur/professionnel et contrôle/douanes — constituent la fondation du domaine physique. L'IA exploite les événements et signaux entourant leur utilisation pour renforcer l'analyse. Elle ne modifie pas leur séparation fonctionnelle ni la sémantique VERT / JAUNE / ROUGE.

10. Statuts fondamentaux et scores de risque

VERT signifie original ; JAUNE signifie original mais déjà vérifié ou vendu ; ROUGE signifie contrefaçon ou code inexistant dans le système Authenticity Plus©. Un score de risque produit par l'IA doit être affiché séparément lorsqu'il est utile. Il ne doit pas créer silencieusement une quatrième signification des statuts fondamentaux.

11. Apprentissage supervisé et données de référence

Les modèles supervisés nécessitent des données d'entraînement correctement qualifiées. Des erreurs d'étiquetage, biais sectoriels ou références insuffisantes peuvent dégrader les résultats. Les jeux de données doivent donc être documentés, gouvernés et réévalués à mesure que les produits et méthodes de fraude évoluent.

12. Détection non supervisée

Lorsque les fraudes futures ne sont pas connues à l'avance, des méthodes non supervisées peuvent rechercher des comportements qui s'écartent fortement des distributions habituelles. Une anomalie statistique n'est toutefois pas synonyme de fraude : elle constitue un signal à contextualiser avant toute action défavorable.

13. AP Core et orchestration des résultats IA

AP Core peut recevoir des scores, classifications et alertes produits par plusieurs moteurs analytiques. Il doit conserver le modèle ou service source, la date, le niveau de confiance et les règles de traitement. Les décisions automatisées critiques doivent être limitées et soumises aux contrôles appropriés.

14. Explicabilité et traçabilité

Lorsqu'un résultat algorithmique influence une investigation ou une décision importante, le système doit conserver suffisamment d'informations pour comprendre son origine : données utilisées, version

du modèle, seuil appliqué et contexte. L'explicabilité doit être proportionnée au risque et compatible avec la sécurité du système.

15. Contrôle humain

Les cas ambigus, sensibles ou à fort impact doivent pouvoir être examinés par un acteur habilité. Le contrôle humain ne doit pas être purement symbolique : l'opérateur doit disposer des preuves, du contexte et de la capacité réelle de confirmer, corriger ou contester le résultat algorithmique.

16. Biais et faux positifs

Un système trop sensible peut multiplier les faux positifs ; un système trop permissif peut manquer des fraudes. Deep Authenticity© doit mesurer précision, rappel, taux d'erreur et effets différenciés selon les contextes. Les seuils doivent être adaptés au coût réel des erreurs et non choisis uniquement pour maximiser un indicateur technique.

17. Sécurité des modèles

Les moteurs d'IA peuvent eux-mêmes être ciblés : manipulation des entrées, empoisonnement des données, extraction ou contournement. AP Shield et les mécanismes de sécurité doivent protéger les modèles, leurs données et leurs interfaces. Les mises à jour doivent être versionnées et testées avant déploiement.

18. IA, Jumeaux Numériques et anticipation

Les modèles d'IA peuvent analyser les données agrégées des Jumeaux Numériques afin de détecter tendances, pénuries, surplus, rappels, anomalies de flux ou signaux institutionnels. Ces résultats peuvent ensuite alimenter la Simulation Institutionnelle Profonde, à condition de distinguer clairement observation, prédiction et scénario.

19. Gouvernance de l'IA

Chaque usage d'IA doit disposer d'une finalité définie, d'un responsable, de métriques, d'une procédure d'audit et de règles de retrait ou de correction. Les modèles à fort impact doivent faire l'objet d'une surveillance renforcée. La performance ne doit jamais supprimer les exigences de légitimité, de proportionnalité et de recours.

20. Critères d'acceptation et conclusion

L'IA est correctement intégrée si elle reste complémentaire aux preuves ; si les trois QR codes d' Authenticity Plus© conservent leur rôle fondamental ; si le QR Code Dynamique documentaire reste relié à la source administrative compétente ; si les scores de risque sont distingués des statuts VERT / JAUNE / ROUGE ; si les modèles sont versionnés, mesurés et auditables ; si les faux positifs et biais sont surveillés ; si un contrôle humain existe pour les décisions sensibles ; et si les Jumeaux Numériques et simulations distinguent données observées, prédictions et scénarios.

Dans Deep Authenticity©, l'intelligence artificielle n'est donc pas la vérité : elle est un instrument de perception avancée autour d'une infrastructure de preuve.

Sa valeur réside dans sa capacité à révéler plus tôt ce que les mécanismes déterministes ne voient pas immédiatement, tout en laissant la preuve, le droit et la responsabilité conserver leur place.

Le Chapitre 12 développera les Jumeaux Numériques : du produit et de l'entreprise au territoire, à l'État et au Jumeau Numérique National et Institutionnel.

Note de cadrage institutionnel

Les performances des modèles d'intelligence artificielle dépendent des données, des contextes et des méthodes utilisées. Aucun résultat probabiliste ne doit être présenté comme une preuve certaine sans mécanisme de validation approprié. Les usages à fort impact doivent respecter les cadres juridiques, les droits des personnes et les exigences d'audit applicables.

VOLUME I — VISION ET FONDEMENTS

CHAPITRE 12 — LES JUMEAUX NUMÉRIQUES : DU PRODUIT AU JUMEAU NUMÉRIQUE NATIONAL ET INSTITUTIONNEL

JUMEAUX NUMÉRIQUES — PRODUIT — ENTREPRISE — SECTEUR — TERRITOIRE — ÉTAT — INSTITUTION — DONNÉES VÉRIFIÉES — MODÉLISATION — ANTICIPATION

1. Objet du chapitre

Ce chapitre définit la doctrine des Jumeaux Numériques de Deep Authenticity©. Le jumeau numérique est une représentation structurée et évolutive d'un élément réel, d'une organisation, d'un secteur ou d' un territoire. Sa spécificité dans Deep Authenticity© réside dans sa capacité à s'appuyer, autant que possible, sur des données dont la provenance, le statut et la qualité sont explicitement identifiables.

2. Du Passeport Numérique au jumeau numérique

Le Passeport Numérique Universel suit l'identité et le cycle de vie d'un élément. Le jumeau numérique exploite ces informations pour construire une représentation de son état, de ses relations et de son évolution. Le passeport constitue donc une source structurante, tandis que le jumeau ajoute une capacité de représentation, d'analyse et de projection.

3. Jumeau numérique du produit

À l'échelle d'un produit, le jumeau peut représenter identité, provenance, statut, localisation autorisée, maintenance, propriété, certifications et événements de cycle de vie. Dans le domaine physique, la fiabilité de cette représentation s'appuie notamment sur Authenticity Plus© et son architecture fondamentale des trois QR codes.

4. Jumeau numérique de l'entreprise

L'agrégation contrôlée des produits, stocks, flux, capacités, anomalies et événements peut alimenter un jumeau numérique d'entreprise. Celui-ci peut aider à comprendre l'activité opérationnelle, identifier les tensions, anticiper certains besoins et suivre l'effet d'une décision, tout en respectant la confidentialité des informations stratégiques.

5. Jumeau numérique sectoriel

Plusieurs entreprises et sources institutionnelles peuvent, selon des règles de gouvernance, alimenter une représentation sectorielle. Agriculture, industrie, santé, transport, énergie ou commerce peuvent ainsi disposer d'indicateurs consolidés sur capacités, flux, dépendances, pénuries potentielles, surplus ou anomalies.

6. Jumeau numérique territorial

À l'échelle d'une ville, wilaya, région ou autre territoire, le jumeau peut relier données économiques, logistiques, administratives et infrastructurelles autorisées. Il fournit une représentation dynamique du territoire destinée à améliorer la compréhension des flux et non à construire une surveillance exhaustive de la population.

7. Jumeau Numérique National et Institutionnel

Le Jumeau Numérique National et Institutionnel constitue l'échelle la plus stratégique de cette architecture. Il peut représenter certains systèmes critiques d'un État ou d'une institution à partir de données distribuées : production, stocks, infrastructures, flux, services publics, indicateurs économiques et autres variables autorisées.

8. Une fédération de sources plutôt qu'une base unique

Le Jumeau Numérique National ne nécessite pas que toutes les données nationales soient copiées dans Deep Authenticity©. Les ministères, entreprises publiques, registres, collectivités et systèmes sectoriels peuvent conserver leurs bases. AP Core relie les preuves et données autorisées selon une architecture fédérée.

9. Données internes et données externes

Le jumeau peut combiner des données natives de Deep Authenticity© avec des données externes nécessaires à la compréhension d'un phénomène. Chaque source externe doit conserver son origine, sa date, sa méthode et son niveau de confiance. L'intégration ne doit jamais effacer la distinction entre donnée observée, déclarée, estimée ou simulée.

10. Injection et ingestion des données

Les données peuvent être injectées par API, flux sécurisés, imports contrôlés, événements IoT ou connexions à des registres autorisés. Les mécanismes d'ingestion doivent valider format, identité de la source, horodatage, droits et qualité avant que l'information soit utilisée dans une représentation institutionnelle.

11. Architecture par rubriques

Le Jumeau Numérique National peut organiser les données par rubriques fonctionnelles : économie, industrie, agriculture, santé, transport, énergie, commerce, administration, infrastructures ou autres domaines pertinents. Les rubriques servent à structurer l'analyse tout en permettant des relations transversales lorsque les droits l'autorisent.

12. Tableaux de bord et visualisation

Les décideurs peuvent consulter des tableaux de bord représentant stocks, capacités, flux, tendances, alertes et indicateurs. Les graphiques doivent permettre de distinguer valeurs observées, estimations et projections. Une visualisation claire est indispensable pour éviter qu'une précision graphique apparente soit confondue avec une certitude réelle.

13. Détection des pénuries et surplus

En combinant stocks, production, consommation et flux, le jumeau peut contribuer à détecter des tensions ou surplus potentiels. L'objectif est de produire des alertes précoces et des scénarios, non de garantir une prévision parfaite. Les résultats doivent préciser leur horizon, leurs hypothèses et leur niveau d'incertitude.

14. Santé, risques et signaux territoriaux

Des données agrégées et juridiquement autorisées peuvent aider à identifier certaines tendances sanitaires, ruptures d'approvisionnement ou besoins de capacité. Les informations de santé individuelles exigent une protection renforcée ; les fonctions institutionnelles doivent privilégier l' agrégation et la minimisation lorsque l'identité personnelle n'est pas nécessaire.

15. Rappels, maintenance et non-conformités

Les données de produits et infrastructures peuvent permettre au jumeau d'identifier les zones ou actifs concernés par un rappel, une maintenance ou une non-conformité. Les trois QR codes d' Authenticity Plus© et le Passeport Numérique Universel peuvent fournir une granularité vérifiable dans le domaine physique.

16. IA et analyse prédictive

Les moteurs d'intelligence artificielle peuvent analyser le jumeau pour détecter tendances, corrélations, anomalies et signaux faibles. Leurs résultats restent probabilistes. Le jumeau doit donc conserver la séparation entre les données sources, les indicateurs calculés et les prédictions produites par les modèles.

17. Préparation à la Simulation Institutionnelle Profonde

Le jumeau numérique fournit l'état de référence sur lequel la Simulation Institutionnelle Profonde peut construire des scénarios. Une décision hypothétique peut modifier certaines variables du modèle afin d'en explorer les conséquences possibles. La qualité de la simulation dépend directement de la qualité du jumeau et de ses hypothèses.

18. Monitoring continu après décision

Après la mise en œuvre réelle d'une décision, les mêmes indicateurs peuvent être suivis afin de comparer trajectoire observée et trajectoire anticipée. Cette boucle de monitoring permet d'identifier des écarts, d'ajuster les politiques et d'améliorer progressivement les modèles sans prétendre supprimer l'incertitude.

19. Souveraineté, sécurité et gouvernance

Un jumeau national concentre une valeur stratégique élevée même lorsque les données restent distribuées. Les accès doivent donc être segmentés, authentifiés, journalisés et soumis à une gouvernance stricte. Les informations sensibles doivent rester sous contrôle souverain et les usages analytiques être limités à des finalités légitimes.

20. Critères d'acceptation et conclusion

L'architecture des Jumeaux Numériques est cohérente si le Passeport Numérique Universel fournit une continuité de base ; si les données conservent leur provenance ; si les sources restent distribuées lorsque nécessaire ; si les niveaux produit, entreprise, secteur, territoire et État sont distingués ; si les tableaux de bord séparent observation, estimation et prédiction ; si l'IA reste analytique ; si les données sensibles sont protégées ; et si le Jumeau Numérique National prépare la simulation sans se substituer à la décision.

Deep Authenticity© transforme ainsi des preuves dispersées en représentations structurées capables d'éclairer le fonctionnement d'un produit, d'une entreprise, d'un secteur ou d'un État.

Le Jumeau Numérique National et Institutionnel devient le pont entre l'infrastructure de vérité vérifiable et la capacité d'anticipation stratégique.

Le Chapitre 13 développera la Simulation Institutionnelle Profonde : scénarios de décision, anticipation des impacts, exécution réelle et monitoring continu.

Note de cadrage institutionnel

Les Jumeaux Numériques décrits dans ce chapitre sont des représentations analytiques dépendantes de la qualité, de la couverture et de la fraîcheur des données disponibles. Ils ne constituent pas une reproduction parfaite de la réalité. Les usages institutionnels doivent expliciter les hypothèses, incertitudes, droits d'accès et responsabilités.

VOLUME I — VISION ET FONDEMENTS

CHAPITRE 13 — SIMULATION INSTITUTIONNELLE PROFONDE : ANTICIPATION, DÉCISION ET MONITORING CONTINU

SIMULATION INSTITUTIONNELLE PROFONDE — SCÉNARIOS — DÉCISION — IMPACTS — JUMEAU NUMÉRIQUE — EXÉCUTION — MONITORING — RÉTROACTION — INCERTITUDE — GOUVERNANCE

1. Objet du chapitre

Ce chapitre définit la Simulation Institutionnelle Profonde comme une capacité stratégique de Deep Authenticity© permettant d'explorer les conséquences possibles d'une décision avant sa mise en œuvre, puis de suivre son exécution réelle. Elle s'appuie sur les Jumeaux Numériques, les données vérifiées, les modèles analytiques et des scénarios explicitement documentés.

2. De l'observation à l'anticipation

Un tableau de bord décrit principalement ce qui est observé ; un jumeau numérique structure l'état d'un système ; la Simulation Institutionnelle Profonde ajoute la question : que pourrait-il se produire si certaines variables, règles ou décisions étaient modifiées ? Elle transforme ainsi l'infrastructure d'observation en environnement d'exploration stratégique.

3. Le Jumeau Numérique comme état de référence

Toute simulation sérieuse nécessite un état initial. Le Jumeau Numérique National et Institutionnel peut fournir cette base à partir de données économiques, industrielles, logistiques, administratives ou territoriales autorisées. La simulation doit conserver la date, la qualité et les limites des données utilisées.

4. Construction d'un scénario

Un scénario combine une décision hypothétique, des paramètres, des hypothèses et un horizon temporel. Il peut représenter une politique publique, une modification réglementaire, un investissement, une restriction, un changement logistique ou une réponse à une crise. Chaque hypothèse doit être visible afin que le résultat puisse être interprété correctement.

5. Scénario de référence

Avant de mesurer l'effet d'une décision, le système doit définir un scénario de référence représentant l'évolution plausible sans intervention nouvelle. La comparaison entre référence et scénarios alternatifs permet d'identifier les effets attribuables au changement simulé, dans les limites du modèle.

6. Scénarios multiples

Une décision ne doit pas être évaluée à partir d'un résultat unique. La Simulation Institutionnelle Profonde peut comparer plusieurs variantes : prudente, centrale, ambitieuse, contrainte ou de crise. Cette approche révèle les conditions dans lesquelles une politique reste robuste et celles dans lesquelles elle devient vulnérable.

7. Simulation économique

Les modèles peuvent explorer certains effets sur production, stocks, prix, commerce, investissement, recettes ou capacités. Les résultats économiques doivent être présentés comme des trajectoires conditionnelles dépendant des hypothèses, et non comme des prévisions certaines.

8. Simulation sociale et territoriale

Lorsque les données et le cadre juridique le permettent, les scénarios peuvent analyser des effets agrégés sur accès aux services, disparités territoriales, mobilité, emploi ou autres indicateurs sociaux. Les simulations doivent éviter le profilage individuel inutile et privilégier des niveaux d'agrégation compatibles avec les droits.

9. Simulation des chaînes d'approvisionnement

Les données de produits, entreprises, stocks et flux peuvent permettre de simuler une rupture, une fermeture de corridor, une pénurie de matière ou une hausse de demande. L'objectif est d'identifier les dépendances critiques, les capacités alternatives et les délais nécessaires à une réponse.

10. Santé, crises et capacités critiques

Dans des contextes autorisés, les modèles peuvent explorer l'évolution de besoins en médicaments, équipements, capacités hospitalières ou autres ressources critiques. Les données individuelles de santé doivent rester fortement protégées ; l'aide institutionnelle repose prioritairement sur des informations agrégées et pertinentes.

11. IA et modèles prédictifs

L'intelligence artificielle peut contribuer à estimer certaines relations, détecter des tendances ou générer des scénarios. Ses résultats doivent rester identifiés comme probabilistes. La Simulation Institutionnelle Profonde doit permettre de distinguer les données observées, les paramètres imposés, les sorties de modèles et les choix humains.

12. Incertitude et sensibilité

Chaque simulation comporte une incertitude. Le système doit permettre de tester la sensibilité des résultats à plusieurs hypothèses : demande, coûts, délais, comportements ou événements externes. Une décision robuste est celle qui conserve des résultats acceptables dans plusieurs configurations plausibles.

13. De la simulation à la décision

Deep Authenticity© ne prend pas la décision politique à la place de l'autorité compétente. La plateforme fournit scénarios, indicateurs, hypothèses, risques et conséquences possibles. L'autorité

conserve la responsabilité de pondérer les objectifs, arbitrer les valeurs et décider selon le droit et le mandat institutionnel.

14. Exécution réelle d'une décision

Après décision, les paramètres retenus peuvent être transformés en jalons, responsabilités et indicateurs de suivi. Deep Authenticity© peut relier l'intention stratégique à des événements réels observables, sans confondre le plan avec son exécution effective.

15. Monitoring continu

Le monitoring continu compare les indicateurs observés aux trajectoires attendues. Écarts, retards, effets inattendus ou nouveaux risques peuvent déclencher une alerte ou une réévaluation. L'objectif n' est pas de surveiller les personnes, mais de suivre l'exécution et les effets d'une politique à partir d' indicateurs légitimes.

16. Boucle de rétroaction

Les écarts entre simulation et réalité constituent une information précieuse. Ils peuvent être utilisés pour recalibrer les modèles, corriger des hypothèses et améliorer les simulations futures. La plateforme devient ainsi un système d'apprentissage institutionnel, à condition de conserver la traçabilité des changements.

17. Traçabilité de la décision

Une simulation institutionnelle doit conserver l'identité des modèles, versions, hypothèses, sources de données, dates et scénarios utilisés. Cette mémoire permet de comprendre a posteriori pourquoi une projection a été produite et de distinguer une erreur de données, de modèle, d'hypothèse ou d' exécution.

18. Gouvernance et séparation des pouvoirs

L'accès aux scénarios sensibles, aux modèles et aux données doit être segmenté. Les équipes techniques ne doivent pas pouvoir transformer seules une simulation en décision exécutoire. Des rôles distincts pour analyse, validation, décision, exécution et audit renforcent la responsabilité institutionnelle.

19. Souveraineté et résilience

La Simulation Institutionnelle Profonde peut concerner des informations stratégiques nationales. Les données, modèles et scénarios sensibles doivent pouvoir être hébergés et exploités dans des environnements souverains, avec redondance, contrôle d'accès et capacité de fonctionnement en situation dégradée.

20. Critères d'acceptation et conclusion

La Simulation Institutionnelle Profonde est cohérente si elle part d'un état de référence documenté ; si plusieurs scénarios sont comparés ; si les hypothèses et incertitudes restent visibles ; si l'IA est distinguée de la preuve ; si les résultats ne se substituent pas à la décision politique ; si l'exécution réelle est suivie par des indicateurs ; si les écarts alimentent une boucle de rétroaction ; si les modèles sont traçables ; et si gouvernance, droits, souveraineté et résilience sont préservés.

Deep Authenticity© introduit ainsi une continuité nouvelle : observer le réel, construire un jumeau, simuler plusieurs futurs, décider, exécuter, mesurer puis apprendre.

La Simulation Institutionnelle Profonde ne promet pas de supprimer l'incertitude. Elle vise à rendre les décisions complexes plus explicites, comparables et vérifiables avant et après leur mise en œuvre.

Le Chapitre 14 développera les tableaux de bord économiques, sociaux et stratégiques : pénuries, surplus, disparités, rappels, maintenance, flux et signaux faibles.

Note de cadrage institutionnel

La Simulation Institutionnelle Profonde constitue un outil d'aide à la décision et non un mécanisme autonome de gouvernement. Ses résultats dépendent des données, hypothèses et modèles employés. Toute utilisation à fort impact doit prévoir validation humaine, transparence méthodologique, sécurité, audit et voies de contestation appropriées.

VOLUME I — VISION ET FONDEMENTS

CHAPITRE 14 — TABLEAUX DE BORD ÉCONOMIQUES, SOCIAUX ET STRATÉGIQUES

TABLEAUX DE BORD — PÉNURIES — SURPLUS — DISPARITÉS — RAPPELS — MAINTENANCE — FLUX — SIGNAUX FAIBLES — ALERTES — DÉCISION

1. Objet du chapitre

Ce chapitre définit les tableaux de bord économiques, sociaux et stratégiques de Deep Authenticity© comme une couche de lecture opérationnelle du réel. Ils transforment les données autorisées provenant des produits, organisations, systèmes sectoriels et institutions en indicateurs compréhensibles, traçables et actionnables.

2. Du flux de données à l'intelligence décisionnelle

Un tableau de bord ne doit pas être une accumulation de graphiques. Il organise les informations selon une finalité : comprendre une situation, détecter une évolution, hiérarchiser les risques et éclairer une décision. AP Core relie les sources et conserve leur provenance afin que l'indicateur puisse être interprété dans son contexte.

3. Architecture multi-niveaux

Les tableaux de bord peuvent exister aux niveaux producteur, entreprise, secteur, territoire, institution et État. Chaque niveau dispose d'une granularité et de droits différents. Les indicateurs nationaux ne nécessitent pas l'exposition de toutes les données unitaires, et les acteurs locaux ne doivent pas accéder automatiquement aux informations stratégiques globales.

4. Tableau de bord producteur

Le producteur peut suivre volumes activés, lots, statuts, vérifications, zones de circulation, anomalies, rappels, maintenance et distribution. Les événements issus des trois QR codes d'Authenticity Plus© constituent une source essentielle du domaine physique, complétée lorsque nécessaire par ERP, logistique, IoT ou autres systèmes autorisés.

5. Pénuries et tensions d'approvisionnement

En combinant stocks, production, consommation, délais et flux, Deep Authenticity© peut détecter des signaux de tension sur un produit ou une ressource. Une alerte de pénurie doit indiquer son horizon, ses sources et son degré d'incertitude afin de distinguer une tension observée d'une pénurie simplement projetée.

6. Surplus et déséquilibres

La même infrastructure peut identifier des excédents persistants, stocks immobilisés ou capacités sous-utilisées. Ces informations peuvent aider producteurs et institutions à réorienter certains flux, réduire les pertes et mieux coordonner l'offre avec les besoins, sans transformer une recommandation analytique en ordre automatique.

7. Disparités territoriales

Les tableaux de bord peuvent comparer l'accès à certains produits, services ou infrastructures entre territoires. Les écarts doivent être contextualisés par population, capacité, distance, saisonnalité ou autres facteurs pertinents. L'objectif est de révéler des déséquilibres structurels sans produire de classement simpliste des populations.

8. Rappels et non-conformités

Lorsqu'un fabricant ou une autorité déclenche un rappel, le système peut identifier les références, lots ou zones concernés et suivre la progression de l'action corrective. Le Passeport Numérique Universel et Authenticity Plus© permettent de relier l'alerte aux unités concernées avec une granularité adaptée.

9. Maintenance et révisions

Pour les équipements et actifs suivis, les tableaux de bord peuvent afficher échéances de maintenance, révisions obligatoires, incidents et taux de conformité. Cette capacité permet de passer d'une maintenance purement réactive à une supervision préventive lorsque les données disponibles sont suffisamment fiables.

10. Flux physiques et commerciaux

Les flux de production, distribution, vente et transfert peuvent être représentés de manière agrégée. Les cartes etséries temporelles peuvent révéler ralentissements, concentrations, ruptures ou changements de trajectoire. La visualisation doit conserver la distinction entre mouvement observé et mouvement estimé.

11. Indicateurs sociaux

Des indicateurs agrégés peuvent représenter accès aux services, disponibilité de ressources, mobilité ou autres dimensions sociales légitimes. Deep Authenticity© doit appliquer minimisation et protection des données personnelles, en privilégiant l'analyse collective lorsque l'identité individuelle n'est pas nécessaire.

12. Signaux faibles et alertes précoces

Les moteurs analytiques peuvent rapprocher plusieurs anomalies modestes afin de détecter un phénomène émergent avant qu'il ne devienne critique. Un signal faible doit rester présenté comme un indice à examiner. La plateforme doit permettre de remonter jusqu'aux données et règles ayant conduit à l'alerte.

13. Hiérarchisation des alertes

Toutes les alertes n’ont pas la même urgence. Le système peut les classer selon impact potentiel, confiance, horizon temporel, population ou actifs concernés et capacité de réponse. Les seuils doivent être gouvernés, documentés et ajustables afin d’éviter la saturation des décideurs.

14. Données observées, estimées et simulées

Chaque graphique doit permettre de distinguer clairement trois catégories : données observées ou vérifiées, valeurs estimées par calcul ou modèle, et trajectoires simulées. Cette séparation visuelle et sémantique est essentielle pour empêcher qu’une projection soit interprétée comme un fait acquis.

15. Jumeaux Numériques et tableaux de bord

Les Jumeaux Numériques fournissent une représentation structurée dont les tableaux de bord constituent l’une des interfaces de lecture. Le décideur peut passer d’un indicateur agrégé vers les niveaux autorisés de détail, tandis que la provenance des données reste conservée dans l’architecture.

16. Simulation Institutionnelle Profonde

Les tableaux de bord servent également d’interface à la Simulation Institutionnelle Profonde. Ils permettent de comparer scénario de référence, scénarios alternatifs et trajectoire réelle après décision. Le même environnement peut ainsi soutenir anticipation, décision, exécution et monitoring continu.

17. Personnalisation par rôle

Un ministre, un responsable local, un producteur, un contrôleur ou un analyste n’a pas besoin de la même vue. Les tableaux de bord doivent être configurables par rôle, finalité et niveau d’habilitation. La personnalisation ne doit jamais contourner les règles d’accès définies par AP Core.

18. Souveraineté et confidentialité

Les indicateurs stratégiques peuvent révéler des vulnérabilités nationales, industrielles ou économiques. Les tableaux de bord sensibles doivent pouvoir être hébergés dans des environnements souverains, avec authentification forte, segmentation, journalisation et restrictions sur l’export des données.

19. Gouvernance des indicateurs

Chaque indicateur important doit disposer d’une définition, d’une source, d’une fréquence de mise à jour, d’un responsable et d’une méthode de calcul documentée. Les changements de définition doivent être versionnés afin qu’une évolution statistique ne soit pas confondue avec une modification méthodologique.

20. Critères d’acceptation et conclusion

Les tableaux de bord sont cohérents si chaque indicateur conserve sa provenance ; si les niveaux producteur, sectoriel, territorial et institutionnel sont distingués ; si pénuries, surplus, disparités, rappels, maintenance et flux peuvent être suivis ; si les signaux faibles restent des alertes et non des verdicts ; si observation, estimation et simulation sont clairement séparées ; si les vues sont adaptées aux rôles ; et si confidentialité, souveraineté et gouvernance méthodologique sont garanties.

Deep Authenticity© transforme ainsi des données vérifiables en capacité de lecture stratégique. L’ objectif n’est pas seulement de savoir ce qui s’est produit, mais de comprendre ce qui évolue, où se situent les tensions et quelles actions méritent une attention prioritaire.

Ces tableaux de bord constituent l'interface opérationnelle entre le réel vérifiable, les Jumeaux Numériques et la Simulation Institutionnelle Profonde.

Le Chapitre 15 développera la résilience systémique : continuité de service, modes dégradés, sécurité, redondance et capacité de fonctionnement en situation de crise.

Note de cadrage institutionnel

Les tableaux de bord de Deep Authenticity© sont des instruments d'observation et d'aide à la décision. La précision de leurs indicateurs dépend de la couverture, de la qualité et de la fraîcheur des sources. Les estimations, alertes et simulations doivent toujours être distinguées des données directement observées ou vérifiées.

VOLUME I — VISION ET FONDEMENTS

CHAPITRE 15 — RÉSILIENCE SYSTÉMIQUE : CONTINUITÉ, MODES DÉGRADÉS ET FONCTIONNEMENT EN SITUATION DE CRISE

RÉSILIENCE — CONTINUITÉ — OFFLINE — MODES DÉGRADÉS — REDONDANCE — CYBERSÉCURITÉ — CRISE — REPRISE — SOUVERAINETÉ — CONFIANCE

1. Objet du chapitre

Ce chapitre définit la résilience systémique de Deep Authenticity© : la capacité de l'infrastructure à préserver ses fonctions essentielles malgré pannes, ruptures de réseau, cyberincidents, défaillances de fournisseurs, catastrophes ou crises institutionnelles. La résilience ne signifie pas que tous les services restent identiques en toute circonstance ; elle impose que les fonctions critiques disposent de niveaux de continuité explicitement conçus.

2. Identifier les fonctions critiques

Toutes les fonctions de Deep Authenticity© n'ont pas la même criticité. L'authentification d'un produit sensible, la vérification d'un document administratif, un contrôle douanier ou une alerte de rappel peuvent exiger une priorité supérieure à une fonction analytique non urgente. La continuité doit donc être organisée selon des niveaux de service et d'impact.

3. Architecture sans point unique de défaillance

Les composants critiques doivent éviter, lorsque le risque le justifie, une dépendance à un serveur, une région, une clé ou un fournisseur unique. Réplication, segmentation, basculement et diversité d' infrastructure permettent de limiter l'effet d'une défaillance locale sur l'ensemble de l'écosystème.

4. Fonctionnement online et offline

Deep Authenticity© doit pouvoir traiter les contextes de connectivité variable. Certaines vérifications peuvent utiliser des preuves préalablement sécurisées ou des mécanismes locaux lorsque la connexion n'est pas disponible. L'interface doit toujours indiquer si le résultat est temps réel, hors ligne ou provisoire afin d'éviter une fausse certitude.

5. Modes dégradés

Un mode dégradé conserve un sous-ensemble contrôlé des fonctions lorsque l'environnement normal n'est plus disponible. Il peut limiter les opérations à la consultation, suspendre certains changements d'état ou utiliser des données mises en cache. Le principe fondamental est de réduire les capacités plutôt que de diminuer silencieusement le niveau de sécurité.

6. Resynchronisation après interruption

Après restauration de la connectivité, les événements produits hors ligne doivent être resynchronisés de manière contrôlée. AP Core doit détecter duplications, conflits, incohérences temporelles ou changements de statut intervenus pendant l'interruption. Les conflits critiques doivent pouvoir être soumis à une validation supplémentaire.

7. Résilience des trois QR codes

Dans le domaine physique, les trois QR codes d'Authenticity Plus© restent la fondation de l' authentification. Les mécanismes de continuité doivent préserver la séparation consommateur, revendeur/professionnel et contrôle/douanes ainsi que la signification VERT / JAUNE / ROUGE, sans inventer un statut définitif lorsque l'état central ne peut pas être confirmé.

8. Résilience du QR Code Dynamique documentaire

Dans le domaine administratif, le QR Code Dynamique documentaire dépend de l'accès à l'état vivant du document. En situation dégradée, une preuve locale peut confirmer certains éléments d'intégrité, mais l'interface doit signaler lorsqu'elle ne peut pas confirmer une révocation, une expiration ou un remplacement intervenu récemment.

9. Redondance des données et des services

Les données et services critiques doivent disposer de stratégies de réplication adaptées à leur sensibilité. La redondance peut être locale, régionale, souveraine ou fédérée. Elle doit être testée régulièrement : une copie de secours non restaurable ne constitue pas une véritable capacité de reprise.

10. Sauvegarde et reprise

Les sauvegardes doivent protéger contre panne, erreur humaine, corruption et certaines attaques. Des objectifs de point de reprise et de délai de reprise doivent être définis par niveau de criticité. Les procédures de restauration doivent être documentées, testées et indépendantes autant que possible du système qu'elles doivent restaurer.

11. AP Shield et cybersécurité

AP Shield contribue à la détection, au confinement et à la réponse aux incidents. Une architecture résiliente doit prévoir authentification forte, segmentation, gestion des secrets, journalisation, supervision et mécanismes de révocation. La continuité ne doit jamais devenir un prétexte pour désactiver les contrôles de sécurité essentiels.

12. Compromission d'identifiants et de clés

La compromission d'une clé, d'un compte ou d'un service de signature doit pouvoir être isolée. Les mécanismes de rotation, révocation et remplacement doivent limiter la propagation de l'incident. Les preuves historiques doivent conserver suffisamment de contexte pour rester interprétables après une migration cryptographique.

13. Dépendances externes

ERP, clouds, réseaux télécoms, fournisseurs d'identité, registres et services tiers peuvent devenir indisponibles. AP Core doit connaître les dépendances critiques et prévoir des stratégies de temporisation, cache, file d'attente ou basculement. Une panne externe ne doit pas être présentée comme une invalidité du produit ou du document.

14. Continuité des tableaux de bord

En situation de crise, les tableaux de bord doivent indiquer la fraîcheur des données et les sources indisponibles. Une valeur ancienne ne doit pas apparaître comme une mesure actuelle. Les décideurs doivent pouvoir identifier quelles parties du Jumeau Numérique restent fiables et lesquelles fonctionnent avec une information partielle.

15. Jumeaux Numériques en situation de crise

Les Jumeaux Numériques peuvent aider à représenter capacités disponibles, stocks, flux interrompus et infrastructures affectées. Leur utilité augmente en crise, mais leur incertitude peut également augmenter. Le système doit donc rendre visibles les zones de données manquantes et éviter une précision artificielle.

16. Simulation Institutionnelle Profonde et scénarios de crise

La Simulation Institutionnelle Profonde peut explorer des scénarios de rupture : fermeture de corridor, indisponibilité d'un fournisseur, cyberattaque, catastrophe ou pénurie. Ces simulations permettent de tester les plans de continuité avant une crise réelle et d'identifier les dépendances qui nécessitent des alternatives.

17. Exercices et tests de résilience

La résilience doit être testée, pas seulement documentée. Des exercices peuvent simuler perte de réseau, indisponibilité d'un centre de données, corruption de données ou défaillance d'une intégration. Les résultats alimentent les plans d'amélioration, les responsabilités et les priorités d'investissement.

18. Gouvernance de crise

En situation exceptionnelle, les rôles de décision, sécurité, exploitation, communication et audit doivent être clairement définis. Les pouvoirs temporaires accordés pour gérer une crise doivent être limités, journalisés et retirés lorsque la situation normale est rétablie. L'urgence ne doit pas supprimer la responsabilité.

19. Résilience et souveraineté

Une infrastructure de vérité utilisée par des États ou secteurs critiques doit pouvoir conserver une autonomie opérationnelle suffisante. Des déploiements souverains ou fédérés, des compétences locales, des procédures de reprise et une maîtrise des dépendances stratégiques contribuent à réduire le risque de paralysie externe.

20. Critères d'acceptation et conclusion

La résilience de Deep Authenticity© est cohérente si les fonctions critiques sont identifiées ; si les points uniques de défaillance sont réduits ; si online, offline et modes dégradés sont explicitement distingués ; si la resynchronisation est contrôlée ; si les trois QR codes et le QR Code Dynamique documentaire conservent leurs garanties essentielles ; si sauvegardes et reprises sont testées ; si AP Shield protège les opérations de crise ; si les dépendances externes sont cartographiées ; et si souveraineté, gouvernance et exercices réguliers sont intégrés.

La confiance dans Deep Authenticity© ne dépend donc pas seulement de sa capacité à fonctionner lorsque tout va bien. Elle dépend de sa capacité à rester intelligible, sécurisée et utile lorsque l'environnement se dégrade.

La résilience devient ainsi une propriété fondamentale de l'infrastructure universelle de vérité.

Le Chapitre 16 développera la souveraineté numérique, économique et institutionnelle : maîtrise des données, autonomie stratégique, fédération et coopération internationale.

Note de cadrage institutionnel

Les mécanismes de continuité et de fonctionnement hors ligne doivent être adaptés au niveau de risque. Lorsqu'une vérification temps réel est impossible, Deep Authenticity© doit indiquer explicitement la limite de la preuve disponible plutôt que de produire un résultat définitif non confirmé.

VOLUME I — VISION ET FONDEMENTS

CHAPITRE 16 — SOUVERAINETÉ NUMÉRIQUE, ÉCONOMIQUE ET INSTITUTIONNELLE

SOUVERAINETÉ — DONNÉES — AUTONOMIE STRATÉGIQUE — INFRASTRUCTURES — FÉDÉRATION — INTEROPÉRABILITÉ — ÉCONOMIE — INSTITUTIONS — COOPÉRATION — CONFIANCE

1. Objet du chapitre

Ce chapitre définit la souveraineté comme une propriété structurante de Deep Authenticity©. Une infrastructure universelle de vérité ne peut devenir crédible si son universalité exige l'abandon du contrôle national, institutionnel ou économique. Deep Authenticity© doit permettre la coopération et l'interopérabilité tout en préservant la capacité de chaque acteur légitime à gouverner ses données, ses règles et ses infrastructures critiques.

2. Souveraineté et infrastructure de vérité

La souveraineté ne signifie pas isolement. Elle signifie capacité à décider qui émet une preuve, où résident les données sensibles, qui peut y accéder, selon quelles règles et avec quelles possibilités de recours. Deep Authenticity© fournit une architecture commune de vérification sans prétendre devenir une autorité supérieure aux États et institutions compétents.

3. Souveraineté des données

Les données stratégiques, administratives, industrielles ou personnelles doivent pouvoir rester sous le contrôle de leur détenteur légitime. AP Core peut interroger des preuves ou statuts sans exiger la copie de toutes les données sources. Cette séparation réduit la concentration informationnelle et permet des politiques de localisation adaptées aux juridictions.

4. Souveraineté numérique

La souveraineté numérique implique la maîtrise des infrastructures, identités, clés, interfaces, dépendances et capacités de reprise nécessaires aux fonctions critiques. Les États et organisations

doivent pouvoir exploiter des composants essentiels dans des environnements maîtrisés et conserver une capacité de migration lorsque leurs exigences évoluent.

5. Souveraineté économique

Authenticity Plus© peut contribuer à la souveraineté économique en améliorant la connaissance des produits authentiques, des flux, de la distribution et des anomalies. Une meilleure visibilité peut aider à protéger producteurs, recettes, consommateurs et marchés contre la contrefaçon, tout en fournissant des indicateurs plus fiables pour l'analyse économique.

6. Protection des producteurs et créateurs

La souveraineté économique concerne aussi les artisans, agriculteurs, industriels, artistes, développeurs et innovateurs. Le Passeport Numérique Universel et les mécanismes de provenance peuvent renforcer la capacité de ces acteurs à démontrer origine, authenticité, création ou continuité de propriété sans dépendre exclusivement de grandes plateformes privées.

7. Souveraineté institutionnelle

Les institutions doivent conserver la compétence sur leurs actes, registres, autorisations et décisions. Dans le domaine administratif, le QR Code Dynamique documentaire rend l'état d'un document vérifiable mais ne crée pas sa validité juridique. La source institutionnelle reste l'autorité qui émet, suspend, révoque ou remplace le document.

8. Registres souverains

Les registres fonciers, d'identité, professionnels ou autres bases publiques peuvent rester dans leurs infrastructures nationales. Deep Authenticity© peut recevoir une attestation ou interroger un statut autorisé sans absorber le registre. Cette architecture permet de construire l'interopérabilité autour de la souveraineté plutôt que contre elle.

9. Les trois QR codes et le contrôle national

Dans le domaine physique, les trois QR codes d'Authenticity Plus© — consommateur, revendeur/professionnel et contrôle/douanes — permettent de distribuer la vérification selon les rôles. Le canal contrôle/douanes peut s'intégrer aux procédures nationales et aux habilitations des autorités sans exposer les mêmes fonctions au public.

10. Autonomie stratégique et dépendances

Une infrastructure critique doit cartographier ses dépendances : cloud, télécommunications, composants, bibliothèques, fournisseurs d'identité, matériels et services externes. L'autonomie stratégique ne nécessite pas nécessairement de tout produire localement ; elle exige de connaître les dépendances critiques et de disposer d'alternatives, de contrats et de plans de migration.

11. Architecture fédérée

Deep Authenticity© peut fonctionner comme une fédération d'instances ou de systèmes compatibles. Chaque État, institution ou organisation peut conserver certaines données et fonctions localement, tandis que des protocoles communs permettent d'échanger des preuves. La fédération combine autonomie locale et capacité de coopération.

12. Interopérabilité sans subordination

L'interopérabilité doit permettre à deux systèmes souverains de comprendre une preuve sans que l'un devienne techniquement subordonné à l'autre. Standards documentés, API versionnées, signatures

vérifiables et politiques de confiance explicites réduisent le risque qu'un acteur unique devienne indispensable à l'ensemble de l'écosystème.

13. Corridors de confiance

Des États ou institutions compatibles peuvent établir des corridors de confiance pour certains produits, documents ou échanges. Ces corridors reposent sur la reconnaissance de règles, autorités, preuves et contrôles définis conjointement. Ils peuvent faciliter le commerce et la coopération tout en laissant à chaque partie la maîtrise de son périmètre souverain.

14. Douanes et commerce international

L'architecture de contrôle d'Authenticity Plus© peut soutenir des échanges de preuves entre producteurs, autorités et douanes. L'objectif est de faciliter la vérification de l'origine et de l' authenticité sans créer une autorité douanière supranationale. Chaque juridiction conserve ses pouvoirs de contrôle, décision et sanction.

15. Jumeau Numérique National et souveraineté

Le Jumeau Numérique National et Institutionnel peut devenir un outil stratégique de compréhension du territoire, des capacités et des dépendances. Parce qu'il peut révéler des informations sensibles, son architecture doit prévoir segmentation, accès restreint, hébergement maîtrisé et séparation entre données publiques, opérationnelles et stratégiques.

16. Simulation Institutionnelle Profonde et autonomie de décision

La Simulation Institutionnelle Profonde peut aider un État à tester des politiques sans externaliser entièrement sa capacité d'analyse. Les modèles, hypothèses et données stratégiques doivent pouvoir être gouvernés souverainement. Deep Authenticity© éclaire la décision ; elle ne remplace ni le mandat politique ni les institutions nationales.

17. Réversibilité technologique

La souveraineté exige la capacité de quitter, remplacer ou faire évoluer un composant. Les formats, API, preuves et historiques doivent être suffisamment documentés pour permettre migration et audit. Une infrastructure universelle ne doit pas créer une dépendance irréversible à un fournisseur, une technologie ou une génération cryptographique.

18. Coopération internationale

La souveraineté et la coopération ne sont pas contradictoires. Des mécanismes de reconnaissance mutuelle peuvent permettre aux États, organisations internationales, entreprises et organismes de certification d'échanger des preuves vérifiables. La coopération doit être contractuelle, transparente et compatible avec les cadres juridiques de chaque partie.

19. Vers une souveraineté de la preuve

Deep Authenticity© introduit l'idée d'une souveraineté de la preuve : la capacité pour une institution, un producteur ou un État de produire des preuves vérifiables selon son autorité, de les partager de manière contrôlée et de conserver la maîtrise des données qui les fondent. Cette approche transforme la confiance en relation interopérable plutôt qu'en dépendance centralisée.

20. Critères d'acceptationet conclusion

La souveraineté est préservée si les données sensibles peuvent rester localisées ; si les autorités conservent leurs compétences ; si les registres ne sont pas absorbés ; si les trois QR codes d'

Authenticity Plus© s'intègrent aux contrôles nationaux ; si le QR Code Dynamique documentaire reste relié à l'autorité émettrice ; si les dépendances critiques sont maîtrisées ; si la fédération permet la coopération sans subordination ; si la réversibilité technologique est prévue ; et si les Jumeaux Numériques et simulations restent sous une gouvernance légitime.

Deep Authenticity© peut ainsi viser une portée universelle sans devenir une infrastructure de centralisation universelle.

Son ambition est de rendre les preuves compatibles à travers les frontières tout en permettant aux nations, institutions, entreprises et créateurs de conserver la maîtrise de ce qui leur appartient.

Le Chapitre 17 développera la confiance interinstitutionnelle et les Corridors de Confiance : reconnaissance mutuelle, échanges transfrontaliers et architecture mondiale de coopération.

Note de cadrage institutionnel

La souveraineté décrite dans ce chapitre est un principe d'architecture et de gouvernance. Sa mise en œuvre dépend des législations, accords internationaux, politiques de localisation, infrastructures et compétences des autorités concernées. Deep Authenticity© ne se substitue pas à la souveraineté juridique des États.

VOLUME I — VISION ET FONDEMENTS

CHAPITRE 17 — CONFIANCE INTERINSTITUTIONNELLE ET CORRIDORS DE CONFIANCE

CONFIANCE — RECONNAISSANCE MUTUELLE — CORRIDORS — FRONTIÈRES — DOUANES — PREUVES — INTEROPÉRABILITÉ — FÉDÉRATION — COOPÉRATION — COMMERCE

1. Objet du chapitre

Ce chapitre définit la confiance interinstitutionnelle dans Deep Authenticity© : la capacité de plusieurs États, administrations, organismes, entreprises ou systèmes à reconnaître et vérifier des preuves sans abandonner leur autonomie. Les Corridors de Confiance constituent une application structurante de cette logique pour les échanges transfrontaliers.

2. De la confiance déclarative à la confiance vérifiable

La coopération repose souvent sur documents, certificats et déclarations dont la vérification peut être lente ou fragmentée. Deep Authenticity© vise à rendre certaines relations de confiance directement vérifiables : identité de l'émetteur, intégrité, statut, validité et historique autorisé d'une preuve.

3. Reconnaissance mutuelle

Deux institutions peuvent reconnaître leurs autorités, formats de preuve, règles de signature et niveaux d'assurance respectifs. Cette reconnaissance n'exige pas l'unification de leurs systèmes. Elle définit les conditions dans lesquelles une preuve émise par l'une peut être comprise et acceptée par l'autre.

4. Le Corridor de Confiance

Un Corridor de Confiance est un cadre technique et institutionnel reliant des acteurs qui ont convenu de règles communes pour certains échanges. Il peut concerner des produits, certificats, documents, contrôles ou événements logistiques. Son périmètre, ses autorités et ses critères d'acceptation doivent être explicitement définis.

5. Produits et Authenticity Plus©

Pour les produits physiques, Authenticity Plus© fournit la fondation d'authentification grâce aux trois QR codes : consommateur, revendeur/professionnel et contrôle/douanes. Dans un corridor, le canal contrôle/douanes peut permettre aux autorités habilitées d'accéder aux preuves convenues sans modifier les fonctions destinées aux autres acteurs.

6. Statuts fondamentaux transfrontaliers

La sémantique VERT — original ; JAUNE — original mais déjà vérifié ou vendu ; ROUGE — contrefaçon ou code inexistant dans Authenticity Plus© doit rester cohérente. Les informations réglementaires ou douanières complémentaires peuvent varier selon les juridictions sans altérer cette lecture fondamentale.

7. Documents et QR Code Dynamique

Les certificats ou documents associés à un échange peuvent utiliser le QR Code Dynamique documentaire de Deep Authenticity©. L'autorité destinataire peut alors vérifier l'état vivant du document : validité, expiration, suspension, révocation ou remplacement, selon les droits et accords applicables.

8. Douanes et contrôles frontaliers

Les autorités douanières peuvent utiliser des interfaces spécifiques pour vérifier produits, lots, certificats et événements pertinents. Deep Authenticity© ne décide pas de l'admission d'une marchandise : elle fournit des preuves et statuts permettant à l'autorité compétente d'appliquer ses propres règles.

9. Passeport Numérique Universel

Le Passeport Numérique Universel peut accompagner le produit ou l'actif à travers plusieurs juridictions. Il permet de relier provenance, certifications, événements et propriété autorisée sans exposer automatiquement l'intégralité des données commerciales ou personnelles.

10. AP Core et politiques de confiance

AP Core applique les politiques définissant quelles autorités sont reconnues, quels attributs peuvent être échangés et quels niveaux de preuve sont requis. Les politiques doivent être versionnées afin qu' une modification d'accord n'efface pas la capacité d'interpréter les transactions historiques.

11. Fédération des infrastructures

Chaque participant peut conserver son infrastructure, ses registres et ses données sensibles. Des passerelles ou protocoles compatibles permettent l'échange de preuves. Cette fédération évite qu'un corridor de confiance devienne nécessairement une base centralisée contrôlée par un seul participant.

12. Certification et conformité

Les certifications sectorielles, sanitaires, techniques ou commerciales peuvent être vérifiées dans le corridor lorsque les organismes compétents sont reconnus. Authenticité du certificat, statut et portée

doivent rester distincts : un certificat authentique ne signifie pas nécessairement qu'il couvre toutes les exigences du pays destinataire.

13. Commerce international

Une vérification plus rapide des preuves peut réduire certaines frictions documentaires, faciliter les contrôles ciblés et améliorer la traçabilité des échanges. Ces gains dépendent toutefois de l'adoption institutionnelle, de l'interopérabilité des systèmes et des cadres juridiques applicables.

14. Lutte contre la contrefaçon transfrontalière

Les événements d'Authenticity Plus© peuvent aider à identifier des codes inexistants, déjà utilisés ou associés à des comportements atypiques. Le partage contrôlé de certains signaux entre autorités peut renforcer les investigations tout en respectant les règles de confidentialité et de compétence.

15. Gestion des incidents entre participants

Un corridor doit prévoir la suspension d'une autorité, d'une clé, d'un service ou d'un type de preuve en cas d'incident. Les mécanismes de révocation doivent être rapides, documentés et réversibles lorsque l'incident est résolu. La confiance doit pouvoir être réduite sans arrêter tout l'écosystème.

16. Gouvernance des Corridors de Confiance

Chaque corridor nécessite des règles de gouvernance : adhésion, responsabilités, audits, gestion des versions, résolution des différends, sécurité et retrait. Aucun participant ne doit obtenir silencieusement des droits supérieurs à ceux prévus par l'accord.

17. Souveraineté et réciprocité

La coopération transfrontalière doit préserver la souveraineté des participants. La réciprocité peut être symétrique ou adaptée aux compétences de chacun, mais elle doit être explicite. Un État peut reconnaître une preuve étrangère sans transférer son pouvoir de décision à l'émetteur étranger.

18. Résilience des corridors

Les échanges doivent prévoir indisponibilité réseau, panne d'un participant ou rupture temporaire d' une passerelle. Les modes dégradés doivent indiquer clairement les limites de vérification. Une architecture fédérée permet de contenir une panne locale sans nécessairement interrompre tous les corridors.

19. Vers un réseau mondial de confiance

Plusieurs corridors compatibles peuvent progressivement former un réseau de confiance interopérable entre régions, secteurs et institutions. L'objectif n'est pas une autorité mondiale unique, mais un ensemble de relations vérifiables permettant à des systèmes souverains de coopérer avec davantage de certitude.

20. Critères d'acceptation et conclusion

La confiance interinstitutionnelle est cohérente si les autorités et niveaux de preuve sont explicitement reconnus ; si les Corridors de Confiance disposent d'un périmètre et d'une gouvernance ; si les trois QR codes d'Authenticity Plus© restent la fondation du contrôle physique ; si le QR Code Dynamique documentaire permet la vérification des documents ; si AP Core applique des politiques versionnées ; si les données restent fédérées lorsque nécessaire ; si incidents, révocations et modes dégradés sont prévus ; et si souveraineté, réciprocité et responsabilité sont préservées.

Deep Authenticity© peut ainsi transformer la confiance internationale d'une relation principalement déclarative en une relation davantage vérifiable, sans supprimer la diversité juridique et institutionnelle du monde.

Les Corridors de Confiance constituent le mécanisme de passage entre souveraineté nationale et coopération mondiale.

Le Chapitre 18 développera l'éthique, les droits fondamentaux et la gouvernance de la confiance : proportionnalité, confidentialité, non-surveillance, recours et responsabilité.

Note de cadrage institutionnel

Les Corridors de Confiance constituent un cadre conceptuel de coopération. Leur reconnaissance effective dépend d'accords, de cadres juridiques, de normes techniques et de décisions des autorités compétentes. Deep Authenticity© fournit une infrastructure de preuve ; elle ne crée pas automatiquement la reconnaissance réglementaire ou douanière.

VOLUME I — VISION ET FONDEMENTS

CHAPITRE 18 — ÉTHIQUE, DROITS FONDAMENTAUX ET GOUVERNANCE DE LA CONFIANCE

ÉTHIQUE — DROITS — PROPORTIONNALITÉ — CONFIDENTIALITÉ — NON-SURVEILLANCE — RECOURS — RESPONSABILITÉ — TRANSPARENCE — GOUVERNANCE — CONFIANCE

1. Objet du chapitre

Ce chapitre définit les principes éthiques et de gouvernance qui doivent encadrer Deep Authenticity©. Une infrastructure capable de relier produits, contenus, documents et systèmes institutionnels ne peut être légitime uniquement parce qu'elle est techniquement performante. Sa conception doit intégrer proportionnalité, confidentialité, sécurité, responsabilité, recours et contrôle des pouvoirs.

2. La confiance comme responsabilité

Deep Authenticity© vise à rendre certaines preuves plus vérifiables. Cette capacité crée une responsabilité : éviter qu'un mécanisme conçu pour protéger l'authenticité devienne un instrument de collecte excessive, d'exclusion arbitraire ou de surveillance. La confiance technique doit rester subordonnée à des finalités légitimes et à des règles explicites.

3. Principe de proportionnalité

Chaque donnée, contrôle ou niveau d'identification doit être proportionné à la finalité. Vérifier qu'un produit est authentique ne nécessite pas toujours de connaître l'identité du consommateur ; vérifier qu' un document est valide ne nécessite pas nécessairement d'exposer toutes les informations qu'il contient. La minimisation doit être intégrée dès la conception.

4. Confidentialité par conception

Les données personnelles, commerciales, industrielles et institutionnelles doivent être protégées selon leur sensibilité. Segmentation, chiffrement, contrôle d'accès, pseudonymisation ou divulgation

sélective peuvent être utilisés selon les contextes. L'interopérabilité ne doit jamais être assimilée à une transparence universelle.

5. Principe de non-surveillance

L'existence d'événements de vérification ne doit pas conduire automatiquement à la constitution de profils détaillés des personnes. Les données de localisation, d'usage ou d'identité doivent être limitées lorsque leur collecte n'est pas nécessaire. Les fonctions institutionnelles doivent privilégier les agrégations lorsqu'un suivi individuel n'est pas légitime.

6. Les trois QR codes et la vie privée

Les trois QR codes d'Authenticity Plus© remplissent des fonctions différentes : consommateur, revendeur/professionnel et contrôle/douanes. Cette séparation permet aussi de limiter les données accessibles selon le rôle. Le consommateur ne doit pas être obligé de révéler davantage d' informations que nécessaire pour obtenir une vérification d'authenticité.

7. QR Code Dynamique documentaire et minimisation

Le QR Code Dynamique documentaire peut confirmer qu'un document est valide, expiré, suspendu, révoqué ou remplacé sans nécessairement révéler son contenu intégral. L'interface doit retourner le minimum d'informations permettant au vérificateur autorisé de prendre la décision correspondant à sa fonction.

8. Consentement et bases légitimes

Le consentement peut être approprié pour certains usages, mais il n'est pas la seule base possible dans les contextes administratifs ou réglementaires. Chaque traitement doit reposer sur une base légitime applicable, avec une information compréhensible sur la finalité, les acteurs et les droits disponibles.

9. Transparence des statuts

Dans Authenticity Plus©, VERT signifie original ; JAUNE signifie original mais déjà vérifié ou vendu ; ROUGE signifie contrefaçon ou code inexistant dans le système. Cette sémantique doit rester stable. Lorsqu'un autre signal — par exemple un risque IA — est présenté, il doit être clairement distingué afin de ne pas tromper l'utilisateur.

10. Transparence algorithmique

Lorsqu'une analyse automatisée influence une alerte ou une décision importante, l'utilisateur ou l' autorité de contrôle doit pouvoir comprendre suffisamment la nature du résultat : source, modèle ou règle, niveau de confiance et limites. La transparence doit être compatible avec la sécurité et la protection de la propriété intellectuelle.

11. Droit au recours et à la correction

Un producteur, citoyen, professionnel ou institution peut être affecté par une donnée incorrecte, un statut erroné ou une alerte algorithmique. Des procédures doivent permettre de signaler l'erreur, présenter des éléments de preuve, demander une correction et obtenir un examen par un acteur compétent.

12. Contrôle humain des décisions sensibles

Les décisions à fort impact ne doivent pas reposer uniquement sur une inférence algorithmique lorsqu'une validation humaine ou institutionnelle est nécessaire. Le contrôle humain doit être réel : accès au contexte, possibilité de corriger le résultat et responsabilité clairement attribuée.

13. Responsabilité des acteurs

Émetteurs, opérateurs, intégrateurs, autorités et utilisateurs professionnels doivent connaître leurs responsabilités. Deep Authenticity© fournit une infrastructure de preuve, mais la responsabilité d'une certification, d'une décision administrative, d'une sanction ou d'un usage commercial reste attribuée aux acteurs qui disposent de la compétence correspondante.

14. Gouvernance des données

Les données importantes doivent disposer d'un responsable, d'une finalité, d'une durée de conservation, d'un niveau d'accès et d'une politique de qualité. Les données obsolètes ou incorrectes doivent pouvoir être corrigées selon des procédures compatibles avec la conservation des traces nécessaires à l'audit.

15. Gouvernance des modèles et simulations

Les modèles d'IA, Jumeaux Numériques et simulations doivent être versionnés et documentés. Les hypothèses, limites et sources doivent rester accessibles aux acteurs habilités. Une simulation institutionnelle ne doit pas être présentée comme une prédiction certaine ni devenir automatiquement une décision exécutoire.

16. Auditabilité

Les opérations sensibles doivent produire des traces suffisantes pour permettre un audit : accès privilégiés, changements de statut, révocations, décisions de gouvernance et modifications critiques. L'auditabilité doit être conçue sans transformer la journalisation en collecte indéfinie de données inutiles.

17. Inclusion et accessibilité

Une infrastructure universelle doit rester accessible aux petites entreprises, artisans, producteurs et territoires disposant de moyens limités. AP Léger peut fournir des fonctions essentielles avec une complexité réduite. L'inclusion implique également des interfaces compréhensibles, multilingues et adaptées aux capacités des utilisateurs.

18. Gouvernance institutionnelle

Les fonctions stratégiques de Deep Authenticity© doivent être encadrées par des structures de gouvernance capables de séparer conception technique, exploitation, décision, contrôle et audit. Les pouvoirs exceptionnels ou temporaires doivent être limités, journalisés et réexaminés.

19. Éthique de l'infrastructure universelle

Plus Deep Authenticity© s'étend, plus la retenue devient importante. L'objectif n'est pas de rendre toute activité humaine traçable, mais de rendre vérifiables les éléments pour lesquels la confiance possède une finalité légitime. L'universalité doit désigner la capacité d'application à plusieurs domaines, non une obligation de surveillance universelle.

20. Critères d'acceptation et conclusion

La gouvernance éthique est cohérente si les données sont minimisées ; si les accès sont proportionnés ; si la non-surveillance est un principe explicite ; si les trois QR codes et le QR Code

Dynamique documentaire limitent les informations selon le rôle ; si les statuts restent transparents ; si les résultats IA sont distingués des preuves ; si correction, recours et contrôle humain existent ; si les responsabilités sont attribuées ; et si audit, inclusion et gouvernance institutionnelle accompagnent l'évolution du système.

Deep Authenticity© ne peut devenir une infrastructure de confiance durable que si la puissance de vérification qu'elle crée est accompagnée d'une architecture de limites.

La vérité vérifiable doit servir la confiance sans supprimer la liberté, la confidentialité, la souveraineté ou la responsabilité humaine.

Le Chapitre 19 développera le modèle de déploiement progressif : pilotes, secteurs prioritaires, adoption institutionnelle, montée en charge et internationalisation.

Note de cadrage institutionnel

Les principes exposés dans ce chapitre doivent être adaptés aux législations et cadres de protection des droits applicables. Ils constituent des exigences de conception et de gouvernance de Deep Authenticity© et ne remplacent pas les obligations juridiques, réglementaires ou institutionnelles propres à chaque juridiction.

VOLUME I — VISION ET FONDEMENTS

CHAPITRE 19 — MODÈLE DE DÉPLOIEMENT PROGRESSIF : DES PILOTES À L'INTERNATIONALISATION

DÉPLOIEMENT — PILOTES — SECTEURS PRIORITAIRES — ADOPTION — MONTÉE EN CHARGE — INSTITUTIONS — INDUSTRIE — TERRITOIRES — CORRIDORS DE CONFIANCE — INTERNATIONALISATION

1. Objet du chapitre

Ce chapitre définit une trajectoire de déploiement progressif de Deep Authenticity©. Une infrastructure universelle de vérité ne peut être imposée en une seule étape : elle doit démontrer sa valeur sur des périmètres maîtrisés, mesurer ses résultats, consolider sa gouvernance, puis étendre progressivement ses capacités aux secteurs, institutions, territoires et partenaires internationaux.

2. Principe : commencer par des preuves concrètes

Le déploiement doit commencer par des cas d'usage dont les bénéfices peuvent être observés et mesurés. L'objectif initial n'est pas de connecter immédiatement tous les systèmes, mais de démontrer qu'une chaîne de preuve fiable peut réduire la contrefaçon, simplifier une vérification, améliorer une traçabilité ou sécuriser un document.

3. Pilotes du domaine physique

Les premiers pilotes physiques peuvent concerner des produits à forte exposition à la contrefaçon, à la fraude ou au besoin de traçabilité. Ils doivent tester l'architecture fondamentale des trois QR codes

d'Authenticity Plus© : consommateur, revendeur/professionnel et contrôle/douanes, ainsi que les statuts VERT, JAUNE et ROUGE.

4. Pilotes du domaine numérique

Dans le domaine numérique, les pilotes peuvent porter sur la signature cryptographique native, la provenance et le versionnement de contenus, médias ou logiciels. Ils doivent démontrer la capacité à vérifier une origine et une intégrité sans prétendre certifier automatiquement la vérité factuelle du contenu.

5. Pilotes du domaine administratif

Les pilotes administratifs peuvent porter sur diplômes, certificats, autorisations ou autres documents dont le statut évolue. Le QR Code Dynamique documentaire doit y démontrer sa capacité à refléter un état vivant : valide, expiré, suspendu, révoqué ou remplacé, sous l'autorité de l'émetteur compétent.

6. Choix des secteurs prioritaires

Les secteurs prioritaires doivent être sélectionnés selon plusieurs critères : impact de la fraude, criticité sociale, valeur économique, maturité numérique, disponibilité des acteurs et possibilité de mesurer les résultats. Santé, industrie, agriculture, commerce, documents administratifs ou propriété intellectuelle peuvent suivre des trajectoires distinctes.

7. Critères de réussite d'un pilote

Un pilote doit disposer d'indicateurs définis avant son lancement : taux d'activation, vérifications réussies, anomalies détectées, temps de contrôle, adoption des utilisateurs, incidents, faux positifs, disponibilité et satisfaction des acteurs. La décisiond'extension doit reposer sur des résultats documentés plutôt que sur la seule démonstration technique.

8. Boucle pilote — mesure — correction

Chaque pilote doit alimenter une boucle d'amélioration. Les problèmes d'ergonomie, d'intégration, de sécurité, de gouvernance ou de compréhension des statuts sont identifiés, corrigés puis retestés. Cette discipline permet de stabiliser les composants fondamentaux avant une montée en charge plus coûteuse.

9. Adoption par les producteurs et entreprises

L'adoption industrielle nécessite des outils d'intégration simples, des API documentées, des tableaux de bord utiles et une proposition de valeur claire. Les grandes entreprises peuvent utiliser des intégrations ERP avancées, tandis qu'AP Léger doit permettre aux artisans, petites entreprises et producteurs disposant de moyens limités d'accéder aux fonctions essentielles.

10. Adoption par les consommateurs

La valeur du système dépend aussi de la simplicité de la vérification. Le consommateur doit comprendre rapidement le résultat d'un scan, notamment la signification stable de VERT, JAUNE et ROUGE. L'expérience utilisateur doit réduire la complexité technique sans masquer les limites ou conditions de la preuve.

11. Adoption institutionnelle

Les administrations et autorités doivent pouvoir expérimenter Deep Authenticity© dans des environnements contrôlés avant une intégration à grande échelle. Les pilotes institutionnels doivent

clarifier compétences, responsabilités, hébergement, sécurité, audit, interopérabilité avec les registres et procédures de recours.

12. Déploiement territorial

Après validation sectorielle, un déploiement peut être étendu à une ville, une wilaya, une région ou un autre territoire. Cette étape permet de tester l'interaction entre plusieurs secteurs et de commencer à alimenter des tableaux de bord territoriaux et des Jumeaux Numériques avec des données réellement opérationnelles.

13. Montée en charge technique

L'extension du nombre de produits, documents, utilisateurs et événements exige une architecture capable d'augmenter progressivement ses capacités. Performance, disponibilité, stockage, gestion des clés, observabilité, sécurité et reprise doivent être testés sous charge avant chaque changement d'échelle.

14. Montée en charge organisationnelle

La croissance technique doit être accompagnée par des équipes, procédures et responsabilités adaptées. Support, sécurité, intégration, audit, gouvernance des données, gestion des incidents et relations institutionnelles doivent évoluer en parallèle. Une plateforme techniquement scalable peut échouer si son organisation ne l'est pas.

15. Déploiement du Jumeau Numérique National

Le Jumeau Numérique National et Institutionnel ne doit pas être construit comme un projet massif préalable à toute utilisation. Il peut émerger progressivement à partir de secteurs et sources déjà validés. Chaque nouvelle rubrique enrichit la représentation nationale tout en conservant provenance, droits, incertitudes et souveraineté.

16. Déploiement de la Simulation Institutionnelle Profonde

La Simulation Institutionnelle Profonde doit être introduite après consolidation suffisante des données et des Jumeaux Numériques. Les premiers scénarios peuvent être limités à des domaines bien compris, puis élargis à mesure que les modèles sont validés. Le monitoring des décisions réelles permet ensuite de recalibrer les simulations.

17. Corridors de Confiance pilotes

L'internationalisation peut commencer par des Corridors de Confiance limités entre partenaires volontaires : un produit, un secteur, une route commerciale ou un type de document. Ces pilotes permettent de tester reconnaissance mutuelle, douanes, politiques de confiance, révocation et fédération sans exiger immédiatement une adoption mondiale.

18. Internationalisation progressive

Après validation des corridors, l'architecture peut s'étendre à de nouveaux partenaires et régions. Les standards, API et mécanismes de preuve doivent rester suffisamment ouverts pour permettre l'intégration de systèmes différents. L'expansion internationale doit préserver la souveraineté juridique et technique des participants.

19. Gouvernance de la croissance

Chaque changement d'échelle doit être soumis à une revue de gouvernance : sécurité, droits fondamentaux, résilience, souveraineté, coûts, dépendances et capacité de support. L'objectif n'est

pas la croissance la plus rapide possible, mais une croissance dont la confiance augmente avec l'usage au lieu de se fragiliser.

20. Critères d'acceptation et conclusion

Le déploiement est cohérent si les pilotes commencent par des cas mesurables ; si les trois domaines sont testés selon leurs mécanismes propres ; si les résultats sont évalués avant extension ; si AP Léger préserve l'accessibilité ; si la montée en charge technique et organisationnelle est synchronisée ; si le Jumeau Numérique et la Simulation Institutionnelle Profonde sont construits progressivement ; si les Corridors de Confiance précèdent l'internationalisation large ; et si chaque étape conserve sécurité, éthique, résilience et souveraineté.

Deep Authenticity© doit donc croître par cercles de confiance successifs : preuve locale, adoption sectorielle, intégration institutionnelle, consolidation territoriale, capacité nationale puis coopération internationale.

Cette progression permet de transformer une vision universelle en infrastructure réelle sans sacrifier la maîtrise, la qualité ou la légitimité.

Le Chapitre 20 synthétisera les fondements du Volume I et présentera la trajectoire stratégique de Deep Authenticity© vers une infrastructure universelle de vérité.

Note de cadrage institutionnel

Le présent modèle décrit une trajectoire de déploiement de référence. Les secteurs, calendriers, juridictions et partenaires devront être sélectionnés selon les conditions réelles. Chaque passage à l'échelle doit être précédé d'une évaluation technique, sécuritaire, juridique, économique et institutionnelle.

VOLUME I — VISION ET FONDEMENTS

CHAPITRE 20 — SYNTHÈSE DES FONDEMENTS ET TRAJECTOIRE STRATÉGIQUE

VISION — 3 QR CODES — PASSEPORT NUMÉRIQUE UNIVERSEL — AP CORE — DEEP AUTHENTICITY — JUMEAUX NUMÉRIQUES — SIMULATION — RÉSILIENCE — SOUVERAINETÉ — INFRASTRUCTURE DE VÉRITÉ

1. Objet du chapitre

Ce chapitre clôt le Volume I — Vision et Fondements en réunissant les principes qui structurent Deep Authenticity©. Il ne constitue pas une simple conclusion : il expose la cohérence d'ensemble qui relie Authenticity Plus©, le Passeport Numérique Universel, AP Core, les trois domaines de vérité, les Jumeaux Numériques, la Simulation Institutionnelle Profonde, la résilience et la souveraineté.

2. Le changement de paradigme

Le point de départ est un changement de logique : ne plus demander seulement si une information paraît crédible, mais rechercher la preuve vérifiable qui relie un objet, un contenu ou un document à

une source, un statut et une histoire. Deep Authenticity© organise cette continuité de preuve sans prétendre supprimer le droit, l'autorité humaine ou l'incertitude.

3. Authenticity Plus© comme fondation physique

Dans le domaine physique, Authenticity Plus© demeure la fondation anti-contrefaçon. Son architecture repose sur trois QR codes fonctionnellement distincts — consommateur, revendeur/professionnel et contrôle/douanes — qui accompagnent le produit selon les rôles et les étapes de son cycle de vie.

4. La sémantique universelle VERT / JAUNE / ROUGE

La lecture fondamentale reste stable : VERT signifie original ; JAUNE signifie original mais déjà vérifié ou vendu ; ROUGE signifie contrefaçon ou code inexistant dans Authenticity Plus©. Cette simplicité constitue un langage opérationnel commun qui ne doit pas être dilué par les couches analytiques complémentaires.

5. Le Passeport Numérique Universel

Le Passeport Numérique Universel fournit la continuité d'identité et d'événements. Il peut accompagner un produit, un contenu ou un document à travers création, émission, distribution, vérification, propriété, versionnement, maintenance, certification ou révocation, selon le domaine et les droits applicables.

6. AP Core comme noyau d'orchestration

AP Core relie identités, preuves, statuts, événements, droits, signatures, API et politiques de confiance. Il ne remplace pas les autorités sources : il orchestre la vérification entre des systèmes distribués et permet aux différents modules de Deep Authenticity© de partager une logique commune.

7. Les trois domaines de Deep Authenticity©

Deep Authenticity© englobe trois domaines fondamentaux : le physique — objets et produits ; le numérique — logiciels, médias, contenus et propriété intellectuelle ; l'administratif — documents, identité, certificats et titres. Cette structure permet d'étendre la vérification sans confondre les mécanismes propres à chaque domaine.

8. Le QR Code Dynamique documentaire

Dans le domaine administratif, le QR Code Dynamique documentaire permet de relier une copie ou un document présenté à son état vivant : valide, expiré, suspendu, révoqué ou remplacé. Il reste distinct des trois QR codes d'Authenticity Plus©, tout en partageant avec eux AP Core et la logique générale de preuve.

9. Signature cryptographique native et provenance

Dans le domaine numérique, la signature cryptographique native et les mécanismes de provenance permettent de vérifier origine, intégrité, version et chaîne de transformation. Ils établissent des faits techniques sur la provenance ; ils ne doivent pas être présentés comme une certification automatique de la vérité factuelle d'un contenu.

10. Modules complémentaires

AP Ledger, AP Cloud, AP Shield, AP Business, AP Finance/AP Pay, AP Health, AP Billetterie, AP-Certified™ et AP Léger enrichissent l'infrastructure selon les besoins. Ils constituent des couches

fonctionnelles autour d'AP Core et ne remplacent jamais les mécanismes fondamentaux d' authentification et de preuve.

11. Intelligence artificielle

L'intelligence artificielle apporte détection d'anomalies, analyse d'images, signaux faibles et capacités prédictives. Elle reste une couche d'inférence. Deep Authenticity© distingue explicitement preuve déterministe, donnée observée, estimation algorithmique et scénario simulé afin de préserver la lisibilité de la décision.

12. Les Jumeaux Numériques

Les Jumeaux Numériques transforment les preuves et données autorisées en représentations structurées du produit, de l'entreprise, du secteur, du territoire ou de l'État. Le Jumeau Numérique National et Institutionnel devient une capacité stratégique lorsqu'il conserve provenance, incertitudes, segmentation et souveraineté des sources.

13. La Simulation Institutionnelle Profonde

La Simulation Institutionnelle Profonde prolonge le jumeau numérique en permettant d'explorer plusieurs futurs avant décision. Elle organise une boucle complète : observer, modéliser, simuler, comparer, décider, exécuter, monitorer et apprendre. La décision politique ou institutionnelle demeure sous la responsabilité de l'autorité compétente.

14. Tableaux de bord stratégiques

Les tableaux de bord économiques, sociaux et stratégiques rendent visibles pénuries, surplus, disparités, rappels, maintenance, flux et signaux faibles. Ils doivent distinguer données vérifiées, estimations et simulations, afin que la puissance de visualisation ne crée jamais une illusion de certitude.

15. Résilience systémique

Deep Authenticity© doit rester utile lorsque les conditions normales disparaissent. Redondance, sauvegarde, reprise, modes dégradés, fonctionnement offline contrôlé, resynchronisation et AP Shield constituent les fondations d'une continuité de service adaptée au niveau de criticité.

16. Souveraineté

La portée universelle de Deep Authenticity© ne suppose pas une centralisation universelle. Les données et registres sensibles peuvent rester sous contrôle souverain. L'architecture fédérée, la réversibilité technologique et la souveraineté de la preuve permettent de coopérer sans abandonner l' autonomie stratégique.

17. Corridors de Confiance

Les Corridors de Confiance offrent une trajectoire vers la coopération transfrontalière. États, douanes, organismes et entreprises peuvent reconnaître certaines preuves selon des politiques communes tout en conservant leurs compétences. Plusieurs corridors compatibles peuvent former progressivement un réseau mondial de confiance vérifiable.

18. Éthique et limites

La puissance de vérification doit être accompagnée de limites : proportionnalité, minimisation, confidentialité, non-surveillance, transparence, contrôle humain, recours et responsabilité. L'

universalité signifie capacité d'application à de nombreux domaines ; elle ne signifie pas traçabilité totale de toute activité humaine.

19. Trajectoire stratégique

La trajectoire recommandée procède par cercles successifs : pilotes mesurables, adoption sectorielle, intégration institutionnelle, déploiement territorial, consolidation nationale, Jumeaux Numériques, Simulation Institutionnelle Profonde, Corridors de Confiance puis internationalisation. Chaque changement d'échelle doit renforcer plutôt qu'affaiblir la confiance.

20. Conclusion du Volume I

Le Volume I établit ainsi l'architecture intellectuelle de Deep Authenticity© : une infrastructure de vérité universelle capable de relier le monde physique, numérique et administratif par des preuves vérifiables, tout en préservant souveraineté, résilience, droits et responsabilité humaine.

Authenticity Plus© fournit la fondation anti-contrefaçon du monde physique ; le Passeport Numérique Universel assure la continuité ; AP Core orchestre les relations ; les modules étendent les fonctions ; les Jumeaux Numériques représentent le réel ; la Simulation Institutionnelle Profonde explore les futurs possibles ; la résilience protège la continuité ; et la souveraineté garantit que l'interopérabilité ne devienne pas dépendance.

À son niveau conceptuel le plus élevé, Deep Authenticity© peut être décrite comme le système d' exploitation de la civilisation moderne : non parce qu'elle gouvernerait la civilisation, mais parce qu'elle ambitionne de fournir une couche commune de vérification, de provenance et de confiance entre ses systèmes physiques, numériques et administratifs.

Le Volume II pourra désormais développer cette architecture fondatrice en profondeur, avec ses mécanismes techniques, ses protocoles, ses modèles de données, sa cybersécurité et ses conditions opérationnelles de mise en œuvre.

Note de cadrage institutionnel

Ce chapitre synthétise la doctrine du Volume I. Les architectures, mécanismes et trajectoires présentés constituent le cadre conceptuel de Deep Authenticity© ; leur mise en œuvre concrète devra être validée par des travaux techniques, juridiques, économiques, sécuritaires et institutionnels adaptés à chaque secteur et juridiction.

VOLUME II — ARCHITECTURE TECHNOLOGIQUE ET CYBERSÉCURITÉ

CHAPITRE 1 — ARCHITECTURE TECHNOLOGIQUE GLOBALE DE DEEP AUTHENTICITY©

ARCHITECTURE — AP CORE — AP LEDGER — AP CLOUD — AP SHIELD — API — CRYPTOGRAPHIE — IA/CNN — IOT/NFC — ONLINE/OFFLINE — ERP — CYBERSÉCURITÉ

1. Objet du chapitre

Ce chapitre ouvre le Volume II — Architecture technologique et cybersécurité. Il traduit les fondements du Volume I en architecture technique cohérente. Deep Authenticity© est conçue comme une infrastructure distribuée de vérification, de provenance et de confiance reliant le monde physique, numérique et administratif, avec AP Core comme noyau d'orchestration et des couches spécialisées de sécurité, données, preuve, intégration et résilience.

2. Principe d'architecture en couches

L'architecture est organisée en couches séparant interaction, identité, preuve, orchestration, données, intégration, analyse et sécurité. Cette séparation permet de faire évoluer un composant sans remettre en cause l'ensemble du système. Les couches communiquent par interfaces contrôlées, avec des droits, formats et responsabilités explicitement définis.

3. AP Core — noyau technologique

AP Core constitue le moteur d'orchestration. Il relie identifiants, statuts, événements, droits, signatures, politiques de confiance et modules. Il détermine quelles preuves doivent être consultées, quelles opérations sont autorisées et quelles réponses peuvent être restituées selon le rôle de l'utilisateur, sans exiger la centralisation de toutes les données sources.

4. Architecture des trois domaines

Le domaine physique s'appuie sur Authenticity Plus© et ses trois QR codes ; le domaine numérique sur signatures natives, empreintes et provenance ; le domaine administratif sur le QR Code Dynamique documentaire et les autorités émettrices. Les trois domaines utilisent des services communs d'AP Core mais conservent leurs mécanismes de preuve propres.

5. Fondation physique — les trois QR codes

Les trois QR codes d'Authenticity Plus© — consommateur, revendeur/professionnel et contrôle/douanes — restent le mécanisme anti-contrefaçon fondamental du domaine physique. Leur séparation fonctionnelle doit être préservée dans toute l'architecture technique. Les couches AP Ledger, Cloud, Shield, IA, IoT ou ERP les renforcent sans s'y substituer.

6. Statuts fondamentaux

Le moteur de vérification doit préserver une sémantique stable : VERT signifie original ; JAUNE signifie original mais déjà vérifié ou vendu ; ROUGE signifie contrefaçon ou code inexistant dans Authenticity Plus©. Les scores IA, alertes de risque ou états opérationnels complémentaires doivent être techniquement et visuellement séparés de ces trois statuts.

7. AP Ledger — registre de preuves

AP Ledger fournit une couche d'auditabilité pour les événements qui nécessitent une preuve durable : émission, activation, changement de statut, transfert, certification, révocation ou ancrage d'empreinte. Son architecture doit éviter d'y inscrire inutilement des données sensibles ; références, empreintes et événements minimaux peuvent suffire selon le cas d'usage.

8. AP Cloud — services et infrastructure

AP Cloud fournit les services de calcul, stockage, distribution, supervision et montée en charge nécessaires aux composants de Deep Authenticity©. Il doit pouvoir fonctionner dans des

architectures publiques, privées, hybrides ou souveraines. La conception évite de confondre AP Cloud avec une obligation de centraliser toutes les données dans un cloud unique.

9. AP Shield — sécurité transversale

AP Shield constitue la couche transversale de protection : identité et accès, détection d'incidents, gestion des secrets, journalisation, segmentation, protection des API, surveillance et réponse. Il doit couvrir les services centraux comme les intégrations externes, avec une approche fondée sur le risque et le principe du moindre privilège.

10. API et interopérabilité

Les API constituent les interfaces d'échange avec ERP, registres, applications, systèmes douaniers, partenaires et modules sectoriels. Elles doivent être authentifiées, versionnées, documentées et limitées par politiques d'accès. L'interopérabilité vise l'échange de preuves utiles, non l'exposition systématique des bases de données internes.

11. Cryptographie et gestion des clés

La cryptographie protège confidentialité, intégrité, authenticité et non-altération des échanges. L' architecture doit couvrir signatures, chiffrement, empreintes, certificats, rotation, révocation et gestion du cycle de vie des clés. Les algorithmes doivent pouvoir évoluer afin d'éviter qu'une dépendance cryptographique ancienne fragilise durablement les preuves.

12. Signature native des contenus

Les contenus numériques peuvent recevoir une signature cryptographique native ou une preuve liée à leur empreinte lors de la création, publication ou validation. Le système peut ensuite vérifier source, intégrité et version. Cette preuve technique de provenance ne doit jamais être confondue avec une certification automatique de la véracité du contenu.

13. Intelligence artificielle et CNN

Les moteurs IA/CNN analysent images, anomalies, comportements de scan, incohérences et signaux faibles. Ils peuvent renforcer la détection de contrefaçons et de manipulations, mais leurs résultats restent probabilistes. AP Core doit conserver modèle, version, score et contexte afin que l'inférence reste distincte de la preuve déterministe.

14. IoT, NFC et liaison objet-numérique

IoT, NFC, puces et capteurs peuvent renforcer le lien entre l'objet physique et son identité numérique ou transmettre des événements supplémentaires. Ces technologies sont complémentaires aux trois QR codes. L'architecture doit authentifier les dispositifs, protéger leurs clés et vérifier la provenance des données avant intégration au Passeport Numérique Universel.

15. Architecture Online/Offline

Deep Authenticity© doit fonctionner dans des environnements de connectivité variable. Certaines preuves peuvent être vérifiées localement ou mises en cache de manière sécurisée, avec indication explicite du niveau de fraîcheur. Après reconnexion, la resynchronisation doit traiter conflits, duplications et changements de statut intervenus pendant la période hors ligne.

16. Intégration ERP et systèmes industriels

Les ERP peuvent transmettre production, lots, stocks, expéditions, ventes ou événements de maintenance. Deep Authenticity© ne remplace pas l'ERP : elle sélectionne les événements

nécessaires à la continuité de preuve. Des connecteurs et API permettent de préserver les processus industriels existants tout en ajoutant une couche de vérification.

17. Architecture des données et événements

Chaque événement doit être relié à une source, un identifiant, un horodatage, un type, un statut et un niveau d'assurance. Les données peuvent rester distribuées tandis qu'AP Core maintient les relations nécessaires. Cette architecture événementielle prépare les tableaux de bord, Jumeaux Numériques et fonctions de simulation sans effacer la provenance.

18. Cybersécurité de bout en bout

La cybersécurité doit couvrir applications mobiles, QR, API, cloud, ledger, clés, postes administratifs, intégrations ERP, IoT et infrastructures souveraines. L'approche repose sur défense en profondeur, segmentation, moindre privilège, supervision, tests, gestion des vulnérabilités, réponse aux incidents et capacité de reprise.

19. Résilience, souveraineté et fédération

L'architecture doit supporter redondance, haute disponibilité, sauvegarde, reprise et modes dégradés. Les États et institutions doivent pouvoir conserver leurs registres et données sensibles dans des environnements maîtrisés. Une fédération d'instances compatibles permet la coopération et les Corridors de Confiance sans imposer une base mondiale unique.

20. Critères d'acceptation et conclusion

L'architecture technologique globale est cohérente si AP Core orchestre sans centralisation obligatoire ; si les trois QR codes d'Authenticity Plus© restent la fondation physique ; si AP Ledger conserve des preuves minimales et auditables ; si AP Cloud reste déployable selon plusieurs modèles ; si AP Shield protège transversalement l'écosystème ; si les API assurent l'interopérabilité ; si cryptographie, signatures natives, IA/CNN et IoT/NFC sont correctement séparés selon leur rôle ; si Online/Offline et ERP sont intégrés ; et si cybersécurité, résilience, souveraineté et fédération sont conçues dès l'origine.

Deep Authenticity© repose ainsi sur une architecture où chaque technologie possède une fonction précise et où aucune couche complémentaire ne remplace le mécanisme de preuve qu'elle est destinée à renforcer.

Cette architecture constitue la colonne vertébrale technique du Volume II.

Le Chapitre 2 développera AP Core : noyau technologique, moteur d'orchestration, politiques de confiance, identités, statuts, événements et coordination des modules.

Note de cadrage institutionnel

Le présent chapitre fixe l'architecture technologique de référence du Volume II. Les choix d'implémentation précis — protocoles, fournisseurs, algorithmes, infrastructures et standards — devront être validés par des études techniques et de cybersécurité adaptées aux secteurs, niveaux de risque et juridictions. La matrice institutionnelle définie ici sera conservée pour l'ensemble du Volume II.

VOLUME II — ARCHITECTURE TECHNOLOGIQUE ET CYBERSÉCURITÉ

CHAPITRE 2 — AP CORE : NOYAU TECHNOLOGIQUE ET MOTEUR D’ ORCHESTRATION

AP CORE — ORCHESTRATION — IDENTITÉS — STATUTS — ÉVÉNEMENTS — POLITIQUES DE CONFIANCE — PREUVES — MODULES — API — SÉCURITÉ — FÉDÉRATION

1. Objet du chapitre

Ce chapitre définit AP Core comme le noyau technologique de Deep Authenticity©. AP Core n’est ni une simple base de données ni un module métier isolé : il constitue la couche d’orchestration qui relie identités, preuves, statuts, événements, droits, politiques de confiance, modules et systèmes externes dans les trois domaines physique, numérique et administratif.

2. Rôle architectural d’AP Core

AP Core reçoit une demande de vérification ou d’opération, identifie le contexte, détermine les règles applicables, consulte les sources autorisées et produit une réponse structurée. Il permet ainsi aux différents composants de Deep Authenticity© de fonctionner selon une logique commune sans imposer que toutes les données soient stockées dans un même système.

3. Modèle d’identité

Chaque produit, contenu, document, organisation, dispositif ou autre élément pertinent doit disposer d’ un identifiant permettant de le résoudre sans ambiguïté. AP Core gère les relations entre ces identifiants et leurs autorités sources. L’identité technique doit rester distincte de l’identité personnelle lorsque cette dernière n’est pas nécessaire.

4. Résolution des identifiants

Lorsqu’un QR code, une signature, un identifiant API ou un dispositif NFC est présenté, AP Core doit déterminer à quel élément il se rapporte et quelles sources peuvent confirmer son état. La résolution doit résister aux collisions, aux références obsolètes et aux tentatives de substitution ou de réutilisation.

5. Orchestration des trois QR codes

Dans le domaine physique, AP Core orchestre les trois QR codes d’Authenticity Plus© : consommateur, revendeur/professionnel et contrôle/douanes. Il applique des droits et fonctions distincts à chacun tout en les reliant au même produit. Cette séparation fonctionnelle reste une règle fondamentale de l’ architecture.

6. Moteur des statuts VERT / JAUNE / ROUGE

AP Core restitue la sémantique fondamentale d’Authenticity Plus© : VERT signifie original ; JAUNE signifie original mais déjà vérifié ou vendu ; ROUGE signifie contrefaçon ou code inexistant dans le système. Les règles de transition doivent être déterministes, journalisées et séparées des scores probabilistes produits par l’IA.

7. QR Code Dynamique documentaire

Pour le domaine administratif, AP Core résout le QR Code Dynamique documentaire et interroge l’état vivant du document auprès des sources compétentes. Il peut restituer valide, expiré, suspendu, révoqué ou remplacé selon les droits. Cette logique reste techniquement distincte du moteur des trois QR codes physiques.

8. Moteur d’événements

Activation, scan, vente, transfert, certification, maintenance, révocation ou changement de version sont représentés comme événements structurés. AP Core valide leur source, leur type, leur horodatage et leurs droits avant de les accepter. Les événements deviennent la matière première de la continuité de preuve.

9. Politiques de confiance

Une politique de confiance définit quelles autorités, signatures, systèmes ou attributs sont acceptés pour une opération donnée. AP Core doit pouvoir appliquer des politiques différentes selon secteur, juridiction, rôle ou Corridor de Confiance. Ces politiques sont versionnées afin de préserver l’interprétation des opérations historiques.

10. Moteur d’autorisation

AP Core applique le principe du moindre privilège. Un consommateur, revendeur, douanier, producteur, administrateur ou système externe ne reçoit que les opérations et données nécessaires à son rôle. Les décisions d’autorisation doivent être explicites, auditables et indépendantes de la seule possession d’un identifiant visible.

11. Orchestration des preuves

Une vérification peut nécessiter plusieurs preuves : existence d’un identifiant, signature valide, événement dans AP Ledger, statut d’un registre, information ERP ou attestation IoT. AP Core combine les résultats selon une politique définie sans confondre absence de preuve, indisponibilité technique et preuve négative.

12. Coordination avec AP Ledger

AP Core détermine quels événements doivent être ancrés ou consultés dans AP Ledger. Le ledger apporte auditabilité et chronologie ; AP Core conserve la logique métier et les politiques de décision. Cette séparation évite de transformer le registre de preuve en moteur applicatif universel.

13. Coordination avec AP Cloud

AP Cloud fournit les ressources de calcul, stockage, messagerie et distribution nécessaires à AP Core selon le modèle de déploiement retenu. AP Core doit cependant rester architecturé pour fonctionner dans des environnements cloud, privés, hybrides ou souverains afin d’éviter une dépendance structurelle à un fournisseur unique.

14. Coordination avec AP Shield

AP Shield protège AP Core par authentification, contrôle des accès, gestion des secrets, détection d’incidents, journalisation et supervision. Les événements de sécurité peuvent modifier temporairement les politiques de confiance, suspendre une clé ou isoler une intégration compromise sans arrêter nécessairement l’ensemble de la plateforme.

15. API et intégrations

Les systèmes ERP, registres publics, applications, dispositifs IoT et partenaires utilisent des API contrôlées pour interagir avec AP Core. Chaque interface doit disposer d’un contrat, d’une version, d’un mécanisme d’authentification, de limites et d’une politique d’erreur permettant une intégration fiable.

16. Online, Offline et cohérence

En mode offline, certaines décisions peuvent s'appuyer sur des preuves locales sécurisées. AP Core doit distinguer confirmation temps réel et résultat provisoire. Lors de la resynchronisation, il traite l'ordre des événements, les doublons, conflits et changements de statut intervenus pendant l'interruption.

17. IA et moteur de décision

Les moteurs IA/CNN peuvent fournir à AP Core des scores ou alertes. AP Core conserve ces résultats comme signaux analytiques accompagnés de leur modèle, version et niveau de confiance. Une inférence ne doit pas modifier silencieusement la signification des statuts fondamentaux ni se substituer à une preuve déterministe.

18. Fédération et souveraineté

Plusieurs instances d'AP Core peuvent coopérer dans une architecture fédérée. Chaque organisation ou État peut conserver certaines données et politiques localement tout en échangeant des preuves selon des protocoles communs. Cette capacité prépare les Corridors de Confiance et limite la centralisation mondiale.

19. Observabilité, audit et performance

AP Core doit être observable : latence, disponibilité, erreurs, files d'événements, décisions d'autorisation et dépendances critiques doivent pouvoir être supervisées. Les journaux d'audit doivent être protégés et minimisés. Les objectifs de performance doivent être définis selon la criticité des opérations.

20. Critères d'acceptation et conclusion

AP Core est cohérent si les identités sont résolues sans ambiguïté ; si les trois QR codes d'Authenticity Plus© conservent leurs fonctions distinctes ; si VERT, JAUNE et ROUGE restent déterministes ; si le QR Code Dynamique documentaire utilise son propre moteur de statut ; si événements, politiques et autorisations sont versionnés et auditables ; si AP Ledger, AP Cloud et AP Shield conservent des responsabilités séparées ; si les API, modes Online/Offline et résultats IA sont correctement orchestrés ; et si la fédération permet la souveraineté.

AP Core constitue ainsi le système nerveux de Deep Authenticity© : il ne remplace pas les preuves, les autorités ou les modules, mais coordonne leurs relations afin de produire une vérification cohérente et gouvernable.

Sa robustesse conditionne la capacité de l'ensemble de l'écosystème à fonctionner comme une infrastructure unifiée sans devenir une architecture monolithique.

Le Chapitre 3 développera l'architecture technique des trois QR codes d'Authenticity Plus© : génération, unicité, protection, rôles, cycle de vie, statuts et résistance à la copie.

Note de cadrage institutionnel

AP Core est défini ici comme une architecture logique d'orchestration. Les technologies d'implémentation, protocoles, moteurs de règles, formats d'événements et mécanismes de résolution devront être sélectionnés après analyse des exigences de sécurité, performance, souveraineté et interopérabilité. La matrice institutionnelle du Volume II reste inchangée.

VOLUME II — ARCHITECTURE TECHNOLOGIQUE ET CYBERSÉCURITÉ

CHAPITRE 3 — ARCHITECTURE TECHNIQUE DES TROIS QR CODES ET SIGNATURE CRYPTOGRAPHIQUE

3 QR CODES — SIGNATURE CRYPTOGRAPHIQUE — UNICITÉ — AP CORE — CONSOMMATEUR — REVENDEUR — CONTRÔLE/DOUANES — CYCLE DE VIE — VERT/JAUNE/ROUGE — ANTI-COPIE

1. Objet du chapitre

Ce chapitre définit l'architecture technique fondamentale des trois QR codes d'Authenticity Plus© et leur liaison avec la signature cryptographique. Dans le domaine physique, les QR codes constituent les vecteurs d'accès à la preuve ; la cryptographie protège l'intégrité et l'authenticité des preuves associées ; AP Core orchestre les statuts, droits et événements.

2. Principe des trois QR codes

Chaque unité protégée peut être associée à trois QR codes fonctionnellement distincts : consommateur, revendeur/professionnel et contrôle/douanes. Ils se rapportent au même produit mais n'accordent ni les mêmes informations ni les mêmes opérations. Cette séparation réduit l'exposition des fonctions sensibles et structure le cycle de vie.

3. QR code consommateur

Le QR code consommateur permet la vérification destinée au public et l'accès aux informations autorisées du Passeport Numérique Universel. Sa conception doit privilégier simplicité, rapidité et confidentialité. La vérification doit conduire à une réponse compréhensible sans exiger inutilement l'identité du consommateur.

4. QR code revendeur/professionnel

Le QR code revendeur/professionnel permet les opérations réservées à la chaîne commerciale : réception, enregistrement, vente, transfert ou mise à jour autorisée. Il peut également permettre l'intégration du produit dans la fenêtre revendeur d'Authenticity Plus©. Ses privilèges sont contrôlés par AP Core et l'identité professionnelle.

5. QR code contrôle/douanes

Le QR code contrôle/douanes est destiné aux autorités et agents habilités. Il peut donner accès à des preuves ou fonctions de contrôle non exposées au public. Même lorsqu'il est physiquement visible, ses opérations sensibles restent protégées par authentification, habilitation et politiques de confiance.

6. Génération et unicité

Chaque QR code doit être généré à partir d'un identifiant suffisamment unique et non prévisible. L'unicité doit être contrôlée avant activation et reliée au produit, au rôle du QR et à son cycle de vie. L'identifiant visible ne doit pas contenir directement des secrets cryptographiques ou des données sensibles.

7. Signature cryptographique associée

La signature cryptographique permet de vérifier qu'une preuve ou un ensemble de données associé au QR provient d'un émetteur autorisé et n'a pas été altéré. Elle peut couvrir l'identifiant, le contexte d'

émission, des attributs essentiels et des références de version. La clé privée ne doit jamais être encodée dans le QR code.

8. Séparation identifiant, signature et secret

L'architecture distingue trois notions : l'identifiant qui permet de résoudre le produit ; la signature qui permet de vérifier une preuve ; et les secrets ou clés privées qui restent dans des environnements protégés. Cette séparation limite l'impact d'une copie visuelle du QR et facilite la rotation des clés.

9. Protection physique et couche à gratter

Lorsque le scénario le prévoit, les QR codes ou éléments sensibles peuvent être protégés par une couche à gratter ou un dispositif physique équivalent. Cette protection contribue à détecter une première ouverture ou utilisation. Elle complète la vérification numérique et ne doit pas être considérée comme une protection cryptographique à elle seule.

10. Résistance à la copie

Une photographie ou une reproduction parfaite du motif QR ne doit pas suffire à créer un produit authentique. AP Core vérifie l'existence, le rôle, l'état, l'historique et les événements associés. Les duplications, scans incompatibles ou réutilisations peuvent produire des signaux d'anomalie et déclencher des contrôles supplémentaires.

11. Moteur VERT / JAUNE / ROUGE

La logique fondamentale reste : VERT signifie original ; JAUNE signifie original mais déjà vérifié ou vendu ; ROUGE signifie contrefaçon ou code inexistant dans Authenticity Plus©. Les transitions de statut doivent être définies par des événements autorisés et journalisés. Les alertes IA restent séparées de cette sémantique.

12. Cycle de vie du QR

Le cycle de vie peut comprendre génération, affectation, activation, première vérification, vente, transfert, contrôle, suspension, révocation ou clôture. Chaque étape doit être reliée à un acteur ou système autorisé. Les états historiques nécessaires à l'audit sont conservés sans exposer inutilement les données personnelles.

13. Liaison avec AP Core

AP Core résout le QR, vérifie son rôle, consulte les preuves et applique la politique de confiance. Il détermine les opérations permises et restitue le statut approprié. Le QR code reste ainsi un point d' entrée ; la logique de confiance réside dans l'infrastructure et non dans l'image imprimée.

14. Liaison avec AP Ledger

Les événements critiques peuvent être enregistrés ou ancrés dans AP Ledger afin de renforcer l' auditabilité. Le ledger peut conserver empreintes, références et horodatages sans stocker toutes les informations du produit. AP Core reste responsable de l'interprétation métier de ces preuves.

15. Liaison avec AP Shield

AP Shield protège les services de génération, activation, résolution et administration des QR codes. Il surveille accès privilégiés, clés, API, comportements anormaux et tentatives d'abus. Une compromission suspectée doit permettre la suspension ciblée d'un compte, d'une clé, d'un lot ou d' une intégration.

16. Online / Offline

En mode connecté, AP Core peut confirmer l'état courant du QR en temps réel. En mode offline, une preuve cryptographique locale peut permettre une vérification limitée lorsque le modèle de risque l' autorise. L'interface doit indiquer clairement qu'un statut récent ou une révocation peut nécessiter une resynchronisation.

17. IoT/NFC et preuve complémentaire

Une puce NFC, un capteur ou un composant IoT peut fournir une preuve supplémentaire de présence ou d'intégrité de l'objet. Ces technologies renforcent la liaison objet-numérique mais ne remplacent pas l'architecture des trois QR codes. Leurs identités et clés doivent être authentifiées et gérées séparément.

18. ERP, production et activation

Les systèmes ERP ou de production peuvent demander la création, l'affectation et l'activation de QR codes via API. Les opérations doivent être authentifiées, limitées par rôle et rapprochées des lots ou unités réellement produits. Les écarts entre volumes déclarés, codes générés et activations doivent être détectables.

19. Gestion cryptographique et révocation

Les clés de signature doivent disposer d'un cycle de vie : création sécurisée, stockage protégé, usage contrôlé, rotation, sauvegarde, révocation et remplacement. La révocation d'une clé ne doit pas effacer l'histoire ; les anciennes preuves doivent rester interprétables avec leur contexte et leur période de validité.

20. Critères d'acceptation et conclusion

L'architecture est cohérente si les trois QR codes restent distincts par fonction ; si chaque code est unique et relié au bon produit ; si la signature cryptographique protège les preuves sans exposer de clé privée ; si une copie visuelle ne suffit pas à établir l'authenticité ; si VERT, JAUNE et ROUGE restent stables ; si le cycle de vie est journalisé ; si AP Core orchestre, AP Ledger audite et AP Shield protège ; si Online/Offline, IoT/NFC et ERP restent complémentaires ; et si les clés peuvent être révoquées et renouvelées.

Authenticity Plus© transforme ainsi le QR code d'un simple motif lisible en point d'accès à une infrastructure de preuve vivante, cryptographiquement protégée et gouvernée.

La sécurité ne repose pas sur le secret du dessin QR, mais sur l'unicité, l'état, les preuves, les signatures, les droits et l'historique vérifiés par l'écosystème.

Le Chapitre 4 développera l'architecture du QR Code Dynamique documentaire et sa signature cryptographique : état vivant, autorité émettrice, révocation, versionnement et vérification.

Note de cadrage institutionnel

La signature cryptographique renforce l'authenticité et l'intégrité des preuves associées aux QR codes ; elle ne rend pas physiquement impossible la copie d'un motif imprimé. La résistance à la contrefaçon résulte de la combinaison entre unicité, état serveur ou fédéré, cycle de vie, contrôles d' usage, protection physique, signatures et mécanismes de détection. Les choix cryptographiques précis devront être validés par des spécialistes de sécurité.

VOLUME II — ARCHITECTURE TECHNOLOGIQUE ET CYBERSÉCURITÉ

CHAPITRE 4 — QR CODE DYNAMIQUE ET QR CODE DYNAMIQUE DOCUMENTAIRE

QR CODE DYNAMIQUE — IDENTIFIANT PERSISTANT — SIGNATURE CRYPTOGRAPHIQUE — ÉTAT VIVANT — AP CORE — VERSIONNEMENT — RÉVOCATION — DOCUMENTS — CYCLE DE VIE — VÉRIFICATION

1. Objet du chapitre

Ce chapitre définit le QR Code Dynamique comme un mécanisme technologique transversal de Deep Authenticity© et distingue son application spécialisée au domaine administratif : le QR Code Dynamique documentaire. Le principe central consiste à conserver un identifiant persistant tandis que les informations, droits, destinations logiques et états associés peuvent évoluer dans AP Core sans imposer la réimpression du QR.

2. QR statique et QR dynamique

Un QR statique encode directement une information ou une destination relativement fixe. Le QR Code Dynamique de Deep Authenticity© agit principalement comme un pointeur sécurisé vers une identité et un état gérés par l'infrastructure. Sa valeur ne réside donc pas dans l'image elle-même, mais dans la résolution contrôlée de l'identifiant et des preuves qui lui sont associées.

3. Identifiant persistant

Le QR Code Dynamique doit utiliser un identifiant unique, durable et non ambigu. Cet identifiant peut rester inchangé pendant le cycle de vie alors que les données présentées évoluent. Il ne doit pas contenir de clé privée ni exposer inutilement des informations sensibles. AP Core détermine les informations accessibles selon le contexte et le rôle.

4. Résolution dynamique par AP Core

Lors d'un scan, AP Core résout l'identifiant, identifie le domaine, applique les politiques de confiance et sélectionne la réponse appropriée. La destination logique peut évoluer sans modifier le QR imprimé : nouvelle version d'une fiche, changement de propriétaire, maintenance, certification, révocation ou autre événement autorisé.

5. Signature cryptographique

La signature cryptographique protège l'authenticité et l'intégrité des données ou attestations associées au QR Code Dynamique. Elle permet de vérifier qu'un état ou une preuve provient d'une autorité ou d'un système autorisé. Les clés privées restent protégées dans l'infrastructure ; le QR transporte au plus les références nécessaires à la vérification.

6. État vivant

Le caractère dynamique permet au même QR de refléter un état vivant. Une vérification peut retourner une information différente après un événement légitime sans changer l'identifiant physique. Cette capacité est fondamentale pour les documents, mais peut également enrichir les produits, actifs, services, équipements et autres objets suivis par Deep Authenticity©.

7. QR Code Dynamique dans le domaine physique

Dans le domaine physique, le principe dynamique peut enrichir les trois QR codes d'Authenticity Plus© en permettant l'évolution des informations et droits associés. Il ne fusionne pas leurs fonctions : consommateur, revendeur/professionnel et contrôle/douanes restent trois rôles distincts, avec la sémantique fondamentale VERT / JAUNE / ROUGE.

8. QR Code Dynamique documentaire

Dans le domaine administratif, le QR Code Dynamique documentaire relie le document présenté à son enregistrement ou à son autorité source. Il permet de vérifier son état actuel plutôt que de se limiter à l'apparence d'une copie. Il constitue ainsi une passerelle entre document physique ou numérique et registre vivant.

9. États documentaires

Selon le cadre applicable, le moteur documentaire peut restituer notamment : valide, expiré, suspendu, révoqué ou remplacé. Ces états sont distincts de VERT / JAUNE / ROUGE d'Authenticity Plus©. La séparation sémantique évite de confondre authenticité d'un produit et validité administrative d'un document.

10. Autorité émettrice

La validité juridique ou administrative reste déterminée par l'autorité compétente. Deep Authenticity© ne crée pas l'autorité du document ; elle rend vérifiable l'état communiqué par l'émetteur ou le registre reconnu. AP Core doit identifier l'autorité, vérifier sa signature et appliquer les règles de confiance correspondantes.

11. Versionnement et remplacement

Un document peut être corrigé, renouvelé ou remplacé. Le QR Code Dynamique permet de conserver une continuité tout en indiquant qu'une version antérieure n'est plus la version active. Les relations entre versions doivent être traçables afin de distinguer mise à jour légitime, révocation et falsification.

12. Révocation et suspension

Une révocation doit pouvoir être propagée rapidement aux vérificateurs connectés. Une suspension peut représenter un état temporaire distinct. Les événements critiques peuvent être journalisés ou ancrés dans AP Ledger. En mode offline, l'interface doit signaler lorsqu'elle ne peut pas confirmer l' état de révocation le plus récent.

13. Divulgation sélective

La vérification d'un document ne nécessite pas toujours l'exposition de son contenu complet. AP Core peut retourner uniquement les attributs nécessaires : existence, validité, autorité, catégorie ou autre information autorisée. Cette minimisation protège les données personnelles et institutionnelles tout en conservant la valeur de la preuve.

14. AP Ledger et historique

AP Ledger peut conserver des empreintes, références, horodatages et événements nécessaires à l' audit du cycle de vie. Le contenu sensible peut rester dans le registre source. Cette architecture permet de prouver qu'un état ou une version existait à un moment donné sans transformer le ledger en copie universelle des documents.

15. AP Shield et protection

AP Shield protège les services de génération, résolution, signature, administration et révocation. Les accès privilégiés, clés et API doivent être surveillés. Une compromission d'autorité ou de clé doit pouvoir entraîner suspension, rotation et mise à jour des politiques de confiance sans rendre illisibles les preuves historiques.

16. Online / Offline

En mode online, le QR Code Dynamique peut fournir l'état le plus récent disponible. En mode offline, une signature ou preuve locale peut confirmer certains éléments d'intégrité et de provenance, mais pas nécessairement une révocation récente. Le niveau de fraîcheur et la limite de la vérification doivent être explicitement indiqués.

17. API et registres administratifs

Les registres publics ou institutionnels peuvent exposer uniquement les statuts et attributs nécessaires via API sécurisées. AP Core agit comme couche d'orchestration et de politique. Les registres restent souverains, et leur indisponibilité technique doit être distinguée d'un statut invalide ou révoqué.

18. Résistance à la copie et à la falsification

Copier le QR Code Dynamique d'un document ne crée pas une nouvelle preuve valide : le scan renvoie vers l'identité et l'état du document original. Des contrôles contextuels, signatures, attributs et politiques peuvent révéler des incohérences. Le système doit néanmoins éviter de prétendre qu'un QR imprimé est physiquement incopiable.

19. Cycle de vie universel

Le modèle dynamique peut couvrir émission, activation, mise à jour, transfert, renouvellement, suspension, révocation, remplacement et archivage. Cette continuité prépare le Passeport Numérique Universel : un identifiant persistant devient le point d'accès à une histoire structurée, gouvernée et cryptographiquement vérifiable.

20. Critères d'acceptation et conclusion

L'architecture est cohérente si le QR Code Dynamique utilise un identifiant persistant ; si AP Core peut faire évoluer les informations et droits sans réimpression ; si la signature cryptographique protège les preuves ; si le domaine physique conserve les trois QR codes et VERT / JAUNE / ROUGE ; si le domaine administratif possède ses propres états documentaires ; si l'autorité émettrice reste souveraine ; si versionnement, suspension, révocation et remplacement sont traçables ; si Online/Offline exprime la fraîcheur de la preuve ; et si AP Ledger et AP Shield renforcent auditabilité et sécurité.

Le QR Code Dynamique transforme ainsi un code imprimé en interface durable vers une identité et un état vivant. Sa stabilité physique peut coexister avec l'évolution numérique du cycle de vie.

Dans le domaine documentaire, cette propriété permet de dépasser la copie figée pour vérifier directement l'état actuel reconnu par l'autorité compétente.

Le Chapitre 5 développera le Passeport Numérique Universel : architecture technique, identité persistante, événements, propriété, provenance et continuité du cycle de vie.

Note de cadrage institutionnel

Le QR Code Dynamique ne doit pas être présenté comme physiquement incopiable. Sa sécurité provient de la résolution de l'identifiant, de l'état vivant, des signatures cryptographiques, des politiques d'accès et de la vérification auprès des sources autorisées. Dans le domaine administratif, la valeur juridique du document demeure déterminée par l'autorité compétente.

VOLUME II — ARCHITECTURE TECHNOLOGIQUE ET CYBERSÉCURITÉ

CHAPITRE 5 — PASSEPORT NUMÉRIQUE UNIVERSEL : ARCHITECTURE TECHNIQUE ET CONTINUITÉ DU CYCLE DE VIE

PASSEPORT NUMÉRIQUE UNIVERSEL — IDENTITÉ PERSISTANTE — PROVENANCE — PROPRIÉTÉ — ÉVÉNEMENTS — SIGNATURE CRYPTOGRAPHIQUE — AP CORE — AP LEDGER — CYCLE DE VIE — INTEROPÉRABILITÉ

1. Objet du chapitre

Ce chapitre définit l'architecture technique du Passeport Numérique Universel de Deep Authenticity©. Le passeport constitue une continuité numérique vérifiable reliant une entité à son identité, sa provenance, ses états et les événements autorisés de son cycle de vie. Il peut s'appliquer, selon des mécanismes propres, aux domaines physique, numérique et administratif.

2. Principe d'identité persistante

Le Passeport Numérique Universel repose sur une identité persistante capable de survivre aux changements d'état, de propriétaire, de localisation, de version ou de contexte. Cette identité ne doit pas être confondue avec une donnée personnelle : elle représente d'abord l'élément suivi et permet à AP Core de résoudre les preuves qui lui sont associées.

3. Passeport du domaine physique

Pour un produit physique, le passeport peut relier origine, fabricant, lot, activation, distribution, vente, propriété, maintenance, certification, rappel et fin de vie. Les trois QR codes d'Authenticity Plus© constituent les mécanismes fondamentaux d'accès et d'authentification selon les rôles consommateur, revendeur/professionnel et contrôle/douanes.

4. Passeport du domaine numérique

Pour un contenu, média, logiciel ou actif intellectuel, le passeport peut relier créateur ou émetteur, empreinte, signature cryptographique native, versions, licences et transformations autorisées. Il établit une chaîne de provenance technique sans prétendre certifier automatiquement la véracité intellectuelle ou factuelle du contenu.

5. Passeport du domaine administratif

Pour un document ou titre administratif, le passeport peut relier autorité émettrice, date d'émission, version, état, renouvellement, suspension, révocation ou remplacement. Le QR Code Dynamique documentaire permet d'accéder à cet état vivant tout en laissant la validité juridique sous l'autorité de l'institution compétente.

6. Modèle d'événements

Le passeport est construit comme une suite d'événements structurés plutôt que comme une fiche figée. Chaque événement possède un type, une source, un horodatage, un niveau d'assurance et des

droits. AP Core valide la cohérence de la transition avant d'intégrer l'événement dans l'histoire exploitable de l'entité.

7. Provenance

La provenance décrit d'où vient l'entité et comment son histoire peut être reliée à des sources vérifiables. Elle peut s'appuyer sur signatures, attestations, registres, ERP, AP Ledger ou autres systèmes reconnus. Une provenance inconnue ou incomplète doit être distinguée d'une provenance explicitement invalide.

8. Signature cryptographique

Les événements et attestations critiques peuvent être signés cryptographiquement afin de protéger leur authenticité et leur intégrité. La signature permet d'identifier l'autorité ou le système ayant produit la preuve. Le passeport conserve les références nécessaires à la vérification sans exposer les clés privées ni multiplier les données sensibles.

9. Propriété et transfert

Lorsqu'un cas d'usage prévoit la propriété, le passeport peut enregistrer un transfert numérique sécurisé entre acteurs autorisés. Le transfert doit vérifier l'identité ou l'habilitation nécessaire, empêcher les doubles transferts incohérents et conserver la chronologie. La preuve numérique complète les règles juridiques de propriété applicables sans s'y substituer.

10. Cycle commercial et seconde main

Après la première vente, le passeport peut continuer à accompagner le produit dans la seconde main. Les transferts autorisés permettent de maintenir une continuité entre produit authentique et détenteur légitime lorsque le cadre le permet. Les données des anciens propriétaires doivent rester protégées et ne pas être exposées au nouvel acquéreur sans nécessité.

11. Maintenance, réparation et rappel

Les interventions de maintenance, réparations, révisions ou rappels peuvent devenir des événements du passeport lorsqu'elles sont réalisées par des acteurs habilités. Cette continuité améliore la compréhension de l'état de l'actif et permet aux producteurs ou autorités de cibler plus précisément les unités concernées par une action corrective.

12. Certifications et AP-Certified™

Les certifications peuvent être reliées au passeport avec leur organisme émetteur, portée, période de validité et statut. AP-Certified™ peut constituer une couche de certification de l'écosystème, mais chaque certification doit rester interprétée selon sa portée réelle. Authenticité d'un certificat et conformité globale d'un produit sont deux notions distinctes.

13. AP Core et orchestration

AP Core constitue le moteur de résolution du passeport. Il détermine quelles informations peuvent être lues ou modifiées, quelles preuves sont requises et quelles transitions sont autorisées. Il permet de présenter des vues différentes du même passeport selon le rôle sans dupliquer nécessairement l' identité de l'entité.

14. AP Ledger et auditabilité

AP Ledger peut ancrer les empreintes et événements critiques nécessaires à l'audit. Le passeport complet n'a pas besoin d'être stocké intégralement dans le ledger. Une architecture de références

permet de conserver les données sensibles dans leurs systèmes appropriés tout en prouvant l'existence et la chronologie d'événements essentiels.

15. AP Cloud et disponibilité

AP Cloud peut fournir stockage, calcul, distribution et synchronisation du passeport selon le modèle de déploiement. Les architectures souveraines ou hybrides doivent rester possibles. Les mécanismes de cache et réplication doivent préserver la disponibilité tout en indiquant la fraîcheur des informations lorsque la source principale est momentanément inaccessible.

16. AP Shield et protection du passeport

AP Shield protège création, lecture sensible, modification, transfert et révocation. Les opérations critiques exigent authentification et journalisation adaptées. Les anomalies de comportement, tentatives de modification non autorisée ou compromissions de compte doivent pouvoir déclencher des mesures ciblées sans altérer l'histoire légitime du passeport.

17. Online / Offline et synchronisation

Certaines informations du passeport peuvent être vérifiées offline grâce à des preuves cryptographiques locales lorsque le risque le permet. Les changements récents peuvent toutefois nécessiter une connexion. Après reconnexion, AP Core synchronise les événements et résout les conflits afin de préserver une chronologie cohérente.

18. Interopérabilité API, ERP, IoT et NFC

Le passeport peut recevoir des événements depuis ERP, API, dispositifs IoT ou NFC et fournir des informations aux systèmes autorisés. Chaque source doit être authentifiée et son niveau de confiance connu. L'intégration technique ne signifie pas que toutes les données externes deviennent automatiquement des preuves fiables.

19. Passeport, Jumeau Numérique et échelle universelle

Le Passeport Numérique Universel fournit l'histoire vérifiable d'une entité ; le Jumeau Numérique utilise cette histoire et d'autres données pour représenter son état et ses relations. À grande échelle, l'agrégation contrôlée des passeports peut contribuer aux représentations sectorielles, territoriales et nationales sans exposer inutilement les données unitaires.

20. Critères d'acceptation et conclusion

Le Passeport Numérique Universel est cohérent si son identité reste persistante ; si les trois domaines conservent leurs mécanismes propres ; si les trois QR codes d'Authenticity Plus© restent fondamentaux pour le physique ; si le QR Code Dynamique documentaire reste lié à l'autorité administrative ; si les événements ont provenance, horodatage et niveau d'assurance ; si les signatures cryptographiques protègent les preuves ; si propriété, maintenance et certifications sont gouvernées ; si AP Core orchestre, AP Ledger audite, AP Cloud distribue et AP Shield protège ; et si Online/Offline, API, ERP, IoT et NFC restent interopérables.

Le Passeport Numérique Universel transforme l'identité numérique d'un élément en continuité de preuve à travers le temps.

Il constitue le lien technique entre authentification ponctuelle et histoire vérifiable, puis entre cette histoire et les Jumeaux Numériques de Deep Authenticity©.

Le Chapitre 6 développera AP Ledger : registre de preuves, événements, horodatage, intégrité et auditabilité.

Note de cadrage institutionnel

Le Passeport Numérique Universel constitue une architecture de continuité de preuve. Son contenu et ses effets juridiques varient selon le domaine, le secteur et la juridiction. Les événements provenant de systèmes externes doivent être qualifiés selon leur niveau de confiance, et les données personnelles ou sensibles doivent être minimisées et protégées.

VOLUME II — ARCHITECTURE TECHNOLOGIQUE ET CYBERSÉCURITÉ

CHAPITRE 6 — AP LEDGER : REGISTRE DE PREUVES, ÉVÉNEMENTS, INTÉGRITÉ ET AUDITABILITÉ

AP LEDGER — PREUVES — ÉVÉNEMENTS — HORODATAGE — EMPREINTES — SIGNATURE CRYPTOGRAPHIQUE — INTÉGRITÉ — AUDIT — TRAÇABILITÉ — SOUVERAINETÉ

1. Objet du chapitre

Ce chapitre définit AP Ledger comme la couche de registre de preuves et d'auditabilité de Deep Authenticity©. Sa fonction n'est pas de devenir une base universelle contenant toutes les données, mais de conserver ou d'ancrer les éléments nécessaires pour démontrer l'existence, l'intégrité, la chronologie et l'origine d'événements critiques.

2. Principe du registre de preuve

AP Ledger organise une mémoire vérifiable des événements qui méritent une conservation renforcée. Il peut enregistrer des références, empreintes cryptographiques, signatures, horodatages et métadonnées minimales. Les données opérationnelles volumineuses ou sensibles peuvent rester dans AP Cloud, ERP, registres souverains ou autres systèmes sources.

3. Séparation AP Core / AP Ledger

AP Core applique la logique métier, les droits, les statuts et les politiques de confiance. AP Ledger conserve la preuve et la chronologie de certains événements. Cette séparation est fondamentale : le ledger ne doit pas devenir le moteur universel de décision, et AP Core ne doit pas pouvoir modifier silencieusement une preuve historique ancrée.

4. Modèle d'événement

Un événement peut comporter un identifiant, un type, une source, un horodatage, une référence à l'entité concernée, une empreinte, une signature et un niveau d'assurance. Le schéma doit être versionné afin que les preuves anciennes restent interprétables lorsque l'architecture évolue.

5. Empreintes cryptographiques

Une empreinte cryptographique permet de représenter de manière compacte l'état d'une donnée ou d'un document. AP Ledger peut conserver cette empreinte plutôt que le contenu lui-même. Une vérification ultérieure recalcule l'empreinte afin de détecter une modification, sans exposer nécessairement l'information originale.

6. Signature cryptographique

Les événements critiques peuvent être signés par l'acteur, le service ou l'autorité qui les émet. La signature permet de vérifier origine et intégrité. AP Ledger doit conserver les références nécessaires à la validation de la signature, y compris le contexte de clé et de certificat applicable à la date de l' événement.

7. Horodatage et chronologie

L'horodatage fournit un repère temporel à la preuve. Les sources de temps et niveaux de confiance doivent être définis selon la criticité. AP Ledger doit distinguer l'heure déclarée par une source, l'heure de réception et, lorsque nécessaire, un horodatage de confiance afin d'éviter une fausse précision.

8. Événements des trois QR codes

Les événements importants liés aux trois QR codes d'Authenticity Plus© peuvent être ancrés dans AP Ledger : émission, activation, première vérification, vente, transfert, contrôle, suspension ou révocation. Le ledger renforce l'auditabilité sans modifier les rôles consommateur, revendeur/professionnel et contrôle/douanes.

9. VERT / JAUNE / ROUGE et preuve historique

Lorsqu'un événement entraîne une transition de statut, AP Ledger peut conserver la preuve de la transition. VERT, JAUNE et ROUGE restent déterminés par AP Core selon les règles d'Authenticity Plus©. Le ledger permet ensuite de démontrer quand et sur quelle base un changement d'état a été enregistré.

10. QR Code Dynamique et documents

Les événements de création, versionnement, suspension, révocation ou remplacement d'un document peuvent être ancrés dans AP Ledger. Le QR Code Dynamique documentaire interroge l'état vivant auprès de l'autorité compétente ; le ledger apporte une mémoire vérifiable des changements importants sans remplacer le registre administratif source.

11. Passeport Numérique Universel

AP Ledger renforce la continuité du Passeport Numérique Universel en ancrant certains événements critiques de son cycle de vie. Le passeport peut conserver une histoire riche dans des systèmes adaptés, tandis que le ledger fournit des points de preuve indépendants permettant de vérifier que certaines étapes n'ont pas été réécrites silencieusement.

12. Modèle permissionné, distribué ou hybride

AP Ledger n'impose pas une technologie unique. Selon le secteur et la souveraineté recherchée, il peut être implémenté sous forme de registre append-only, infrastructure permissionnée, système distribué ou architecture hybride. Le choix doit être guidé par sécurité, performance, gouvernance, coût et exigences juridiques.

13. AP Ledger et blockchain

Une blockchain peut être utilisée pour certains cas, mais AP Ledger ne doit pas être défini comme synonyme de blockchain. L'objectif est l'auditabilité vérifiable. Une architecture plus simple peut être préférable lorsque la gouvernance est centralisée et fiable ; une architecture distribuée peut être justifiée lorsque plusieurs autorités doivent partager la confiance.

14. Confidentialité et minimisation

Le caractère durable d'un ledger exige une forte minimisation. Les données personnelles, secrets industriels et documents complets ne doivent pas y être inscrits sans nécessité démontrée. Les empreintes, références pseudonymisées et preuves sélectives permettent de préserver l'auditabilité tout en réduisant l'exposition.

15. Immutabilité et correction

L'immutabilité ne signifie pas qu'une erreur devient vraie. Lorsqu'une donnée est incorrecte, une correction peut être ajoutée comme nouvel événement qui référence l'ancien, sans effacer la trace historique lorsque la loi et la gouvernance l'exigent. L'état courant est déterminé par AP Core à partir de la séquence d'événements valides.

16. Révocation et cycle de vie des clés

Une signature historique doit rester interprétable même après expiration ou révocation d'une clé. AP Ledger conserve le contexte nécessaire pour savoir si la clé était valide au moment pertinent. Rotation et révocation doivent être journalisées afin de distinguer preuve historiquement valide et nouvelle utilisation interdite.

17. AP Shield et sécurité du registre

AP Shield protège les interfaces d'écriture, lecture administrative, réplication et maintenance d'AP Ledger. Les droits d'écriture doivent être particulièrement restreints. Les tentatives d'altération, divergences de réplication, accès anormaux ou compromissions de clés doivent déclencher des mécanismes de détection et de réponse.

18. Performance, archivage et montée en charge

Tous les événements de Deep Authenticity© ne doivent pas nécessairement être écrits dans AP Ledger. Des politiques de sélection, regroupement ou ancrage périodique peuvent réduire coûts et latence. L'architecture doit prévoir indexation, archivage, vérification et conservation à long terme sans sacrifier la capacité d'audit.

19. Fédération et souveraineté

Des ledgers nationaux, sectoriels ou institutionnels peuvent rester sous contrôle local et échanger des preuves ou ancrages selon des protocoles communs. Cette fédération permet aux Corridors de Confiance de vérifier certaines chronologies sans imposer un registre mondial unique ni exposer les données souveraines.

20. Critères d'acceptation et conclusion

AP Ledger est cohérent s'il conserve des preuves plutôt que toutes les données ; si AP Core reste le moteur de décision ; si empreintes, signatures et horodatages sont vérifiables ; si les événements critiques des trois QR codes, du QR Code Dynamique et du Passeport Numérique Universel peuvent être audités ; si la technologie de registre reste adaptable ; si blockchain et ledger ne sont pas confondus ; si confidentialité et correction sont prévues ; si le cycle des clés reste interprétable ; si AP Shield protège les écritures ; et si fédération et souveraineté restent possibles.

AP Ledger constitue ainsi la mémoire probante de Deep Authenticity© : une couche destinée à rendre les événements importants vérifiables dans le temps sans transformer la plateforme en dépôt central de toutes les informations.

Sa valeur réside moins dans une technologie particulière que dans la capacité à préserver intégrité, provenance, chronologie et auditabilité.

Le Chapitre 7 développera AP Cloud : infrastructure distribuée, stockage, calcul, synchronisation, souveraineté et montée en charge.

Note de cadrage institutionnel

AP Ledger désigne une fonction architecturale de registre de preuves et non l'obligation d'utiliser une blockchain publique. Le choix d'une technologie de registre doit résulter d'une analyse des menaces, de la gouvernance, des performances, des coûts, de la confidentialité, de la souveraineté et des exigences réglementaires.

VOLUME II — ARCHITECTURE TECHNOLOGIQUE ET CYBERSÉCURITÉ

CHAPITRE 7 — AP CLOUD : INFRASTRUCTURE DISTRIBUÉE, STOCKAGE, CALCUL ET SOUVERAINETÉ

AP CLOUD — INFRASTRUCTURE — DISTRIBUTION — STOCKAGE — CALCUL — SYNCHRONISATION — SOUVERAINETÉ — HAUTE DISPONIBILITÉ — AP CORE — AP SHIELD — MONTÉE EN CHARGE

1. Objet du chapitre

Ce chapitre définit AP Cloud comme la couche d'infrastructure distribuée de Deep Authenticity©. AP Cloud fournit les capacités de calcul, stockage, messagerie, distribution, synchronisation et supervision nécessaires à AP Core et aux modules, tout en permettant des modèles publics, privés, hybrides ou souverains selon les exigences institutionnelles.

2. Principe : un cloud, plusieurs modèles de déploiement

AP Cloud ne désigne pas l'obligation d'utiliser un fournisseur mondial unique. Il définit une architecture de services pouvant être déployée dans plusieurs environnements. Cette abstraction permet à Deep Authenticity© de conserver une logique commune tout en adaptant hébergement, localisation et exploitation aux contraintes de chaque acteur.

3. Architecture distribuée

Les services peuvent être répartis entre plusieurs zones, centres de données ou infrastructures souveraines. La distribution vise disponibilité, proximité, résilience et maîtrise des données. Les composants doivent communiquer par interfaces authentifiées et éviter les dépendances implicites qui transformeraient une panne locale en panne globale.

4. Relation AP Cloud / AP Core

AP Core orchestre identités, statuts, preuves et politiques ; AP Cloud lui fournit les ressources d'exécution. Cette séparation permet de déplacer ou répliquer des services sans modifier la doctrine de confiance. Les données et fonctions critiques doivent conserver des contrats techniques stables indépendamment de leur emplacement physique.

5. Stockage selon la nature des données

Les données ne possèdent pas toutes les mêmes exigences. Métadonnées de produit, documents, journaux, preuves, modèles IA et données institutionnelles peuvent utiliser des stockages différents. AP Cloud doit appliquer classification, chiffrement, durée de conservation, réplication et contrôle d'accès selon la sensibilité et la finalité.

6. Données des trois QR codes

Les informations liées aux trois QR codes d'Authenticity Plus© doivent être structurées de manière à préserver leurs rôles distincts : consommateur, revendeur/professionnel et contrôle/douanes. AP Cloud assure leur disponibilité technique, tandis qu'AP Core applique les droits et maintient la sémantique VERT / JAUNE / ROUGE.

7. QR Code Dynamique et données vivantes

Le QR Code Dynamique dépend de la capacité à résoudre rapidement un identifiant vers son état courant. AP Cloud peut héberger ou répliquer les données nécessaires à cette résolution. Les mécanismes de cache doivent respecter la fraîcheur, notamment pour les révocations, suspensions et changements de droits.

8. Passeport Numérique Universel

AP Cloud peut stocker les vues, événements et objets nécessaires au Passeport Numérique Universel lorsque leur hébergement dans le cloud est autorisé. Les sources souveraines ou externes peuvent rester à distance ; le passeport utilise alors des références et API. L'architecture évite de dupliquer sans nécessité toutes les données sources.

9. Calcul et services applicatifs

AP Cloud fournit les ressources de calcul pour résolution de preuves, traitement d'événements, API, génération de vues, analyses et autres services. Les charges peuvent être isolées selon leur criticité. Les traitements lourds d'IA ou de simulation ne doivent pas compromettre les fonctions essentielles de vérification.

10. Synchronisation et messagerie événementielle

Les événements provenant d'ERP, applications, IoT, AP Ledger ou registres peuvent être transmis par des mécanismes de messagerie et de files. La synchronisation doit gérer répétition, ordre, doublons et reprises. Les opérations critiques doivent pouvoir être rejouées de façon contrôlée sans produire de transitions incohérentes.

11. Haute disponibilité

Les services critiques doivent disposer d'objectifs de disponibilité adaptés à leur usage. Réplication, bascule, équilibrage de charge et redondance permettent de limiter les interruptions. Une haute disponibilité réelle nécessite également des tests réguliers de bascule et non la seule présence théorique de ressources secondaires.

12. Sauvegarde et restauration

AP Cloud doit distinguer réplication et sauvegarde. Une erreur ou attaque peut être répliquée ; des sauvegardes protégées et restaurables restent donc nécessaires. Les procédures doivent définir fréquence, rétention, chiffrement, isolement et tests de restauration selon la criticité des données.

13. AP Shield et sécurité du cloud

AP Shield protège identités techniques, secrets, API, réseaux, charges de travail, journaux et interfaces administratives d'AP Cloud. Les accès privilégiés doivent être particulièrement contrôlés. La segmentation limite les mouvements latéraux et permet d'isoler un service compromis sans exposer l'ensemble de l'écosystème.

14. Chiffrement et gestion des clés

Les données sensibles doivent pouvoir être chiffrées en transit et au repos selon les exigences applicables. Les clés doivent être gérées séparément des données, avec rotation, contrôle d'accès et journalisation. Pour certains déploiements souverains, les autorités peuvent exiger la maîtrise locale des clés de chiffrement.

15. Online / Offline et périphérie

AP Cloud constitue la couche connectée de référence, mais Deep Authenticity© doit pouvoir fonctionner en mode dégradé. Des caches ou services de périphérie peuvent conserver certaines preuves vérifiables. Après reconnexion, la synchronisation réconcilie les événements et actualise les états dont la fraîcheur ne pouvait être garantie offline.

16. ERP, IoT/NFC et connectivité

Les intégrations ERP et dispositifs IoT/NFC peuvent transmettre des événements à AP Cloud via passerelles sécurisées. Les flux doivent être authentifiés, limités et observables. Une indisponibilité d'un connecteur ne doit pas être interprétée comme une preuve négative concernant le produit ou l'actif.

17. Montée en charge

La croissance du nombre de produits, documents, scans et événements exige une capacité d'élasticité. Les services doivent pouvoir être répliqués ou partitionnés selon la charge. Les tests de performance doivent couvrir les pics réels, notamment campagnes de contrôle, rappels, événements publics ou déploiements nationaux.

18. Observabilité et exploitation

Métriques, journaux, traces et alertes doivent permettre de comprendre disponibilité, latence, erreurs, saturation et dépendances. L'observabilité doit être conçue avec minimisation des données. Les équipes d'exploitation doivent disposer de procédures claires d'escalade, diagnostic et retour à l'état normal.

19. Souveraineté, localisation et fédération

AP Cloud doit permettre à un État, une institution ou une entreprise de conserver certaines données et services dans des environnements qu'ilsmaîtrisent. Des instances fédérées peuvent échanger des preuves sans transférer toutes leurs bases. Cette architecture soutient les Corridors de Confiance et la souveraineté numérique.

20. Critères d'acceptation et conclusion

AP Cloud est cohérent s'il supporte plusieurs modèles de déploiement ; si AP Core reste indépendant de l'emplacement d'exécution ; si stockage et calcul sont adaptés à la sensibilité ; si les trois QR codes, le QR Code Dynamique et le Passeport Numérique Universel restent disponibles sans perdre leurs règles propres ; si synchronisation, haute disponibilité, sauvegarde et restauration sont testées ; si AP Shield et la cryptographie protègent l'infrastructure ; si Online/Offline, ERP et IoT/NFC sont intégrés ; et si montée en charge, observabilité, souveraineté et fédération sont prévues.

AP Cloud constitue ainsi la couche d'exécution distribuée de Deep Authenticity© : il rend les services disponibles à grande échelle sans imposer que la confiance ou les données soient centralisées dans une infrastructure unique.

Le cloud devient un moyen de distribution et de résilience, non un substitut à la souveraineté.

Le Chapitre 8 développera AP Shield : architecture globale de protection, Zero Trust, identités, secrets, surveillance, détection et réponse aux incidents.

Note de cadrage institutionnel

AP Cloud désigne une architecture logique d'infrastructure et de services. Les fournisseurs, technologies, régions d'hébergement et niveaux de service devront être sélectionnés selon sécurité, souveraineté, localisation des données, performance, coût, résilience et obligations réglementaires. La matrice institutionnelle du Volume II reste inchangée.

VOLUME II — ARCHITECTURE TECHNOLOGIQUE ET CYBERSÉCURITÉ

CHAPITRE 8 — AP SHIELD : ARCHITECTURE GLOBALE DE PROTECTION ET CYBERSÉCURITÉ

AP SHIELD — ZERO TRUST — IDENTITÉS — ACCÈS — CLÉS — SECRETS — DÉTECTION — RÉPONSE AUX INCIDENTS — SEGMENTATION — SUPERVISION — CYBERSÉCURITÉ

1. Objet du chapitre

Ce chapitre définit AP Shield comme la couche transversale de protection de Deep Authenticity©. AP Shield coordonne les mécanismes de cybersécurité qui protègent AP Core, AP Ledger, AP Cloud, les API, les trois QR codes d'Authenticity Plus©, le QR Code Dynamique, les signatures cryptographiques, les ERP, les dispositifs IoT/NFC et les interfaces institutionnelles.

2. Principe de défense en profondeur

La sécurité ne repose jamais sur un contrôle unique. AP Shield combine identité, autorisation, segmentation, chiffrement, journalisation, surveillance, détection et réponse. Une défaillance locale doit être contenue par d'autres couches afin d'empêcher qu'elle compromette l'ensemble de l'infrastructure.

3. Architecture Zero Trust

AP Shield applique une logique Zero Trust : aucune identité, machine, application ou connexion n'est considérée comme fiable uniquement parce qu'elle se trouve dans un réseau interne. Chaque accès doit être authentifié, autorisé et contextualisé selon le niveau de risque et le principe du moindre privilège.

4. Identités et accès

Les comptes consommateurs, professionnels, autorités, administrateurs, services et machines possèdent des niveaux d'assurance différents. AP Shield protège authentification, sessions, privilèges

et élévations de droits. Les comptes sensibles peuvent exiger des facteurs renforcés et des contrôles supplémentaires.

5. Protection des trois QR codes

AP Shield protège les services de génération, affectation, activation et résolution des trois QR codes d'Authenticity Plus©. Une copie du motif ne doit pas donner accès à des fonctions privilégiées. Les opérations consommateur, revendeur/professionnel et contrôle/douanes restent séparées et gouvernées par AP Core.

6. Protection du QR Code Dynamique

Le QR Code Dynamique dépend d'un service de résolution vivant. AP Shield protège les redirections, règles, statuts et interfaces d'administration afin d'empêcher un détournement de destination ou une modification non autorisée. Les changements sensibles doivent être authentifiés, journalisés et réversibles selon la gouvernance.

7. Clés et secrets cryptographiques

Clés privées, secrets d'API, certificats et jetons doivent être stockés dans des environnements protégés, séparés du code applicatif et des QR visibles. Leur cycle de vie couvre création, distribution, usage, rotation, sauvegarde, révocation et destruction. Les accès aux clés critiques doivent être fortement restreints.

8. Signature cryptographique

AP Shield protège l'infrastructure de signature des preuves et la signature cryptographique native des contenus. Il doit empêcher l'utilisation non autorisée d'une clé de signature et permettre de suspendre rapidement une clé compromise. Les signatures historiques restent interprétables avec leur contexte de validité.

9. Sécurité des API

Les API constituent une surface d'exposition majeure. AP Shield impose authentification, autorisation, validation des entrées, quotas, limitation de débit, journalisation et protections contre les abus. Les versions obsolètes doivent être retirées selon un processus contrôlé afin de réduire les surfaces d'attaque persistantes.

10. Segmentation des infrastructures

Les composants critiques doivent être segmentés selon leur fonction et leur sensibilité. AP Ledger, services de clés, administration, traitements IA, connecteurs ERP et passerelles IoT ne doivent pas partager implicitement le même niveau de confiance. La segmentation limite les mouvements latéraux en cas de compromission.

11. Surveillance et observabilité de sécurité

AP Shield collecte des signaux de sécurité provenant des applications, API, infrastructures, identités et dispositifs. Les journaux doivent être corrélés sans collecter inutilement des données personnelles. Les événements critiques doivent être suffisamment contextualisés pour permettre investigation et reconstruction chronologique.

12. Détection des anomalies

Des règles et modèles analytiques peuvent détecter scans anormaux, volumes inhabituels, accès impossibles, modifications sensibles ou comportements de comptes. Les alertes IA restent

probabilistes et doivent être qualifiées avant action. La détection complète les preuves déterministes sans modifier la signification VERT / JAUNE / ROUGE.

13. Réponse aux incidents

AP Shield doit permettre identification, confinement, éradication, restauration et retour d'expérience. Une réponse ciblée peut suspendre un compte, une clé, une API, un lot ou une instance compromise. Les procédures doivent préserver les preuves nécessaires à l'investigation et éviter une destruction involontaire des traces.

14. Gestion des vulnérabilités

Les logiciels, bibliothèques, systèmes et équipements doivent être inventoriés, analysés et corrigés selon leur criticité. Les correctifs urgents doivent pouvoir être déployés sans attendre les cycles ordinaires. Les dépendances tierces et chaînes d'approvisionnement logicielles font partie du périmètre de sécurité.

15. Sécurité AP Cloud et AP Ledger

AP Shield protège AP Cloud contre compromission des charges, mauvaises configurations et accès privilégiés abusifs. Pour AP Ledger, les droits d'écriture, mécanismes de réplication et preuves d' intégrité nécessitent une protection renforcée. Les sauvegardes et systèmes de reprise doivent également être protégés contre l'altération.

16. ERP, IoT et NFC

Les ERP et dispositifs IoT/NFC sont des sources externes potentiellement exposées. Les passerelles doivent authentifier les systèmes, limiter leurs droits et valider les données reçues. Un dispositif compromis ne doit pas pouvoir injecter automatiquement une preuve de confiance élevée dans le Passeport Numérique Universel.

17. Online / Offline et sécurité dégradée

Le mode offline ne doit pas contourner les contrôles essentiels. Les preuves locales doivent être signées, limitées dans le temps et adaptées au risque. À la reconnexion, AP Shield et AP Core vérifient la cohérence des événements, détectent les manipulations et appliquent les révocations ou changements intervenus pendant l'interruption.

18. Continuité et cyber-résilience

La cybersécurité inclut la capacité à continuer ou restaurer les fonctions essentielles. AP Shield doit être coordonné avec redondance, sauvegardes isolées, reprise après sinistre et exercices de crise. Les scénarios doivent inclure compromission de clés, indisponibilité cloud, attaque sur API et défaillance d'un partenaire.

19. Gouvernance et souveraineté cyber

Les politiques de sécurité doivent définir responsabilités, habilitations, audits, gestion des exceptions et contrôle des fournisseurs. Les États et institutions peuvent imposer des exigences de localisation, de maîtrise des clés ou d'exploitation souveraine. AP Shield doit pouvoir appliquer ces politiques dans une architecture fédérée.

20. Critères d'acceptation et conclusion

AP Shield est cohérent si la défense en profondeur et Zero Trust sont appliqués ; si identités, clés et secrets sont protégés ; si les trois QR codes et le QR Code Dynamique disposent de contrôles

adaptés ; si signatures, API et infrastructures sont surveillées ; si segmentation et moindre privilège limitent les mouvements latéraux ; si détection et réponse aux incidents sont opérationnelles ; si vulnérabilités, ERP, IoT/NFC et Online/Offline sont couverts ; et si continuité, audit et souveraineté cyber sont intégrés.

AP Shield constitue ainsi le système immunitaire technologique de Deep Authenticity© : il observe, limite, détecte, contient et contribue à restaurer la confiance lorsque l'infrastructure est confrontée à une menace.

La cybersécurité devient une propriété transversale de l'architecture et non une couche ajoutée après sa construction.

Le Chapitre 9 développera les API : interopérabilité, authentification, gouvernance, intégration des systèmes et échanges sécurisés de preuves.

Note de cadrage institutionnel

AP Shield désigne l'architecture transversale de cybersécurité de Deep Authenticity©. Sa mise en œuvre devra être fondée sur une analyse de risques, des tests indépendants, des procédures opérationnelles et les normes applicables. Aucun mécanisme de sécurité ne doit être présenté comme garantissant une invulnérabilité absolue.

VOLUME II — ARCHITECTURE TECHNOLOGIQUE ET CYBERSÉCURITÉ

CHAPITRE 9 — API : INTEROPÉRABILITÉ, GOUVERNANCE ET ÉCHANGES SÉCURISÉS DE PREUVES

API — INTEROPÉRABILITÉ — AP CORE — AUTHENTIFICATION — AUTORISATION — PREUVES — ERP — IOT/NFC — REGISTRES — VERSIONNEMENT — CYBERSÉCURITÉ

1. Objet du chapitre

Ce chapitre définit l'architecture API de Deep Authenticity© comme la couche d'interopérabilité permettant aux applications, ERP, registres, institutions, partenaires, équipements et modules d' échanger des preuves et événements avec AP Core. L'API n'est pas une simple interface technique : elle constitue une frontière de confiance gouvernée, authentifiée, versionnée et surveillée.

2. Principe d'interopérabilité

Deep Authenticity© doit pouvoir coopérer avec des systèmes hétérogènes sans exiger leur remplacement. Les API fournissent des contrats d'échange stables entre les composants. L' interopérabilité vise à transmettre les informations et preuves nécessaires à une opération déterminée, et non à ouvrir indistinctement les bases de données des participants.

3. AP Core comme point d'orchestration

AP Core reçoit les requêtes, identifie le demandeur, applique les politiques de confiance, consulte les sources autorisées et construit la réponse. Les API exposent des capacités contrôlées d'AP Core sans

permettre aux systèmes externes de contourner les règles de statut, d'identité, de preuve ou d' autorisation.

4. Architecture des interfaces

Les interfaces peuvent être organisées par domaines et fonctions : authentification produit, passeport, documents, événements, propriété, certification, contrôle, intégration industrielle ou administration. Cette séparation facilite la sécurité, la documentation, le versionnement et l'attribution de privilèges minimaux.

5. Authentification des systèmes

Tout système appelant une API sensible doit être authentifié par un mécanisme adapté au niveau de risque. Identités applicatives, certificats, jetons ou signatures de requêtes peuvent être utilisés. Les secrets statiques partagés doivent être limités et protégés ; l'identité technique doit être révocable et traçable.

6. Autorisation et moindre privilège

Après authentification, AP Core détermine précisément les opérations permises. Un ERP de producteur, une application revendeur et un système douanier ne disposent pas des mêmes droits. Les autorisations doivent être limitées par fonction, ressource, contexte et durée lorsque nécessaire.

7. API des trois QR codes

Les services liés aux trois QR codes d'Authenticity Plus© doivent conserver leurs fonctions distinctes : consommateur, revendeur/professionnel et contrôle/douanes. Une intégration API ne doit jamais permettre de fusionner silencieusement ces rôles. La sémantique VERT, JAUNE et ROUGE reste gouvernée par AP Core.

8. API du QR Code Dynamique

Les API du QR Code Dynamique permettent de résoudre l'identifiant persistant, récupérer l'état autorisé et appliquer les changements légitimes de cycle de vie. Dans le domaine documentaire, elles peuvent interroger l'autorité source pour connaître validité, expiration, suspension, révocation ou remplacement.

9. API du Passeport Numérique Universel

Le Passeport Numérique Universel peut exposer des vues différentes selon le rôle : provenance, statut, propriété, maintenance, certification ou événements autorisés. Les API doivent permettre une divulgation sélective afin que l'interopérabilité ne conduise pas à l'exposition de l'histoire complète lorsqu'elle n'est pas nécessaire.

10. Échanges de preuves cryptographiques

Une API peut transmettre signatures, empreintes, attestations et références nécessaires à la vérification. Le destinataire doit pouvoir distinguer la donnée déclarée de la preuve cryptographique qui la protège. Les clés privées ne transitent jamais dans les échanges ; seules les informations nécessaires à la validation sont exposées.

11. Intégration ERP

Les ERP peuvent créer ou transmettre des événements de production, lot, activation, expédition, vente, maintenance ou stock. Les connecteurs doivent valider schémas, identités et droits avant acceptation.

Deep Authenticity© ajoute une couche de preuve sans imposer le remplacement des processus de gestion existants.

12. IoT, NFC et passerelles

Les dispositifs IoT/NFC peuvent communiquer par passerelles spécialisées plutôt que directement avec les services centraux. La passerelle authentifie les dispositifs, contrôle les volumes et normalise les événements. Les données de capteur doivent conserver leur source et leur niveau de confiance avant intégration au Passeport Numérique Universel.

13. Registres publics et institutionnels

Les registres administratifs, douaniers ou sectoriels peuvent exposer uniquement les statuts nécessaires. AP Core doit distinguer une réponse négative, une donnée absente et une source momentanément indisponible. La souveraineté du registre source est préservée : l'API permet la vérification sans exiger la réplication complète.

14. Versionnement des API

Les contrats d'API évoluent avec le système. Chaque version importante doit être identifiée, documentée et maintenue pendant une période de transition adaptée. Les changements incompatibles ne doivent pas casser silencieusement les intégrations existantes. Les politiques de retrait doivent être annoncées et observables.

15. Validation, erreurs et idempotence

Les requêtes doivent être validées avant traitement. Les réponses d'erreur doivent distinguer authentification, autorisation, format, conflit, indisponibilité et résultat métier sans divulguer d' informations exploitables par un attaquant. Les opérations critiques doivent utiliser des mécanismes d'idempotence pour éviter les doubles événements lors d'une reprise.

16. Protection contre les abus

Les API doivent disposer de limites de débit, quotas, détection d'automatisation abusive et protections contre les entrées malveillantes. Les interfaces publiques et institutionnelles peuvent avoir des profils de risque différents. AP Shield surveille les anomalies et peut ralentir, bloquer ou isoler une identité technique compromise.

17. Journalisation et auditabilité

Les appels sensibles doivent produire des traces permettant d'identifier système, opération, résultat et contexte pertinent. La journalisation doit rester proportionnée et protéger les données personnelles ou commerciales. Les événements critiques peuvent être ancrés dans AP Ledger lorsque leur auditabilité renforcée est nécessaire.

18. Online / Offline et synchronisation

Les API sont principalement une capacité connectée, mais les applications peuvent conserver localement des opérations autorisées en mode offline. Lors de la reconnexion, les événements sont transmis avec identifiants de déduplication et contexte temporel. AP Core vérifie leur cohérence avant de modifier l'état courant.

19. Gouvernance et Corridors de Confiance

Dans un Corridor de Confiance, les API deviennent les frontières techniques entre systèmes souverains. Les participants doivent convenir des formats, autorités reconnues, niveaux d'assurance,

responsabilités, politiques de révocation et versions compatibles. La gouvernance contractuelle et institutionnelle accompagne donc la spécification technique.

20. Critères d'acceptation et conclusion

L'architecture API est cohérente si les systèmes externes sont authentifiés et autorisés selon le moindre privilège ; si AP Core reste le moteur d'orchestration ; si les trois QR codes et leurs rôles sont préservés ; si QR Code Dynamique et Passeport Numérique Universel utilisent une divulgation contrôlée ; si les preuves cryptographiques sont transportées sans exposer les secrets ; si ERP, IoT/NFC et registres sont intégrés par contrats versionnés ; si erreurs, idempotence, quotas et journalisation sont prévus ; si AP Shield protège les interfaces et AP Ledger audite les événements critiques ; et si les échanges interinstitutionnels restent compatibles avec la souveraineté.

Les API constituent ainsi les frontières programmables de Deep Authenticity© : elles permettent à des systèmes différents de participer à une même infrastructure de confiance sans devenir un système unique.

L'interopérabilité n'est durable que lorsqu'elle est accompagnée d'identité, de preuve, de gouvernance et de cybersécurité.

Le Chapitre 10 développera la cryptographie avancée, l'identité numérique, la gestion des clés et la signature cryptographique de Deep Authenticity©.

Note de cadrage institutionnel

Les protocoles, standards d'authentification, formats d'API et mécanismes de transport devront être sélectionnés selon les exigences de sécurité, d'interopérabilité et de souveraineté de chaque déploiement. Les API doivent être considérées comme des surfaces d'attaque critiques et faire l'objet de tests, supervision, gestion de versions et gouvernance continue.

VOLUME II — ARCHITECTURE TECHNOLOGIQUE ET CYBERSÉCURITÉ

CHAPITRE 10 — CRYPTOGRAPHIE AVANCÉE, IDENTITÉ NUMÉRIQUE ET GESTION DES CLÉS

CRYPTOGRAPHIE — SIGNATURE CRYPTOGRAPHIQUE — IDENTITÉ NUMÉRIQUE — CLÉS — PKI — EMPREINTES — CHIFFREMENT — HORODATAGE — RÉVOCATION — AP SHIELD — CRYPTO-AGILITÉ

1. Objet du chapitre

Ce chapitre définit la couche cryptographique de Deep Authenticity©. Elle protège l'intégrité, l'authenticité, la confidentialité et la provenance des preuves qui circulent entre AP Core, AP Ledger, AP Cloud, les API et les systèmes externes. La cryptographie ne remplace pas la gouvernance de confiance : elle fournit les mécanismes techniques permettant de vérifier les assertions émises par des acteurs autorisés.

2. Principes cryptographiques

L’architecture repose sur plusieurs fonctions distinctes : empreinte pour détecter une modification, signature pour authentifier une preuve, chiffrement pour protéger une information, mécanismes d’ authentification pour établir une identité technique et horodatage pour situer un événement. Ces fonctions ne doivent pas être confondues ni utilisées comme substituts les unes des autres.

3. Identité numérique des acteurs

Producteurs, revendeurs, autorités, services, applications et dispositifs peuvent disposer d’identités numériques adaptées à leur rôle. AP Core relie l’identité à ses habilitations et politiques de confiance. L’identité d’une organisation ou d’un service doit rester distincte de l’identité personnelle lorsque l’ opération ne nécessite pas d’identifier une personne.

4. Infrastructure de clés et certificats

Une infrastructure de gestion des clés peut associer clés publiques, certificats, autorités et politiques de confiance. Les clés privées restent protégées dans des environnements dédiés. La validation d’une signature doit prendre en compte la chaîne de confiance, le contexte d’usage, la période de validité et les éventuelles révocations.

5. Génération des clés

Les clés cryptographiques critiques doivent être générées à l’aide de sources d’aléa et de mécanismes adaptés au niveau de risque. Leur création doit être traçable sans révéler le secret. Les clés de haute sensibilité peuvent nécessiter des modules matériels ou environnements isolés afin de réduire les risques d’extraction.

6. Stockage et protection des secrets

Les clés privées, secrets API et autres éléments sensibles ne doivent pas être stockés avec les données qu’ils protègent lorsque cela augmente le risque. AP Shield supervise les accèset l’utilisation des secrets. Les applications doivent recevoir uniquement les capacités nécessaires plutôt qu’un accès général aux clés maîtresses.

7. Signature cryptographique des preuves

Une signature cryptographique peut protéger un événement, une attestation, un statut, une transaction ou un ensemble de données. Le vérificateur doit pouvoir déterminer qui a signé, quoi, avec quelle clé et dans quel contexte. Une signature valide prouve une relation cryptographique avec le signataire ; elle ne garantit pas à elle seule que l’information signée est factuellement vraie.

8. Trois QR codes et cryptographie

Les trois QR codes d’Authenticity Plus© restent les mécanismes fondamentaux du domaine physique. Ils peuvent pointer vers des preuves signées, mais ne doivent jamais contenir une clé privée. La cryptographie renforce l’unicité et l’intégrité du système sans modifier les rôles consommateur, revendeur/professionnel et contrôle/douanes ni VERT / JAUNE / ROUGE.

9. QR Code Dynamique et signatures

Le QR Code Dynamique permet de résoudre un identifiant persistant vers un état vivant. Les états critiques peuvent être signés afin que leur origine et leur intégrité soient vérifiables. Dans le domaine documentaire, cette signature complète la relation avec l’autorité émettrice et le mécanisme de révocation ou de remplacement.

10. Empreintes cryptographiques

Les empreintes permettent d'identifier l'état d'un contenu, document, événement ou ensemble de données sans inscrire nécessairement le contenu complet dans AP Ledger. Les algorithmes doivent offrir une résistance suffisante aux collisions et pouvoir être remplacés lorsque les standards de sécurité évoluent.

11. Chiffrement des données

Les données sensibles peuvent être chiffrées en transit et au repos selon leur classification. Le chiffrement doit être accompagné d'une gestion rigoureuse des clés, car une clé compromise ou perdue peut annuler la protection ou rendre les données indisponibles. Les exigences souveraines peuvent imposer une maîtrise locale des clés.

12. Horodatage cryptographique

Certaines preuves nécessitent de démontrer qu'une donnée ou signature existait à un moment déterminé. Les services d'horodatage doivent être choisis selon la criticité et le cadre juridique. AP Ledger peut conserver la chronologie et les références permettant d'interpréter durablement l'événement.

13. Rotation et révocation

Aucune clé ne doit être considérée comme éternelle. L'architecture prévoit rotation planifiée, révocation d'urgence, remplacement et propagation du nouvel état de confiance. La révocation d'une clé interdit ses nouveaux usages mais ne doit pas rendre automatiquement invalides les signatures correctement produites lorsqu'elle était légitime.

14. Conservation des preuves historiques

Les preuves à longue durée de vie doivent rester vérifiables malgré expiration des certificats ou évolution des algorithmes. Deep Authenticity© doit conserver les métadonnées nécessaires à l'interprétation historique : algorithme, clé, certificat, statut et contexte temporel. Des mécanismes de renouvellement de preuve peuvent être nécessaires pour les archives de longue durée.

15. Crypto-agilité

La crypto-agilité est la capacité de remplacer algorithmes, tailles de clés, bibliothèques ou infrastructures sans reconstruire tout l'écosystème. Les formats de preuve doivent identifier explicitement les mécanismes utilisés. Cette abstraction prépare la plateforme aux évolutions réglementaires, aux vulnérabilités futures et à la transition vers de nouveaux standards.

16. Préparation post-quantique

Deep Authenticity© doit être conçue pour permettre une migration vers des mécanismes post-quantiques lorsque les standards, performances et risques le justifient. L'objectif n'est pas d'imposer prématurément une technologie unique, mais d'éviter les dépendances architecturales qui rendraient une future transition impossible ou excessivement coûteuse.

17. AP Ledger, AP Cloud et cryptographie

AP Ledger utilise empreintes, signatures et horodatages pour renforcer l'auditabilité. AP Cloud protège données et communications par chiffrement et contrôle des clés. La séparation des responsabilités évite qu'un même composant détienne automatiquement toutes les données, clés et capacités de modification.

18. API, ERP, IoT/NFC et authentification

Les échanges API et ERP peuvent être authentifiés et signés selon leur criticité. Les dispositifs IoT/NFC disposent de contraintes spécifiques de puissance, stockage et cycle de vie. Les mécanismes cryptographiques doivent être adaptés au matériel tout en permettant révocation, renouvellement et identification d'un dispositif compromis.

19. Gouvernance cryptographique

La sécurité dépend autant de la gouvernance que des algorithmes. Les rôles de création, utilisation, sauvegarde, récupération, rotation et révocation doivent être séparés. Des audits périodiques doivent vérifier inventaire des clés, permissions, dépendances et conformité des bibliothèques. AP Shield supervise les événements de sécurité liés à cette gouvernance.

20. Critères d'acceptation et conclusion

La couche cryptographique est cohérente si empreinte, signature, chiffrement, authentification et horodatage sont clairement distingués ; si les identités numériques sont liées à des habilitations ; si les clés privées restent protégées ; si les trois QR codes et le QR Code Dynamique utilisent la cryptographie sans exposer les secrets ; si signatures et empreintes restent auditables ; si rotation, révocation et conservation historique sont prévues ; si AP Ledger, AP Cloud, API, ERP et IoT/NFC utilisent des mécanismes adaptés ; et si la crypto-agilité prépare l'évolution future.

La cryptographie constitue ainsi la grammaire technique de la preuve dans Deep Authenticity© : elle permet de vérifier origine, intégrité et confidentialité sans confondre preuve cryptographique et vérité métier.

Sa valeur dépend de la qualité des clés, des identités, des politiques et de la gouvernance qui l'entourent.

Le Chapitre 11 développera la signature cryptographique native des contenus : création, provenance, intégrité, versionnement, transformations et chaîne de confiance numérique.

Note de cadrage institutionnel

Les algorithmes, tailles de clés, infrastructures de certificats et mécanismes post-quantiques doivent être sélectionnés selon les standards reconnus au moment du déploiement et faire l'objet d'une revue cryptographique spécialisée. Ce chapitre définit l'architecture et les exigences de gouvernance ; il ne prescrit pas un algorithme unique pour tous les usages.

VOLUME II — ARCHITECTURE TECHNOLOGIQUE ET CYBERSÉCURITÉ

CHAPITRE 11 — SIGNATURE CRYPTOGRAPHIQUE NATIVE DES CONTENUS ET PROVENANCE NUMÉRIQUE

SIGNATURE NATIVE — CONTENUS — PROVENANCE — INTÉGRITÉ — EMPREINTE — AUTEUR/ÉMETTEUR — VERSIONNEMENT — TRANSFORMATIONS — AP CORE — AP LEDGER — CHAÎNE DE CONFIANCE

1. Objet du chapitre

Ce chapitre définit la signature cryptographique native des contenus comme un mécanisme fondamental du domaine numérique de Deep Authenticity©. L'objectif est d'attacher, dès la création, l'émission ou la validation d'un contenu, une preuve vérifiable de provenance et d'intégrité capable de l'accompagner à travers ses versions et transformations autorisées.

2. Principe de signature native

La signature est dite native lorsqu'elle est intégrée au processus de création ou de publication plutôt qu'ajoutée uniquement après circulation. Le système calcule une empreinte du contenu ou de ses éléments pertinents et associe cette empreinte à une signature émise par une identité ou un service autorisé.

3. Domaines de contenus concernés

Le mécanisme peut s'appliquer, selon les formats et droits, aux images, vidéos, fichiers audio, textes, documents numériques, logiciels, modèles, créations intellectuelles et autres contenus. Chaque type de contenu nécessite une stratégie de canonicalisation, d'empreinte et de métadonnées adaptée à ses transformations légitimes.

4. Identité de l'auteur ou de l'émetteur

La signature peut établir qu'un contenu a été signé par une identité cryptographique donnée. Cette identité peut représenter un créateur, une organisation, un média, un logiciel ou une autorité. Deep Authenticity© doit distinguer identité vérifiée, pseudonyme et simple clé technique afin de ne pas attribuer une identité humaine sans preuve suffisante.

5. Empreinte du contenu

Une empreinte cryptographique représente l'état exact d'un contenu. Toute modification pertinente produit normalement une empreinte différente. Pour certains formats, des représentations normalisées peuvent être nécessaires afin d'éviter que des changements purement techniques et sans effet sur le contenu produisent des ruptures de provenance inutiles.

6. Signature et intégrité

La signature protège la relation entre l'empreinte, l'émetteur et les métadonnées signées. Lors de la vérification, le système recalcule l'empreinte et contrôle la signature. Une différence peut indiquer une modification, une corruption ou une version différente ; elle ne permet pas à elle seule de déterminer l'intention de cette modification.

7. Provenance numérique

La provenance décrit la chaîne des origines et transformations vérifiables. Un contenu peut posséder une version initiale signée puis plusieurs dérivés autorisés. Chaque étape peut référencer la version précédente, l'opération réalisée et l'acteur ou outil responsable afin de construire une généalogie numérique vérifiable.

8. Versionnement

Toute modification substantielle peut produire une nouvelle version avec sa propre empreinte et signature. AP Core relie les versions et indique laquelle est active, antérieure, remplacée ou dérivée. L'ancienne version n'est pas nécessairement fausse : elle représente un état historique distinct dont la provenance doit rester interprétable.

9. Transformations autorisées

Recadrage, compression, traduction, montage, conversion ou autre transformation peuvent être légitimes. Deep Authenticity© doit pouvoir enregistrer ces opérations lorsqu'elles sont connues et autorisées. La chaîne de provenance permet alors de distinguer un dérivé déclaré d'une modification sans relation vérifiable avec la source.

10. Contenus générés ou modifiés par IA

Lorsqu'un contenu est généré ou transformé par un système d'IA intégré à la chaîne, la provenance peut enregistrer l'outil ou service, la version et la nature générale de l'opération selon les droits applicables. Cette information renseigne sur le processus de création sans permettre de conclure automatiquement sur la qualité ou la véracité du contenu.

11. Vérification des contenus

Lorsqu'un utilisateur ou système vérifie un contenu, AP Core peut restituerl'existence d'une provenance reconnue, l'intégrité de la version, l'identité ou catégorie de l'émetteur et l'historique autorisé. L'interface doit distinguer clairement « signature valide », « provenance incomplète », « contenu modifié » et « absence de preuve disponible ».

12. Vérité factuelle et authenticité

Une signature cryptographique valide ne prouve pas qu'une affirmation contenue dans un texte, une image ou une vidéo est vraie. Elle prouve qu'une entité donnée a signé une version déterminée. Deep Authenticity© sépare donc authenticité/provenance technique, analyse de contenu et éventuelle vérification factuelle.

13. AP Core et politiques de confiance

AP Core détermine quelles identités, autorités ou signatures sont reconnues selon le contexte. Un média, une administration, un créateur ou une entreprise peuvent disposer de niveaux d'assurance différents. Les politiques sont versionnées afin que la signification d'une signature reste compréhensible dans le temps.

14. AP Ledger et ancrage des preuves

AP Ledger peut ancrer l'empreinte, la signature, l'horodatage ou la relation entre versions pour les contenus nécessitant une auditabilité renforcée. Le fichier complet peut rester hors ledger. Cette approche permet de démontrer l'existence d'une version à une date donnée sans publier le contenu lui-même.

15. AP Cloud et distribution

AP Cloud peut héberger les métadonnées de provenance, certificats, manifestes ou services de résolution nécessaires à la vérification. La provenance doit cependant rester portable et vérifiable dans des architectures souveraines ou fédérées afin qu'elle ne dépende pas exclusivement d'un service cloud central.

16. AP Shield et protection des identités de signature

AP Shield protège les comptes, services, clés et interfaces utilisés pour signer. Une clé compromise peut permettre de produire de fausses signatures techniquement valides ; la détection, la révocation et la rotation sont donc essentielles. Les opérations de signature à forte valeur peuvent exiger des contrôles renforcés.

17. QR Code Dynamique et contenus

Un QR Code Dynamique peut fournir un point d'accès vers la provenance d'un contenu présenté sur un support physique ou numérique. Il permet de résoudre l'état courant, les versions ou la source reconnue sans inscrire toutes les métadonnées dans le QR. Il reste un vecteur d'accès, tandis que la preuve réside dans la signature et l'infrastructure.

18. Interopérabilité et standards de provenance

Deep Authenticity© doit pouvoir échanger des preuves de provenance avec des standards et écosystèmes externes lorsque cela est pertinent. Les adaptateurs doivent préserver l'origine, les signatures et les relations entre versions. L'interopérabilité ne doit pas affaiblir la capacité à distinguer une preuve native d'une métadonnée non vérifiée.

19. Droits, confidentialité et propriété intellectuelle

La provenance doit respecter droits d'auteur, secrets commerciaux, données personnelles et règles de publication. Toutes les métadonnées de création n'ont pas vocation à être publiques. Des vues sélectives peuvent confirmer l'origine ou l'intégrité sans révéler des informations confidentielles sur le processus de création.

20. Critères d'acceptation et conclusion

La signature native des contenus est cohérente si elle est créée au plus près de l'émission ou de la validation ; si empreinte, identité et métadonnées signées sont vérifiables ; si versions et transformations sont reliées ; si les contenus générés ou modifiés par IA peuvent conserver leur provenance ; si signature valide et vérité factuelle sont distinguées ; si AP Core applique les politiques de confiance ; si AP Ledger peut ancrer les preuves ; si AP Cloud distribue sans centralisation obligatoire ; si AP Shield protège les clés ; et si interopérabilité, droits et confidentialité sont préservés.

La signature cryptographique native permet ainsi à un contenu de transporter une histoire de provenance vérifiable plutôt qu'une simple apparence numérique.

Elle constitue la fondation technique de la vérification des contenus dans le domaine numérique de Deep Authenticity©.

Le Chapitre 12 développera l'intelligence artificielle et les CNN : analyse d'images, détection d' anomalies, contrefaçons, signaux faibles et gouvernance des modèles.

Note de cadrage institutionnel

La signature cryptographique native établit principalement provenance, intégrité et relation avec une identité de signature. Elle ne constitue pas, à elle seule, une preuve de véracité factuelle, de titularité juridique définitive ou d'absence de manipulation antérieure à la signature. Les formats, standards de provenance et mécanismes de signature devront être choisis selon les usages et l'état de l'art.

VOLUME II — ARCHITECTURE TECHNOLOGIQUE ET CYBERSÉCURITÉ

CHAPITRE 12 — INTELLIGENCE ARTIFICIELLE ET CNN : DÉTECTION DES ANOMALIES ET CONTREFAÇONS

1. Objet du chapitre

Ce chapitre définit la couche d'intelligence artificielle de Deep Authenticity©, notamment les réseaux neuronaux convolutifs (CNN) appliqués à l'analyse visuelle. L'IA constitue une couche complémentaire de détection : elle recherche anomalies, incohérences et signaux faibles afin de renforcer les preuves déterministes fournies par les identifiants, signatures cryptographiques, événements et registres.

2. Positionnement de l'IA dans l'architecture

L'IA ne remplace ni AP Core, ni les trois QR codes d'Authenticity Plus©, ni la cryptographie. Elle produit des observations et scores de risque qu'AP Core interprète selon des politiques définies. Cette séparation empêche qu'une prédiction probabiliste devienne silencieusement une décision d' authenticité irréversible.

3. CNN et analyse d'images

Les CNN peuvent analyser formes, textures, impressions, logos, micro-détails, emballages ou autres caractéristiques visuelles lorsqu'un modèle a été entraîné pour ce cas d'usage. Leur efficacité dépend directement de la qualité des images, de la représentativité des données d'entraînement et des conditions réelles de capture.

4. Détection de contrefaçons

Un modèle peut comparer les caractéristiques d'un objet observé avec celles de références authentiques et détecter des divergences. Le résultat doit être exprimé comme signal de risque ou probabilité, et non comme preuve absolue. Une alerte élevée peut déclencher une vérification complémentaire par QR, NFC, registre ou contrôle humain.

5. Trois QR codes et IA

Les trois QR codes d'Authenticity Plus© restent le mécanisme anti-contrefaçon fondamental du domaine physique. L'IA peut analyser les comportements de scan, incohérences géographiques ou répétitions anormales, mais elle ne modifie pas leur séparation consommateur, revendeur/professionnel et contrôle/douanes.

6. VERT / JAUNE / ROUGE et score IA

VERT signifie original ; JAUNE signifie original mais déjà vérifié ou vendu ; ROUGE signifie contrefaçon ou code inexistant dans Authenticity Plus©. Un score IA doit être présenté séparément de ces statuts. Un signal algorithmique peut déclencher une investigation sans redéfinir la sémantique fondamentale des couleurs.

7. Analyse comportementale des scans

Les événements de scan peuvent révéler des anomalies : même identifiant observé dans des contextes incompatibles, volumes inhabituels, séquences impossibles ou réutilisations répétées. Les modèles peuvent prioriser ces signaux pour les équipes de contrôle, tout en tenant compte des voyages, reventes et autres explications légitimes.

8. Fusion multimodale des signaux

Une décision de risque peut combiner image, QR, signature, provenance, données ERP, IoT/NFC et historique d'événements. Chaque source doit conserver son niveau de confiance. La fusion ne doit pas

masquer l'origine des signaux : le vérificateur doit pouvoir comprendre quelles preuves et observations ont contribué à l'alerte.

9. IA appliquée aux contenus numériques

Dans le domaine numérique, l'IA peut détecter certaines manipulations, anomalies ou ressemblances. Elle complète la signature cryptographique native des contenus, qui établit provenance et intégrité d' une version. L'absence de signature ne prouve pas une manipulation, et une analyse IA ne remplace pas la chaîne de provenance.

10. Données d'entraînement

Les modèles nécessitent des données représentatives des produits, conditions d'éclairage, appareils, régions et variantes légitimes. Les jeux de données doivent être documentés, versionnés et protégés. Des données déséquilibrées ou mal étiquetées peuvent produire des taux d'erreur incompatibles avec un usage de contrôle.

11. Validation et métriques

Avant déploiement, chaque modèle doit être évalué sur des données distinctes de l'entraînement. Précision, rappel, faux positifs, faux négatifs et robustesse doivent être mesurés selon le risque métier. Un seuil acceptable pour une alerte exploratoire peut être insuffisant pour une décision à conséquence juridique.

12. Explicabilité et traçabilité

Pour les usages sensibles, Deep Authenticity© doit conserver modèle, version, date, données d'entrée pertinentes, score et règle ayant transformé ce score en action. L'explication peut prendre la forme de facteurs ou zones d'attention sans prétendre révéler une causalité que le modèle ne démontre pas.

13. Humain dans la boucle

Les alertes à fort impact peuvent être soumises à un agent habilité avant action définitive. Le contrôle humain permet d'examiner contexte, preuves et exceptions. L'objectif n'est pas de neutraliser l' automatisation, mais d'adapter le niveau d'intervention humaine à la gravité et à l'incertitude.

14. Dérive des modèles

Les produits, méthodes de contrefaçon, appareils photo et comportements évoluent. Un modèle performant aujourd'hui peut se dégrader. La plateforme doit surveiller dérive des données, taux d' erreur et nouvelles typologies d'attaque, puis organiser réentraînement, validation et remplacement contrôlé.

15. Attaques adversariales

Les systèmes IA peuvent être ciblés par des images ou données conçues pour tromper le modèle. AP Shield doit traiter cette surface d'attaque : validation des entrées, limitation des requêtes, surveillance des comportements, tests adversariaux et séparation entre modèle d'analyse et mécanismes déterministes de preuve.

16. Confidentialité et minimisation

L'analyse IA doit collecter uniquement les données nécessaires. Les images peuvent contenir personnes, lieux ou informations sensibles sans rapport avec l'authentification. Des politiques de conservation, masquage ou traitement local doivent limiter les risques et respecter les exigences applicables.

17. Online / Offline et IA embarquée

Certains modèles légers peuvent fonctionner localement sur smartphone ou dispositif de contrôle afin de produire une première analyse offline. Les modèles plus lourds peuvent utiliser AP Cloud. Le résultat local doit indiquer version du modèle et niveau de fraîcheur, puis être synchronisé lorsque la connectivité revient.

18. AP Cloud, AP Core et AP Shield

AP Cloud fournit les ressources d'entraînement et d'inférence ; AP Core orchestre les scores avec les preuves ; AP Shield protège modèles, données, API et pipelines. Cette séparation réduit le risque qu'un composant IA compromis puisse modifier directement les identités, signatures ou historiques de preuve.

19. Gouvernance et audit des modèles

Chaque modèle doit disposer d'un propriétaire, d'une finalité, d'une version, d'un périmètre d'usage, de métriques et d'une procédure de retrait. Les changements importants doivent être auditables. Les modèles utilisés par des autorités ou secteurs critiques nécessitent des exigences renforcées de validation, sécurité et documentation.

20. Critères d'acceptation et conclusion

La couche IA/CNN est cohérente si elle reste complémentaire aux preuves déterministes ; si les trois QR codes et VERT/JAUNE/ROUGE conservent leur rôle fondamental ; si les scores sont séparés des statuts d'authenticité ; si les données d'entraînement et métriques sont documentées ; si les faux positifs et faux négatifs sont maîtrisés selon le risque ; si l'humain intervient lorsque l'impact le justifie ; si dérive et attaques adversariales sont surveillées ; si confidentialité et Online/Offline sont prévus ; et si AP Core, AP Cloud et AP Shield encadrent l'ensemble du cycle de vie des modèles.

L'intelligence artificielle devient ainsi le système d'observation avancée de Deep Authenticity© : elle révèle des signaux difficiles à détecter par des règles simples, tout en restant subordonnée à une architecture de preuve vérifiable.

La force du système réside dans la combinaison de preuves déterministes et d'analyses probabilistes clairement distinguées.

Le Chapitre 13 développera IoT, NFC, capteurs et liaison sécurisée entre l'objet physique et son identité numérique.

Note de cadrage institutionnel

Les performances d'un modèle IA/CNN dépendent du cas d'usage, des données, des conditions de capture et de la validation indépendante. Aucun taux universel de détection ne doit être affirmé sans essais mesurés. Les usages à conséquences importantes doivent intégrer gouvernance, supervision humaine, cybersécurité et procédures de recours adaptées.

VOLUME II — ARCHITECTURE TECHNOLOGIQUE ET CYBERSÉCURITÉ

CHAPITRE 13 — IOT, NFC, CAPTEURS ET LIAISON SÉCURISÉE OBJET–NUMÉRIQUE

IOT — NFC — CAPTEURS — OBJET PHYSIQUE — IDENTITÉ NUMÉRIQUE — 3 QR CODES — CRYPTOGRAPHIE — AP CORE — PASSEPORT NUMÉRIQUE UNIVERSEL — ONLINE/OFFLINE — CYBERSÉCURITÉ

1. Objet du chapitre

Ce chapitre définit l'intégration de l'Internet des objets (IoT), du NFC, des puces et des capteurs dans Deep Authenticity©. Ces technologies renforcent la liaison entre un objet physique et son identité numérique en produisant des signaux ou événements complémentaires. Elles ne remplacent pas l' architecture fondamentale des trois QR codes d'Authenticity Plus©.

2. Principe de liaison objet–numérique

Une identité numérique n'est utile que si la relation avec l'objet réel est suffisamment fiable. Deep Authenticity© combine identifiants visuels, preuves cryptographiques et, lorsque le cas d'usage le justifie, composants électroniques. Chaque technologie apporte un niveau de preuve différent qui doit rester explicitement qualifié.

3. Rôle fondamental des trois QR codes

Les trois QR codes — consommateur, revendeur/professionnel et contrôle/douanes — demeurent le mécanisme anti-contrefaçon central du domaine physique. IoT et NFC constituent des couches complémentaires. Une puce ne doit donc pas conduire à supprimer la séparation fonctionnelle des trois QR codes ni la logique VERT / JAUNE / ROUGE.

4. NFC et identification de proximité

Le NFC permet à un smartphone ou lecteur compatible d'interroger une puce à courte distance. Selon le matériel, celle-ci peut fournir un identifiant, une donnée signée ou un mécanisme de défi-réponse. AP Core résout ensuite l'identité et applique les politiques de confiance correspondant au produit et au rôle du vérificateur.

5. Puces sécurisées et éléments matériels

Pour les actifs à forte valeur ou à risque élevé, des composants sécurisés peuvent protéger des clés ou exécuter certaines opérations cryptographiques sans exposer le secret. Leur utilisation doit être proportionnée au coût, au niveau de menace et au cycle de vie du produit.

6. Capteurs et événements physiques

Température, humidité, choc, ouverture, localisation ou autres paramètres peuvent être collectés lorsqu'ils sont pertinents. Ces données deviennent des événements du Passeport Numérique Universel seulement après qualification de leur source. Une mesure de capteur n'est pas automatiquement une vérité absolue : le dispositif peut être défaillant ou compromis.

7. Identité cryptographique du dispositif

Un dispositif IoT/NFC peut disposer d'une identité cryptographique propre permettant à AP Core de vérifier l'origine de ses messages. Les clés doivent être générées, provisionnées, stockées et renouvelées selon le niveau de risque. Une identité de dispositif compromise doit pouvoir être révoquée sans invalider l'identité du produit lui-même.

8. Association produit–dispositif

L’association entre une puce et un produit doit être créée dans un processus contrôlé de fabrication, d’assemblage ou d’activation. AP Core conserve la relation entre identifiant produit, trois QR codes et dispositif électronique. Un remplacement légitime de composant doit produire un événement traçable plutôt qu’une modification silencieuse.

9. Signature cryptographique des données

Les messages critiques peuvent être signés par le dispositif ou une passerelle de confiance. La signature protège origine et intégrité, tandis qu’un horodatage ou compteur peut limiter les attaques par rejeu. Les clés privées ne doivent jamais être transmises avec les données ni encodées dans les QR codes.

10. AP Core et fusion des preuves

AP Core peut combiner l’état des QR codes, la preuve NFC, les événements IoT, les signatures et l’historique du Passeport Numérique Universel. Chaque signal conserve sa provenance et son niveau d’assurance. Une divergence entre QR, puce et registre peut déclencher une alerte ou un contrôle renforcé.

11. AP Ledger et auditabilité

Les événements IoT critiques peuvent être ancrés dans AP Ledger sous forme d’empreintes, références et horodatages. Il n’est pas nécessaire d’inscrire tous les flux de télémétrie dans le registre. Les politiques sélectionnent les événements dont la valeur probante justifie une conservation renforcée.

12. AP Cloud et traitement des flux

AP Cloud peut recevoir, normaliser et traiter de grands volumes de télémétrie. Les files d’événements, mécanismes de reprise et règles de rétention permettent d’absorber les variations de charge. Les traitements analytiques lourds doivent rester isolés des services critiques de vérification.

13. AP Shield et cybersécurité IoT

Les dispositifs connectés élargissent la surface d’attaque. AP Shield doit couvrir authentification, segmentation, inventaire, mises à jour, détection d’anomalies et révocation. Les mots de passe par défaut, interfaces inutiles et dépendances non maintenues doivent être éliminés ou strictement maîtrisés.

14. Mises à jour et cycle de vie logiciel

Un dispositif connecté peut rester en service plusieurs années. Son logiciel ou micrologiciel doit pouvoir être mis à jour de manière authentifiée lorsque l’architecture matérielle le permet. Les versions, correctifs et changements critiques doivent être traçables afin de détecter les équipements devenus vulnérables.

15. Online / Offline

NFC et certains capteurs peuvent fournir des preuves locales même sans réseau. Une application peut vérifier une signature ou stocker temporairement un événement. Toutefois, les révocations et changements récents peuvent nécessiter une connexion. L’interface doit distinguer clairement vérification locale et confirmation de l’état courant.

16. Passerelles et environnements industriels

Dans les usines, entrepôts ou transports, les dispositifs peuvent communiquer par une passerelle locale plutôt que directement avec AP Cloud. La passerelle authentifie, agrège et filtre les flux. Elle peut aussi maintenir un mode dégradé avant synchronisation sécurisée avec AP Core.

17. ERP et continuité industrielle

Les événements IoT/NFC peuvent être rapprochés des données ERP : production, lot, expédition, réception, maintenance ou stock. Les deux sources doivent rester distinctes afin de détecter les incohérences. Une donnée ERP déclarée ne doit pas écraser automatiquement une observation physique contradictoire.

18. IA/CNN et données capteurs

L'IA peut analyser les séries de capteurs ou combiner télémétrie, images et scans pour détecter des anomalies. Les résultats restent probabilistes et sont séparés des preuves cryptographiques. Les modèles doivent tenir compte des variations normales d'usage afin d'éviter une multiplication de faux signaux.

19. Confidentialité, autonomie et proportionnalité

La collecte continue peut révéler localisation, habitudes ou informations commerciales sensibles. Les capteurs doivent donc être utilisés pour une finalité définie, avec minimisation et durée de conservation adaptée. Tous les produits n'ont pas besoin d'un composant connecté : l'architecture doit rester accessible aux objets protégés uniquement par les mécanismes QR.

20. Critères d'acceptation et conclusion

L'architecture IoT/NFC est cohérente si les trois QR codes restent fondamentaux ; si les dispositifs renforcent sans remplacer le mécanisme physique ; si l'identité cryptographique des dispositifs est distincte de celle du produit ; si l'association produit–dispositif est traçable ; si les données signées conservent provenance et niveau d'assurance ; si AP Core fusionne les preuves, AP Ledger audite les événements critiques, AP Cloud traite les flux et AP Shield protège la surface IoT ; si Online/Offline, passerelles, ERP et IA sont intégrés ; et si collecte et coûts restent proportionnés.

IoT et NFC permettent ainsi à Deep Authenticity© d'étendre la preuve au comportement et à l'état physique d'un objet, sans transformer la connectivité en condition obligatoire de l'authenticité.

Le système conserve une architecture graduée : QR codes comme fondation universelle, puis preuves électroniques lorsque le risque et la valeur le justifient.

Le Chapitre 14 développera l'architecture Online/Offline : vérification locale, cache sécurisé, synchronisation, gestion des conflits et continuité de service.

Note de cadrage institutionnel

IoT, NFC et capteurs constituent des mécanismes complémentaires dont la pertinence dépend du secteur, du coût, de la durée de vie et du niveau de menace. La sécurité doit couvrir le dispositif pendant tout son cycle de vie, y compris provisionnement, mises à jour, révocation et fin de support. La matrice institutionnelle du Volume II reste inchangée.

VOLUME II — ARCHITECTURE TECHNOLOGIQUE ET CYBERSÉCURITÉ

CHAPITRE 14 — ARCHITECTURE ONLINE/OFFLINE : CONTINUITÉ DE VÉRIFICATION ET SYNCHRONISATION SÉCURISÉE

ONLINE/OFFLINE — VÉRIFICATION LOCALE — CACHE SÉCURISÉ — SIGNATURE CRYPTOGRAPHIQUE — SYNCHRONISATION — CONFLITS — AP CORE — 3 QR CODES — QR CODE DYNAMIQUE — RÉSILIENCE

1. Objet du chapitre

Ce chapitre définit l'architecture Online/Offline de Deep Authenticity©. L'objectif est de préserver une capacité utile de vérification et d'enregistrement d'événements lorsque la connectivité est absente, instable ou volontairement isolée, tout en évitant de présenter une information locale ancienne comme un état temps réel.

2. Principe de continuité de service

Deep Authenticity© distingue les opérations nécessitant une confirmation connectée de celles pouvant être exécutées localement avec un niveau d'assurance défini. Le mode offline n'est pas une copie autonome de toute la plateforme : il constitue un mode dégradé contrôlé, fondé sur des preuves cryptographiques, caches limités et politiques de fraîcheur.

3. Classification des opérations

Chaque fonction doit être classée : autorisée offline, autorisée sous conditions, ou obligatoirement online. Une lecture d'information signée peut être possible localement, tandis qu'une révocation, un transfert de propriété ou une opération administrative critique peut nécessiter une confirmation serveur ou une resynchronisation avant finalisation.

4. Trois QR codes en mode offline

Les trois QR codes d'Authenticity Plus© restent fonctionnellement distincts en mode offline. Une application peut reconnaître le rôle du code et vérifier certaines preuves locales, mais la sémantique VERT / JAUNE / ROUGE doit tenir compte de la fraîcheur : l'état courant peut avoir changé depuis la dernière synchronisation.

5. Statuts et fraîcheur

VERT signifie original ; JAUNE signifie original mais déjà vérifié ou vendu ; ROUGE signifie contrefaçon ou code inexistant dans le système. En absence de confirmation récente, l'interface doit signaler que le résultat est fondé sur une preuve locale ou un cache daté, plutôt que d'inventer un quatrième sens aux couleurs fondamentales.

6. QR Code Dynamique offline

Le QR Code Dynamique dépend par nature d'un état vivant. Offline, l'application peut résoudre un identifiant vers une information précédemment mise en cache ou vérifier une preuve embarquée, mais elle ne peut garantir une modification récente. La date ou période de validité de la donnée locale doit donc être visible ou exploitable.

7. Signature cryptographique locale

Une signature cryptographique permet de vérifier localement l'intégrité et l'origine d'une preuve lorsque la clé publique ou chaîne de confiance nécessaire est disponible. Cette capacité ne confirme

pas automatiquement que la preuve n’a pas été révoquée depuis la dernière synchronisation. Provenance et fraîcheur restent deux dimensions distinctes.

8. Cache sécurisé

Le cache offline doit contenir uniquement les données nécessaires, chiffrées ou protégées selon leur sensibilité. Il doit avoir une durée de vie, une version et une origine identifiables. Les données expirées peuvent être conservées pour audit, mais ne doivent pas être présentées comme état courant sans avertissement approprié.

9. Listes de révocation et données critiques

Lorsque le cas d’usage le permet, des listes de révocation ou ensembles de statuts critiques peuvent être téléchargés avant une mission de terrain. Leur horodatage permet d’évaluer le niveau de fraîcheur. Les environnements à haut risque peuvent imposer une durée offline maximale avant qu’une confirmation connectée devienne obligatoire.

10. File locale d’événements

Les scans, contrôles ou opérations autorisées offline peuvent être placés dans une file locale sécurisée. Chaque événement reçoit un identifiant unique, un contexte temporel et, lorsque possible, une signature. Cette file doit résister aux duplications et modifications avant son envoi à AP Core.

11. Resynchronisation avec AP Core

Après reconnexion, AP Core reçoit les événements locaux, vérifie leur authenticité, leur ordre et leur compatibilité avec l’état actuel. Une opération offline n’est intégrée définitivement que si elle respecte les politiques applicables. Les événements rejetés ou conflictuels restent traçables pour analyse.

12. Gestion des doublons

Une interruption réseau peut provoquer plusieurs tentatives d’envoi du même événement. Des identifiants d’idempotence permettent à AP Core de reconnaître une répétition sans appliquer deux fois une vente, un transfert ou une activation. Cette propriété est essentielle pour préserver la cohérence des cycles de vie.

13. Gestion des conflits

Deux opérations légitimes peuvent avoir été réalisées offline sur des copies différentes d’un état ancien. Les règles de résolution dépendent du type d’événement : priorité temporelle, autorité supérieure, mise en attente ou contrôle humain. Les conflits critiques ne doivent pas être résolus arbitrairement par le terminal.

14. AP Ledger et chronologie offline

Les événements validés après resynchronisation peuvent être ancrés dans AP Ledger avec distinction entre moment de l’action et moment de réception. Cette séparation évite de falsifier la chronologie. Les niveaux de confiance de l’horloge locale et de la signature doivent être conservés lorsque l’ordre temporel est important.

15. AP Shield et sécurité du terminal

Un terminal offline peut être perdu, volé ou compromis. AP Shield doit prévoir authentification locale, chiffrement, verrouillage, expiration de session, limitation des données et révocation du terminal. Une application compromise ne doit pas pouvoir fabriquer des preuves équivalentes à celles d’un service central autorisé.

16. IoT/NFC et périphérie

Les dispositifs NFC, IoT et passerelles peuvent continuer à collecter ou vérifier certaines données sans connexion centrale. Les événements sont stockés localement puis synchronisés. Les compteurs, signatures ou mécanismes anti-rejeu contribuent à détecter la duplication ou la réinjection de messages anciens.

17. ERP et sites isolés

Une usine, un entrepôt, un navire, une frontière ou un site distant peut fonctionner temporairement isolé. Un nœud local peut assurer les fonctions autorisées et synchroniser ensuite avec AP Cloud. Les politiques doivent définir précisément quelles opérations industrielles peuvent être finalisées sans connexion.

18. IA embarquée en mode offline

Des modèles IA légers peuvent analyser une image ou un signal localement. Leur résultat doit inclure la version du modèle et rester distinct des preuves déterministes. Après reconnexion, l'analyse peut être enrichie par des modèles cloud ou comparée à de nouvelles informations de risque.

19. Résilience et souveraineté opérationnelle

L'architecture Online/Offline réduit la dépendance à une connectivité permanente et améliore la continuité en cas de panne, catastrophe, zone blanche ou isolement souverain. Elle ne doit cependant pas créer plusieurs vérités concurrentes : AP Core reste responsable de la réconciliation et de l'état consolidé.

20. Critères d'acceptation et conclusion

L'architecture Online/Offline est cohérente si les opérations sont classées selon leur besoin de connectivité ; si les trois QR codes restent distincts ; si VERT/JAUNE/ROUGE ne sont pas redéfinis par le mode offline ; si le QR Code Dynamique indique la fraîcheur de l'état ; si les signatures permettent une vérification locale sans masquer les limites de révocation ; si le cache est sécurisé ; si les événements utilisent files, idempotence et résolution des conflits ; si AP Core réconcilie, AP Ledger conserve la chronologie et AP Shield protège les terminaux ; et si IoT/NFC, ERP et IA peuvent fonctionner en mode dégradé.

L'architecture Online/Offline donne à Deep Authenticity© une continuité opérationnelle sans sacrifier la distinction entre preuve locale et état courant.

Elle transforme l'absence de réseau d'une rupture totale en mode de fonctionnement gouverné, limité et réconciliable.

Le Chapitre 15 développera l'intégration ERP et les infrastructures industrielles : production, lots, stocks, événements, connecteurs et continuité de preuve.

Note de cadrage institutionnel

Le mode offline doit être défini selon le niveau de risque de chaque opération. Une preuve cryptographique locale peut confirmer intégrité et provenance, mais ne garantit pas nécessairement l' absence d'une révocation ou modification récente. Les durées de cache, politiques de resynchronisation et opérations autorisées hors ligne doivent être formellement gouvernées.

VOLUME II — ARCHITECTURE TECHNOLOGIQUE ET CYBERSÉCURITÉ

CHAPITRE 15 — ERP ET INFRASTRUCTURES INDUSTRIELLES : INTÉGRATION ET CONTINUITÉ DE PREUVE

ERP — PRODUCTION — LOTS — STOCKS — CONNECTEURS — API — AP CORE — 3 QR CODES — IOT/NFC — ÉVÉNEMENTS — TRAÇABILITÉ — CYBERSÉCURITÉ

1. Objet du chapitre

Ce chapitre définit l'intégration de Deep Authenticity© avec les ERP et infrastructures industrielles. L' objectif n'est pas de remplacer les systèmes de gestion existants, mais de transformer certains événements de production, logistique, vente et maintenance en éléments de continuité de preuve reliés à AP Core et au Passeport Numérique Universel.

2. Principe de non-substitution

L'ERP demeure le système de gestion des processus de l'entreprise : commandes, production, stocks, achats, ventes ou maintenance selon son périmètre. Deep Authenticity© ajoute une couche de vérification, provenance et confiance. Cette séparation réduit les coûts de transformation et facilite l' adoption progressive.

3. Architecture des connecteurs

Les ERP peuvent communiquer avec AP Core par API, middleware, bus d'événements ou connecteurs spécialisés. Chaque connecteur traduit les données sources vers des schémas contrôlés sans modifier leur signification. Il doit être versionné, authentifié, observable et isolable en cas de défaillance.

4. Référentiels produits

Avant l'émission de preuves unitaires, les références produit, variantes, unités et organisations doivent êtrerapprochées des identités de Deep Authenticity©. Les correspondances doivent être explicites afin d'éviter qu'une erreur de mapping ERP associe un QR code, un lot ou un événement au mauvais produit.

5. Production et création des unités

Lors de la production, l'ERP ou le système industriel peut déclencher la création ou l'affectation d' identifiants. AP Core contrôle les droits et la cohérence des volumes. La génération de codes doit rester séparée de leur activation afin de limiter l'utilisation frauduleuse de codes non associés à des unités réellement produites.

6. Lots, séries et unités

Deep Authenticity© doit pouvoir représenter différents niveaux de granularité : lot, série et unité. Les événements peuvent être hérités d'un lot lorsqu'ils s'appliquent à toutes les unités, tout en permettant des exceptions unitaires. Cette hiérarchie évite de dupliquer inutilement les mêmes informations.

7. Trois QR codes et activation industrielle

Les trois QR codes d'Authenticity Plus© — consommateur, revendeur/professionnel et contrôle/douanes — sont reliés à l'unité selon un processus contrôlé. L'ERP peut fournir le contexte industriel, mais AP Core conserve les règles d'activation, de rôle et de statut VERT / JAUNE / ROUGE.

8. QR Code Dynamique et données industrielles

Le QR Code Dynamique peut présenter des informations actualisées issues de l'ERP lorsque leur exposition est autorisée : référence, maintenance, disponibilité d'une notice ou autre donnée. Le QR ne doit pas devenir un accès direct à l'ERP ; AP Core filtre et contrôle les informations accessibles.

9. Stocks et mouvements

Réception, mise en stock, transfert interne, expédition et livraison peuvent produire des événements. La comparaison entre mouvements ERP et scans physiques peut révéler des incohérences. Deep Authenticity© doit distinguer une déclaration logistique d'une observation physique afin de conserver la provenance de chaque signal.

10. Vente et changement de statut

Une vente confirmée par un système autorisé peut déclencher les événements nécessaires au cycle de vie du produit. AP Core applique les règles de changement de statut et, lorsque prévu, de transfert numérique de propriété. L'ERP ne doit pas pouvoir forcer arbitrairement un état contraire aux politiques de confiance.

11. Seconde main et continuité après ERP

Le Passeport Numérique Universel peut continuer après la sortie du produit du système ERP initial. Les événements de seconde main, transfert, réparation ou contrôle sont gérés par l'écosystème Deep Authenticity©. L'histoire industrielle reste une composante de provenance sans devenir la seule source du cycle de vie.

12. Maintenance et systèmes EAM/CMMS

Les systèmes de gestion de maintenance peuvent transmettre inspections, interventions, changements de pièces et révisions. Les opérations sensibles doivent être associées à un acteur ou prestataire habilité. Cette continuité permet au Passeport Numérique Universel de refléter l'histoire technique d'un équipement.

13. IoT/NFC et rapprochement industriel

Les données IoT/NFC peuvent être rapprochées des événements ERP. Une machine peut signaler une production ou un capteur confirmer un passage physique. Les divergences entre systèmes deviennent des signaux d'investigation. Aucune source ne doit écraser silencieusement une preuve contradictoire.

14. AP Ledger et audit des événements critiques

Les événements industriels à forte valeur probante peuvent être ancrés dans AP Ledger : création d'un lot, activation, expédition, vente, maintenance critique ou rappel. Les volumes de télémétrie et transactions courantes peuvent rester dans leurs systèmes sources afin de préserver performance et confidentialité.

15. Online / Offline dans les sites industriels

Une usine ou un entrepôt peut subir une perte de connectivité. Les connecteurs locaux peuvent mettre en file les événements autorisés et les signer ou protéger avant resynchronisation. L'idempotence et la gestion des conflits empêchent qu'une reprise de réseau produise des activations ou mouvements en double.

16. Qualité des données

La valeur de la continuité de preuve dépend de la qualité des données sources. Les contrôles doivent détecter identifiants manquants, volumes incohérents, dates impossibles et mappings erronés. Les corrections sont tracées afin de distinguer erreur opérationnelle, rectification légitime et tentative de manipulation.

17. Cybersécurité IT/OT

L'intégration entre ERP, systèmes industriels et Deep Authenticity© crée un pont entre environnements IT et OT. Les réseaux doivent être segmentés, les flux limités et les passerelles durcies. AP Shield surveille les identités, secrets, API et anomalies sans imposer un accès direct aux équipements industriels sensibles.

18. Continuité et reprise

Une panne de Deep Authenticity© ne doit pas nécessairement arrêter une chaîne de production lorsque la politique industrielle l'autorise. Les événements peuvent être mis en attente puis réconciliés. Inversement, une panne ERP ne doit pas être interprétée comme une preuve que les produits sont invalides.

19. Gouvernance des intégrations

Chaque connecteur doit disposer d'un propriétaire, d'une version, d'un périmètre de données, d'un niveau de service et d'une procédure de retrait. Les modifications ERP doivent être testées avant production. Les responsabilités entre fabricant, intégrateur et opérateur Deep Authenticity© doivent être clairement définies.

20. Critères d'acceptation et conclusion

L'intégration ERP est cohérente si Deep Authenticity© complète sans remplacer les systèmes de gestion ; si les référentiels sont correctement rapprochés ; si création et activation des identifiants restent contrôlées ; si les trois QR codes conservent leurs rôles et VERT/JAUNE/ROUGE leur sémantique ; si stocks, ventes, maintenance et IoT/NFC produisent des événements qualifiés ; si AP Core applique les règles, AP Ledger audite les événements critiques et AP Shield protège le pont IT/OT ; si Online/Offline, qualité des données, continuité et gouvernance sont prévus.

L'intégration ERP transforme les processus industriels existants en sources structurées de continuité de preuve sans imposer la reconstruction du système d'information de l'entreprise.

Deep Authenticity© devient ainsi une couche de confiance interopérable au-dessus des infrastructures de production et de gestion déjà déployées.

Le Chapitre 16 développera l'architecture des données, des événements et des flux de confiance de Deep Authenticity©.

Note de cadrage institutionnel

L'intégration ERP et industrielle doit être conçue selon les contraintes propres à chaque site. Les interfaces avec les environnements OT exigent une segmentation et une analyse de risque spécifiques. Deep Authenticity© ne doit pas créer de dépendance susceptible d'interrompre inutilement les fonctions de sûreté ou de production essentielles.

VOLUME II — ARCHITECTURE TECHNOLOGIQUE ET CYBERSÉCURITÉ

CHAPITRE 16 — ARCHITECTURE DES DONNÉES, DES ÉVÉNEMENTS ET DES FLUX DE CONFIANCE

DONNÉES — ÉVÉNEMENTS — FLUX DE CONFIANCE — PROVENANCE — AP CORE — AP LEDGER — AP CLOUD — API — QUALITÉ — SOUVERAINETÉ — JUMEAUX NUMÉRIQUES

1. Objet du chapitre

Ce chapitre définit l'architecture des données, des événements et des flux de confiance de Deep Authenticity©. L'objectif est de transformer des informations provenant de multiples acteurs et systèmes en éléments traçables, qualifiés et interprétables, sans confondre donnée déclarée, observation, preuve cryptographique, événement validé et décision.

2. Donnée, preuve et décision

Une donnée représente une information ; une preuve apporte des éléments permettant d'en vérifier certains attributs ; une décision applique une règle ou politique à ces éléments. Deep Authenticity© sépare ces trois niveaux afin qu'une donnée reçue d'un système externe ne devienne pas automatiquement une vérité de plateforme.

3. Modèle canonique d'identité

Produits, contenus, documents, organisations, dispositifs et événements doivent pouvoir être référencés par des identifiants stables. AP Core maintient les relations entre identités locales et identités de l'écosystème. Le modèle canonique évite qu'une même entité soit interprétée comme plusieurs objets incompatibles.

4. Modèle canonique d'événement

Chaque événement doit préciser au minimum son type, son origine, l'entité concernée, son contexte temporel et son niveau d'assurance. Selon le cas, il peut inclure empreinte, signature, acteur, localisation ou référence à un événement précédent. Les schémas sont versionnés pour préserver l'interprétation historique.

5. Provenance des données

Toute donnée critique doit conserver une provenance : producteur, ERP, autorité, application, capteur, utilisateur ou autre source reconnue. La provenance permet d'évaluer la confiance et de remonter à l'origine d'une anomalie. Une donnée sans provenance suffisante peut être utilisée à titre indicatif mais doit être qualifiée comme telle.

6. Niveaux d'assurance

Les informations peuvent recevoir un niveau d'assurance selon leur mode d'obtention : déclaration, observation locale, signature cryptographique, registre institutionnel, dispositif sécurisé ou combinaison de preuves. Le niveau d'assurance ne remplace pas la décision métier ; il permet à AP Core d'appliquer une politique adaptée au risque.

7. Flux des trois QR codes

Les événements issus des trois QR codes d'Authenticity Plus© conservent leur contexte de rôle : consommateur, revendeur/professionnel et contrôle/douanes. Cette information accompagne le flux

jusqu'à AP Core. Les statuts VERT, JAUNE et ROUGE sont produits selon les règles fondamentales et ne sont pas déduits d'une simple agrégation statistique.

8. Flux du QR Code Dynamique

Le QR Code Dynamique déclenche une résolution vers l'état autorisé d'une identité persistante. La réponse peut agréger plusieurs sources, mais chaque donnée conserve sa provenance et sa fraîcheur. Dans le domaine documentaire, l'état de l'autorité émettrice reste distinct des informations secondaires enrichissant la vue.

9. Flux du Passeport Numérique Universel

Le Passeport Numérique Universel organise les événements dans le temps. Il ne doit pas devenir une succession opaque de données copiées : chaque événement reste relié à sa source, sa preuve et ses droits. Cette architecture permet de reconstruire une histoire vérifiable et de distinguer état courant et états historiques.

10. AP Core et orchestration des flux

AP Core reçoit, valide, normalise et route les événements selon les politiques de confiance. Il peut demander des preuves complémentaires, refuser un événement incompatible ou le placer en attente. L'orchestration conserve les raisons de la décision afin que le système reste auditable.

11. AP Ledger et preuves durables

Les événements nécessitant une auditabilité renforcée peuvent être ancrés dans AP Ledger. Les empreintes et références permettent de vérifier l'intégrité sans dupliquer toutes les données. Le flux opérationnel et le flux probant sont ainsi liés mais restent techniquement distincts.

12. AP Cloud et traitement distribué

AP Cloud fournit stockage, calcul, files et services de traitement. Les données peuvent être partitionnées selon domaine, sensibilité, juridiction ou performance. Les traitements distribués doivent préserver l'ordre logique des événements critiques et éviter qu'une réplication temporairement divergente crée plusieurs états définitifs.

13. API, ERP et systèmes externes

Les API et connecteurs ERP convertissent les formats externes vers les schémas de Deep Authenticity©. La normalisation ne doit pas effacer la source ni inventer une précision absente. Les erreurs de mapping, unités ou référentiels doivent être détectables avant qu'elles contaminent les analyses et passeports.

14. IoT/NFC et flux de télémétrie

Les dispositifs peuvent produire des volumes importants de données. La plateforme distingue télémétrie brute, événements significatifs et preuves à conserver. Des règles d'agrégation réduisent le volume sans perdre les événements critiques. L'identité et l'état de sécurité du dispositif accompagnent les données pertinentes.

15. Qualité, cohérence et correction

Des contrôles automatiques recherchent doublons, valeurs impossibles, séquences incohérentes et références inconnues. Une correction légitime doit être enregistrée comme telle plutôt que d'effacer silencieusement l'erreur initiale lorsque l'audit l'exige. La qualité devient une propriété mesurée du flux.

16. Temps, ordre et causalité

Un système distribué reçoit parfois les événements dans un ordre différent de leur occurrence. Deep Authenticity© distingue temps de l'action, temps de réception et temps d'ancrage. Les relations causales explicites permettent de reconstruire les séquences importantes sans supposer qu'un simple horodatage suffit toujours.

17. Confidentialité et minimisation

Les flux de confiance ne justifient pas une collecte illimitée. Les données personnelles, secrets industriels et informations souveraines doivent être minimisés, compartimentés et protégés. Des identifiants pseudonymisés, preuves sélectives et agrégations peuvent permettre l'analyse sans exposer inutilement les données unitaires.

18. Données pour IA, tableaux de bord et Jumeaux Numériques

Les données qualifiées peuvent alimenter IA/CNN, tableaux de bord et Jumeaux Numériques. Les analyses doivent conserver la traçabilité vers les sources et niveaux d'assurance. Une donnée estimée, simulée ou prédite doit rester identifiable comme telle et ne jamais être confondue avec un événement observé.

19. Fédération, souveraineté et Corridors de Confiance

Les flux peuvent traverser plusieurs organisations ou États sans centralisation complète. Des contrats de données définissent formats, preuves, autorités reconnues, niveaux d'assurance et responsabilités. Les Corridors de Confiance permettent ainsi l'échange de preuves tout en laissant les données sensibles dans leurs environnements souverains.

20. Critères d'acceptation et conclusion

L'architecture est cohérente si donnée, preuve et décision restent séparées ; si identités et événements utilisent des modèles versionnés ; si provenance et niveau d'assurance accompagnent les informations critiques ; si les flux des trois QR codes, du QR Code Dynamique et du Passeport Numérique Universel conservent leur contexte ; si AP Core orchestre, AP Ledger ancre et AP Cloud distribue ; si API, ERP et IoT/NFC préservent la source ; si qualité, temporalité et confidentialité sont gouvernées ; et si IA, tableaux de bord et Jumeaux Numériques distinguent observation, estimation et simulation.

Les flux de confiance constituent le système circulatoire informationnel de Deep Authenticity© : ils transportent non seulement des données, mais aussi leur origine, leur niveau d'assurance et leur histoire.

Cette discipline rend possible une infrastructure universelle de vérité vérifiable sans créer une base mondiale indifférenciée.

Le Chapitre 17 développera la cybersécurité globale de Deep Authenticity© : modèle de menace, défense en profondeur, sécurité applicative, opérations cyber et protection de bout en bout.

Note de cadrage institutionnel

L'architecture des données doit être adaptée aux réglementations, politiques de souveraineté et exigences sectorielles applicables. Les niveaux d'assurance, schémas d'événements et contrats de

données doivent être formalisés et versionnés. Les données simulées, prédites ou inférées doivent rester explicitement distinguées des observations et preuves sources.

VOLUME II — ARCHITECTURE TECHNOLOGIQUE ET CYBERSÉCURITÉ

CHAPITRE 17 — CYBERSÉCURITÉ GLOBALE DE DEEP AUTHENTICITY©

CYBERSÉCURITÉ — MODÈLE DE MENACE — DÉFENSE EN PROFONDEUR — ZERO TRUST — AP SHIELD — AP CORE — SÉCURITÉ APPLICATIVE — SOC — INCIDENTS — RÉSILIENCE — SOUVERAINETÉ

1. Objet du chapitre

Ce chapitre définit la cybersécurité globale de Deep Authenticity© comme une propriété transversale de l'architecture. Elle couvre les applications, AP Core, AP Ledger, AP Cloud, AP Shield, API, cryptographie, QR codes, IoT/NFC, ERP, données et opérations. L'objectif est de prévenir, détecter, contenir et récupérer face aux attaques sans dépendre d'une défense unique.

2. Modèle de menace

Le modèle de menace identifie actifs critiques, adversaires plausibles, surfaces d'attaque, scénarios d'abus et impacts. Il doit couvrir fraude, compromission de comptes, vol de clés, attaques API, falsification d'événements, logiciels malveillants, attaques de chaîne d'approvisionnement, déni de service et menaces internes.

3. Défense en profondeur

La sécurité repose sur plusieurs barrières indépendantes : identité, segmentation, chiffrement, validation, journalisation, surveillance et reprise. La compromission d'une couche ne doit pas donner automatiquement accès à toutes les autres. Les contrôles sont proportionnés à la criticité des actifs et des opérations.

4. Zero Trust et identité

Aucun utilisateur, service, terminal ou réseau n'est implicitement digne de confiance du seul fait de sa localisation. Chaque accès sensible est authentifié et autorisé selon le moindre privilège. Les identités techniques et humaines disposent de cycles de vie, révocation, authentification renforcée et surveillance adaptés.

5. Protection des trois QR codes

Les trois QR codes d'Authenticity Plus© restent la fondation anti-contrefaçon du domaine physique. Leur sécurité dépend de l'unicité, de l'état, des preuves cryptographiques et des contrôles d'usage, non du secret du motif QR. Les rôles consommateur, revendeur/professionnel et contrôle/douanes restent séparés.

6. QR Code Dynamique et surfaces de redirection

Le QR Code Dynamique ajoute une couche de résolution qui doit être protégée contre détournement, redirection malveillante et modification non autorisée. AP Core contrôle la destination logique et l'état. Les changements administratifs sensibles nécessitent authentification, journalisation et possibilité de révocation.

7. Sécurité cryptographique

Les clés privées, certificats, signatures et secrets constituent des actifs critiques. Leur protection couvre génération, stockage, utilisation, rotation, révocation et récupération. La crypto-agilité permet de remplacer un mécanisme devenu insuffisant sans reconstruire l'ensemble de la plateforme.

8. Sécurité applicative

Les applications mobiles, web et services doivent intégrer la sécurité dès la conception : validation des entrées, contrôle d'accès, gestion sûre des sessions, protection des données locales et réduction des dépendances vulnérables. Les fonctions sensibles doivent être testées contre les abus métier, pas uniquement contre les failles techniques classiques.

9. Sécurité des API

Les API sont des frontières critiques. Authentification forte, autorisation fine, quotas, validation de schémas, idempotence et journalisation réduisent les risques. Les erreurs ne doivent pas divulguer d' informations sensibles. AP Shield peut détecter des comportements anormaux et isoler une identité technique compromise.

10. Sécurité AP Cloud

AP Cloud doit appliquer segmentation, chiffrement, gestion des secrets, durcissement, supervision et séparation des environnements. Les configurations sont contrôlées et auditées. La réplication et la haute disponibilité ne remplacent pas les sauvegardes protégées contre suppression, corruption ou chiffrement malveillant.

11. Sécurité AP Ledger

Les droits d'écriture dans AP Ledger sont strictement contrôlés. L'architecture doit détecter divergences, tentatives d'altération et compromission des identités d'écriture. L'intégrité du registre ne dispense pas de vérifier la qualité de l'événement avant son inscription : une donnée fausse correctement signée reste une donnée fausse.

12. IoT/NFC et environnement industriel

Les dispositifs connectés et passerelles élargissent la surface d'attaque. Inventaire, authentification, mises à jour, segmentation et révocation sont nécessaires. Les interfaces avec les environnements OT doivent éviter qu'une compromission de la plateforme fournisse un chemin direct vers les fonctions de sûreté industrielle.

13. ERP et chaîne d'approvisionnement logicielle

Les connecteurs ERP, bibliothèques, composants tiers et pipelines de déploiement constituent une chaîne d'approvisionnement numérique. Les dépendances doivent être inventoriées, vérifiées et mises à jour. Les changements de connecteurs et configurations critiques sont soumis à contrôle et traçabilité.

14. Gestion des vulnérabilités

La plateforme doit disposer d'un processus continu d'identification, qualification, correction et vérification des vulnérabilités. Les priorités dépendent de l'exploitabilité et de l'impact, pas seulement d'un score générique. Les actifs exposés et les clés compromises nécessitent des procédures accélérées.

15. Surveillance et SOC

Les événements de sécurité sont centralisés ou fédérés vers des capacités de supervision adaptées. Le SOC recherche anomalies, corrélations et indicateurs de compromission. Les alertes doivent être priorisées pour éviter la saturation, avec des procédures d'escalade reliant équipes techniques, responsables métiers et autorités lorsque nécessaire.

16. Réponse aux incidents

Un incident doit pouvoir être contenu sans arrêter inutilement toute l'infrastructure. Les procédures prévoient qualification, isolation, préservation des preuves, remédiation, restauration et retour d' expérience. Une clé, un compte, un lot, un connecteur ou une région peuvent être suspendus de manière ciblée.

17. Sauvegarde, reprise et cyber-résilience

Les sauvegardes critiques doivent être protégées, testées et suffisamment isolées pour survivre à une compromission majeure. Les objectifs de reprise sont définis selon les services. Les exercices doivent vérifier la capacité réelle à reconstruire AP Core, données essentielles, configurations et chaînes de confiance.

18. Sécurité Online/Offline

Le mode offline protège les caches, files d'événements et identités du terminal. Après reconnexion, AP Core vérifie signatures, ordre, doublons et conflits. La capacité offline améliore la résilience mais ne doit pas permettre de contourner durablement les révocations ou politiques centrales.

19. Gouvernance, souveraineté et audits

La cybersécurité exige rôles, responsabilités, politiques, audits, exercices et amélioration continue. Les déploiements souverains peuvent imposer localisation des données, maîtrise des clés et opérations locales. La fédération permet de partager des preuves de sécurité sans exposer l'ensemble des journaux ou infrastructures nationales.

20. Critères d'acceptation et conclusion

La cybersécurité globale est cohérente si un modèle de menace est maintenu ; si défense en profondeur et Zero Trust couvrent les identités ; si les trois QR codes et le QR Code Dynamique sont protégés par l'infrastructure ; si cryptographie, applications, API, AP Cloud, AP Ledger, IoT/NFC et ERP disposent de contrôles spécifiques ; si vulnérabilités, surveillance et incidents sont gérés ; si sauvegarde, reprise et Online/Offline assurent la cyber-résilience ; et si gouvernance, audits et souveraineté sont intégrés.

La cybersécurité de Deep Authenticity© ne constitue donc pas un module ajouté après conception : elle traverse chaque couche de la chaîne de confiance.

La capacité à préserver l'intégrité de la preuve dépend autant de la prévention que de la détection, du confinement et de la reconstruction après incident.

Le Chapitre 18 développera la résilience, la haute disponibilité, la reprise et la continuité technologique de Deep Authenticity©.

Note de cadrage institutionnel

La cybersécurité doit faire l'objet d'analyses de risque, tests techniques, audits et exercices réguliers adaptés à chaque déploiement. Aucun contrôle isolé ne garantit une sécurité absolue. Les mesures doivent évoluer avec les menaces, les vulnérabilités, les usages et les obligations réglementaires.

VOLUME II — ARCHITECTURE TECHNOLOGIQUE ET CYBERSÉCURITÉ

CHAPITRE 18 — RÉSILIENCE, HAUTE DISPONIBILITÉ, REPRISE ET CONTINUITÉ TECHNOLOGIQUE

RÉSILIENCE — HAUTE DISPONIBILITÉ — CONTINUITÉ — REPRISE — REDONDANCE — AP CORE — AP CLOUD — AP LEDGER — AP SHIELD — ONLINE/OFFLINE — SOUVERAINETÉ

1. Objet du chapitre

Ce chapitre définit la résilience technologique de Deep Authenticity© comme la capacité à maintenir les fonctions essentielles, absorber les perturbations, fonctionner en mode dégradé et restaurer un état de confiance après incident. La résilience complète la cybersécurité : elle considère aussi pannes matérielles, ruptures réseau, erreurs humaines, catastrophes, défaillances de fournisseurs et indisponibilités régionales.

2. Services essentiels et priorités

Toutes les fonctions ne possèdent pas la même criticité. La vérification d'authenticité, les contrôles institutionnels, les changements de statut critiques et certaines opérations de sécurité peuvent recevoir une priorité supérieure aux traitements analytiques ou historiques. Cette classification guide redondance, reprise et allocation des ressources.

3. Haute disponibilité

La haute disponibilité vise à limiter les interruptions par redondance des composants, équilibrage de charge et bascule contrôlée. Elle doit être mesurée par service et testée dans des conditions réalistes. La présence de plusieurs serveurs ne constitue pas à elle seule une garantie si tous dépendent d'un même point de défaillance.

4. Élimination des points uniques de défaillance

Les dépendances critiques — identité, DNS, clés, bases, files, stockage, réseau ou services de résolution — doivent être analysées afin d'identifier les points uniques de défaillance. La redondance doit couvrir les dépendances réelles, y compris celles fournies par des tiers.

5. AP Core et continuité décisionnelle

AP Core constitue le moteur d'orchestration de confiance. Son architecture doit permettre la reprise ou la bascule sans produire plusieurs états contradictoires. Les opérations critiques doivent préserver idempotence, ordre logique et cohérence lors d'une transition entre instances ou régions.

6. AP Cloud et résilience distribuée

AP Cloud peut distribuer calcul, stockage et services entre plusieurs zones ou environnements. Les stratégies de réplication dépendent de la sensibilité et de la latence. Les déploiements souverains ou hybrides doivent pouvoir conserver des capacités essentielles même si une infrastructure externe devient indisponible.

7. AP Ledger et continuité de la preuve

AP Ledger doit préserver l'intégrité des preuves même pendant une panne partielle. Les écritures peuvent être mises en attente lorsque la politique le permet, puis réconciliées. La reprise doit vérifier la cohérence du registre avant de réouvrir les opérations d'écriture critiques.

8. AP Shield et continuité de sécurité

Les mécanismes de sécurité doivent rester disponibles pendant les incidents. Une bascule ne doit pas supprimer authentification, autorisation, journalisation ou protection des secrets. AP Shield doit également permettre l'isolement ciblé d'une région, d'un service ou d'une identité compromise.

9. Trois QR codes et continuité opérationnelle

Les trois QR codes d'Authenticity Plus© doivent rester exploitables selon le niveau de service disponible. En mode dégradé, certaines vérifications locales peuvent subsister grâce aux preuves cryptographiques et caches autorisés. Les rôles consommateur, revendeur/professionnel et contrôle/douanes restent distincts.

10. QR Code Dynamique et indisponibilité

Le QR Code Dynamique nécessite un service de résolution pour fournir l'état vivant. Des caches ou nœuds de proximité peuvent maintenir une réponse limitée pendant une panne. La fraîcheur doit être indiquée afin qu'une information ancienne ne soit pas confondue avec une confirmation temps réel.

11. Online / Offline comme mécanisme de résilience

L'architecture Online/Offline constitue une composante directe de la continuité. Les terminaux et sites autorisés peuvent poursuivre certaines opérations puis les synchroniser. Les limites de durée, droits et fraîcheur sont définies à l'avance afin que le mode dégradé ne devienne pas un contournement permanent.

12. Sauvegardes et copies de sécurité

La sauvegarde protège contre suppression, corruption, ransomware et erreurs logiques qui peuvent se propager aux répliques. Les copies critiques doivent être chiffrées, isolées et soumises à des politiques de rétention. Une sauvegarde non testée ne doit pas être considérée comme une capacité de reprise démontrée.

13. Objectifs de reprise

Chaque service critique doit disposer d'objectifs de temps de reprise et de perte de données tolérable adaptés à son usage. Ces objectifs doivent être réalistes, documentés et alignés avec les capacités techniques. Les fonctions institutionnelles les plus sensibles peuvent nécessiter des objectifs renforcés.

14. Reprise après sinistre

La reprise après sinistre doit permettre de reconstruire services, configurations, identités techniques, données essentielles et chaînes de confiance dans un environnement sain. Les procédures incluent ordre de restauration, vérifications d'intégrité et critères permettant de déclarer le retour à un état fiable.

15. Tests de bascule et exercices

La résilience doit être testée régulièrement. Les exercices peuvent simuler perte de région, indisponibilité réseau, corruption de données, compromission de clé ou panne d'un fournisseur. Les résultats servent à corriger les dépendances cachées et à mesurer le temps réel de rétablissement.

16. Continuité ERP, IoT/NFC et sites industriels

Les usines, entrepôts et infrastructures terrain peuvent disposer de files locales, passerelles et procédures de fonctionnement dégradé. Une panne de Deep Authenticity© ne doit pas provoquer inutilement l'arrêt d'une fonction industrielle essentielle lorsque les politiques permettent une reprise différée.

17. Résilience des API et intégrations

Les systèmes externes doivent pouvoir gérer temporisation, reprise, files et réponses d'indisponibilité sans multiplier les transactions. Les API doivent fournir des mécanismes d'idempotence et des codes d'erreur cohérents. Les partenaires doivent connaître les procédures de reprise des échanges.

18. Dépendances fournisseurs et réversibilité

Une infrastructure universelle ne doit pas dépendre irréversiblement d'un fournisseur unique. Les composants critiques doivent disposer de plans de réversibilité, formats exportables et procédures de migration lorsque cela est possible. La portabilité renforce à la fois continuité et souveraineté.

19. Résilience nationale et fédération

Des instances nationales ou institutionnelles peuvent maintenir leurs capacités essentielles tout en participant à un réseau fédéré. Si une liaison internationale est interrompue, les fonctions souveraines continuent localement puis réconcilient les preuves lorsque les échanges reprennent. Cette architecture évite qu'un incident mondial devienne automatiquement une paralysie nationale.

20. Critères d'acceptation et conclusion

La résilience est cohérente si les services essentiels sont classés ; si haute disponibilité et points uniques de défaillance sont testés ; si AP Core préserve la cohérence, AP Cloud distribue, AP Ledger protège la continuité de preuve et AP Shield maintient la sécurité ; si les trois QR codes, le QR Code Dynamique et Online/Offline disposent de modes dégradés gouvernés ; si sauvegardes et reprise sont réellement testées ; si ERP, IoT/NFC et API tolèrent les interruptions ; si la dépendance fournisseur est maîtrisée ; et si les architectures nationales peuvent continuer localement.

La résilience transforme Deep Authenticity© d'une plateforme disponible en une infrastructure capable de survivre aux perturbations sans perdre sa fonction de confiance.

Elle relie haute disponibilité, cyber-résilience, continuité opérationnelle et souveraineté technologique dans une même doctrine d'architecture.

Le Chapitre 19 développera la souveraineté technologique, la fédération des infrastructures et les modèles de déploiement nationaux et institutionnels.

Note de cadrage institutionnel

Les objectifs de disponibilité et de reprise doivent être définis pour chaque déploiement à partir d'une analyse d'impact et testés régulièrement. La redondance, la réplication et la sauvegarde répondent à

des risques différents et doivent être conçues conjointement. La résilience ne signifie pas absence d'incident, mais capacité démontrée à maintenir ou restaurer les fonctions essentielles.

VOLUME II — ARCHITECTURE TECHNOLOGIQUE ET CYBERSÉCURITÉ

CHAPITRE 19 — SOUVERAINETÉ TECHNOLOGIQUE, FÉDÉRATION ET DÉPLOIEMENTS NATIONAUX

SOUVERAINETÉ TECHNOLOGIQUE — FÉDÉRATION — DÉPLOIEMENT NATIONAL — DONNÉES — CLÉS — AP CLOUD — AP LEDGER — AP CORE — CORRIDORS DE CONFIANCE — INTEROPÉRABILITÉ

1. Objet du chapitre

Ce chapitre définit la souveraineté technologique de Deep Authenticity© comme la capacité d'un État, d'une institution ou d'un acteur autorisé à maîtriser les éléments critiques de son déploiement tout en participant à une infrastructure de confiance interopérable. La souveraineté n'implique pas l'isolement : elle organise les conditions techniques d'une coopération sans dépendance structurelle.

2. Principe de souveraineté par architecture

La souveraineté doit être conçue dans l'architecture plutôt qu'ajoutée contractuellement après déploiement. Localisation des données, maîtrise des clés, administration, journaux, politiques d'accès et capacités de reprise peuvent être répartis selon les exigences nationales. L'objectif est d'éviter qu'une autorité externe puisse devenir un point de contrôle obligatoire.

3. Fédération plutôt que centralisation mondiale

Deep Authenticity© peut fonctionner comme une fédération d'instances nationales, sectorielles ou institutionnelles. Chaque instance conserve ses données et responsabilités tout en échangeant des preuves selon des protocoles communs. Cette approche permet une infrastructure universelle sans imposer une base mondiale unique.

4. AP Core dans un déploiement souverain

Une instance souveraine d'AP Core applique les politiques de confiance et règles autorisées dans son périmètre. Les règles universelles nécessaires à l'interopérabilité sont séparées des règles nationales ou sectorielles. Cette séparation permet la compatibilité internationale sans effacer les compétences institutionnelles locales.

5. AP Cloud souverain, hybride ou fédéré

AP Cloud peut être déployé dans des infrastructures nationales, privées, hybrides ou certifiées. Les services essentiels peuvent rester localisés tandis que certains traitements non sensibles utilisent d'autres environnements. La portabilité des composants et des données réduit le verrouillage fournisseur.

6. AP Ledger et registres souverains

Les preuves critiques peuvent être ancrées dans un AP Ledger national ou institutionnel. Les autres participants n'ont pas besoin d'accéder au registre complet : des preuves ou attestations vérifiables peuvent être échangées. La fédération des ledgers doit préserver l'autorité de chaque registre sur son propre périmètre.

7. Maîtrise souveraine des clés

Les clés cryptographiques de haute sensibilité peuvent rester sous le contrôle de l'État, de l'institution ou de l'organisation compétente. Les politiques définissent génération, conservation, rotation, révocation et récupération. Une architecture fédérée doit permettre de reconnaître des autorités étrangères sans leur remettre les clés locales.

8. Trois QR codes et déploiements nationaux

Les trois QR codes d'Authenticity Plus© conservent leurs fonctions fondamentales dans chaque déploiement : consommateur, revendeur/professionnel et contrôle/douanes. Les États peuvent connecter leurs systèmes de contrôle à l'architecture sans modifier la sémantique VERT, JAUNE et ROUGE.

9. QR Code Dynamique et autorités nationales

Dans le domaine administratif, le QR Code Dynamique peut résoudre l'état d'un document auprès de l' autorité nationale compétente. L'infrastructure internationale ne se substitue pas à cette autorité. Elle fournit les mécanismes permettant à un tiers autorisé de vérifier une attestation sans exiger l'accès complet au registre source.

10. Passeport Numérique Universel et frontières

Le Passeport Numérique Universel peut accompagner un produit, document ou actif à travers plusieurs juridictions. Les événements locaux restent soumis aux autorités compétentes, tandis que les preuves interopérables assurent la continuité. La plateforme distingue clairement reconnaissance technique et reconnaissance juridique.

11. Corridors de Confiance

Un Corridor de Confiance relie deux ou plusieurs écosystèmes qui ont convenu de leurs autorités reconnues, formats, niveaux d'assurance et procédures de révocation. Il permet d'échanger des preuves de commerce, contrôle ou conformité sans créer une administration supranationale des données.

12. Passerelles de fédération

Les passerelles de fédération vérifient l'origine des demandes, traduisent les formats lorsque nécessaire et appliquent les politiques d'échange. Elles ne doivent pas devenir des points uniques de confiance mondiale. Plusieurs routes ou mécanismes de secours peuvent préserver la continuité des échanges.

13. Résolution des identités inter-domaines

Une même organisation ou entité peut être identifiée différemment dans plusieurs systèmes. Des mécanismes de résolution et d'attestation permettent de relier ces identités sans imposer un identifiant mondial unique pour tous les usages. Les correspondances doivent être gouvernées et auditables.

14. Localisation et minimisation des données

La fédération doit privilégier l'échange de la preuve nécessaire plutôt que le transfert systématique de la donnée source. Des réponses minimales, signatures, empreintes ou attestations peuvent suffire. Cette approche réduit les risques de concentration, facilite la conformité et renforce la souveraineté informationnelle.

15. Continuité en cas d'isolement

Une instance nationale doit pouvoir continuer ses fonctions essentielles même si les liaisons internationales sont interrompues. Les événements sont conservés localement puis réconciliés lorsque la connexion revient. Cette autonomie opérationnelle constitue une composante de la résilience souveraine.

16. Réversibilité technologique

Les formats, preuves, configurations et données essentielles doivent pouvoir être exportés ou migrés selon des procédures documentées. La réversibilité réduit la dépendance à un fournisseur, une région cloud ou une technologie particulière. Elle constitue un critère stratégique de souveraineté à long terme.

17. Gouvernance des standards communs

La fédération nécessite un socle de standards : schémas d'événements, formats de preuve, protocoles d'authentification et règles de compatibilité. Leur gouvernance doit permettre évolution, versionnement et participation des acteurs concernés sans créer une dépendance technique opaque.

18. Cybersécurité des échanges souverains

Les connexions entre instances sont des frontières critiques. Authentification mutuelle, chiffrement, signatures, quotas, journalisation et procédures de suspension sont nécessaires. AP Shield protège les échanges et permet d'isoler une relation compromise sans interrompre toutes les autres fédérations.

19. Modèles de déploiement institutionnel

Deep Authenticity© peut être déployée à l'échelle d'une entreprise, d'un secteur, d'une administration, d'un État ou d'un ensemble de partenaires. Chaque modèle définit responsabilités, données, clés, exploitation, continuité et interopérabilité. Le même socle architectural permet ainsi plusieurs degrés de souveraineté.

20. Critères d'acceptation et conclusion

La souveraineté technologique est cohérente si elle est intégrée à l'architecture ; si la fédération évite une centralisation mondiale obligatoire ; si AP Core, AP Cloud et AP Ledger peuvent être déployés localement ; si les clés critiques restent maîtrisables par les autorités compétentes ; si les trois QR codes, le QR Code Dynamique et le Passeport Numérique Universel restent interopérables ; si les Corridors de Confiance échangent des preuves minimales ; si continuité, réversibilité, standards et cybersécurité sont gouvernés ; et si plusieurs modèles de déploiement institutionnel sont possibles.

Deep Authenticity© peut ainsi viser l'universalité sans exiger l'uniformité : une infrastructure commune de preuve, composée d'écosystèmes capables de conserver leur autonomie technologique et institutionnelle.

La fédération transforme la souveraineté d'une logique d'isolement en capacité de coopération maîtrisée.

Le Chapitre 20 développera l'architecture technologique intégrée de Deep Authenticity© : synthèse des couches, flux de bout en bout, dépendances et modèle de référence du Volume II.

Note de cadrage institutionnel

La souveraineté technologique dépend des exigences juridiques, institutionnelles et stratégiques de chaque déploiement. Elle doit être évaluée sur l'ensemble de la chaîne : données, clés, logiciels, infrastructures, fournisseurs, compétences, opérations et capacité de reprise. La fédération n'emporte aucune reconnaissance juridique automatique entre juridictions.

VOLUME II — ARCHITECTURE TECHNOLOGIQUE ET CYBERSÉCURITÉ

CHAPITRE 20 — ARCHITECTURE TECHNOLOGIQUE INTÉGRÉE DE DEEP AUTHENTICITY©

ARCHITECTURE INTÉGRÉE — AP CORE — AP LEDGER — AP CLOUD — AP SHIELD — API — CRYPTOGRAPHIE — 3 QR CODES — QR CODE DYNAMIQUE — IA/CNN — IOT/NFC — ERP — SOUVERAINETÉ

1. Objet du chapitre

Ce chapitre clôt le Volume II en présentant le modèle technologique intégré de Deep Authenticity©. Il relie les mécanismes étudiés séparément — AP Core, AP Ledger, AP Cloud, AP Shield, API, cryptographie, signatures natives, IA/CNN, IoT/NFC, Online/Offline, ERP et architecture des données — afin de montrer comment ils forment une chaîne cohérente de confiance.

2. Principe d'architecture en couches

Deep Authenticity© est organisée en couches aux responsabilités distinctes. Les mécanismes d'accès et d'identification déclenchent la vérification ; AP Core orchestre ; la cryptographie protège ; AP Ledger audite ; AP Cloud exécute et distribue ; AP Shield sécurise ; les API interconnectent ; l'IA, l'IoT et les systèmes externes enrichissent les preuves.

3. Fondation physique : les trois QR codes

Dans le domaine physique, les trois QR codes d'Authenticity Plus© restent le mécanisme anti-contrefaçon fondamental : consommateur, revendeur/professionnel et contrôle/douanes. Leur séparation fonctionnelle structure les parcours de vérification. VERT signifie original ; JAUNE signifie original mais déjà vérifié ou vendu ; ROUGE signifie contrefaçon ou code inexistant dans le système.

4. QR Code Dynamique

Le QR Code Dynamique constitue un mécanisme transversal d'accès à un état vivant. Il relie un identifiant persistant à une information actualisée et gouvernée. Dans le domaine documentaire, il permet notamment de vérifier l'état d'un document auprès de l'autorité compétente sans transformer le QR lui-même en registre.

5. AP Core : moteur d'orchestration

AP Core constitue le cœur logique de l'architecture. Il résout les identités, applique les rôles, vérifie les preuves, détermine les statuts, orchestre les événements et contrôle les transitions. Il évite que les bases, modèles IA, ERP ou dispositifs externes deviennent individuellement des autorités universelles.

6. Passeport Numérique Universel

Le Passeport Numérique Universel organise la continuité d'identité et d'événements à travers le cycle de vie. Il relie provenance, propriété, maintenance, certifications et autres états autorisés. Il devient la mémoire opérationnelle de l'entité, tandis qu'AP Ledger fournit les ancrages probants nécessaires.

7. AP Ledger : mémoire probante

AP Ledger conserve ou ancre empreintes, signatures, horodatages et références d'événements critiques. Il ne constitue pas nécessairement une blockchain et n'a pas vocation à stocker toutes les données. Son rôle est de rendre l'histoire essentielle vérifiable et auditable.

8. AP Cloud : couche d'exécution

AP Cloud fournit calcul, stockage, files, distribution et synchronisation. Il peut être public, privé, hybride ou souverain. L'architecture dissocie la logique de confiance de l'emplacement d'hébergement afin de préserver portabilité, résilience et souveraineté.

9. AP Shield : protection transversale

AP Shield protège identités, clés, API, applications, réseaux, données, terminaux et opérations. Zero Trust, défense en profondeur, surveillance et réponse aux incidents traversent toutes les couches. La sécurité n'est pas un composant périphérique mais une propriété continue du système.

10. API : frontières programmables

Les API permettent aux modules, ERP, registres, partenaires et dispositifs d'interagir avec AP Core. Elles imposent authentification, autorisation, validation, versionnement et audit. Elles rendent l' écosystème extensible sans ouvrir directement les systèmes sources.

11. Cryptographie et signature native

Empreintes, signatures, chiffrement et horodatage constituent la grammaire technique de la preuve. Dans le domaine numérique, la signature cryptographique native des contenus établit provenance et intégrité dès la création ou l'émission. La plateforme distingue toujours authenticité cryptographique et vérité factuelle.

12. IA/CNN : couche probabiliste

L'IA/CNN analyse images, comportements et signaux faibles afin de détecter des anomalies. Elle complète les mécanismes déterministes mais ne remplace ni les trois QR codes ni les signatures. Les scores restent séparés des statuts d'authenticité et sont gouvernés selon le risque.

13. IoT/NFC : liaison objet–numérique

IoT, NFC, puces et capteurs peuvent renforcer la relation entre l'objet et son identité numérique. Les dispositifs possèdent leurs propres identités et preuves. Ils constituent une couche optionnelle adaptée aux secteurs où la valeur, le risque ou le besoin de télémétrie le justifient.

14. Online/Offline : continuité de vérification

Le mode offline permet certaines vérifications locales et opérations en file grâce aux signatures et caches sécurisés. Après reconnexion, AP Core réconcilie événements, doublons et conflits. La plateforme distingue toujours preuve locale et fraîcheur de l'état courant.

15. ERP et infrastructures industrielles

Les ERP restent les systèmes de gestion des entreprises. Deep Authenticity© reçoit des événements de production, lot, stock, vente ou maintenance par connecteurs sécurisés. Cette approche transforme les processus existants en sources de continuité de preuve sans imposer leur remplacement.

16. Architecture des données et flux de confiance

Chaque information conserve provenance, temporalité et niveau d'assurance. Donnée, preuve et décision restent séparées. Les événements circulent entre sources, AP Core, AP Cloud et AP Ledger sans perdre leur origine. Les données observées, estimées, inférées ou simulées restent explicitement distinguées.

17. Flux de bout en bout

Un flux type peut commencer par un scan, une API, un événement ERP ou un signal NFC. L'identité est résolue ; les preuves sont vérifiées ; AP Core applique les politiques ; AP Ledger peut ancrer l' événement ; AP Cloud distribue l'état ; AP Shield surveille ; le Passeport Numérique Universel est actualisé ; les systèmes autorisés reçoivent une réponse proportionnée à leur rôle.

18. Résilience et cybersécurité intégrées

Haute disponibilité, sauvegarde, reprise, mode dégradé et cyberdéfense assurent la continuité. Une panne ou compromission doit pouvoir être isolée sans détruire la chaîne entière. La résilience technique rejoint ainsi la résilience institutionnelle et la continuité de confiance.

19. Fédération et souveraineté

L'architecture intégrée peut être déployée sous forme d'instances nationales, institutionnelles ou sectorielles fédérées. Les Corridors de Confiance échangent les preuves nécessaires sans centraliser toutes les données. Les États et institutions peuvent maîtriser données, clés et infrastructures critiques tout en participant à l'interopérabilité mondiale.

20. Modèle de référence et conclusion du Volume II

Le modèle technologique du Volume II est cohérent si les trois QR codes restent la fondation physique ; si le QR Code Dynamique gère l'accès à l'état vivant ; si AP Core orchestre ; si le Passeport Numérique Universel maintient la continuité ; si AP Ledger audite ; si AP Cloud distribue ; si AP Shield protège ; si API, cryptographie et signature native sécurisent les échanges ; si IA/CNN et IoT/NFC enrichissent sans remplacer les preuves fondamentales ; si Online/Offline et ERP assurent la continuité opérationnelle ; et si données, résilience, fédération et souveraineté sont gouvernées.

Deep Authenticity© apparaît ainsi non comme une application isolée, mais comme une architecture technologique de confiance capable de relier le physique, le numérique et l'administratif.

Le Volume II établit la mécanique technique de cette infrastructure : identité, preuve, orchestration, sécurité, continuité et souveraineté.

Le Volume III pourra désormais développer les modules, usages sectoriels et déploiements opérationnels sur cette base technologique consolidée.

Note de cadrage institutionnel

Ce chapitre constitue la synthèse architecturale du Volume II. Il décrit un modèle de référence : les choix d'implémentation, standards, technologies, niveaux de disponibilité et contrôles doivent être adaptés aux secteurs et juridictions concernés, puis validés par des analyses techniques, cyber et institutionnelles appropriées.

1. Objet de la mise à niveau

Le Passeport Numérique Universel doit être traité dans le Volume II comme l'objet logique de continuité qui relie l'identité vérifiée aux événements autorisés de son cycle de vie. L'architecture technologique rend cette continuité sécurisée, distribuée, auditable et interopérable.

2. AP Core : orchestration

AP Core orchestre l'identité du Passeport Numérique Universel, ses statuts, événements, droits d' accès et relations avec les services de Deep Authenticity©. Il maintient la séparation entre donnée, preuve et décision tout en préservant le contexte de chaque événement.

3. AP Ledger : ancrage et audit

AP Ledger apporte l'ancrage, l'horodatage et l'audit nécessaires aux événements exigeant une preuve renforcée. Cela n'impose pas d'inscrire tout le contenu du passeport dans un registre unique : empreintes, références et événements critiques peuvent être ancrés tandis que les données restent dans leurs environnements autorisés.

4. AP Cloud et infrastructures souveraines

AP Cloud fournit calcul, stockage, synchronisation et distribution. Le Passeport Numérique Universel doit aussi rester compatible avec des architectures hybrides, locales et souveraines afin que son universalité n'impose jamais une centralisation mondiale des données.

5. AP Shield : protection

AP Shield protège accès, API, identités techniques, secrets, clés et opérations associés au Passeport Numérique Universel. Les événements sensibles sont soumis à autorisation, journalisation, détection d'anomalies et réponse aux incidents.

6. Cryptographie et preuves

Signatures, empreintes, horodatages, gestion des clés et attestations permettent de vérifier l'origine et l'intégrité des événements critiques. Les mécanismes précis varient selon le domaine, le secteur et le niveau d'assurance.

7. Trois QR Codes et naissance du passeport physique

Les trois QR Codes restent le mécanisme anti-contrefaçon fondateur du domaine physique. Le QR consommateur protégé par le film à gratter possède un rôle particulier : sa première activation légitime déclenche le Passeport Numérique Universel et permet son rattachement initial au premier propriétaire. Les flux techniques préservent la distinction entre QR consommateur, QR revendeur/professionnel et QR contrôle/douanes.

8. IoT, NFC et liaison objet–numérique

IoT, NFC et capteurs peuvent enrichir le Passeport Numérique Universel par des événements supplémentaires. Ils restent complémentaires aux trois QR Codes et ne les remplacent pas. Chaque donnée conserve provenance, horodatage, contexte et niveau de confiance.

9. Online/Offline

Le passeport doit fonctionner dans les scénarios de connectivité dégradée prévus par Deep Authenticity©. Offline ne signifie pas validation incontrôlée : preuves locales, droits temporaires et événements en attente doivent être réconciliés de manière sécurisée au retour de connectivité.

10. API, ERP et interopérabilité

API et connecteurs ERP permettent aux acteurs autorisés d'alimenter ou consulter le Passeport Numérique Universel. Les contrats d'interface préservent identifiant, provenance, schéma d'événement, niveau d'assurance et droits.

11. Modèle de données

Le noyau de référence distingue notamment : identité persistante, type d'actif, origine, identifiants de preuve, statut, événements horodatés, propriété et transferts lorsque pertinents, certifications, droits d'accès, références, provenance et clôture ou fin de vie. Les extensions sectorielles sont versionnées.

12. Trois domaines, trois mécanismes natifs

Dans le physique, le Passeport Numérique Universel s'articule avec les trois QR Codes. Dans le numérique, avec l'Empreinte Cryptographique Native. Dans l'administratif, avec le QR Code Dynamique documentaire. Le principe de continuité est universel ; le mécanisme de preuve source reste propre à chaque domaine.

13. Nœuds Souverains Nationaux

Les Nœuds Souverains Nationaux permettent aux États et autorités compétentes de conserver la maîtrise des données, clés, registres et règles relevant de leur souveraineté. Le Passeport Numérique Universel échange des preuves minimales entre environnements souverains sans imposer la copie générale des données.

14. Cybersécurité

Le modèle de menace couvre notamment usurpation d'identité, falsification d'événements, détournement de transfert, rejeu, compromission de clés, accès non autorisé, corruption de données et attaques contre API ou dispositifs. La défense est en profondeur.

15. Confidentialité et minimisation

Universalité ne signifie pas visibilité universelle. Le Passeport Numérique Universel sépare informations publiques, privées, professionnelles, réglementaires et souveraines. Chaque acteur n'accède qu'aux informations nécessaires et autorisées.

16. Architecture technologique de référence

Mécanisme natif de vérité → identité du Passeport Numérique Universel → AP Core pour l'orchestration → AP Ledger pour les ancrages nécessaires → AP Cloud ou infrastructure souveraine pour l'exécution → AP Shield pour la protection → API/ERP/IoT pour les interactions → Nœuds Souverains pour la fédération internationale.

17. Conclusion

Le Volume II doit faire apparaître le Passeport Numérique Universel comme un objet central de l'architecture. AP Core, AP Ledger, AP Cloud, AP Shield, cryptographie, IoT/NFC, API, ERP et cybersécurité permettent ensemble de maintenir son identité et son histoire vérifiable. La preuve

établit l'authenticité ; l'architecture protège la preuve ; le Passeport Numérique Universel conserve la continuité ; Deep Authenticity© fédère cette continuité.

RÈGLE DE CONSOLIDATION DANS LE DMC

Lors de l'assemblage final, ces développements sont absorbés dans les chapitres technologiques concernés du Volume II. Le rappel des principes fondateurs est limité à ce qui est nécessaire pour comprendre les contraintes techniques. La doctrine générale du Passeport Numérique Universel reste exposée une seule fois dans le chapitre fondateur placé dans l'ouverture du Livre Blanc.

INVARIANT DU VOLUME II

Les trois QR Codes restent la fondation anti-contrefaçon du domaine physique ; l'Empreinte Cryptographique Native reste le mécanisme natif du domaine numérique ; le QR Code Dynamique reste le mécanisme natif du domaine administratif. Le Passeport Numérique Universel assure la continuité de l'identité et des événements. Les couches technologiques rendent cette continuité sécurisée, distribuée, auditable, résiliente et interopérable.

LIVRE BLANC 2026

DEEP AUTHENTICITY©

VOLUME III

ÉCOSYSTÈME ÉCONOMIQUE, COMMERCIAL ET FINANCIER

Document maître consolidé — 26 chapitres

Édition 2026

DOCTRINE TRANSVERSALE — TRILOGIE DE LA VÉRITÉ

1. Les 3 QR Codes — vérité du produit physique

Consommateur, Revendeur/Professionnel et Contrôle/Douanes constituent le socle anti-contrefaçon du domaine physique. La lecture utilisateur demeure : VERT = original ; JAUNE = original mais déjà vérifié ou vendu ; ROUGE = contrefait ou code inexistant dans Authenticity Plus©.

2. Empreinte Cryptographique Native — vérité de l'information et des médias

Elle constitue le sésame de l'information et des médias : une identité cryptographique native permettant de vérifier provenance et intégrité des contenus numériques, en articulation avec la signature cryptographique native lorsque l'identité de l'émetteur doit être attestée.

3. QR Code Dynamique — vérité du document vérifiable

Il constitue le sésame du document : le support peut rester stable tandis que le statut vérifiable peut évoluer selon l'autorité compétente — valide, expiré, révoqué, remplacé ou autre état gouverné.

Cette Trilogie de la Vérité constitue désormais une doctrine transversale permanente de Deep Authenticity© couvrant les domaines physique, numérique et administratif.

SOMMAIRE DU VOLUME III

CHAPITRE 1 — ARCHITECTURE GÉNÉRALE DE L'ÉCOSYSTÈME ÉCONOMIQUE, COMMERCIAL ET FINANCIER

CHAPITRE 2 — PRODUCTEUR : IDENTITÉ ÉCONOMIQUE, ACTIVATION ET TABLEAU DE BORD

CHAPITRE 3 — REVENDEUR : QR PROFESSIONNEL, FENÊTRE REVENDEUR ET STOCKS AUTHENTIFIÉS

CHAPITRE 4 — PREMIER ACQUÉREUR : ACHAT AUTHENTIFIÉ ET NAISSANCE DE LA PROPRIÉTÉ NUMÉRIQUE

CHAPITRE 5 — SECONDE MAIN : MARCHÉ SECONDAIRE AUTHENTIFIÉ ET CONTINUITÉ DE PROVENANCE

CHAPITRE 6 — TRANSFERT NUMÉRIQUE SÉCURISÉ DE PROPRIÉTÉ

CHAPITRE 7 — PROPRIÉTÉ : REGISTRE DES RELATIONS PATRIMONIALES ET CONTINUITÉ DES DROITS

CHAPITRE 8 — AP BUSINESS : INFRASTRUCTURE COMMERCIALE DE CONFIANCE

CHAPITRE 9 — RECHERCHE COMMERCIALE ET LOCALISATION DU REVENDEUR LE PLUS PROCHE

CHAPITRE 10 — ARTISANS, AGRICULTEURS, ÉLEVEURS, ARTISTES, CRÉATEURS, INNOVATEURS ET PME

CHAPITRE 11 — AP FINANCE : ARCHITECTURE FINANCIÈRE DE CONFIANCE

CHAPITRE 12 — AP PAY : PAIEMENT, RÈGLEMENT ET ORCHESTRATION DES FLUX

CHAPITRE 13 — AP PAY ET PAIEMENTS TRANSFRONTALIERS : CORRIDORS FINANCIERS DE CONFIANCE

CHAPITRE 14 — TRAÇABILITÉ ÉCONOMIQUE : RAPPROCHEMENT PRODUIT–TRANSACTION–PROPRIÉTÉ

CHAPITRE 15 — SAAS : MODÈLE DE SERVICES, ABONNEMENTS ET ACCESSIBILITÉ

CHAPITRE 16 — LICENCES : DROITS D'USAGE, PROPRIÉTÉ INTELLECTUELLE ET GOUVERNANCE

CHAPITRE 17 — ROYALTIES : ASSIETTES, TAUX, GOUVERNANCE ET AUDIT

CHAPITRE 18 — MODÈLE ÉCONOMIQUE CONSOLIDÉ : CRÉATION DE VALEUR ET SOUTENABILITÉ

CHAPITRE 19 — TABLEAUX DE BORD ÉCONOMIQUES ET COMMERCIAUX

CHAPITRE 20 — INTELLIGENCE ÉCONOMIQUE PRÉDICTIVE : ANTICIPER LES TENSIONS ET LES BESOINS

CHAPITRE 21 — VALEUR ÉCONOMIQUE DES DONNÉES AGRÉGÉES : CONNAISSANCE, SOUVERAINETÉ ET GOUVERNANCE

CHAPITRE 22 — SOUVERAINETÉ ÉCONOMIQUE ET COMMERCIALE : RÉSILIENCE, AUTONOMIE ET COMMERCE DE CONFIANCE

CHAPITRE 23 — CORRIDORS COMMERCIAUX DE CONFIANCE : COOPÉRATION, RECONNAISSANCE ET INTEROPÉRABILITÉ

CHAPITRE 24 — CRÉATION DE VALEUR POUR LES ACTEURS : CONFIANCE, EFFICACITÉ ET EFFETS DE RÉSEAU

CHAPITRE 25 — STRATÉGIE D'ADOPTION ÉCONOMIQUE : PILOTES, INCITATIONS ET PASSAGE À L'ÉCHELLE

MISE À NIVEAU TRANSVERSALE — PASSEPORT NUMÉRIQUE UNIVERSEL

Continuité économique, commerciale et patrimoniale

Le Volume III consacre le Passeport Numérique Universel comme référence persistante de l'actif à travers sa vie économique. Le producteur initialise l'identité du produit ; la première activation légitime du QR Code Consommateur protégé par le film à gratter déclenche le passeport et permet son rattachement initial au premier propriétaire selon les règles applicables.

Le premier acquéreur ouvre ainsi une continuité patrimoniale sans fusionner paiement, vente et propriété. Le Passeport Numérique Universel conserve l'identité du même actif lorsque la relation de propriété évolue.

Lors d’un transfert numérique sécurisé, le titulaire reconnu peut changer tandis que l’identité persistante du produit et l’historique autorisé demeurent. Le transfert ne crée pas un nouvel actif. Il prolonge la continuité du même produit. Le paiement, à lui seul, ne vaut pas nécessairement transfert patrimonial.

La Seconde Main devient une extension naturelle de cette continuité : provenance, statut, interventions, réparations et événements autorisés peuvent accompagner la revente, tandis que les données privées des propriétaires précédents restent protégées.

AP Business peut utiliser le Passeport Numérique Universel comme référence commune entre producteur, distributeur, revendeur, prestataire et client. La Fenêtre Revendeur et la recherche de proximité exploitent uniquement les informations nécessaires à la fonction commerciale ; elles ne remplacent pas le passeport.

AP Finance et AP Pay peuvent relier une opération financière ou un paiement à l’identité vérifiée de l’ actif. Ils ne se substituent ni au Passeport Numérique Universel, ni aux infrastructures financières autorisées, ni aux obligations réglementaires applicables.

Garantie, maintenance, réparation, assurance, réemploi, reconditionnement, recyclage et fin de vie peuvent devenir des événements du Passeport Numérique Universel. Cette continuité améliore l’ information disponible sur l’histoire de l’actif sans garantir une valeur marchande déterminée.

Invariant : les trois QR Codes restent le mécanisme anti-contrefaçon fondateur du domaine physique. Le Passeport Numérique Universel prolonge cette protection dans le temps en reliant l’actif authentifié à son histoire économique et patrimoniale.

CHAPITRE 26 — CONCLUSION STRATÉGIQUE DU VOLUME III : DE LA CONFIANCE À L’ÉCONOMIE VÉRIFIABLE

CHAPITRE 1 — ARCHITECTURE GÉNÉRALE DE L'ÉCOSYSTÈME ÉCONOMIQUE, COMMERCIAL ET FINANCIER

ÉCOSYSTÈME ÉCONOMIQUE — PRODUCTEUR — REVENDEUR — PREMIER ACQUÉREUR — SECONDE MAIN — PROPRIÉTÉ — AP BUSINESS — AP FINANCE — AP PAY — SAAS — LICENCES — ROYALTIES

1. Objet du chapitre

Ce chapitre ouvre le Volume III et définit l'architecture économique, commerciale et financière de Deep Authenticity©. Il montre comment l'infrastructure de confiance établie dans les Volumes I et II accompagne un produit depuis sa création par le producteur jusqu'à ses ventes, transferts successifs, services commerciaux et opérations financières autorisées.

2. De la preuve à l'activité économique

L'authenticité ne constitue pas une fin isolée. Une fois l'identité d'un produit établie, Deep Authenticity© peut relier les événements économiques qui l'accompagnent : mise sur le marché, distribution, vente, acquisition, transfert de propriété, seconde main, maintenance et services. La preuve devient ainsi une infrastructure de continuité commerciale.

3. Le producteur comme origine économique

Le producteur crée ou fait enregistrer l'identité du produit et initie son Passeport Numérique Universel. Son tableau de bord peut suivre production, lots, activation, distribution, ventes, alertes, rappels et statistiques. Il demeure la source de référence pour les informations industrielles qu'il est habilité à déclarer.

4. Les trois QR codes dans le circuit commercial

Les trois QR codes d'Authenticity Plus© restent la fondation du domaine physique. Le QR consommateur sert à la vérification par l'acheteur ; le QR revendeur/professionnel permet l'intégration du produit au circuit commercial autorisé ; le QR contrôle/douanes soutient les opérations institutionnelles. Leurs rôles restent strictement distincts.

5. Le revendeur et la mise en visibilité commerciale

Le revendeur authentifié peut enregistrer les produits qu'il détient selon les droits prévus. La Fenêtre Revendeur permet à l'écosystème de relier disponibilité commerciale et preuve d'authenticité. Un consommateur peut ainsi rechercher un produit et, lorsque les données sont disponibles, identifier les revendeurs autorisés ou les plus proches qui le proposent.

6. Le premier acquéreur

La première vente marque une transition importante entre circulation commerciale et propriété. Après les vérifications prévues, le premier acquéreur peut être associé au produit dans le système de propriété numérique. Cette association doit respecter la minimisation des données et ne signifie pas que des informations personnelles deviennent publiques.

7. Propriété et preuve de possession

Deep Authenticity© distingue l'identité du produit, la possession opérationnelle et les droits juridiques de propriété. Le système peut enregistrer une preuve numérique de transfert ou de détention lorsque le cadre le permet. Cette preuve renforce la continuité du cycle de vie sans se substituer aux règles légales applicables.

8. Transfert numérique sécurisé de propriété

Le transfert de propriété constitue un mécanisme central du Volume III. Il relie l'ancien détenteur, le nouvel acquéreur et l'identité persistante du produit par une opération authentifiée, autorisée et traçable. AP Core vérifie la cohérence du transfert et AP Ledger peut ancrer l'événement critique.

9. Seconde main authentifiée

Le marché secondaire prolonge la valeur du Passeport Numérique Universel. Un produit authentique peut être proposé à la revente avec son historique autorisé, puis transféré au nouvel acquéreur. La Fenêtre Seconde Main permet de distinguer les actifs disposant d'une continuité de preuve de ceux dont la provenance est incomplète.

10. AP Business

AP Business constitue la couche de services commerciaux de Deep Authenticity©. Elle peut réunir recherche de produits, visibilité des revendeurs, relations B2B/B2C, services aux producteurs, gestion d'opportunités et accès à des informations commerciales autorisées. Elle exploite la confiance créée par AP Core sans devenir une place de marché obligatoire.

11. AP Finance

AP Finance étend la continuité de preuve vers les opérations financières liées aux activités économiques. Son rôle est de relier, lorsque cela est autorisé, identité des acteurs, transaction, produit, événement économique et preuves nécessaires. Il doit rester compatible avec les institutions financières, obligations réglementaires et systèmes de paiement existants.

12. AP Pay

AP Pay constitue la couche de paiement et de règlement envisagée dans l'écosystème. Elle peut orchestrer des paiements liés à des produits ou services vérifiés et faciliter le rapprochement entre transaction et événement commercial. Elle ne remplace pas automatiquement les banques, réseaux de paiement ou infrastructures réglementées : elle doit s'y intégrer selon les juridictions.

13. Paiements transfrontaliers et interopérabilité

Pour les échanges internationaux, AP Pay peut servir de couche d'orchestration et de preuve autour des infrastructures financières autorisées. Les Corridors de Confiance peuvent relier acteurs commerciaux, autorités et prestataires financiers. Les mécanismes de conformité, change, règlement et contrôle restent ceux exigés par les cadres applicables.

14. Rapprochement produit–transaction–propriété

L'une des valeurs majeures du modèle réside dans la possibilité de relier trois continuités : l'identité du produit, l'événement commercial et la propriété numérique. Ce rapprochement réduit les zones d' opacité et permet, avec les droits appropriés, de vérifier qu'une transaction correspond à un actif identifié et à une transition cohérente.

15. SaaS

Le modèle SaaS permet de proposer des capacités de Deep Authenticity© sous forme de services numériques adaptés aux producteurs, revendeurs, entreprises et institutions. Les offres peuvent varier selon volume, fonctionnalités, niveau de service, intégrations et exigences de souveraineté. Le SaaS constitue un mode d'accès économique, non l'unique modèle de déploiement.

16. Licences

Les licences permettent l'utilisation de technologies, modules ou capacités de Deep Authenticity© dans des périmètres définis : entreprise, secteur, territoire ou institution. Les contrats doivent préciser droits, durée, support, sécurité, propriété intellectuelle et conditions d'interopérabilité.

17. Royalties

Les royalties constituent un mécanisme possible de rémunération lié à l'utilisation, aux volumes ou à la valeur créée par certaines capacités protégées. Leur structure doit être transparente, mesurable et contractuellement définie. Les taux ne doivent pas être considérés comme universels : ils peuvent varier selon secteurs, modèles de licence et stratégie de déploiement.

18. Modèle économique multi-acteurs

L'écosystème peut combiner abonnements SaaS, licences, royalties, services d'intégration, certifications et autres prestations autorisées. Les producteurs, revendeurs, institutions et partenaires n'ont pas nécessairement le même modèle tarifaire. La soutenabilité économique doit préserver accessibilité, sécurité et capacité de déploiement à grande échelle.

19. Commerce éthique et souveraineté économique

En reliant authenticité, provenance, propriété et transaction, Deep Authenticity© peut contribuer à réduire l'économie de la contrefaçon et à améliorer la transparence des circuits commerciaux. Pour les États, l'enjeu concerne également souveraineté économique, protection des producteurs, formalisation des échanges et qualité des données économiques, dans le respect des compétences institutionnelles.

20. Critères d'acceptation et conclusion

L'écosystème du Volume III est cohérent si le producteur initie l'identité économique ; si les trois QR codes restent la fondation du commerce physique ; si le revendeur dispose d'un parcours professionnel distinct ; si le premier acquéreur peut devenir le point de départ d'une chaîne de propriété ; si transfert et seconde main conservent la continuité du Passeport Numérique Universel ; si AP Business structure les services commerciaux ; si AP Finance et AP Pay s'intègrent aux cadres financiers existants ; si SaaS, licences et royalties forment des modèles économiques gouvernés ; et si la souveraineté économique reste compatible avec l'interopérabilité.

Le Volume III transforme ainsi l'infrastructure de vérité en infrastructure de confiance économique : l' objet authentifié devient un actif capable de conserver une continuité commerciale, patrimoniale et financière.

Le Chapitre 2 développera le Producteur : création de l'identité économique du produit, activation, tableau de bord producteur, statistiques, alertes et pilotage du cycle commercial.

Note de cadrage institutionnel

Ce volume décrit une architecture économique et fonctionnelle. Les services financiers, paiements, transferts de propriété, licences et royalties doivent être adaptés aux lois, réglementations, obligations fiscales, financières, de protection des consommateurs et de propriété applicables dans chaque juridiction. Deep Authenticity© fournit une infrastructure de preuve et d'orchestration ; elle ne confère pas automatiquement un statut juridique ou financier réglementé.

CHAPITRE 2 — PRODUCTEUR : IDENTITÉ ÉCONOMIQUE, ACTIVATION ET TABLEAU DE BORD

PRODUCTEUR — IDENTITÉ PRODUIT — 3 QR CODES — ACTIVATION — PASSEPORT NUMÉRIQUE UNIVERSEL — TABLEAU DE BORD — STATISTIQUES — ALERTES — RAPPELS — PILOTAGE COMMERCIAL

1. Objet du chapitre

Ce chapitre définit la place du producteur dans l'écosystème économique de Deep Authenticity©. Le producteur constitue l'origine industrielle et économique du produit : il crée ou fait enregistrer son identité, associe les preuves nécessaires, initialise son Passeport Numérique Universel et pilote son entrée dans le circuit commercial.

2. Identité numérique du producteur

Avant de créer des produits, le producteur doit disposer d'une identité organisationnelle vérifiée et d' habilitations adaptées. AP Core relie cette identité à ses marques, sites, gammes, opérateurs et systèmes autorisés. Les actions sensibles restent attribuables à une identité humaine ou technique selon le contexte.

3. Référentiel produit

Le producteur déclare les références, variantes, caractéristiques, lots et autres informations nécessaires à l'identification. Le référentiel constitue la base commune entre production, ERP, Passeport Numérique Universel et services commerciaux. Toute modification importante doit être versionnée afin de préserver l'histoire.

4. Création de l'identité économique unitaire

Chaque unité protégée reçoit une identité persistante reliée à sa référence et, le cas échéant, à son lot ou numéro de série. Cette identité devient le point d'ancrage des événements futurs : activation, distribution, vente, propriété, seconde main, maintenance, contrôle et rappel.

5. Génération et affectation des trois QR codes

Les trois QR codes d'Authenticity Plus© sont affectés selon leurs rôles : consommateur, revendeur/professionnel et contrôle/douanes. Leur génération et leur association à l'unité doivent être contrôlées. Aucun QR ne doit exposer une clé privée ni permettre de déduire les secrets des autres codes.

6. Activation contrôlée

La création d'un identifiant ne signifie pas automatiquement qu'un produit existe physiquement. L' activation intervient après un événement industriel autorisé confirmant l'existence de l'unité ou du lot. Cette séparation limite l'utilisation frauduleuse de codes générés mais jamais associés à une production réelle.

7. Passeport Numérique Universel à l'origine

Le producteur initialise le Passeport Numérique Universel avec les informations qu'il est habilité à fournir : origine, référence, lot, caractéristiques, certifications ou autres éléments applicables. Les événements ultérieurs complètent ce passeport sans permettre au producteur d'effacer silencieusement l'histoire déjà validée.

8. Tableau de bord Producteur

Le tableau de bord Producteur constitue le poste de pilotage de ses produits dans Deep Authenticity©. Il agrège production enregistrée, activations, distribution, scans, ventes, alertes, retours, rappels et autres événements autorisés. Les vues doivent être filtrables par période, gamme, produit, lot, région et canal.

9. Indicateurs de production et activation

Le producteur peut suivre quantités créées, identifiants générés, unités activées, unités non activées, lots ouverts ou clôturés et écarts entre production ERP et activation Deep Authenticity©. Ces indicateurs permettent de détecter des anomalies avant la mise sur le marché.

10. Cartographie de distribution

Lorsque les données sont disponibles et légalement utilisables, le tableau de bord peut visualiser les mouvements et zones de distribution. L'objectif est d'identifier les circuits réels, retards, détournements ou marchés inattendus. Les informations individuelles sont minimisées et les vues peuvent être agrégées.

11. Statistiques de scans

Les scans peuvent être analysés par rôle, période, zone, produit ou lot. Le producteur peut observer l' intensité des vérifications sans accéder automatiquement à l'identité personnelle des consommateurs. Des répétitions anormales ou incohérences géographiques peuvent alimenter les mécanismes d'alerte.

12. Alertes anti-contrefaçon

Des scans ROUGES, codes inexistants, répétitions incompatibles ou signaux IA/CNN peuvent déclencher des alertes. Le producteur reçoit un niveau de risque et les éléments disponibles pour investigation. Une alerte algorithmique reste distincte d'une décision institutionnelle de contrefaçon lorsque celle-ci exige un contrôle formel.

13. Statuts VERT / JAUNE / ROUGE

La lecture reste uniforme : VERT signifie original ; JAUNE signifie original mais déjà vérifié ou vendu ; ROUGE signifie contrefaçon ou code inexistant dans Authenticity Plus©. Le tableau de bord peut présenter les volumes et tendances associés sans modifier cette sémantique fondamentale.

14. Ventes et premier acquéreur

Lorsque la vente est confirmée par un canal autorisé, le tableau de bord peut enregistrer la transition vers le premier acquéreur et le nouveau statut du produit. Le producteur peut suivre les ventes agrégées sans disposer automatiquement des données personnelles de l'acheteur.

15. Rappels et alertes qualité

Le producteur peut cibler un produit, lot ou série pour publier un rappel, une alerte de sécurité, une révision ou une information de maintenance. Le Passeport Numérique Universel et le QR Code Dynamique permettent de diffuser l'état actualisé aux acteurs autorisés. Chaque campagne reste traçable.

16. Analyse commerciale et demande

Les données agrégées de distribution, scans et ventes peuvent aider à comprendre la demande, les zones de forte activité, les ruptures potentielles ou les écarts entre expédition et consommation. Ces

analyses soutiennent le pilotage commercial sans transformer Deep Authenticity© en système de surveillance des consommateurs.

17. AP Business et visibilité des revendeurs

Le producteur peut utiliser AP Business pour structurer son réseau commercial et rendre visibles les revendeurs autorisés disposant de ses produits. La disponibilité peut être alimentée par les revendeurs ou systèmes intégrés. Cette visibilité améliore la rencontre entre demande authentifiée et offre vérifiée.

18. ERP, API et automatisation

Les grandes entreprises peuvent connecter ERP, MES, WMS ou autres systèmes par API afin d' automatiser création, activation et événements logistiques. Les petits producteurs peuvent utiliser des interfaces simplifiées. Deep Authenticity© doit ainsi rester accessible à la fois aux industries et aux artisans ou petites structures.

19. Gouvernance, confidentialité et droits

Le producteur ne possède pas un droit illimité sur toutes les données générées autour de ses produits. Les accès sont définis selon finalité, rôle, réglementation et consentements applicables. Les données commerciales sensibles, informations personnelles et preuves institutionnelles sont compartimentées.

20. Critères d'acceptation et conclusion

Le parcours Producteur est cohérent si son identité est vérifiée ; si les référentiels sont versionnés ; si chaque unité peut recevoir une identité persistante ; si les trois QR codes sont générés et affectés de manière contrôlée ; si création et activation sont séparées ; si le Passeport Numérique Universel commence à l'origine ; si le tableau de bord couvre production, activation, scans, alertes, ventes et rappels ; si VERT/JAUNE/ROUGE restent inchangés ; si AP Business, ERP et API sont intégrables ; et si confidentialité et gouvernance limitent les accès.

Le producteur devient ainsi le premier acteur de la chaîne économique de confiance : il ne se contente plus de fabriquer un produit, il initialise une identité capable d'accompagner celui-ci pendant tout son cycle de vie.

Le Chapitre 3 développera le Revendeur : intégration commerciale, QR professionnel, Fenêtre Revendeur, stocks authentifiés et relation avec le consommateur.

Note de cadrage institutionnel

Le tableau de bord Producteur doit appliquer les règles de minimisation, confidentialité et séparation des rôles. Les statistiques et alertes constituent des instruments de pilotage ; elles ne confèrent pas automatiquement au producteur un droit d'accès aux données personnelles des acquéreurs ni une compétence institutionnelle de sanction.

CHAPITRE 3 — REVENDEUR : QR PROFESSIONNEL, FENÊTRE REVENDEUR ET STOCKS AUTHENTIFIÉS

REVENDEUR — QR PROFESSIONNEL — FENÊTRE REVENDEUR — STOCKS AUTHENTIFIÉS — VISIBILITÉ COMMERCIALE — PROXIMITÉ — AP BUSINESS — VENTE — PREMIER ACQUÉREUR — TRAÇABILITÉ

1. Objet du chapitre

Ce chapitre définit le rôle du revendeur dans l'écosystème économique de Deep Authenticity©. Le revendeur constitue l'interface entre la distribution professionnelle et l'acquisition par le consommateur. Son environnement doit permettre d'intégrer les produits authentifiés, gérer leur présence commerciale, confirmer les ventes et contribuer à la continuité du Passeport Numérique Universel.

2. Identité professionnelle du revendeur

Le revendeur dispose d'une identité professionnelle vérifiée, reliée à ses établissements, points de vente, opérateurs et systèmes autorisés. AP Core applique les habilitations correspondant à son rôle. L'accès professionnel est distinct du parcours consommateur afin d'éviter qu'une fonction commerciale sensible soit disponible à une identité non autorisée.

3. Le QR revendeur/professionnel

Parmi les trois QR codes d'Authenticity Plus©, le QR revendeur/professionnel permet l'intégration du produit dans l'environnement commercial du revendeur. Il confirme la relation entre une unité identifiée et un acteur professionnel autorisé. Il ne remplace ni le QR consommateur ni le QR contrôle/douanes.

4. Entrée du produit dans le stock authentifié

Lors de la réception, le revendeur peut scanner ou importer les produits afin de les inscrire dans son stock authentifié. AP Core vérifie identité, statut et cohérence de l'événement. Un produit déjà affecté à un circuit incompatible, signalé ou inexistant doit déclencher une réponse adaptée avant sa mise en vente.

5. Fenêtre Revendeur

La Fenêtre Revendeur constitue l'espace commercial dédié au professionnel dans Deep Authenticity©. Elle présente les produits authentifiés détenus, leurs références, quantités, statuts, alertes et informations commerciales autorisées. Elle devient le point de liaison entre stock vérifié, visibilité commerciale et parcours du consommateur.

6. Gestion des stocks

Les entrées, sorties, réservations, ventes, retours et transferts entre établissements peuvent être enregistrés directement ou synchronisés depuis un ERP. Le système distingue stock déclaré et preuve physique issue d'un scan ou autre événement. Les divergences deviennent des signaux à examiner plutôt que des corrections silencieuses.

7. Visibilité des produits disponibles

Le revendeur peut choisir de rendre visibles certains produits disponibles dans AP Business. La publication doit refléter un stock suffisamment récent et indiquer les conditions pertinentes. Deep

Authenticity© ne doit pas présenter comme disponible un produit dont l'information n'a pas été actualisée selon la politique définie.

8. Recherche par le consommateur

Un consommateur recherchant un produit peut accéder aux revendeurs qui déclarent le proposer et qui répondent aux critères de confiance. Cette recherche relie l'authenticité à l'utilité commerciale : vérifier un produit et savoir où l'acquérir dans un circuit reconnu deviennent deux fonctions complémentaires.

9. Localisation du revendeur le plus proche

Lorsque l'utilisateur autorise la localisation et que les données du revendeur sont disponibles, AP Business peut classer les points de vente selon la proximité. La fonction doit utiliser uniquement les informations nécessaires et permettre des recherches par zone sans exiger une localisation précise lorsque celle-ci n'est pas indispensable.

10. Fiche commerciale du revendeur

Une fiche peut présenter identité professionnelle, établissement, catégories de produits, horaires ou informations commerciales autorisées. La présence dans l'écosystème ne constitue pas automatiquement une certification de toutes les pratiques du commerçant. Les badges ou niveaux de confiance doivent correspondre à des critères explicites.

11. Vérification avant vente

Avant la vente, le revendeur peut vérifier que l'unité correspond à son stock et qu'aucune alerte ne bloque l'opération. Cette étape limite la circulation de produits substitués ou de codes réutilisés. Elle peut être automatisée dans les systèmes de caisse ou ERP lorsque l'intégration est disponible.

12. Confirmation de la vente

La vente constitue un événement majeur du cycle de vie. Le système enregistre la sortie du stock professionnel et applique les règles correspondantes au statut du produit. Cette confirmation prépare, lorsque prévu, la relation avec le premier acquéreur et le transfert numérique de propriété.

13. Statuts VERT / JAUNE / ROUGE

La sémantique fondamentale reste inchangée : VERT signifie original ; JAUNE signifie original mais déjà vérifié ou vendu ; ROUGE signifie contrefaçon ou code inexistant dans Authenticity Plus©. Le revendeur dispose d'informations professionnelles complémentaires, mais celles-ci ne redéfinissent jamais ces trois statuts.

14. Retours et annulations

Un retour commercial ou une annulation ne doit pas simplement effacer la vente précédente. Deep Authenticity© enregistre un nouvel événement et applique une politique déterminant si le produit peut revenir en stock vendable, nécessite une inspection ou conserve un état particulier. Cette approche protège l'historique.

15. Alertes, rappels et blocages

Le revendeur peut recevoir des alertes du producteur ou d'une autorité concernant un produit, lot ou série. Un rappel, une suspension ou un contrôle renforcé peut empêcher temporairement une vente. La Fenêtre Revendeur doit rendre ces informations visibles avant l'opération commerciale.

16. AP Business et réseau commercial

AP Business peut permettre au producteur et aux revendeurs autorisés d'organiser un réseau commercial vérifiable. Les professionnels peuvent être reliés aux gammes qu'ils distribuent, tandis que les consommateurs disposent d'un moyen de trouver une offre authentifiée. Deep Authenticity© reste une infrastructure de confiance et ne devient pas nécessairement le vendeur contractuel.

17. ERP, caisse et API

Les revendeurs structurés peuvent connecter ERP, gestion de stock ou caisse par API. Les petits commerces peuvent utiliser l'application directement. Les intégrations doivent préserver idempotence, sécurité et séparation des rôles afin qu'une erreur de caisse ne produise pas plusieurs ventes ou transferts.

18. Tableau de bord Revendeur

Le tableau de bord peut présenter stocks authentifiés, ventes, produits les plus recherchés, alertes, retours, rotations, demandes locales et indicateurs de disponibilité. Ces données aident le professionnel à piloter son activité et peuvent alimenter, sous forme agrégée, les analyses de la chaîne commerciale.

19. Confidentialité et concurrence

Les données de stock, prix, ventes et performance peuvent être commercialement sensibles. Les producteurs, concurrents ou autres acteurs ne doivent pas y accéder automatiquement. Les règles de partage doivent être explicites et permettre des statistiques agrégées lorsque l'objectif ne nécessite pas la divulgation des données détaillées.

20. Critères d'acceptation et conclusion

Le parcours Revendeur est cohérent si l'identité professionnelle est vérifiée ; si le QR revendeur/professionnel conserve sa fonction spécifique ; si les produits reçus peuvent entrer dans un stock authentifié ; si la Fenêtre Revendeur relie stock, alertes et visibilité commerciale ; si le consommateur peut rechercher les revendeurs et, avec les autorisations nécessaires, le plus proche ; si la vente est enregistrée comme événement ; si VERT/JAUNE/ROUGE restent inchangés ; si retours, rappels, ERP, caisse et API sont gérés ; et si la confidentialité commerciale est protégée.

Le revendeur devient ainsi un maillon actif de la chaîne de confiance : il ne distribue plus seulement un produit, il participe à la continuité vérifiable entre origine, disponibilité, vente et acquisition.

Le Chapitre 4 développera le Premier acquéreur : achat authentifié, activation de la relation de propriété, droits numériques et entrée dans le cycle patrimonial.

Note de cadrage institutionnel

La Fenêtre Revendeur et les fonctions de proximité doivent respecter les règles applicables de protection des données, de concurrence et de commerce. La présence d'un produit dans un stock déclaré ne constitue pas, à elle seule, une garantie absolue de disponibilité physique ; les politiques de fraîcheur et les événements de vérification doivent être explicitement distingués.

CHAPITRE 4 — PREMIER ACQUÉREUR : ACHAT AUTHENTIFIÉ ET NAISSANCE DE LA PROPRIÉTÉ NUMÉRIQUE

PREMIER ACQUÉREUR — ACHAT AUTHENTIFIÉ — PROPRIÉTÉ NUMÉRIQUE — PREUVE D'ACQUISITION — PASSEPORT NUMÉRIQUE UNIVERSEL — TRANSFERT — 3 QR CODES — AP CORE — AP LEDGER — CONFIDENTIALITÉ

1. Objet du chapitre

Ce chapitre définit le rôle du premier acquéreur dans l'écosystème économique de Deep Authenticity©. La première acquisition constitue le passage entre le cycle commercial initial du produit et son cycle patrimonial. L'objectif est de relier un produit authentifié à une acquisition vérifiable, puis d'ouvrir une continuité de propriété sans exposer inutilement l'identité personnelle de l'acheteur.

2. Définition du premier acquéreur

Le premier acquéreur est la première personne ou organisation qui reçoit le produit à l'issue d'une vente ou cession reconnue par le système. Il doit être distingué du simple utilisateur, du payeur et du bénéficiaire lorsque ces rôles diffèrent. Cette distinction permet d'éviter qu'un paiement soit automatiquement interprété comme une preuve définitive de propriété.

3. Vérification avant acquisition

Avant ou au moment de l'achat, le consommateur peut utiliser le QR consommateur pour vérifier l'état du produit. Cette vérification complète les contrôles du revendeur. Elle permet au futur acquéreur d'interroger l'identité et le statut du produit avant l'entrée dans son patrimoine numérique.

4. Trois QR codes et transition commerciale

Les trois QR codes d'Authenticity Plus© conservent leurs rôles pendant la transition : consommateur pour la vérification, revendeur/professionnel pour le circuit commercial et contrôle/douanes pour les autorités compétentes. La première acquisition ne fusionne pas ces fonctions et ne transforme pas les codes en identifiants personnels.

5. Statuts VERT / JAUNE / ROUGE

VERT signifie original ; JAUNE signifie original mais déjà vérifié ou vendu ; ROUGE signifie contrefaçon ou code inexistant dans Authenticity Plus©. Après une vente reconnue, le passage vers JAUNE peut matérialiser qu'un produit original a déjà été vérifié ou vendu, sans remettre en cause son authenticité.

6. Confirmation de la vente

Le revendeur, la caisse, l'ERP ou un autre système autorisé peut transmettre l'événement de vente à AP Core. La plateforme vérifie l'identité du produit, le droit du vendeur, l'unicité de l'opération et la cohérence de l'état. La vente devient alors un événement du Passeport Numérique Universel.

7. Preuve d'acquisition

Deep Authenticity© peut produire une preuve numérique indiquant qu'une acquisition reconnue a eu lieu. Cette preuve peut référencer produit, événement, date et acteurs selon les droits applicables. Elle ne remplace pas automatiquement facture, contrat, titre ou autres documents exigés par la loi.

8. Naissance de la relation de propriété numérique

Lorsque le cadre et le type de produit le permettent, l'acquisition peut ouvrir une relation de propriété numérique entre l'identité persistante du produit et l'acquéreur. Cette relation sert à gérer les droits fonctionnels dans la plateforme : consultation privée, transfert ultérieur, déclaration de perte ou accès à certains services.

9. Identité du propriétaire et confidentialité

La plateforme ne doit pas rendre publiquement visible le nom du propriétaire par défaut. AP Core peut utiliser une identité de compte, un identifiant pseudonymisé ou une preuve sélective. Les autorités ou acteurs habilités n'accèdent aux informations personnelles que selon les règles applicables.

10. Passeport Numérique Universel après acquisition

Le Passeport Numérique Universel continue après la vente. L'historique industriel et commercial reste conservé selon les droits, tandis que de nouveaux événements patrimoniaux peuvent être ajoutés : maintenance, garantie, réparation, transfert, seconde main ou fin de vie.

11. Droits numériques associés

La propriété numérique peut donner accès à des fonctions liées au produit : recevoir des alertes, gérer une garantie, consulter des documents privés, initier un transfert ou autoriser une intervention. Ces droits sont des capacités de plateforme ; ils doivent être distingués des droits juridiques de propriété définis par la loi.

12. AP Core et contrôle de cohérence

AP Core vérifie qu'un produit ne soit pas attribué simultanément à plusieurs propriétaires incompatibles lorsque le modèle exige une propriété exclusive. Les opérations répétées ou contradictoires sont bloquées ou mises en attente. Les règles peuvent varier selon la catégorie d'actif.

13. AP Ledger et ancrage patrimonial

Les événements de première acquisition ou de transfert à forte valeur peuvent être ancrés dans AP Ledger sous forme de preuve, empreinte, signature et horodatage. Le registre renforce l'auditabilité sans nécessiter la publication des données personnelles de l'acquéreur.

14. Garantie et services après-vente

La relation entre produit et acquéreur peut faciliter l'activation de la garantie, les rappels, la maintenance et le service après-vente. Le producteur ou revendeur peut vérifier l'éligibilité sans recevoir automatiquement toutes les informations personnelles du propriétaire.

15. Perte, vol et contestation

Le propriétaire peut disposer de mécanismes permettant de signaler une perte, un vol présumé ou une contestation. Ces déclarations doivent être distinguées d'une décision officielle. AP Core peut restreindre certaines opérations ou signaler un risque selon les politiques sans se substituer aux autorités compétentes.

16. Préparation du transfert futur

La relation de propriété numérique prépare la seconde main. Le propriétaire légitime dans le système peut initier une demande de transfert vers un nouvel acquéreur. L'opération exige authentification et validation afin d'éviter qu'un simple détenteur physique puisse transférer arbitrairement l'identité numérique du produit.

17. Achat cadeau et acquisition pour autrui

Un payeur peut acheter un produit pour une autre personne. Le système doit permettre de différer ou d'orienter l'attribution vers le bénéficiaire lorsque cela est nécessaire. Cette distinction empêche d'assimiler automatiquement l'identité du payeur à celle du propriétaire.

18. Achat professionnel et actifs d'entreprise

Une entreprise peut être premier acquéreur d'équipements, véhicules, machines ou autres actifs. La propriété numérique peut alors être rattachée à l'organisation et gérée par des utilisateurs habilités. Les changements d'employés ne doivent pas modifier l'identité du propriétaire organisationnel.

19. Portabilité et souveraineté patrimoniale

Le propriétaire ne doit pas être prisonnier d'un terminal ou d'un compte unique. Des mécanismes de récupération, changement d'appareil et continuité d'identité sont nécessaires. Dans les déploiements souverains, les preuves patrimoniales peuvent rester sous gouvernance locale tout en demeurant interopérables.

20. Critères d'acceptation et conclusion

Le parcours Premier acquéreur est cohérent si la vérification précède ou accompagne l'achat ; si les trois QR codes conservent leurs rôles ; si VERT/JAUNE/ROUGE restent inchangés ; si la vente est confirmée par un acteur autorisé ; si une preuve d'acquisition peut être produite ; si la relation de propriété numérique respecte la confidentialité ; si le Passeport Numérique Universel continue après la vente ; si AP Core empêche les incohérences et AP Ledger peut ancrer les événements critiques ; si garantie, contestation, achat pour autrui et propriété organisationnelle sont gérés ; et si le transfert futur est préparé.

Le premier acquéreur marque ainsi la naissance du cycle patrimonial de l'objet dans Deep Authenticity© : l'identité créée par le producteur et transmise par le revendeur devient une relation de propriété capable de se poursuivre dans le temps.

Le Chapitre 5 développera la Seconde main : marché secondaire authentifié, Fenêtre Seconde Main, continuité de provenance et préparation du changement de propriétaire.

Note de cadrage institutionnel

La « propriété numérique » décrite dans ce chapitre désigne une relation fonctionnelle et probante au sein de Deep Authenticity©. Sa portée juridique dépend du droit applicable, de la nature de l'actif et des preuves requises. Elle ne remplace pas automatiquement un titre de propriété, un contrat, une facture ou une inscription dans un registre public lorsque ceux-ci sont juridiquement nécessaires.

CHAPITRE 5 — SECONDE MAIN : MARCHÉ SECONDAIRE AUTHENTIFIÉ ET CONTINUITÉ DE PROVENANCE

SECONDE MAIN — FENÊTRE SECONDE MAIN — PROVENANCE — PROPRIÉTAIRE — REVENTE — PASSEPORT NUMÉRIQUE UNIVERSEL — TRANSFERT — AP BUSINESS — 3 QR CODES — CONFIANCE

1. Objet du chapitre

Ce chapitre définit le marché de seconde main dans Deep Authenticity©. L'objectif est de prolonger la chaîne de confiance au-delà de la première vente afin qu'un produit puisse être revendu sans perdre son identité, sa provenance et les événements autorisés de son Passeport Numérique Universel.

2. Principe du marché secondaire authentifié

Dans un marché classique de seconde main, l'acheteur dispose souvent de peu de moyens pour vérifier l'origine d'un bien. Deep Authenticity© ajoute une couche de confiance : l'identité du produit persiste, son statut peut être interrogé et le propriétaire numérique peut initier une cession traçable.

3. Continuité de l'identité du produit

La revente ne crée pas une nouvelle identité pour l'objet. L'identifiant persistant et le Passeport Numérique Universel continuent d'accompagner le même produit. Les changements concernent son état, son propriétaire et les événements de cycle de vie, non son identité fondamentale.

4. Les trois QR codes en seconde main

Les trois QR codes d'Authenticity Plus© conservent leurs fonctions. Le QR consommateur permet au candidat acquéreur de vérifier le produit ; le QR professionnel reste réservé aux usages professionnels prévus ; le QR contrôle/douanes demeure destiné aux autorités compétentes. La revente n'efface pas cette séparation.

5. Statuts VERT / JAUNE / ROUGE

VERT signifie original ; JAUNE signifie original mais déjà vérifié ou vendu ; ROUGE signifie contrefaçon ou code inexistant dans Authenticity Plus©. Un produit authentique de seconde main sera fréquemment associé à la logique JAUNE, ce qui reflète son histoire de vérification ou de vente sans remettre en cause son authenticité.

6. Fenêtre Seconde Main

La Fenêtre Seconde Main constitue l'espace de consultation et, selon le modèle retenu, de mise en relation pour les produits authentifiés proposés à la revente. Elle peut présenter l'identité du produit, son statut, les informations publiques de provenance et les éléments commerciaux autorisés par le vendeur.

7. Mise en vente par le propriétaire

Le propriétaire numérique peut initier une mise en vente depuis son espace. AP Core vérifie qu'il dispose du droit fonctionnel nécessaire et qu'aucun blocage n'interdit l'opération. La mise en vente ne transfère pas encore la propriété : elle crée un état commercial temporaire et révocable.

8. Fiche de seconde main

La fiche peut inclure référence, images, état déclaré, prix, localisation approximative, historique de maintenance autorisé et preuve d'authenticité. Les informations déclarées par le vendeur doivent être

distinguées des événements vérifiés par la plateforme afin que l'acheteur connaisse leur niveau de confiance.

9. Recherche et découverte

AP Business peut permettre la recherche de produits de seconde main par catégorie, marque, modèle, zone ou autres critères. La découverte commerciale s'appuie sur des identités de produits reconnues plutôt que sur de simples annonces textuelles, ce qui réduit l'ambiguïté entre l'objet annoncé et l'objet effectivement transféré.

10. Vérification avant acquisition

Le candidat acquéreur doit pouvoir vérifier l'identité et le statut du produit avant de finaliser la transaction. Selon le secteur, des contrôles complémentaires peuvent porter sur maintenance, rappel, perte déclarée, garantie ou autres événements pertinents. Les informations privées du propriétaire précédent restent protégées.

11. Provenance visible et provenance protégée

Le Passeport Numérique Universel peut contenir davantage d'informations que celles affichées publiquement. La plateforme fournit une vue proportionnée : événements nécessaires à la confiance, attestations pertinentes et historique autorisé. Les identités personnelles des propriétaires précédents ne sont pas exposées par défaut.

12. État physique et authenticité

Un produit peut être authentique tout en étant usé, endommagé ou modifié. Deep Authenticity© doit distinguer authenticité, état physique et conformité. Le vendeur peut déclarer l'état, tandis que des inspections ou réparations vérifiées peuvent ajouter des preuves distinctes au Passeport Numérique Universel.

13. Réparations et pièces remplacées

Une réparation ne doit pas automatiquement rompre la provenance. Lorsqu'un prestataire habilité intervient, l'événement peut préciser nature de l'intervention et pièces remplacées. Pour certains produits, une modification substantielle peut nécessiter une alerte ou une qualification spécifique sans supprimer l'identité historique.

14. Produit perdu, volé ou contesté

Une déclaration de perte, vol présumé ou contestation peut empêcher ou suspendre la mise en vente et le transfert selon les politiques. Une telle déclaration doit rester distincte d'une décision officielle. Le système fournit un signal de risque et une procédure de résolution ou d'escalade.

15. Transaction de seconde main

La transaction peut être réalisée directement entre parties ou via un intermédiaire. Deep Authenticity© peut relier l'événement commercial au produit etpréparer le transfert de propriété. AP Pay peut ultérieurement offrir des fonctions de paiement ou d'orchestration lorsque le cadre réglementaire et le modèle de service le permettent.

16. Préparation du transfert de propriété

La vente n'est pleinement cohérente dans le système que lorsque l'ancien propriétaire initie ou autorise le transfert et que le nouvel acquéreur l'accepte selon les règles définies. AP Core vérifie identité, état, autorisations et unicité de l'opération avant la modification de la relation patrimoniale.

17. Professionnels de la seconde main

Les revendeurs spécialisés, reconditionneurs ou maisons de vente peuvent disposer de parcours professionnels adaptés. Un produit peut entrer temporairement dans un stock professionnel avant d'être revendu. Les événements professionnels doivent rester distincts des transferts de propriété définitifs.

18. Valeur économique de la provenance

Une provenance vérifiable peut réduire l'incertitude qui pèse sur le marché secondaire. Historique de propriété pseudonymisé, maintenance, réparations et authenticité peuvent améliorer la confiance entre parties. La plateforme ne garantit toutefois pas un prix de revente ni une valeur marchande déterminée.

19. Confidentialité, fraude et gouvernance

La Fenêtre Seconde Main doit limiter les risques d'usurpation d'annonce, collecte abusive de données et détournement de comptes. Les informations publiques sont minimisées ; les actions sensibles exigent authentification ; les comportements anormaux peuvent être signalés. Les règles de recours et contestation doivent être accessibles.

20. Critères d'acceptation et conclusion

Le marché secondaire est cohérent si l'identité du produit persiste ; si les trois QR codes conservent leurs rôles ; si VERT/JAUNE/ROUGE restent inchangés ; si la Fenêtre Seconde Main relie annonce et produit authentifié ; si le propriétaire numérique contrôle la mise en vente ; si provenance publique et données privées sont séparées ; si authenticité et état physique sont distingués ; si réparations, pertes et contestations sont traçables ; si les professionnels disposent d'un parcours adapté ; et si la transaction prépare un transfert de propriété sécurisé.

La seconde main devient ainsi une extension naturelle de la chaîne de confiance : le produit ne perd plus son histoire au moment où il quitte son premier acquéreur.

Le Chapitre 6 développera le Transfert numérique sécurisé de propriété : consentement des parties, contrôle d'autorité, changement de détenteur, preuve, révocation et continuité patrimoniale.

Note de cadrage institutionnel

La Fenêtre Seconde Main fournit une infrastructure de confiance et de mise en relation selon le modèle retenu. Elle ne garantit pas automatiquement l'état physique, la valeur marchande, la licéité de toute vente ni la validité juridique d'un transfert. Les obligations de consommation, fiscalité, propriété, biens volés et plateformes de marché doivent être respectées dans chaque juridiction.

CHAPITRE 6 — TRANSFERT NUMÉRIQUE SÉCURISÉ DE PROPRIÉTÉ

TRANSFERT DE PROPRIÉTÉ — CÉDANT — ACQUÉREUR — CONSENTEMENT — AP CORE — AP LEDGER — SIGNATURE CRYPTOGRAPHIQUE — PASSEPORT NUMÉRIQUE UNIVERSEL — SECONDE MAIN — CONTINUITÉ PATRIMONIALE

1. Objet du chapitre

Ce chapitre définit le transfert numérique sécurisé de propriété dans Deep Authenticity©. Il organise le passage contrôlé d'une relation patrimoniale d'un propriétaire à un autre, sans recréer l'identité du produit et sans rompre son Passeport Numérique Universel. Le transfert constitue un événement majeur de la chaîne économique de confiance.

2. Principe fondamental

Le transfert ne consiste pas à déplacer un simple fichier ou QR code. Il modifie, sous contrôle d'AP Core, la relation entre l'identité persistante d'un actif et l'identité autorisée à exercer les droits fonctionnels de propriétaire. L'objet conserve son identité, son historique et ses preuves antérieures.

3. Identification du cédant

Le cédant doit être authentifié et disposer du droit d'initier le transfert. La possession physique seule ne suffit pas lorsque le système exige une relation de propriété numérique préalable. Les mécanismes de récupération ou de contestation doivent traiter séparément les situations où le propriétaire ne peut plus accéder à son compte.

4. Identification du nouvel acquéreur

Le nouvel acquéreur doit disposer d'une identité ou d'un mécanisme d'acceptation compatible avec le niveau de risque du bien. Pour les actifs courants, le parcours peut rester simple ; pour les actifs de valeur ou réglementés, des vérifications supplémentaires peuvent être exigées.

5. Consentement des deux parties

Le transfert doit matérialiser la volonté du cédant et l'acceptation de l'acquéreur. Une opération initiée mais non acceptée reste en attente ou expire selon la politique. Cette double validation limite les erreurs d'adresse, les transferts accidentels et les prises de contrôle unilatérales.

6. Vérification de l'actif avant transfert

AP Core vérifie l'identité de l'actif, son statut, les éventuels blocages, rappels, contestations ou transferts déjà en cours. Une incohérence peut suspendre l'opération. La plateforme doit éviter qu'un même actif soit transféré simultanément dans plusieurs chaînes incompatibles.

7. Trois QR codes et transfert

Les trois QR codes d'Authenticity Plus© conservent leurs rôles pendant et après le transfert. Aucun changement de propriétaire ne crée de nouveaux rôles pour ces codes. Le QR consommateur reste destiné à la vérification, le QR revendeur/professionnel au circuit professionnel et le QR contrôle/douanes aux autorités compétentes.

8. Statuts VERT / JAUNE / ROUGE

La propriété et l'authenticité sont deux dimensions distinctes. VERT signifie original ; JAUNE signifie original mais déjà vérifié ou vendu ; ROUGE signifie contrefaçon ou code inexistant dans Authenticity Plus©. Un changement de propriétaire n'altère pas cette sémantique fondamentale.

9. AP Core comme autorité d'orchestration

AP Core contrôle les préconditions, verrouille logiquement l'opération lorsque nécessaire, recueille les validations et applique la transition patrimoniale. Il doit assurer idempotence et atomicité logique afin qu'une interruption réseau ne crée ni double transfert ni état ambigu.

10. Signature cryptographique de l'opération

Les éléments critiques du transfert peuvent être signés : identité de l'actif, référence de l'ancien propriétaire, nouvel acquéreur, horodatage et contexte de l'opération. La signature cryptographique protège l'intégrité et l'attribution de la transaction numérique sans rendre publiques les données personnelles.

11. AP Ledger et preuve durable

L'événement finalisé peut être ancré dans AP Ledger. Une empreinte et des références suffisent souvent pour démontrer qu'un transfert déterminé a été enregistré à un moment donné. L'historique patrimonial devient vérifiable tout en permettant la minimisation des données.

12. Mise à jour du Passeport Numérique Universel

Le Passeport Numérique Universel reçoit un nouvel événement de propriété. L'ancien propriétaire n'est pas effacé de l'histoire probante lorsque sa conservation est justifiée ; son identité peut toutefois rester pseudonymisée ou inaccessible aux utilisateurs ordinaires. Le nouvel acquéreur obtient les droits fonctionnels prévus.

13. Remise physique et transfert numérique

Le transfert numérique doit être coordonné avec la remise physique du bien. Selon le modèle commercial, les parties peuvent confirmer la réception avant finalisation. Pour certains secteurs, un tiers professionnel, un transporteur ou un point de contrôle peut fournir une preuve supplémentaire.

14. Paiement et transfert

Le paiement et le transfert de propriété sont liés économiquement mais restent des événements distincts. AP Pay pourra orchestrer leur rapprochement lorsque le service et la réglementation le permettent. Le système doit éviter d'interpréter un paiement seul comme une preuve automatique de remise ou de propriété.

15. Transfert entre particuliers et via professionnel

Le mécanisme doit supporter la cession directe entre particuliers ainsi que les parcours passant par un revendeur, reconditionneur, maison de vente ou autre intermédiaire. Les responsabilités et étapes peuvent varier, mais l'identité persistante de l'actif et la continuité de preuve restent identiques.

16. Annulation, expiration et échec

Une demande non acceptée peut expirer. Une opération échouée ne doit pas modifier la propriété. Après finalisation, une annulation ne doit pas effacer silencieusement l'événement : un transfert inverse ou une procédure de rectification doit produire une nouvelle trace selon le cadre applicable.

17. Contestation et fraude

En cas d'usurpation de compte, coercition alléguée, vol présumé ou litige, AP Core peut suspendre certaines fonctions et préserver les preuves. Deep Authenticity© ne tranche pas automatiquement les litiges juridiques ; elle fournit une histoire technique et des mécanismes d'escalade aux acteurs compétents.

18. Héritage, donation et transferts non commerciaux

Le changement de propriétaire peut résulter d'une donation, succession, réorganisation d'entreprise ou autre événement non commercial. Le moteur de transfert doit pouvoir appliquer des parcours spécifiques et demander les justificatifs ou autorités nécessaires sans imposer un paiement.

19. Portabilité, souveraineté et interopérabilité

Dans une architecture fédérée, un transfert peut impliquer des instances ou juridictions différentes. Les Corridors de Confiance permettent d'échanger les attestations nécessaires sans centraliser toutes les données. Les règles juridiques locales restent applicables à la reconnaissance du changement de propriété.

20. Critères d'acceptation et conclusion

Le transfert numérique sécurisé est cohérent si le cédant est habilité ; si l'acquéreur est identifié au niveau requis ; si le consentement des parties est établi ; si l'actif et ses blocages sont vérifiés ; si les trois QR codes et VERT/JAUNE/ROUGE conservent leur sémantique ; si AP Core garantit une transition unique et cohérente ; si la signature cryptographique protège l'opération et AP Ledger peut l'ancrer ; si le Passeport Numérique Universel poursuit son histoire ; si remise, paiement, annulation et contestation restent des événements distincts ; et si les transferts commerciaux ou non commerciaux sont supportés.

Le transfert de propriété constitue ainsi le mécanisme qui permet à l'identité authentifiée d'un produit de devenir une continuité patrimoniale durable.

Le Chapitre 7 développera la Propriété : registre des relations patrimoniales, droits, possession, preuves, gouvernance et continuité de propriété dans Deep Authenticity©.

Note de cadrage institutionnel

Le transfert numérique sécurisé décrit ici constitue un mécanisme technique et probant de Deep Authenticity©. Sa portée juridique dépend de la nature du bien et du droit applicable. Pour certains actifs — immobilier, véhicules, titres enregistrés ou autres biens réglementés — une autorité publique, un registre officiel, un acte ou des formalités supplémentaires peuvent être nécessaires pour produire le transfert juridique.

CHAPITRE 7 — PROPRIÉTÉ : REGISTRE DES RELATIONS PATRIMONIALES ET CONTINUITÉ DES DROITS

PROPRIÉTÉ — POSSESSION — DÉTENTION — DROITS — REGISTRE PATRIMONIAL — AP CORE — AP LEDGER — PASSEPORT NUMÉRIQUE UNIVERSEL — PREUVE — GOUVERNANCE — SOUVERAINETÉ

1. Objet du chapitre

Ce chapitre définit la couche Propriété de Deep Authenticity©. Elle organise les relations patrimoniales entre une identité persistante — produit, équipement ou autre actif compatible — et les personnes ou organisations habilitées à exercer des droits fonctionnels. Elle prolonge la première acquisition et le transfert sécurisé en une continuité patrimoniale gouvernée.

2. Identité de l'actif et identité du propriétaire

L'identité de l'actif reste indépendante de celle de son propriétaire. Un changement de propriétaire ne crée donc pas un nouvel objet numérique. Cette séparation permet au Passeport Numérique Universel de conserver l'histoire de l'actif tout en faisant évoluer ses relations patrimoniales.

3. Propriété, possession, détention et usage

Deep Authenticity© distingue plusieurs notions : propriété, possession physique, détention temporaire et droit d'usage. Un réparateur, locataire, transporteur ou dépositaire peut détenir l'objet sans en devenir propriétaire. Cette distinction évite les transferts patrimoniaux implicites lors des mouvements opérationnels.

4. Registre des relations patrimoniales

La couche Propriété maintient un état structuré des relations patrimoniales reconnues par la plateforme. Elle peut représenter propriétaire actuel, événements de transfert, droits délégués et restrictions. Ce registre fonctionnel s'appuie sur AP Core et peut utiliser AP Ledger pour les preuves critiques.

5. Naissance de la relation patrimoniale

La relation peut naître lors de la première acquisition, d'une attribution initiale ou d'un événement reconnu par une autorité compétente. La source de cette relation doit être traçable. Pour certains actifs réglementés, Deep Authenticity© doit se référer au registre ou titre juridiquement compétent.

6. Droits fonctionnels du propriétaire

Le propriétaire numérique peut recevoir des capacités telles que consulter des informations privées, recevoir des alertes, gérer une garantie, autoriser une maintenance, déclarer une mise en vente ou initier un transfert. Ces droits sont configurables selon le type d'actif et ne doivent pas être assimilés automatiquement à l'ensemble des prérogatives juridiques de propriété.

7. Droits délégués

Le propriétaire peut, lorsque la politique l'autorise, déléguer certains droits à un tiers sans transférer la propriété : gestionnaire de flotte, membre d'une organisation, réparateur ou mandataire. Les délégations doivent avoir un périmètre, une durée et une révocabilité explicites.

8. Propriété individuelle et organisationnelle

Un actif peut appartenir fonctionnellement à une personne ou à une organisation. Dans le second cas, les utilisateurs agissent au nom de l'entité selon leurs habilitations. Le départ d'un employé ne doit pas rompre la relation entre l'organisation et ses actifs.

9. Copropriété et droits multiples

Certains actifs peuvent relever de plusieurs titulaires ou de droits superposés. Le modèle doit pouvoir représenter copropriété, usufruit, gestion ou autres relations lorsque le secteur le nécessite. Ces configurations doivent être définies par des règles explicites plutôt que déduites automatiquement.

10. AP Core et moteur des droits

AP Core vérifie l'état patrimonial avant toute opération sensible. Il détermine qui peut consulter, déléguer, vendre, transférer ou modifier certaines informations. Les règles peuvent dépendre du type d' actif, du rôle, de la juridiction et de l'existence d'un blocage ou d'une contestation.

11. AP Ledger et preuve patrimoniale

Les acquisitions, transferts, délégations critiques ou décisions institutionnelles peuvent être ancrés dans AP Ledger. L'objectif est de rendre l'évolution des droits vérifiable dans le temps. Les données personnelles peuvent rester hors registre, avec seulement les empreintes ou références nécessaires à la preuve.

12. Passeport Numérique Universel et histoire de propriété

Le Passeport Numérique Universel conserve les événements patrimoniaux autorisés en relation avec les événements industriels, commerciaux et techniques. La vue publique peut indiquer une continuité de provenance sans révéler les identités des propriétaires précédents. Les vues institutionnelles dépendent des habilitations.

13. Les trois QR codes et la propriété

Les trois QR codes d'Authenticity Plus© ne sont pas eux-mêmes des titres de propriété. Ils restent des mécanismes de vérification et de rôle : consommateur, revendeur/professionnel et contrôle/douanes. La propriété est déterminée par les relations et événements contrôlés par AP Core, non par la simple possession d'un QR.

14. Statuts VERT / JAUNE / ROUGE

VERT signifie original ; JAUNE signifie original mais déjà vérifié ou vendu ; ROUGE signifie contrefaçon ou code inexistant dans Authenticity Plus©. Ces statuts concernent l'authenticité et l'historique de vérification ou de vente ; ils ne constituent pas, à eux seuls, une indication du propriétaire actuel.

15. Restrictions, sûretés et blocages

Certains actifs peuvent être soumis à une restriction de transfert, un financement, une saisie, un rappel, une contestation ou une autre limitation reconnue. Lorsque l'intégration juridique existe, AP Core peut empêcher ou conditionner certaines opérations. La source et l'autorité du blocage doivent être identifiables.

16. Perte, vol, succession et incapacité

Les événements patrimoniaux exceptionnels exigent des procédures dédiées. Une déclaration de perte ou de vol peut suspendre les transferts ; une succession peut nécessiter des justificatifs ou une autorité ; l'incapacité d'un titulaire peut impliquer un représentant habilité. La plateforme conserve les preuves sans trancher seule les droits contestés.

17. Rectification et contestation

Une erreur patrimoniale ne doit pas être corrigée par suppression silencieuse de l'histoire. Une rectification produit un nouvel événement relié à l'erreur initiale et à son fondement. Les litiges peuvent conduire à un gel temporaire jusqu'à intervention de l'acteur ou de l'autorité compétente.

18. Confidentialité patrimoniale

L'identité du propriétaire constitue une donnée sensible dans de nombreux contextes. Les interfaces publiques doivent privilégier la preuve d'un droit ou d'une continuité sans révéler plus d'informations que nécessaire. Les accès institutionnels et professionnels sont journalisés et limités par finalité.

19. Souveraineté et registres officiels

Pour les biens dont la propriété est juridiquement déterminée par un registre public, Deep Authenticity© doit fonctionner comme couche d'interopérabilité, de preuve ou de consultation, et non comme autorité concurrente. Les architectures souveraines permettent de maintenir les données et clés sous contrôle national tout en échangeant des attestations.

20. Critères d'acceptation et conclusion

La couche Propriété est cohérente si l'identité de l'actif reste indépendante du propriétaire ; si propriété, possession, détention et usage sont distingués ; si les droits fonctionnels et délégations sont gouvernés ; si personnes, organisations et copropriétés peuvent être représentées lorsque nécessaire ; si AP Core contrôle les opérations et AP Ledger peut ancrer les preuves ; si le Passeport Numérique Universel conserve la continuité patrimoniale ; si les trois QR codes et VERT/JAUNE/ROUGE ne sont jamais confondus avec un titre de propriété ; si restrictions, successions, rectifications et contestations sont traitées ; et si les registres officiels conservent leur autorité juridique.

Deep Authenticity© transforme ainsi la propriété numérique en une continuité de droits vérifiables autour d'une identité persistante, sans confondre la preuve technologique avec la compétence juridique.

Le Chapitre 8 développera AP Business : infrastructure commerciale, relations B2B/B2C, services aux producteurs et revendeurs, recherche de produits et orchestration de l'écosystème marchand.

Note de cadrage institutionnel

La couche Propriété de Deep Authenticity© constitue un registre fonctionnel et probant de relations patrimoniales. Sa portée juridique dépend du droit applicable. Lorsqu'un registre public, un titre, un acte authentique ou une formalité légale détermine la propriété, cette source officielle conserve son autorité et doit être intégrée ou référencée selon les règles applicables.

CHAPITRE 8 — AP BUSINESS : INFRASTRUCTURE COMMERCIALE DE CONFIANCE

AP BUSINESS — B2B — B2C — PRODUCTEUR — REVENDEUR — CONSOMMATEUR — RECHERCHE PRODUITS — STOCK AUTHENTIFIÉ — PROXIMITÉ — PASSEPORT NUMÉRIQUE UNIVERSEL — INTEROPÉRABILITÉ

1. Objet du chapitre

Ce chapitre définit AP Business comme la couche commerciale de Deep Authenticity©. Sa fonction est de transformer l'identité vérifiée des produits, des acteurs et des événements en services économiques utilisables par producteurs, revendeurs, professionnels et consommateurs, sans confondre infrastructure de confiance et rôle contractuel de vendeur.

2. Principe d'AP Business

AP Business ne part pas d'une simple annonce commerciale : il part d'identités et de relations déjà structurées par Deep Authenticity©. Produit, producteur, revendeur, disponibilité et historique peuvent ainsi être reliés à des preuves ou événements qualifiés. Cette architecture réduit l'écart entre information commerciale et réalité du produit.

3. Écosystème multi-acteurs

AP Business relie producteurs, fabricants, artisans, agriculteurs, éleveurs, artistes, créateurs, PME, distributeurs, revendeurs, prestataires et acquéreurs. Chaque acteur conserve un rôle et des droits distincts. La plateforme doit pouvoir servir aussi bien une petite structure qu'un réseau international.

4. Identité commerciale vérifiée

Les organisations professionnelles disposent d'une identité vérifiée reliée à leurs établissements, marques et habilitations. Cette identité permet de distinguer un acteur reconnu d'un compte anonyme. Les informations publiques restent limitées aux données nécessaires à la relation commerciale.

5. Catalogue fondé sur l'identité produit

Les produits visibles dans AP Business peuvent être reliés au référentiel et au Passeport Numérique Universel. La fiche commerciale ne remplace pas la fiche de preuve : elle en exploite les attributs autorisés. Le produit commercial et l'objet authentifié restent ainsi liés par une identité persistante.

6. Fenêtre Producteur

Le producteur peut administrer ses gammes, informations publiques, réseaux de distribution et services commerciaux autorisés. Il peut identifier les produits recherchés, les zones de demande et les circuits disponibles à partir de données agrégées, sans accéder automatiquement aux données personnelles des consommateurs.

7. Fenêtre Revendeur

La Fenêtre Revendeur relie stock authentifié et visibilité commerciale. Le professionnel choisit les produits qu'il souhaite rendre visibles, tandis qu'AP Core vérifie leur relation avec son stock ou ses droits. Les alertes, rappels et incohérences peuvent empêcher ou limiter la publication.

8. Recherche de produits

Le consommateur ou professionnel peut rechercher un produit par marque, catégorie, référence, caractéristiques ou autres critères autorisés. Les résultats peuvent privilégier les offres reliées à des identités de produits et acteurs reconnus plutôt que de simples descriptions non vérifiées.

9. Recherche par proximité

Avec l'autorisation de l'utilisateur, AP Business peut identifier les revendeurs disposant du produit recherché et les classer selon la proximité. Une recherche par ville ou zone doit également être possible lorsque la localisation précise n'est pas souhaitée. La fraîcheur du stock doit être indiquée.

10. Disponibilité et stock authentifié

La disponibilité commerciale peut provenir d'un scan professionnel, d'un ERP, d'une caisse ou d'une déclaration autorisée. AP Business doit afficher le niveau de fraîcheur et distinguer stock déclaré, stock synchronisé et présence physiquement vérifiée lorsque ces niveaux existent.

11. Relations B2C

Dans le parcours B2C, AP Business facilite la découverte d'un produit authentifié et d'un revendeur reconnu. Le consommateur peut passer de la recherche à la vérification, puis à l'achat selon le modèle commercial. Deep Authenticity© peut rester infrastructure de confiance même si la transaction contractuelle se déroule chez le revendeur.

12. Relations B2B

Dans le parcours B2B, producteurs, distributeurs et professionnels peuvent rechercher partenaires, produits, lots ou disponibilités selon leurs habilitations. Les échanges peuvent s'appuyer sur des preuves de provenance et de statut. Les conditions commerciales sensibles restent privées entre les parties.

13. Demandes, offres et opportunités

AP Business peut permettre à un acheteur professionnel de publier une demande ou à un fournisseur de signaler une disponibilité. Les mécanismes de mise en relation doivent distinguer intérêt commercial, offre ferme et contrat. La plateforme conserve la provenance des informations sans imposer un modèle contractuel unique.

14. AP Business et Seconde Main

La Fenêtre Seconde Main peut être reliée à AP Business afin que les produits déjà vendus disposent d' un circuit commercial distinct. Les annonces restent liées à l'identité persistante du produit et au propriétaire ou professionnel habilité à le proposer.

15. AP Business et transfert de propriété

Lorsqu'une vente implique un changement de propriétaire, AP Business prépare les données nécessaires au mécanisme de transfert sécurisé. L'événement commercial, le paiement et le transfert patrimonial restent distincts mais peuvent être orchestrés pour offrir un parcours cohérent.

16. AP Business et AP Pay

AP Pay pourra être intégré comme option de paiement ou d'orchestration financière pour certaines transactions. AP Business fournit le contexte commercial — produit, parties, montant ou référence — tandis qu'AP Pay traite les fonctions financières autorisées. Cette séparation facilite la conformité et l' interopérabilité.

17. Tableaux de bord et intelligence commerciale

Les producteurs et revendeurs peuvent disposer d'indicateurs sur recherches, disponibilité, rotations, ventes, zones de demande et tendances. Les analyses agrégées peuvent contribuer à anticiper pénuries, surstocks ou besoins logistiques. Les données individuelles restent protégées et les estimations sont distinguées des observations.

18. API, ERP et commerce omnicanal

AP Business peut s'intégrer aux sites marchands, ERP, systèmes de caisse et applications partenaires par API. Un même produit peut être découvert dans Deep Authenticity© puis acheté sur un canal externe, tout en conservant sa chaîne de preuve. L'objectif est l'interopérabilité plutôt que l' enfermement dans une place de marché unique.

19. Gouvernance, concurrence et neutralité

La visibilité des offres et le classement des résultats doivent suivre des règles explicites. Les données d'un revendeur ne doivent pas être utilisées pour avantager arbitrairement un concurrent. Les contenus sponsorisés, s'ils existent, doivent être distingués des résultats de confiance et ne jamais modifier un statut d'authenticité.

20. Critères d'acceptation et conclusion

AP Business est cohérent si les acteurs professionnels sont identifiés ; si les catalogues restent reliés aux identités produit ; si les Fenêtres Producteur et Revendeur exploitent des données autorisées ; si la recherche et la proximité distinguent disponibilité et fraîcheur ; si B2B et B2C conservent leurs spécificités ; si la Seconde Main et le transfert de propriété s'intègrent sans confusion ; si AP Pay reste une couche financière distincte ; si tableaux de bord, API et ERP permettent l'interopérabilité ; et si concurrence, confidentialité et neutralité sont gouvernées.

AP Business transforme ainsi Deep Authenticity© en infrastructure commerciale de confiance : non pas une place de marché obligatoire, mais un environnement où l'offre, la demande et la distribution peuvent être reliées à des identités et preuves vérifiables.

Le Chapitre 9 développera la Recherche commerciale et la localisation du revendeur le plus proche : moteur de découverte, disponibilité, géolocalisation, classement et protection de la vie privée.

Note de cadrage institutionnel

AP Business doit être conçu selon les règles applicables au commerce électronique, à la concurrence, à la protection des consommateurs, à la publicité et aux données personnelles. Les résultats de recherche, informations de stock et indicateurs commerciaux doivent préciser leur source et leur fraîcheur. La présence d'un acteur ou produit dans AP Business ne constitue pas automatiquement une certification générale.

CHAPITRE 9 — RECHERCHE COMMERCIALE ET LOCALISATION DU REVENDEUR LE PLUS PROCHE

RECHERCHE COMMERCIALE — PRODUIT AUTHENTIFIÉ — REVENDEUR — PROXIMITÉ — GÉOLOCALISATION — DISPONIBILITÉ — STOCK — AP BUSINESS — CLASSEMENT — VIE PRIVÉE

1. Objet du chapitre

Ce chapitre définit le moteur de recherche commerciale et de localisation de Deep Authenticity©. Sa fonction est de permettre à un utilisateur de rechercher un produit identifié, de repérer les revendeurs qui le proposent et, lorsque cela est autorisé, d'identifier les points de vente les plus proches sans dissocier la découverte commerciale de la chaîne de confiance.

2. De la recherche textuelle à la recherche vérifiée

Un moteur commercial classique recherche principalement des mots, catégories et annonces. AP Business peut ajouter une dimension supplémentaire : relier le résultat à une identité produit, un producteur et un revendeur reconnus. L'utilisateur ne recherche donc pas seulement une description ; il peut rechercher un produit rattaché à l'écosystème de confiance.

3. Sources du catalogue

Les références recherchables peuvent provenir des producteurs, catalogues professionnels, ERP ou autres sources autorisées. Chaque entrée doit conserver sa provenance et son identifiant. La normalisation des noms, variantes et unités permet d'éviter que le même produit apparaisse comme plusieurs références incohérentes.

4. Indexation des produits

Le moteur peut indexer marque, catégorie, modèle, caractéristiques, identifiants, disponibilité et attributs autorisés du Passeport Numérique Universel. Les informations privées ou sensibles ne doivent pas être intégrées à l'index public. Les mises à jour doivent être propagées selon une politique de fraîcheur définie.

5. Recherche par référence et caractéristiques

L'utilisateur peut rechercher par nom, référence, catégorie ou caractéristiques. Des filtres peuvent porter sur zone, disponibilité, type de revendeur ou autres critères pertinents. Les résultats doivent distinguer correspondance exacte, variante compatible et suggestion afin de limiter les confusions.

6. Recherche à partir d'un produit scanné

Après avoir scanné un produit ou une référence, l'utilisateur peut rechercher où acquérir le même produit ou une référence officiellement liée. Cette continuité entre vérification et recherche commerciale réduit la rupture entre l'information d'authenticité et l'accès au réseau de distribution.

7. Fenêtre Revendeur et publication de disponibilité

Les produits visibles dans la recherche proviennent notamment de la Fenêtre Revendeur et des systèmes intégrés. Le professionnel choisit les références publiées selon ses droits. AP Core peut vérifier que la publication correspond à une relation commerciale ou à un stock reconnu.

8. Niveaux de disponibilité

La disponibilité doit être qualifiée : déclarée par le revendeur, synchronisée depuis un ERP ou une caisse, récemment vérifiée, réservée ou indisponible. Une information ancienne doit être signalée. Cette qualification évite de transformer une donnée de stock historique en promesse de disponibilité immédiate.

9. Localisation avec consentement

Lorsque l'utilisateur choisit d'utiliser sa position, le moteur peut comparer sa localisation aux points de vente disponibles. La géolocalisation précise ne doit être demandée que lorsqu'elle améliore réellement le service. L'utilisateur doit également pouvoir rechercher manuellement par ville, commune ou zone.

10. Revendeur le plus proche

Le revendeur le plus proche peut être déterminé selon distance géographique ou temps de déplacement lorsque les données nécessaires existent. Le résultat doit toutefois tenir compte de la disponibilité et de la fraîcheur du stock : le point géographiquement le plus proche n'est pas nécessairement le meilleur résultat commercial.

11. Classement multicritère

Le classement peut combiner pertinence du produit, disponibilité, fraîcheur, distance et critères de confiance explicitement définis. Les règles doivent être documentées. Un paiement publicitaire ne doit jamais transformer un acteur non vérifié en acteur vérifié ni modifier le statut d'authenticité d'un produit.

12. Carte et liste de résultats

Les résultats peuvent être présentés sous forme de liste et de carte. Chaque fiche peut afficher les informations nécessaires : établissement, distance approximative, disponibilité, horaires et moyens de contact autorisés. La carte ne doit pas révéler les adresses privées des vendeurs particuliers sans base appropriée.

13. Réservation ou prise de contact

AP Business peut permettre de contacter le revendeur ou de réserver un produit lorsque le service existe. Une réservation constitue un événement commercial distinct d'une vente. Les délais d' expiration et conditions doivent être clairs afin de ne pas bloquer indéfiniment un stock.

14. Recherche B2B

Les professionnels peuvent disposer de filtres supplémentaires : volumes, lots, zones de livraison, distributeurs ou capacités de fourniture. Les prix négociés et conditions contractuelles restent privés. Le moteur B2B peut ainsi faciliter l'approvisionnement sans exposer les secrets commerciaux.

15. Recherche de seconde main

La Fenêtre Seconde Main peut alimenter un index séparé ou clairement identifié. L'utilisateur doit pouvoir distinguer produit neuf, produit d'occasion et produit reconditionné. L'identité persistante et la provenance autorisée renforcent la confiance dans les résultats secondaires.

16. Protection de la vie privée

La recherche ne doit pas devenir un mécanisme de suivi permanent de l'utilisateur. Les requêtes et positions sont minimisées, protégées et conservées uniquement selon les finalités définies. Les

statistiques commerciales peuvent être agrégées afin d'étudier la demande sans reconstituer inutilement les déplacements individuels.

17. Prévention des manipulations

Le moteur doit détecter faux stocks, répétitions artificielles, usurpation de fiches et tentatives de manipulation du classement. Les changements sensibles de coordonnées ou d'identité professionnelle sont contrôlés. AP Shield peut contribuer à identifier des comportements anormaux.

18. Résilience et mode dégradé

En cas de connectivité limitée, l'application peut conserver certaines informations de catalogue ou points de vente récemment synchronisés. Ces données doivent être marquées comme potentiellement anciennes. Une recherche offline ne doit jamais être présentée comme une confirmation temps réel du stock.

19. Intelligence commerciale agrégée

Les recherches agrégées peuvent aider producteurs et revendeurs à comprendre les zones de demande non satisfaite, les références recherchées et les écarts entre demande et disponibilité. Ces analyses peuvent alimenter les tableaux de bord et, ultérieurement, les modèles prédictifs, en distinguant toujours recherche, intention et vente réelle.

20. Critères d'acceptation et conclusion

Le moteur est cohérent si les résultats restent reliés à des identités produit et revendeur ; si les sources du catalogue sont traçables ; si recherche textuelle, scan et filtres sont supportés ; si disponibilité et fraîcheur sont qualifiées ; si la proximité utilise la localisation avec consentement ou une zone choisie ; si le classement combine pertinence, disponibilité et distance selon des règles explicites ; si neuf, seconde main et B2B sont distingués ; si vie privée et manipulations sont maîtrisées ; et si le mode offline signale ses limites.

La recherche commerciale devient ainsi un prolongement direct de l'authenticité : Deep Authenticity© permet non seulement de demander « ce produit est-il authentique ? », mais aussi « où puis-je trouver ce produit dans un circuit de confiance ? ».

Le Chapitre 10 développera l'écosystème des artisans, agriculteurs, éleveurs, artistes, créateurs, innovateurs et PME : démocratisation de l'accès à la confiance économique.

Note de cadrage institutionnel

Les fonctions de géolocalisation et de classement doivent respecter les règles applicables aux données personnelles, à la concurrence, à la publicité et à la protection des consommateurs. Les informations de disponibilité sont temporelles : elles doivent indiquer leur source et leur fraîcheur et ne constituent pas automatiquement une garantie contractuelle de stock.

CHAPITRE 10 — ARTISANS, AGRICULTEURS, ÉLEVEURS, ARTISTES, CRÉATEURS, INNOVATEURS ET PME

INCLUSION ÉCONOMIQUE — ARTISANS — AGRICULTEURS — ÉLEVEURS — ARTISTES — CRÉATEURS — INNOVATEURS — PME — TRAÇABILITÉ — AP LÉGER — AP BUSINESS — PASSEPORT NUMÉRIQUE UNIVERSEL

1. Objet du chapitre

Ce chapitre définit l'ouverture de Deep Authenticity© aux artisans, agriculteurs, éleveurs, artistes, créateurs, innovateurs, petites entreprises et producteurs locaux. Une infrastructure universelle de confiance ne peut être réservée aux grands groupes : elle doit permettre aux acteurs de petite taille de prouver origine, authenticité, provenance et valeur sans supporter une complexité technologique disproportionnée.

2. Principe de démocratisation de la confiance

La capacité à démontrer l'origine d'un produit ou d'une création peut constituer un avantage économique majeur. Deep Authenticity© vise à rendre cette capacité accessible à des acteurs qui ne disposent ni d'un service informatique important ni d'un ERP complexe. L'architecture doit donc offrir plusieurs niveaux d'intégration.

3. AP Léger

AP Léger constitue un mode simplifié d'accès aux fonctions essentielles de l'écosystème. Il peut permettre l'enregistrement d'une identité professionnelle, la création de références, l'activation de produits, la consultation d'un tableau de bord et l'accès à AP Business depuis un smartphone ou une interface légère.

4. Identité du petit producteur

L'artisan, exploitant, artiste ou PME doit pouvoir établir une identité professionnelle proportionnée à son activité. Les exigences de vérification peuvent varier selon le secteur, la valeur des produits et les obligations réglementaires. L'objectif est d'assurer la confiance sans créer une barrière administrative inutile.

5. Trois QR codes accessibles aux petites structures

Dans le domaine physique, les trois QR codes d'Authenticity Plus© restent la fondation anti-contrefaçon, y compris pour les petites structures : consommateur, revendeur/professionnel et contrôle/douanes. Les processus de génération, impression et activation doivent pouvoir être adaptés à de faibles volumes tout en conservant la sécurité.

6. Artisanat et origine

Un artisan peut associer une création à son identité, son atelier, sa série ou ses matériaux lorsque ces informations sont pertinents. Le Passeport Numérique Universel peut préserver l'histoire de l'objet et renforcer la différenciation entre production authentique et imitation.

7. Agriculture et provenance

Un agriculteur ou groupement peut utiliser Deep Authenticity© pour relier un produit à une exploitation, une récolte, un lot, une origine ou des certifications autorisées. La plateforme doit distinguer les déclarations du producteur des certifications délivrées par une autorité ou un organisme tiers.

8. Élevage et chaîne de provenance

Pour les produits issus de l'élevage, la traçabilité peut relier exploitation, lot, transformation et distribution selon les exigences du secteur. Les données sensibles ou réglementées restent accessibles uniquement aux acteurs habilités. Deep Authenticity© complète les systèmes sanitaires officiels sans s'y substituer.

9. Artistes et œuvres physiques

Un artiste peut associer une œuvre physique à son identité et à un Passeport Numérique Universel. Les événements de création, exposition, vente et transfert peuvent former une provenance vérifiable. La preuve technique renforce l'attribution sans remplacer les droits de propriété intellectuelle définis par la loi.

10. Créateurs et contenus numériques

Pour les créations numériques, la signature cryptographique native peut établir provenance et intégrité dès l'émission. Un créateur peut ainsi disposer d'un mécanisme technique permettant de démontrer qu'une version déterminée provient de son identité reconnue. L'authenticité cryptographique reste distincte de la vérité factuelle du contenu.

11. Innovateurs et petites séries

Les inventeurs, designers et jeunes entreprises produisent souvent des prototypes ou petites séries. Deep Authenticity© doit permettre d'identifier ces unités sans imposer les coûts d'une infrastructure industrielle lourde. Les volumes et fonctions peuvent évoluer progressivement avec la croissance de l'entreprise.

12. PME et intégration progressive

Une PME peut commencer avec AP Léger puis connecter progressivement caisse, ERP, stock ou API. Le modèle doit éviter une migration disruptive : les identités et Passeports Numériques Universels créés au départ continuent lorsque l'organisation adopte des intégrations plus avancées.

13. Tableau de bord simplifié

Le tableau de bord destiné aux petites structures peut présenter produits créés, activations, scans, ventes, alertes, stocks et demandes commerciales. Les indicateurs prioritaires doivent être compréhensibles sans expertise analytique. Les fonctions avancées peuvent être activées selon les besoins.

14. AP Business et accès au marché

AP Business peut donner aux petits producteurs une visibilité commerciale fondée sur des identités vérifiées. Le consommateur peut rechercher un produit, identifier son origine et trouver un point de vente ou producteur autorisé. Cette visibilité peut réduire la dépendance aux intermédiaires purement informationnels.

15. Circuits courts et proximité

La recherche géographique peut soutenir marchés locaux, vente directe, coopératives et circuits courts. Un utilisateur peut rechercher un produit authentifié à proximité lorsque les producteurs choisissent de publier leur disponibilité. Les adresses privées et données de localisation sensibles doivent rester protégées.

16. Coopératives et mutualisation

Plusieurs petits producteurs peuvent partager certaines infrastructures au sein d'une coopérative ou organisation tout en conservant leurs identités propres. Des rôles délégués peuvent permettre l' impression de codes, la gestion logistique ou la commercialisation mutualisée sans effacer la provenance individuelle.

17. Coût, SaaS et accessibilité

Le modèle économique doit permettre des offres proportionnées aux volumes et capacités des petites structures. Abonnements simplifiés, tarification progressive ou programmes institutionnels peuvent favoriser l'adoption. L'accessibilité économique ne doit toutefois pas conduire à réduire les mécanismes essentiels de sécurité.

18. Inclusion numérique et Online/Offline

Dans les zones rurales ou faiblement connectées, Online/Offline devient essentiel. Certaines opérations peuvent être préparées ou vérifiées localement puis synchronisées. Les interfaces doivent être adaptées au smartphone et, lorsque nécessaire, à des processus assistés par des coopératives ou administrations.

19. Impact économique et souveraineté locale

En rendant la provenance et l'identité vérifiables, Deep Authenticity© peut renforcer la capacité des producteurs locaux à différencier leurs produits, protéger leur réputation et accéder à de nouveaux marchés. À l'échelle publique, ces données agrégées peuvent améliorer la compréhension des filières sans transformer la plateforme en instrument de contrôle excessif.

20. Critères d'acceptation et conclusion

L'inclusion économique est cohérente si les petites structures disposent d'un parcours simplifié ; si AP Léger réduit la complexité sans supprimer les contrôles essentiels ; si les trois QR codes restent accessibles aux faibles volumes ; si artisans, agriculteurs, éleveurs, artistes, créateurs et innovateurs disposent de modèles adaptés ; si les PME peuvent évoluer vers ERP/API sans perdre leur historique ; si AP Business et la proximité soutiennent l'accès au marché ; si coopératives et mutualisation sont possibles ; si SaaS et tarification restent proportionnés ; et si Online/Offline permet l'usage dans les zones faiblement connectées.

Deep Authenticity© étend ainsi la confiance économique au-delà des grandes marques : l'authenticité, la provenance et la visibilité deviennent des infrastructures accessibles aux acteurs qui constituent le tissu productif local.

Le Chapitre 11 développera AP Finance : architecture financière de Deep Authenticity©, relation entre identité économique, transaction, preuve et services financiers.

Note de cadrage institutionnel

Les exigences réglementaires diffèrent fortement entre artisanat, agriculture, élevage, alimentation, œuvres, propriété intellectuelle et autres secteurs. Deep Authenticity© doit compléter les certifications, registres et contrôles officiels applicables. Les modèles d'accessibilité économique doivent préserver les exigences fondamentales de sécurité et de confiance.

CHAPITRE 11 — AP FINANCE : ARCHITECTURE FINANCIÈRE DE CONFIANCE

AP FINANCE — IDENTITÉ ÉCONOMIQUE — TRANSACTION — PREUVE — PRODUIT — PROPRIÉTÉ — AP CORE — AP LEDGER — AP PAY — CONFORMITÉ — INTEROPÉRABILITÉ FINANCIÈRE

1. Objet du chapitre

Ce chapitre définit AP Finance comme la couche de Deep Authenticity© destinée à relier, lorsque cela est autorisé, l'identité économique des acteurs, l'identité des actifs, les événements commerciaux et les preuves financières. AP Finance ne se substitue pas aux institutions financières : elle organise une continuité de confiance autour des opérations économiques.

2. Principe fondamental

Dans l'architecture de Deep Authenticity©, une transaction financière ne doit pas être isolée de son contexte lorsque ce contexte est nécessaire et légalement partageable. AP Finance peut relier une référence de paiement à un produit, un service, une facture, un transfert de propriété ou un événement commercial sans transformer toutes les données financières en données publiques.

3. Identité économique des acteurs

Producteur, revendeur, entreprise, professionnel ou acquéreur disposent d'identités et de rôles distincts. AP Finance exploite ces identités selon le niveau de vérification requis par le service. Les obligations réglementaires d'identification restent celles imposées aux acteurs financiers compétents.

4. Identité de la transaction

Chaque opération orchestrée peut recevoir une référence persistante permettant de relier demande, autorisation, exécution, règlement et preuve. Cette identité transactionnelle facilite l'audit et le rapprochement sans exiger qu'AP Finance détienne elle-même les fonds.

5. Relation produit–transaction

Lorsqu'un paiement concerne un produit authentifié, la référence de transaction peut être reliée à son identité persistante. Cette liaison permet de vérifier qu'un événement financier correspond à un actif déterminé, tout en conservant une séparation entre preuve d'authenticité, preuve de paiement et preuve de propriété.

6. Relation transaction–propriété

Un paiement réussi ne constitue pas automatiquement un transfert de propriété. AP Finance transmet ou confirme le contexte financier ; le moteur de propriété applique séparément les règles de transfert. Cette séparation permet de gérer livraison, annulation, litige, remboursement ou paiement par un tiers.

7. AP Core et orchestration financière

AP Core contrôle les droits, états et dépendances entre événements. Il peut vérifier qu'une opération commerciale existe avant d'autoriser certaines transitions et empêcher les doublons logiques. Les décisions purement financières réglementées restent sous la responsabilité des prestataires compétents.

8. AP Ledger et preuve financière

AP Ledger peut ancrer des empreintes, signatures, horodatages et références d'événements financiers critiques. Il fournit une piste d'audit sans nécessairement enregistrer montants détaillés, données bancaires ou informations personnelles en clair.

9. AP Finance et AP Business

AP Business fournit le contexte commercial : produit, vendeur, acheteur, commande ou service. AP Finance reçoit les éléments strictement nécessaires pour orchestrer ou rapprocher l'événement financier. Les conditions commerciales sensibles restent compartimentées.

10. AP Finance et AP Pay

AP Pay constitue la couche opérationnelle de paiement envisagée au sein de l'écosystème. AP Finance représente l'architecture plus large de relations, preuves, règles et services financiers ; AP Pay en constitue un mécanisme d'exécution ou d'orchestration des paiements selon les intégrations autorisées.

11. Interopérabilité bancaire et financière

AP Finance doit pouvoir interagir avec banques, établissements de paiement, réseaux, fintechs et infrastructures nationales ou internationales par des interfaces sécurisées. L'objectif n'est pas de recréer systématiquement ces réseaux, mais de leur fournir un contexte de confiance et de recevoir des confirmations vérifiables.

12. Rapprochement et réconciliation

La plateforme peut rapprocher commande, facture, paiement, livraison et transfert de propriété. Les événements restent séparés mais reliés. Les écarts — paiement sans livraison, double référence, montant incohérent ou transfert sans événement attendu — peuvent être signalés pour traitement.

13. Paiements partiels, acomptes et échéances

Certaines transactions comportent acompte, paiement fractionné ou échéancier. AP Finance doit représenter ces états sans considérer la première autorisation comme règlement complet. Le transfert de propriété peut dépendre de règles commerciales ou juridiques spécifiques.

14. Remboursements et annulations

Un remboursement constitue un nouvel événement financier et ne doit pas effacer le paiement initial. Les annulations, rétrofacturations ou corrections doivent préserver la piste d'audit. Les conséquences sur la propriété et le stock sont appliquées par les modules concernés.

15. Financement et services associés

À terme, des institutions autorisées peuvent utiliser des preuves de provenance, de propriété ou d' activité pour proposer financement, assurance ou autres services. Deep Authenticity© fournit alors des attestations ou données autorisées ; elle ne doit pas produire elle-même une décision de crédit ou d'assurance sans cadre réglementaire approprié.

16. Lutte contre la fraude

La relation entre identité, produit, transaction et propriété peut contribuer à détecter certaines incohérences : actifs inexistants, références dupliquées, schémas transactionnels anormaux ou changements incompatibles. Les signaux algorithmiques doivent rester distincts des décisions réglementaires ou judiciaires.

17. Confidentialité financière

Les données financières sont fortement sensibles. AP Finance applique minimisation, chiffrement, contrôle d'accès, journalisation et séparation des environnements. Un producteur ou revendeur ne

reçoit pas automatiquement les données bancaires d'un acquéreur parce qu'il participe à la même chaîne commerciale.

18. Conformité et gouvernance

Les services doivent être adaptés aux obligations applicables : paiement, identification, lutte contre le blanchiment, sanctions, protection des consommateurs, fiscalité, conservation et localisation des données. Les responsabilités entre Deep Authenticity© et les prestataires réglementés doivent être contractuellement explicites.

19. Souveraineté et architecture fédérée

Les États et institutions peuvent exiger que certaines données ou traitements financiers restent sous contrôle national. AP Finance peut fonctionner dans une architecture fédérée où seules les attestations nécessaires traversent les Corridors de Confiance. L'interopérabilité internationale n'exige donc pas une centralisation universelle des données financières.

20. Critères d'acceptation et conclusion

AP Finance est cohérent si identité des acteurs, transaction, produit et propriété restent distincts mais reliables ; si AP Core orchestre les dépendances ; si AP Ledger peut ancrer les preuves ; si AP Business fournit le contexte commercial ; si AP Pay reste la couche de paiement ; si banques et prestataires existants sont interopérables ; si rapprochement, paiements partiels et remboursements conservent une histoire complète ; si fraude et conformité sont gouvernées ; et si confidentialité et souveraineté financière sont protégées.

AP Finance transforme ainsi la traçabilité économique en continuité financière de confiance : une transaction peut être replacée dans son contexte vérifiable sans confondre paiement, authenticité et propriété.

Le Chapitre 12 développera AP Pay : paiement, règlement, orchestration des flux et articulation avec les infrastructures financières existantes.

Note de cadrage institutionnel

AP Finance constitue une architecture de confiance et d'orchestration. Les activités réglementées de paiement, monnaie électronique, crédit, dépôt, change, assurance ou services d'investissement ne peuvent être exercées que dans les cadres juridiques et avec les agréments requis. Deep Authenticity© doit s'intégrer aux acteurs autorisés lorsque la réglementation l'exige.

CHAPITRE 12 — AP PAY : PAIEMENT, RÈGLEMENT ET ORCHESTRATION DES FLUX

AP PAY — PAIEMENT — RÈGLEMENT — ORCHESTRATION — AP FINANCE — AP CORE — AP LEDGER — PRODUIT — TRANSACTION — PROPRIÉTÉ — INTEROPÉRABILITÉ — CONFORMITÉ

1. Objet du chapitre

Ce chapitre définit AP Pay comme la couche opérationnelle de paiement et d'orchestration financière de Deep Authenticity©. AP Pay vise à relier une intention de paiement à un contexte économique vérifiable — produit, service, commande ou transfert — puis à recevoir et distribuer les confirmations nécessaires sans confondre paiement, règlement et propriété.

2. Positionnement d'AP Pay

AP Pay s'inscrit à l'intérieur de l'architecture plus large d'AP Finance. AP Finance structure les relations financières, les preuves et la gouvernance ; AP Pay orchestre les opérations de paiement autorisées. Selon les juridictions, l'exécution monétaire peut être réalisée par des banques, établissements de paiement, réseaux ou autres prestataires réglementés.

3. Identité de l'opération

Chaque paiement peut recevoir une référence persistante reliée au contexte commercial. Cette référence permet de suivre initiation, autorisation, exécution, confirmation, remboursement ou échec. Elle facilite le rapprochement sans exposer publiquement les coordonnées financières des parties.

4. Initiation du paiement

Une demande de paiement peut provenir d'AP Business, d'une vente chez un revendeur, d'une opération B2B ou d'un autre module autorisé. AP Pay reçoit le montant, la devise, les parties et les références nécessaires. Les données sont validées avant transmission au prestataire financier compétent.

5. Authentification et autorisation

L'utilisateur doit autoriser le paiement selon les mécanismes exigés par le canal et la réglementation. AP Pay ne doit jamais considérer la simple possession d'un QR code produit comme une autorisation financière. L'identité économique du produit et l'identité du payeur restent des dimensions distinctes.

6. Exécution via les infrastructures existantes

AP Pay peut transmettre l'instruction à une banque, un établissement de paiement, un réseau de cartes, un portefeuille ou une infrastructure nationale compatible. La confirmation reçue est reliée à l' identité de l'opération. L'architecture privilégie l'interopérabilité plutôt que la reconstruction systématique des rails financiers.

7. Paiement et règlement

L'autorisation d'un paiement et son règlement final ne sont pas toujours simultanés. AP Pay doit représenter les états intermédiaires : initié, autorisé, en traitement, réglé, refusé, expiré ou remboursé. Les transitions sont horodatées et traçables.

8. AP Core et orchestration

AP Core contrôle la cohérence entre le paiement et les événements de Deep Authenticity©. Il peut empêcher une même référence d'être appliquée plusieurs fois et coordonner les transitions vers livraison ou propriété lorsque les conditions prévues sont remplies. Les décisions réglementées du prestataire financier restent externes.

9. AP Ledger et preuve de paiement

AP Ledger peut ancrer l'empreinte d'une confirmation, d'un reçu ou d'un événement critique. La preuve établit qu'une information déterminée a été enregistrée à un instant donné sans exiger le stockage public des données bancaires ou du moyen de paiement.

10. AP Pay et AP Business

AP Business fournit le contexte de la transaction : vendeur, produit, commande, prix ou référence. AP Pay traite la dimension financière autorisée et renvoie un statut vérifiable. Cette séparation permet à Deep Authenticity© de rester compatible avec plusieurs canaux de vente et prestataires de paiement.

11. AP Pay et transfert de propriété

Le paiement peut être une condition du transfert de propriété mais ne le déclenche pas nécessairement à lui seul. La remise du bien, l'acceptation de l'acquéreur ou d'autres conditions peuvent être requises. Le moteur de propriété reste l'autorité fonctionnelle de la transition patrimoniale.

12. Paiements B2C

Dans un parcours B2C, AP Pay peut simplifier le lien entre produit authentifié, revendeur reconnu et paiement. L'acheteur peut recevoir une confirmation reliée à la transaction et au produit. Les obligations de remboursement, contestation et protection du consommateur restent applicables.

13. Paiements B2B

Les opérations B2B peuvent comporter factures, bons de commande, paiements partiels, échéances et rapprochements multiples. AP Pay doit supporter ces références sans réduire la relation commerciale à un paiement instantané. Les systèmes comptables et ERP peuvent être synchronisés par API.

14. Remboursement et rétrofacturation

Un remboursement ou une rétrofacturation constitue un événement distinct. AP Pay conserve le lien avec l'opération initiale et transmet l'état aux modules concernés. Le stock, la vente et la propriété ne sont modifiés que selon leurs propres règles.

15. Paiement conditionnel et séquencement

Certains parcours peuvent nécessiter un séquencement : autorisation avant expédition, confirmation après livraison ou libération après acceptation. AP Pay peut orchestrer ces étapes avec des prestataires habilités. Les mécanismes assimilables à l'entiercement ou à la conservation de fonds exigent le cadre réglementaire approprié.

16. Devises et conversion

Les transactions peuvent impliquer plusieurs devises. AP Pay peut transmettre les informations de devise et recevoir les résultats de conversion d'un prestataire autorisé. Les taux, frais et responsabilités doivent être transparents. AP Pay ne devient pas automatiquement opérateur de change.

17. Sécurité et lutte contre la fraude

AP Shield protège API, sessions, identités techniques et événements sensibles. Des règles peuvent détecter répétitions, incohérences de contexte ou comportements anormaux. Les signaux de risque complètent les mécanismes antifraude des prestataires financiers sans les remplacer.

18. Confidentialité et conformité

Les données de paiement sont minimisées et compartimentées. Lorsque cela est possible, Deep Authenticity© conserve des références ou jetons plutôt que les données financières brutes. Les exigences applicables d'authentification, lutte contre le blanchiment, sanctions, conservation et protection des consommateurs doivent être respectées.

19. Souveraineté et interopérabilité

AP Pay doit pouvoir s'adapter aux infrastructures nationales, régionales et internationales. Une architecture fédérée permet aux données sensibles de rester dans leur juridiction tandis que les attestations nécessaires circulent. Cette conception prépare les paiements transfrontaliers sans imposer un système monétaire centralisé.

20. Critères d'acceptation et conclusion

AP Pay est cohérent si chaque opération dispose d'une identité traçable ; si initiation, autorisation, exécution et règlement sont distingués ; si AP Core orchestre les dépendances et AP Ledger peut ancrer les preuves ; si AP Business fournit le contexte commercial ; si paiement et propriété restent séparés ; si B2C, B2B, remboursements, paiements conditionnels et devises sont représentables ; si les prestataires réglementés exécutent les activités qui leur sont réservées ; et si sécurité, confidentialité, conformité et souveraineté sont intégrées.

AP Pay devient ainsi le mécanisme qui relie la confiance sur l'actif à la confiance sur l'événement financier, sans prétendre remplacer les infrastructures monétaires et bancaires qui assurent juridiquement le mouvement des fonds.

Le Chapitre 13 développera AP Pay et les paiements transfrontaliers : interopérabilité internationale, corridors financiers de confiance, change, règlement et articulation avec les infrastructures existantes.

Note de cadrage institutionnel

AP Pay est décrit comme une couche d'orchestration et d'intégration. Toute activité de paiement, monnaie électronique, conservation de fonds, change ou autre service financier réglementé doit être exercée par une entité disposant des autorisations requises. Les architectures finales doivent être validées juridiquement et techniquement dans chaque juridiction.

CHAPITRE 13 — AP PAY ET PAIEMENTS TRANSFRONTALIERS : CORRIDORS FINANCIERS DE CONFIANCE

AP PAY — TRANSFRONTALIER — CORRIDORS DE CONFIANCE — INTEROPÉRABILITÉ — CHANGE — RÈGLEMENT — AP FINANCE — AP CORE — AP LEDGER — CONFORMITÉ — SOUVERAINETÉ

1. Objet du chapitre

Ce chapitre définit l'extension transfrontalière d'AP Pay. L'objectif est de relier une transaction commerciale internationale à des identités, actifs et preuves vérifiables, puis d'orchestrer son paiement à travers les infrastructures financières autorisées des juridictions concernées. AP Pay ne crée pas une monnaie universelle : il fournit une couche de confiance et d'interopérabilité.

2. Problématique transfrontalière

Un paiement international traverse potentiellement plusieurs banques, prestataires, devises, systèmes de règlement et cadres réglementaires. Les informations commerciales et financières peuvent être fragmentées. Deep Authenticity© vise à maintenir une référence cohérente reliant produit, transaction, parties, paiement et événements de propriété.

3. Corridors financiers de confiance

Un Corridor de Confiance peut relier deux ou plusieurs écosystèmes nationaux ou institutionnels selon des règles communes d'interopérabilité. Chaque partie conserve la maîtrise de ses infrastructures critiques tandis que les attestations nécessaires à la transaction sont échangées de manière sécurisée et traçable.

4. Identité des parties

Les identités du vendeur, de l'acheteur et des intermédiaires sont vérifiées selon les exigences applicables. Les attestations peuvent confirmer certains attributs sans transférer l'intégralité des dossiers d'identité. Cette approche soutient la minimisation des données et la souveraineté.

5. Identité du produit et contexte commercial

Lorsqu'une transaction concerne un produit authentifié, son identité persistante et les références commerciales peuvent accompagner l'opération. Les parties financières n'accèdent qu'aux informations nécessaires à leur fonction. L'authenticité du produit ne garantit pas, à elle seule, la conformité financière de la transaction.

6. Initiation d'un paiement international

AP Business ou un système externe peut transmettre à AP Pay une demande comprenant montant, devise, bénéficiaire, payeur et référence commerciale. AP Pay valide le contexte et sélectionne ou interroge les voies de paiement compatibles selon les intégrations disponibles.

7. Routage et interopérabilité

AP Pay peut orchestrer plusieurs prestataires ou infrastructures sans imposer un rail unique. Les critères de routage peuvent inclure disponibilité, devise, juridiction, coût, délai, exigences de conformité et niveau de service. Les règles doivent être transparentes pour les acteurs concernés.

8. Change et conversion de devises

Lorsque les devises diffèrent, la conversion est effectuée par un acteur habilité. AP Pay peut transmettre les paramètres, recevoir le taux appliqué, les frais et le résultat, puis relier ces éléments à la transaction. Le taux utilisé et son horodatage doivent rester vérifiables.

9. Autorisation, compensation et règlement

L'autorisation, la compensation et le règlement final constituent des étapes distinctes. AP Pay conserve leur état et les confirmations disponibles. Une transaction ne doit être déclarée définitivement réglée qu'après réception d'une preuve correspondant au niveau de finalité exigé.

10. AP Core et machine d'état transfrontalière

AP Core orchestre les transitions entre contexte commercial, paiement et événements ultérieurs. Il gère idempotence, expiration, reprise et exceptions. Les règles peuvent différer selon les corridors, mais la plateforme doit éviter qu'une interruption ou un message répété produise plusieurs effets économiques.

11. AP Ledger et preuve inter-juridictionnelle

AP Ledger peut ancrer les empreintes des confirmations et attestations échangées. Ces preuves permettent de reconstruire la séquence d'une opération sans centraliser toutes les données financières. Les juridictions peuvent conserver leurs registres locaux tout en partageant des références vérifiables.

12. Articulation avec les infrastructures existantes

AP Pay doit pouvoir s'intégrer aux réseaux bancaires, systèmes de paiement, infrastructures de marché et prestataires internationaux autorisés. Son rôle est d'ajouter contexte, orchestration et preuve, non de prétendre remplacer universellement les infrastructures qui assurent aujourd'hui messagerie, compensation ou règlement.

13. Conformité multi-juridictionnelle

Chaque corridor doit appliquer les obligations pertinentes : identification, lutte contre le blanchiment, sanctions, contrôle des changes, fiscalité, protection des consommateurs et règles de données. Une transaction acceptable dans un pays peut nécessiter des contrôles supplémentaires dans un autre.

14. Sanctions et contrôles

Les prestataires réglementés conservent leurs obligations de filtrage et de décision. AP Pay peut transmettre les attributs requis et recevoir un statut. Un blocage doit conserver sa source et son motif selon les droits d'accès, afin de permettre audit et résolution sans divulgation excessive.

15. Commerce, douanes et paiement

Dans le commerce de biens, le paiement international peut être relié à des événements logistiques ou douaniers lorsque les autorités et acteurs concernés participent au corridor. Le QR contrôle/douanes et les preuves de Deep Authenticity© peuvent enrichir le contexte physique sans devenir un moyen de paiement.

16. Paiement conditionnel international

Certaines opérations peuvent prévoir paiement par étapes selon expédition, réception, inspection ou autres conditions. AP Pay peut orchestrer les déclencheurs et confirmations avec des prestataires habilités. La conservation ou libération de fonds reste une activité réglementée lorsqu'elle relève de l' entiercement.

17. Gestion des exceptions et litiges

Retard, rejet, différence de montant, erreur de bénéficiaire, remboursement ou contestation doivent produire des événements traçables. AP Pay conserve la chaîne technique et facilite le rapprochement. La résolution juridique ou bancaire demeure du ressort des parties et institutions compétentes.

18. Coût, délai et transparence

Un paiement transfrontalier peut comporter frais de réseau, conversion, banque ou intermédiaire. AP Pay doit, lorsque les données sont disponibles, présenter clairement montant initial, frais connus, conversion et montant attendu. Cette transparence améliore la compréhension du coût réel de l'échange.

19. Souveraineté financière et fédération

L'architecture doit permettre à un État de conserver données sensibles, clés et contrôles critiques sur son territoire tout en participant à des échanges internationaux. La fédération remplace l'idée d'une base financière mondiale unique : les preuves circulent, tandis que la souveraineté des systèmes participants demeure.

20. Critères d'acceptation et conclusion

Le paiement transfrontalier est cohérent si les parties et le contexte commercial sont identifiables ; si les Corridors de Confiance fédèrent sans centraliser ; si routage, change, autorisation, compensation et règlement sont distingués ; si AP Core orchestre les états et AP Ledger ancre les preuves ; si les infrastructures existantes restent interopérables ; si conformité, sanctions, douanes, paiements conditionnels et litiges sont gouvernés ; et si coûts, délais et souveraineté sont transparents. AP Pay peut ainsi devenir une couche d'orchestration transfrontalière reliant la confiance sur les acteurs, les produits et les transactions aux infrastructures qui déplacent effectivement les fonds.

Le Chapitre 14 développera la traçabilité économique et le rapprochement produit–transaction–propriété : constitution d'une chaîne économique vérifiable de bout en bout.

Note de cadrage institutionnel

Les paiements transfrontaliers sont soumis à des réglementations financières, monétaires, de sanctions, de change, fiscales et de données qui varient selon les juridictions. AP Pay doit fonctionner avec des banques et prestataires dûment autorisés. Les références à l'interopérabilité ne signifient pas qu'AP Pay dispose, par lui-même, d'un accès ou d'une capacité de règlement sur les réseaux financiers existants.

CHAPITRE 14 — TRAÇABILITÉ ÉCONOMIQUE : RAPPROCHEMENT PRODUIT–TRANSACTION–PROPRIÉTÉ

TRAÇABILITÉ ÉCONOMIQUE — PRODUIT — TRANSACTION — PROPRIÉTÉ — PASSEPORT NUMÉRIQUE UNIVERSEL — AP CORE — AP LEDGER — AP BUSINESS — AP FINANCE — AP PAY — AUDIT — SOUVERAINETÉ

1. Objet du chapitre

Ce chapitre définit la traçabilité économique de Deep Authenticity© comme la capacité à relier, sans les confondre, trois continuités fondamentales : l'identité du produit, l'histoire des transactions et l'évolution de la propriété. L'objectif est de constituer une chaîne économique vérifiable de bout en bout, depuis la production jusqu'aux acquisitions successives.

2. Les trois continuités

La continuité produit décrit l'identité et le cycle de vie de l'actif. La continuité transactionnelle décrit commandes, ventes, paiements, remboursements et règlements. La continuité patrimoniale décrit les relations de propriété et leurs transferts. Leur rapprochement crée une vision économique cohérente tout en conservant des preuves distinctes.

3. Identité persistante du produit

Le produit conserve la même identité à travers production, distribution, première vente et seconde main. Les trois QR codes d'Authenticity Plus© constituent la fondation du domaine physique, tandis que le Passeport Numérique Universel agrège les événements autorisés autour de cette identité persistante.

4. Identité de la transaction

Chaque événement commercial ou financier important peut recevoir une référence permettant de le relier à son contexte. Commande, facture, paiement et règlement ne sont pas fusionnés : chacun conserve son statut, sa source et son horodatage.

5. Identité patrimoniale

La relation entre l'actif et son propriétaire évolue par événements contrôlés. Première acquisition, transfert, donation, succession ou autre changement reconnu sont enregistrés selon les règles applicables. La possession physique ou le paiement seul ne suffit pas nécessairement à modifier cette relation.

6. Rapprochement par AP Core

AP Core agit comme moteur de cohérence entre les trois continuités. Il vérifie les références, états, droits et dépendances avant de déclencher une transition. Il peut signaler un paiement sans vente reconnue, une vente sans produit valide ou un transfert patrimonial incohérent.

7. AP Ledger et chaîne de preuve

AP Ledger peut ancrer les événements critiques des trois dimensions : activation d'un produit, vente, confirmation financière, transfert de propriété ou rectification. Les empreintes et signatures permettent de reconstruire l'histoire probante sans publier l'ensemble des données opérationnelles.

8. Passeport Numérique Universel

Le Passeport Numérique Universel constitue la mémoire de cycle de vie de l'actif. Il référence les événements industriels, commerciaux, techniques et patrimoniaux selon les droits d'accès. Il ne devient pas un dossier public exhaustif : chaque acteur reçoit une vue proportionnée à son rôle.

9. Producteur et origine de la chaîne

Le producteur initie l'identité et les données d'origine. Ses systèmes peuvent fournir références, lots, activation et événements de distribution. Cette origine constitue le premier maillon de la chaîne économique, mais elle ne donne pas au producteur un contrôle illimité sur les événements ultérieurs.

10. Revendeur et continuité commerciale

Le revendeur fait entrer le produit dans son stock authentifié, publie sa disponibilité et confirme la vente. Ces événements permettent de relier la distribution réelle à l'identité du produit et de préparer la transition vers le premier acquéreur.

11. Premier acquéreur et naissance patrimoniale

La première acquisition crée, lorsque le modèle le permet, la première relation de propriété numérique. La preuve de vente, le paiement et l'acceptation peuvent être rapprochés tout en restant distincts. Le produit entre alors dans son cycle patrimonial.

12. Seconde main et continuité

Lors d'une revente, l'identité du produit ne change pas. Une nouvelle transaction commerciale et, après validation, un nouveau transfert patrimonial sont ajoutés. La provenance peut ainsi être prolongée sur plusieurs propriétaires sans révéler publiquement leur identité.

13. AP Business, AP Finance et AP Pay

AP Business fournit le contexte marchand ; AP Finance structure les relations financières ; AP Pay orchestre les paiements ; la couche Propriété contrôle la transition patrimoniale. AP Core relie ces modules par des références communes et des règles de cohérence.

14. Rapprochement comptable et ERP

Les ERP, systèmes de caisse et outils comptables peuvent fournir ou recevoir les références nécessaires au rapprochement. Deep Authenticity© n'a pas vocation à remplacer la comptabilité légale : elle peut fournir une couche supplémentaire permettant de relier les écritures ou pièces aux actifs et événements authentifiés.

15. Détection des incohérences

La chaîne peut révéler des anomalies : produit vendu avant activation, même unité vendue simultanément dans plusieurs lieux, paiement répété, transfert sans vendeur habilité ou stock incompatible. Ces signaux déclenchent une investigation et ne constituent pas automatiquement une preuve de fraude.

16. Rappels, retours et remboursements

Un retour ou remboursement ne supprime pas les événements antérieurs. La chaîne conserve vente, paiement, retour, remboursement et éventuelle restitution de propriété comme événements successifs. Cette approche évite de réécrire l'histoire et facilite l'audit.

17. Audit et preuve institutionnelle

Les acteurs habilités peuvent reconstruire une séquence économique à partir des références et preuves disponibles. Les autorités peuvent recevoir des vues spécifiques selon leur compétence. L'audit doit toujours distinguer donnée déclarée, donnée vérifiée, preuve cryptographique et décision institutionnelle.

18. Confidentialité et minimisation

La traçabilité économique ne signifie pas transparence totale. Les informations personnelles, prix négociés, coordonnées bancaires et secrets commerciaux restent compartimentés. Des attestations ou agrégats peuvent démontrer un fait sans divulguer les données sous-jacentes.

19. Souveraineté et analyse économique

À l'échelle agrégée, des données gouvernées peuvent contribuer à comprendre flux de produits, disponibilités, ventes et dynamiques territoriales. Les États peuvent utiliser ces informations pour l'analyse économique dans les cadres légaux applicables. L'architecture fédérée permet de conserver les données sensibles sous contrôle souverain.

20. Critères d'acceptation et conclusion

La traçabilité économique est cohérente si produit, transaction et propriété disposent d'identités et d'histoires distinctes ; si AP Core rapproche leurs événements sans les fusionner ; si AP Ledger peut ancrer les preuves ; si le Passeport Numérique Universel conserve la continuité ; si producteur, revendeur, premier acquéreur et seconde main s'inscrivent dans la même chaîne ; si AP Business, AP Finance et AP Pay partagent des références cohérentes ; si ERP, retours et audits sont intégrables ; et si confidentialité et souveraineté limitent l'accès aux données.

Deep Authenticity© établit ainsi une chaîne économique vérifiable : non seulement savoir ce qu'est un produit, mais comprendre, selon les droits applicables, comment il a circulé, été vendu, payé et transmis.

Le Chapitre 15 développera le modèle SaaS : services, abonnements, niveaux d'offre, tarification, scalabilité et accessibilité de Deep Authenticity©.

Note de cadrage institutionnel

La traçabilité économique doit respecter les règles applicables en matière de données personnelles, secret des affaires, fiscalité, comptabilité, concurrence et services financiers. Les rapprochements techniques de Deep Authenticity© ne remplacent pas les registres, pièces comptables ou décisions ayant une valeur juridique obligatoire.

CHAPITRE 15 — SAAS : MODÈLE DE SERVICES, ABONNEMENTS ET ACCESSIBILITÉ

SAAS — ABONNEMENTS — AP LÉGER — PRODUCTEUR — REVENDEUR — ENTREPRISE — INSTITUTION — SCALABILITÉ — NIVEAUX DE SERVICE — TARIFICATION — SOUVERAINETÉ

1. Objet du chapitre

Ce chapitre définit le modèle SaaS de Deep Authenticity© comme l'un des principaux modes d'accès à ses capacités numériques. Il permet de fournir des services de confiance sous forme d'abonnements ou d'offres modulaires, tout en conservant la possibilité de déploiements privés, hybrides, institutionnels ou souverains lorsque le contexte l'exige.

2. SaaS comme mode d'accès, non comme architecture unique

Le SaaS ne doit pas être confondu avec l'architecture fondamentale de Deep Authenticity©. AP Core, AP Ledger, AP Cloud, AP Shield et les modules peuvent être proposés comme services mutualisés ou déployés dans des environnements dédiés. Le modèle commercial reste donc dissocié du modèle technologique.

3. Segmentation des utilisateurs

Les offres peuvent être adaptées aux artisans, petites structures, PME, producteurs industriels, revendeurs, grands groupes, institutions et administrations. Les besoins diffèrent en volume, intégration, sécurité, support, souveraineté et niveau de service. La segmentation doit refléter ces différences sans fragmenter la chaîne de confiance.

4. AP Léger et offre d'entrée

AP Léger peut constituer une porte d'entrée SaaS simplifiée pour les petits acteurs. Depuis un smartphone ou une interface web, ils peuvent accéder aux fonctions essentielles : identité, références, activation, tableau de bord, scans, alertes et AP Business. La simplicité d'usage ne doit pas supprimer les contrôles de sécurité fondamentaux.

5. Offres pour producteurs

Les producteurs peuvent disposer de niveaux adaptés au nombre de références, unités, utilisateurs, sites et intégrations. Les fonctions avancées peuvent inclure ERP/API, tableaux de bord approfondis, alertes, campagnes de rappel, analytics et capacités sectorielles.

6. Offres pour revendeurs

Les revendeurs peuvent accéder à la Fenêtre Revendeur, aux stocks authentifiés, à la visibilité AP Business, aux ventes, retours, alertes et tableaux de bord. Les réseaux multi-sites peuvent bénéficier de fonctions centralisées de gestion et de délégation.

7. Offres entreprises et grands comptes

Les grands comptes peuvent nécessiter environnements dédiés, haute disponibilité, intégrations complexes, gestion avancée des identités, observabilité, engagements de service et accompagnement. La tarification peut combiner capacité, volume, modules et niveau de support.

8. Offres institutionnelles et souveraines

Les États, autorités et grandes institutions peuvent exiger hébergement local, contrôle des clés, segmentation des données, audit renforcé et exploitation souveraine. Ces offres peuvent prendre la forme de SaaS souverain, cloud privé ou déploiement dédié, avec gouvernance contractuelle spécifique.

9. Modules et options

Le modèle SaaS peut permettre l'activation progressive de modules : AP Business, fonctions de propriété, Seconde Main, analytics, API, connecteurs ERP ou autres services. Les dépendances entre modules doivent être explicites afin qu'une option commerciale ne compromette pas la cohérence technique.

10. Unités de mesure

La tarification peut utiliser plusieurs unités : nombre d'unités authentifiées, références, utilisateurs, établissements, appels API, stockage ou niveau de service. Les métriques doivent être compréhensibles, auditables et adaptées au secteur. Une unité de facturation ne doit pas devenir artificiellement complexe.

11. Abonnements

Les abonnements peuvent être mensuels, annuels ou contractuels selon le segment. Ils peuvent couvrir l'accès à la plateforme, support, mises à jour et quotas définis. Les dépassements, changements de niveau et renouvellements doivent être transparents.

12. Tarification progressive

Une tarification progressive peut réduire la barrière d'entrée des petits acteurs tout en permettant aux grandes organisations de financer les capacités qu'elles consomment. Les paliers doivent éviter les ruptures brutales et permettre à une PME de grandir sans devoir reconstruire son environnement.

13. Essai, pilote et déploiement progressif

Des périodes d'essai, pilotes sectoriels ou environnements de démonstration peuvent faciliter l' adoption. Les limites de ces environnements doivent être clairement indiquées. Un pilote ne doit pas être présenté comme un déploiement de production lorsqu'il ne possède pas les mêmes garanties.

14. Scalabilité

Le SaaS doit absorber la croissance des utilisateurs, produits, scans, événements et intégrations. AP Cloud peut fournir l'élasticité nécessaire tandis qu'AP Shield protège l'augmentation de la surface d' exposition. Les mécanismes critiques doivent être testés sous charge et surveillés.

15. Niveaux de service

Les offres professionnelles peuvent définir disponibilité, temps de réponse du support, objectifs de reprise et autres engagements. Les SLA doivent être mesurables et associés à des responsabilités explicites. Les fonctions critiques institutionnelles peuvent exiger des engagements supérieurs aux offres standard.

16. Réversibilité et portabilité

Un client doit pouvoir récupérer ses données et preuves selon les droits applicables, notamment lors d' un changement d'offre ou de mode de déploiement. La réversibilité réduit la dépendance technologique et soutient la souveraineté. Les formats d'export et délais doivent être contractuellement définis.

17. Sécurité par niveau sans sécurité au rabais

Les niveaux commerciaux peuvent différer en capacité ou services, mais les protections fondamentales — authentification, chiffrement, isolation, journalisation et gestion des vulnérabilités — ne doivent pas devenir optionnelles. La sécurité minimale fait partie du socle de confiance.

18. Facturation, licences et royalties

Le SaaS peut coexister avec licences et royalties. Un acteur peut payer un abonnement pour le service, une licence pour certains droits technologiques et, dans certains modèles, des royalties liées à l' utilisation ou à la valeur créée. Ces mécanismes doivent être séparés contractuellement pour éviter la double facturation ambiguë.

19. Économie d'échelle et accessibilité universelle

La mutualisation SaaS peut réduire le coût unitaire de l'infrastructure et favoriser l'accès des petits producteurs. À grande échelle, l'objectif est de concilier soutenabilité économique, qualité de service et diffusion mondiale. Les modèles institutionnels peuvent également subventionner certains usages d'intérêt public.

20. Critères d'acceptation et conclusion

Le modèle SaaS est cohérent si l'accès commercial reste distinct de l'architecture technique ; si les offres couvrent petits acteurs, entreprises et institutions ; si AP Léger facilite l'entrée ; si modules, unités de mesure et abonnements sont transparents ; si tarification progressive, pilotes et scalabilité soutiennent l'adoption ; si les niveaux de service sont mesurables ; si réversibilité et souveraineté sont garanties ; si la sécurité fondamentale reste commune ; et si SaaS, licences et royalties sont contractuellement distingués.

Le SaaS permet ainsi à Deep Authenticity© de devenir une infrastructure accessible et scalable, capable d'accompagner un artisan comme une institution nationale sans abandonner ses principes de confiance.

Le Chapitre 16 développera les Licences : modèles industriels, institutionnels, sectoriels et territoriaux, droits d'usage, propriété intellectuelle et gouvernance.

Note de cadrage institutionnel

Le modèle SaaS décrit ici constitue une architecture économique de référence. Les prix, quotas, SLA, périodes d'essai, obligations contractuelles et conditions de réversibilité devront être définis selon les marchés, coûts réels, juridictions et niveaux de service. Les fonctions réglementées restent soumises aux autorisations correspondantes.

CHAPITRE 16 — LICENCES : DROITS D'USAGE, PROPRIÉTÉ INTELLECTUELLE ET GOUVERNANCE

LICENCES — PROPRIÉTÉ INTELLECTUELLE — DROITS D'USAGE — INDUSTRIE — INSTITUTIONS — SECTEURS — TERRITOIRES — API — MARQUE — TECHNOLOGIE — GOUVERNANCE — SOUVERAINETÉ

1. Objet du chapitre

Ce chapitre définit le modèle de licences de Deep Authenticity©. La licence organise juridiquement et économiquement le droit d'utiliser certaines technologies, interfaces, marques, modules ou méthodes de l'écosystème sans transférer la propriété intellectuelle sous-jacente. Elle complète le SaaS et peut coexister avec les royalties selon des contrats distincts.

2. Principe de séparation entre propriété et droit d'usage

La propriété intellectuelle d'une technologie et le droit de l'exploiter sont deux notions différentes. Une licence peut autoriser un État, une entreprise ou un partenaire à utiliser une composante déterminée de Deep Authenticity© dans un périmètre défini, sans lui céder les droits fondamentaux sur l'invention, le code, la marque ou la documentation.

3. Périmètre d'une licence

Toute licence doit définir précisément les éléments concernés : logiciels, API, modules, documentation, marque, méthodes, connecteurs, droits de déploiement ou autres actifs. Elle précise également utilisateurs autorisés, durée, territoire, secteur, volumes, environnements et éventuelles restrictions.

4. Licence industrielle

Une licence industrielle peut permettre à un fabricant ou groupe de déployer certaines capacités dans ses usines, chaînes de production ou réseaux logistiques. Elle peut couvrir génération et activation des identités produit, intégrations ERP/API, tableaux de bord et services associés.

5. Licence institutionnelle

Une administration, autorité ou institution peut obtenir des droits d'usage adaptés à ses missions. Les licences institutionnelles peuvent intégrer gouvernance, audit, hébergement souverain, accès de contrôle et interopérabilité avec les systèmes publics, sans modifier la séparation des compétences juridiques.

6. Licence sectorielle

Certaines adaptations peuvent être accordées pour un secteur : pharmacie, agroalimentaire, luxe, automobile, culture, billetterie ou autres domaines. La licence sectorielle définit les fonctions spécifiques et les obligations applicables sans remettre en cause le socle universel de Deep Authenticity©.

7. Licence territoriale

Une licence territoriale peut autoriser un opérateur ou partenaire à déployer certaines capacités dans une zone déterminée. Elle doit éviter toute ambiguïté sur l'exclusivité, la sous-licence, les obligations de couverture et les droits des acteurs déjà présents.

8. Licence souveraine

Pour un État, la licence peut être associée à un déploiement souverain : données hébergées localement, clés sous contrôle national, exploitation par une entité autorisée et interopérabilité via des Corridors de Confiance. La souveraineté opérationnelle n'implique pas nécessairement un transfert de propriété intellectuelle.

9. Licence API et intégration

Les partenaires technologiques peuvent recevoir des droits d'utilisation des API, SDK ou connecteurs. Les limites d'appels, environnements, usages permis et obligations de sécurité doivent être définis. L' accès technique peut être suspendu en cas de compromission ou d'usage incompatible avec les conditions.

10. Licence de marque et certification

L'utilisation des noms, signes, labels ou marques liés à Authenticity Plus© et Deep Authenticity© doit être encadrée séparément. Une licence technologique n'autorise pas automatiquement l'usage promotionnel d'une marque ou d'une certification. Les critères de conformité et règles graphiques doivent être respectés.

11. Licence du mécanisme des trois QR codes

Dans le domaine physique, le mécanisme fondamental des trois QR codes — consommateur, revendeur/professionnel et contrôle/douanes — peut faire l'objet de droits d'exploitation définis. Une licence ne doit pas altérer leurs fonctions essentielles ni la sémantique VERT / JAUNE / ROUGE de la plateforme.

12. Code source et droits techniques

Une licence peut porter sur un service exécutable sans donner accès au code source. Lorsque l'accès au code est nécessaire pour un déploiement souverain ou une intégration spécifique, ses conditions, dépôts, audits, modifications autorisées et obligations de confidentialité doivent être explicitement encadrés.

13. Sous-licence et partenaires

Le droit de sous-licencier ne doit jamais être présumé. Lorsqu'il est autorisé, les catégories de bénéficiaires, territoires et responsabilités sont définies. Le titulaire principal reste soumis aux obligations de sécurité, conformité et reporting prévues au contrat.

14. Durée, renouvellement et résiliation

Les licences peuvent être temporaires, pluriannuelles ou liées à un programme déterminé. Les conditions de renouvellement, suspension et résiliation doivent être connues à l'avance. La fin d'une licence doit prévoir la continuité des preuves et des Passeports Numériques Universels déjà créés.

15. Réversibilité et continuité de confiance

La résiliation commerciale ne doit pas détruire l'histoire d'authenticité des produits déjà enregistrés. Des mécanismes de réversibilité, export ou conservation minimale doivent préserver les preuves nécessaires. La gouvernance des identités existantes doit être définie avant tout déploiement.

16. Audit et conformité du licencié

Le contrat peut prévoir audits techniques, vérification des usages, conformité de sécurité et contrôle des volumes facturables. Les audits doivent respecter confidentialité et proportionnalité. Les mécanismes automatiques de télémétrie doivent être documentés et limités à leur finalité.

17. Protection de la propriété intellectuelle

Les licences doivent protéger brevets, logiciels, secrets d'affaires, marques, documentation et savoir-faire applicables. Les améliorations ou développements spécifiques doivent faire l'objet de clauses déterminant leur propriété, leur réutilisation et les éventuels droits croisés.

18. Licences, SaaS et royalties

SaaS, licence et royalty sont trois instruments différents. Le SaaS rémunère l'accès à un service ; la licence rémunère ou encadre un droit d'usage ; la royalty peut rémunérer l'exploitation selon une assiette convenue. Un contrat combiné doit identifier clairement chaque composante et éviter les doubles prélèvements non transparents.

19. Gouvernance internationale

À l'échelle internationale, les licences doivent permettre l'interopérabilité tout en protégeant le noyau technologique et les exigences de sécurité. Des standards contractuels peuvent faciliter les déploiements multi-pays, mais les lois impératives, sanctions, règles de concurrence et exigences souveraines de chaque juridiction restent applicables.

20. Critères d'acceptation et conclusion

Le modèle de licences est cohérent si propriété intellectuelle et droit d'usage sont séparés ; si chaque licence définit objet, durée, territoire, secteur et utilisateurs ; si modèles industriel, institutionnel, sectoriel, territorial et souverain sont possibles ; si API, marque, trois QR codes et code source sont encadrés ; si sous-licence, résiliation, réversibilité et audit sont gouvernés ; si la propriété intellectuelle reste protégée ; et si SaaS, licences et royalties sont distingués économiquement et contractuellement.

La licence permet ainsi à Deep Authenticity© de se déployer largement sans perdre la maîtrise de son noyau technologique : elle transforme la propriété intellectuelle en capacité d'usage organisée, contrôlée et interopérable.

Le Chapitre 17 développera les Royalties : assiettes, taux, secteurs, gouvernance, transparence, audit et articulation avec le SaaS et les licences.

Note de cadrage institutionnel

Les modèles de licence devront être adaptés aux droits de propriété intellectuelle effectivement détenus ou enregistrés, aux contrats applicables et aux règles de concurrence de chaque juridiction. Toute exclusivité, licence territoriale, utilisation de marque ou accès au code source doit faire l'objet d' une validation juridique spécifique.

CHAPITRE 17 — ROYALTIES : ASSIETTES, TAUX, GOUVERNANCE ET AUDIT

ROYALTIES — REDEVANCES — ASSIETTE — TAUX — SECTEURS — SAAS — LICENCES — AUDIT — TRANSPARENCE — PROPRIÉTÉ INTELLECTUELLE — GOUVERNANCE — SOUVERAINETÉ

1. Objet du chapitre

Ce chapitre définit les royalties comme un mécanisme possible de rémunération de l'exploitation de Deep Authenticity©. Elles peuvent compléter le SaaS et les licences lorsqu'un contrat prévoit une rémunération proportionnelle à une assiette mesurable. Le modèle doit rester transparent, auditable, sectoriellement adaptable et juridiquement proportionné.

2. Définition de la royalty

Une royalty est une redevance liée à l'exploitation d'un droit, d'une technologie, d'un actif intellectuel ou d'un mécanisme contractuellement défini. Elle ne doit pas être confondue avec un abonnement SaaS, des frais de transaction, une taxe publique ou le prix d'une licence forfaitaire.

3. Principe d'assiette explicite

Aucune royalty ne doit être calculée sur une notion ambiguë de « valeur ». Le contrat définit l'assiette : unités authentifiées, chiffre d'affaires attribuable, transactions éligibles, licences exploitées ou autre métrique objectivement vérifiable. Les exclusions, remboursements et corrections sont également définis.

4. Royalties par unité

Pour certains secteurs, une redevance fixe ou graduée par unité authentifiée peut être appropriée. Ce modèle offre une lecture simple lorsque la valeur des produits est relativement homogène. Il doit néanmoins prévoir les unités annulées, détruites, exportées ou non commercialisées selon le contrat.

5. Royalties proportionnelles à la valeur

Pour des biens à forte valeur ou des modèles économiques spécifiques, une royalty peut être exprimée en pourcentage d'une assiette financière convenue. La définition du montant de référence — prix net, chiffre d'affaires net ou autre base — doitêtre précise afin d'éviter les interprétations divergentes.

6. Adaptation sectorielle

Un taux unique mondial n'est pas nécessairement pertinent. Pharmacie, industrie, luxe, artisanat, agriculture, culture, billetterie ou services numériques présentent des marges et contraintes différentes. Les royalties peuvent donc être sectoriellement adaptées tout en respectant des principes communs de gouvernance.

7. Progressivité et seuils

Des seuils de volume ou de valeur peuvent permettre une progressivité. Une petite structure peut bénéficier d'un niveau réduit, tandis qu'une exploitation industrielle importante applique une grille différente. Les seuils doivent éviter les effets de rupture et rester prévisibles.

8. Articulation avec le SaaS

Le SaaS rémunère l'accès continu aux services de la plateforme. Une royalty, lorsqu'elle existe, rémunère une exploitation définie par contrat. Le client doit pouvoir identifier clairement ce qui relève de l'abonnement et ce qui relève de la redevance variable.

9. Articulation avec les licences

Une licence peut être forfaitaire, comporter des royalties ou combiner les deux. Les droits concédés, l'assiette et le taux doivent être explicitement séparés. La détention d'une licence ne signifie donc ni absence automatique de royalty ni obligation automatique d'en payer une.

10. Éviter la double facturation ambiguë

Lorsqu'un même événement déclenche plusieurs composantes économiques, le contrat doit expliquer leur justification. L'objectif est d'éviter qu'une unité soit facturée plusieurs fois sous des intitulés différents sans transparence. Les tableaux de facturation doivent permettre une réconciliation simple.

11. Mesure et données de calcul

AP Core, AP Business ou les systèmes intégrés peuvent produire les événements nécessaires au calcul des royalties. Les métriques facturables doivent être versionnées, horodatées et distinguées des statistiques indicatives. Une donnée non fiable ne doit pas devenir automatiquement une base de facturation.

12. AP Ledger et preuve d'assiette

Lorsque cela est pertinent, AP Ledger peut ancrer des preuves agrégées ou empreintes des événements servant au calcul. Cette approche facilite l'audit entre les parties sans exposer publiquement les données commerciales détaillées.

13. Déclarations et rapprochement

Le licencié ou client peut recevoir un relevé périodique indiquant assiette, exclusions, taux et montant. Les données de Deep Authenticity© peuvent être rapprochées des ERP ou systèmes comptables. Les écarts doivent suivre une procédure de résolution définie.

14. Audit contractuel

Le contrat peut prévoir un droit d'audit proportionné afin de vérifier les royalties. L'audit doit respecter secret des affaires, données personnelles et confidentialité. Sa fréquence, son périmètre, les seuils d'écart et la répartition des coûts doivent être déterminés à l'avance.

15. Gouvernance des taux

Les taux ne doivent pas évoluer arbitrairement pendant une période contractuelle. Les mécanismes de révision, indexation ou renégociation sont définis. Pour les programmes institutionnels ou sectoriels, une gouvernance spécifique peut examiner l'impact économique avant modification.

16. Royalties et petits acteurs

Artisans, petites exploitations, créateurs et PME ne doivent pas subir une structure disproportionnée par rapport à leur activité. Des franchises, plafonds, taux réduits ou modèles alternatifs peuvent être envisagés afin de préserver l'objectif d'accessibilité universelle.

17. Royalties internationales

Les contrats transfrontaliers doivent prendre en compte devises, retenues fiscales, prix de transfert, conventions fiscales et règles locales. Les responsabilités de déclaration et de paiement doivent être explicites. La plateforme ne remplace pas le conseil fiscal ou les obligations des parties.

18. Transparence et tableaux de bord

Un tableau de bord peut permettre au client de suivre en temps quasi réel les événements susceptibles d'entrer dans l'assiette, les montants estimés et les relevés validés. Les estimations doivent être clairement distinguées des factures définitives.

19. Scénarios économiques et prudence

Les royalties peuvent constituer un levier important de revenus lorsque Deep Authenticity© est déployé à grande échelle. Toutefois, les projections doivent distinguer hypothèses, volumes, taux d' adoption et assiettes réellement capturables. Une projection stratégique ne doit pas être présentée comme un revenu garanti.

20. Critères d'acceptation et conclusion

Le modèle de royalties est cohérent si la redevance est distincte du SaaS, de la licence, des frais et des taxes ; si l'assiette est objectivement définie ; si les taux peuvent être adaptés par secteur et volume ; si la double facturation ambiguë est évitée ; si les données de calcul sont traçables ; si AP Ledger peut renforcer la preuve ; si déclarations et audits sont gouvernés ; si les petits acteurs restent accessibles ; et si les dimensions fiscales et internationales sont intégrées.

Les royalties deviennent ainsi un mécanisme de valorisation de la propriété intellectuelle de Deep Authenticity© fondé sur une exploitation mesurable, transparente et auditable, plutôt qu'un prélèvement indifférencié sur l'économie.

Le Chapitre 18 développera le modèle économique consolidé : articulation SaaS–Licences–Royalties, revenus complémentaires, structure de coûts, création de valeur et soutenabilité à l'échelle mondiale.

Note de cadrage institutionnel

Les taux et assiettes de royalties présentés dans les futurs modèles devront être considérés comme des hypothèses économiques tant qu'ils ne sont pas contractualisés. Leur légalité, fiscalité, traitement comptable, concurrence et éventuelle retenue à la source dépendent des juridictions et doivent faire l' objet d'une validation professionnelle.

CHAPITRE 18 — MODÈLE ÉCONOMIQUE CONSOLIDÉ : CRÉATION DE VALEUR ET SOUTENABILITÉ

MODÈLE ÉCONOMIQUE — SAAS — LICENCES — ROYALTIES — REVENUS — COÛTS — CRÉATION DE VALEUR — SCALABILITÉ — ACCESSIBILITÉ — SOUVERAINETÉ — SOUTENABILITÉ

1. Objet du chapitre

Ce chapitre consolide le modèle économique de Deep Authenticity©. Il articule SaaS, licences et royalties dans une architecture de revenus diversifiée, tout en intégrant coûts technologiques, sécurité, opérations, conformité, déploiements souverains et accessibilité. L'objectif est de construire une infrastructure économiquement soutenable sans transformer la confiance en barrière d'accès.

2. Principe économique général

La valeur économique de Deep Authenticity© provient de sa capacité à fournir une infrastructure de confiance utilisable dans plusieurs secteurs et par plusieurs catégories d'acteurs. Le modèle doit rémunérer la technologie, son exploitation et son évolution tout en restant proportionné à la valeur des services effectivement fournis.

3. Premier pilier : SaaS

Le SaaS génère des revenus récurrents liés à l'accès aux services numériques : tableaux de bord, AP Business, API, gestion des identités, événements, alertes, analytics et autres capacités. Les offres peuvent être segmentées selon volumes, modules, niveau de service et mode de déploiement.

4. Deuxième pilier : licences

Les licences rémunèrent ou encadrent des droits d'usage technologiques, industriels, sectoriels, territoriaux ou institutionnels. Elles peuvent être forfaitaires, périodiques ou associées à des obligations de déploiement. Elles permettent notamment des architectures privées et souveraines.

5. Troisième pilier : royalties

Les royalties peuvent rémunérer l'exploitation de la propriété intellectuelle selon une assiette mesurable : unités, valeur attribuable ou autre métrique contractualisée. Elles doivent être transparentes, auditables et adaptées aux réalités sectorielles.

6. Complémentarité des trois piliers

SaaS, licences et royalties peuvent coexister, mais chaque composante doit correspondre à une fonction économique identifiable. Le modèle évite les doubles prélèvements ambigus. Un client doit pouvoir comprendre ce qu'il paie pour le service, le droit d'usage et l'exploitation variable.

7. Revenus complémentaires

Des revenus complémentaires peuvent provenir de services d'intégration, support avancé, formation, certification, audits techniques ou développements spécifiques lorsque ces prestations existent. Ils doivent rester distincts des fonctions réglementées et ne pas modifier artificiellement les statuts d' authenticité.

8. AP Business et création de valeur

AP Business peut créer de la valeur en améliorant visibilité, découverte des produits, recherche de revendeurs, circulation B2B/B2C et seconde main. Le modèle économique peut rémunérer certains

services commerciaux sans transformer le classement de confiance en mécanisme opaque de paiement.

9. AP Finance et AP Pay

AP Finance et AP Pay peuvent soutenir des modèles de services liés à l'orchestration, à l'intégration ou au rapprochement financier. Toute rémunération associée doit respecter la réglementation applicable et les rôles des prestataires autorisés. Les revenus financiers ne sont pas présumés tant que le cadre opérationnel n'est pas défini.

10. Structure des coûts technologiques

Les coûts comprennent développement logiciel, cloud, stockage, calcul, réseau, observabilité, bases de données, sauvegardes, continuité et intégrations. La croissance des volumes exige une architecture permettant de réduire progressivement le coût moyen par événement.

11. Coûts de cybersécurité

La sécurité constitue un coût structurel et non une option. AP Shield, audits, tests, gestion des vulnérabilités, clés, certificats, surveillance et réponse aux incidents doivent être financés durablement. Une croissance rapide sans budget de sécurité compromettrait la valeur même de l'infrastructure.

12. Coûts opérationnels et humains

Support, opérations, ingénierie, conformité, relation partenaires, documentation, gouvernance et accompagnement des déploiements représentent une part importante des coûts. Les déploiements institutionnels ou internationaux peuvent exiger des équipes spécialisées.

13. Coûts de conformité et souveraineté

Les secteurs réglementés et déploiements multi-pays génèrent des coûts juridiques, audits, certifications, localisation des données et adaptations nationales. Les architectures souveraines peuvent nécessiter infrastructures dédiées, transfert de compétences et exploitation locale.

14. Économie d'échelle

Une infrastructure mutualisée peut répartir certains coûts fixes sur un nombre croissant d'acteurs et d'événements. Cette économie d'échelle peut soutenir des offres accessibles aux petits producteurs. Elle dépend toutefois de l'efficacité technique et ne doit pas être supposée sans mesure des coûts réels.

15. Accessibilité et inclusion

Le modèle doit préserver l'accès des artisans, agriculteurs, créateurs, innovateurs et PME. AP Léger, paliers progressifs, franchises ou programmes institutionnels peuvent limiter la barrière économique. L'accessibilité contribue elle-même à l'effet de réseau de la plateforme.

16. Création de valeur pour les entreprises

Pour les producteurs et revendeurs, la valeur peut provenir de la protection de marque, de la traçabilité, de la réduction de certaines fraudes, de l'amélioration du rappel, de la visibilité commerciale et de l'analyse des flux. Ces bénéfices doivent être mesurés dans les pilotes plutôt que supposés universels.

17. Création de valeur publique

Pour les États et institutions, la valeur potentielle inclut meilleure visibilité sur certaines chaînes, soutien aux contrôles, protection des consommateurs, souveraineté des données et outils d'analyse agrégée. Les bénéfices publics doivent être évalués avec des indicateurs institutionnels et non seulement par les revenus de la plateforme.

18. Scénarios et projections

Les projections économiques doivent utiliser des scénarios explicites : taux d'adoption, volumes authentifiés, revenus unitaires, coûts, investissements et horizon. Les scénarios prudent, central et haut peuvent illustrer la sensibilité du modèle. Les hypothèses ne doivent jamais être présentées comme des résultats garantis.

19. Soutenabilité et gouvernance économique

La soutenabilité exige diversification des revenus, maîtrise des coûts, investissement continu en sécurité et capacité de financer l'innovation. La gouvernance doit surveiller concentration des revenus, dépendance à certains secteurs, risques réglementaires et accessibilité des petites structures.

20. Critères d'acceptation et conclusion

Le modèle économique consolidé est cohérent si SaaS, licences et royalties sont distincts et complémentaires ; si les revenus complémentaires sont identifiés ; si AP Business, AP Finance et AP Pay disposent de modèles compatibles avec leurs fonctions ; si coûts technologiques, sécurité, opérations, conformité et souveraineté sont intégrés ; si les économies d'échelle soutiennent l' accessibilité ; si la création de valeur privée et publique est mesurable ; et si les projections reposent sur des hypothèses transparentes.

Deep Authenticity© peut ainsi viser une soutenabilité mondiale fondée non sur une source unique de revenus, mais sur une architecture économique diversifiée capable de financer durablement une infrastructure universelle de confiance.

Le Chapitre 19 développera les tableaux de bord économiques et commerciaux : indicateurs Producteur, Revendeur, AP Business, flux, demande, stocks, ventes et analyse agrégée.

Note de cadrage institutionnel

Ce chapitre définit une architecture économique conceptuelle et non une prévision financière garantie. Les prix, marges, taux de royalties, coûts, revenus et scénarios devront être établis à partir de données de marché, pilotes, contrats et analyses financières validées. Les modèles réglementés nécessitent en outre les autorisations correspondantes.

CHAPITRE 19 — TABLEAUX DE BORD ÉCONOMIQUES ET COMMERCIAUX

TABLEAUX DE BORD — PRODUCTEUR — REVENDEUR — AP BUSINESS — STOCKS — VENTES — DEMANDE — FLUX — INDICATEURS — ANALYTIQUE — ALERTES — AIDE À LA DÉCISION

1. Objet du chapitre

Ce chapitre définit les tableaux de bord économiques et commerciaux de Deep Authenticity©. Ils transforment les événements authentifiés, commerciaux et logistiques en indicateurs exploitables par les producteurs, revendeurs, entreprises et institutions selon leurs droits. Leur fonction est d'éclairer la décision sans confondre observation, estimation, prévision et décision.

2. Principe de donnée gouvernée

Un indicateur n'a de valeur que si sa provenance, sa période et son niveau de fiabilité sont connus. Deep Authenticity© doit distinguer données observées, déclarées, synchronisées, calculées et prédites. Chaque tableau de bord applique les droits d'accès et la minimisation nécessaires.

3. Tableau de bord Producteur

Le producteur peut suivre références, unités activées, distribution, scans, ventes confirmées, alertes, retours et événements de cycle de vie autorisés. La vue peut être filtrée par produit, lot, période, territoire, canal ou revendeur selon les droits disponibles.

4. Tableau de bord Revendeur

Le revendeur dispose d'une vision de ses stocks authentifiés, entrées, sorties, ventes, retours, disponibilité publiée et alertes. Les indicateurs multi-sites permettent aux réseaux de comparer leurs établissements sans mélanger les données appartenant à d'autres entreprises.

5. Tableau de bord AP Business

AP Business agrège les signaux commerciaux : recherches, produits consultés, disponibilité, demandes B2B/B2C, zones de demande et interactions avec les offres. Ces signaux doivent être distingués des ventes réelles : une recherche exprime un intérêt, non une transaction.

6. Stocks authentifiés

Les tableaux peuvent présenter stock courant, stock déclaré, stock synchronisé, stock réservé et fraîcheur des données. L'identité des unités ou lots permet d'aller au-delà d'un simple nombre comptable lorsque le secteur le nécessite. Les écarts entre stock physique, ERP et événements Deep Authenticity© peuvent être signalés.

7. Ventes et transactions

Les ventes confirmées peuvent être analysées par période, référence, canal, zone et établissement. Les paiements, remboursements et transferts de propriété restent des événements distincts, même lorsqu'ils sont rapprochés dans une vue consolidée.

8. Demande et recherches

Le volume de recherches peut révéler des produits demandés mais indisponibles dans certaines zones. L'analyse doit intégrer la répétition des requêtes, les utilisateurs anonymisés et les biais de couverture afin de ne pas interpréter mécaniquement chaque recherche comme une unité de demande.

9. Flux géographiques

Les données agrégées peuvent représenter les mouvements de produits entre zones de production, distribution et vente. Les cartes de flux doivent éviter l'exposition des trajectoires individuelles ou des informations commercialement sensibles lorsque celles-ci ne sont pas nécessaires.

10. Rotation et vitesse de stock

Les indicateurs de rotation peuvent comparer entrées, disponibilité et ventes afin d'identifier stocks lents ou tensions. Les seuils doivent être sectoriels : une rotation normale pour un produit alimentaire n'est pas celle d'un équipement industriel ou d'une œuvre.

11. Alertes commerciales

Le système peut déclencher des alertes sur rupture probable, surstock, demande inhabituelle, retour élevé ou incohérence de stock. Une alerte est un signal à examiner et non une conclusion automatique. Son origine et ses règles de déclenchement doivent être visibles.

12. Graphiques et visualisation

Les tableaux de bord peuvent utiliser séries temporelles, histogrammes, cartes, répartitions, entonnoirs et indicateurs synthétiques. Les graphiques doivent afficher unités, périodes et sources. Les axes tronqués ou représentations susceptibles d'induire en erreur doivent être évités.

13. KPI sectoriels

Chaque secteur peut disposer de KPI spécifiques : durée de stockage, taux de retour, disponibilité, délai de vente, rappel, seconde main ou autres mesures. Un noyau commun facilite les comparaisons, tandis que les extensions sectorielles préservent la pertinence opérationnelle.

14. Seconde Main et valeur résiduelle

La Fenêtre Seconde Main peut alimenter des indicateurs sur volumes remis en vente, délais de revente, transferts finalisés et autres données autorisées. Une estimation de valeur résiduelle doit être clairement présentée comme une estimation et non comme une garantie de prix.

15. AP Finance et AP Pay

Les utilisateurs habilités peuvent rapprocher ventes, paiements, règlements et remboursements à des fins de suivi. Les données financières détaillées restent compartimentées. Les tableaux commerciaux peuvent afficher des statuts sans exposer les moyens de paiement ou coordonnées bancaires.

16. Analyse comparative

Une organisation peut comparer périodes, sites, références ou canaux. Les benchmarks entre entreprises ne doivent être produits qu'à partir de données agrégées, autorisées et suffisamment anonymisées. Les secrets commerciaux des concurrents restent protégés.

17. Prévision et intelligence artificielle

Les séries historiques peuvent alimenter des modèles de prévision de demande, rupture ou surstock. Les résultats doivent inclure horizon, niveau d'incertitude et principales hypothèses. L'IA assiste la décision ; elle ne transforme pas une prévision probabiliste en certitude.

18. Vue institutionnelle agrégée

Les institutions habilitées peuvent disposer d'indicateurs agrégés sur certaines filières, territoires ou tensions d'approvisionnement. Cette vue prépare les usages de jumeaux numériques et de simulation institutionnelle profonde, tout en respectant compétence légale, confidentialité et souveraineté.

19. Gouvernance, qualité et audit

Les définitions des KPI doivent être versionnées. Les corrections de données, changements de formule et périodes d'indisponibilité sont traçables. Des contrôles de qualité vérifient complétude, fraîcheur, cohérence et anomalies avant que les données n'alimentent les décisions importantes.

20. Critères d'acceptation et conclusion

Les tableaux de bord sont cohérents si Producteur, Revendeur et AP Business disposent de vues adaptées ; si stocks, ventes, demande et flux sont distingués ; si la provenance et la fraîcheur des données sont visibles ; si les alertes restent des signaux ; si les graphiques sont interprétables ; si les KPI sectoriels, Seconde Main et dimensions financières sont intégrables ; si les benchmarks protègent les secrets ; si les prévisions affichent leur incertitude ; et si les vues institutionnelles restent agrégées et gouvernées.

Deep Authenticity© transforme ainsi la traçabilité en capacité d'observation économique : la confiance ne sert plus seulement à vérifier un objet, elle permet de comprendre les dynamiques de production, distribution, disponibilité et demande à partir de données qualifiées.

Le Chapitre 20 développera l'intelligence économique prédictive : pénuries, surstocks, anomalies de marché, tendances et anticipation des besoins.

Note de cadrage institutionnel

Les tableaux de bord doivent être interprétés selon la couverture réelle des données. Une absence de données n'équivaut pas à une absence d'activité. Les indicateurs, benchmarks et prévisions ne constituent pas automatiquement des statistiques officielles, des conseils financiers ou des décisions administratives.

CHAPITRE 20 — INTELLIGENCE ÉCONOMIQUE PRÉDICTIVE : ANTICIPER LES TENSIONS ET LES BESOINS

INTELLIGENCE ÉCONOMIQUE — PRÉVISION — PÉNURIES — SURSTOCKS — DEMANDE — ANOMALIES — TENDANCES — IA — TABLEAUX DE BORD — JUMEAUX NUMÉRIQUES — AIDE À LA DÉCISION

1. Objet du chapitre

Ce chapitre définit l'intelligence économique prédictive de Deep Authenticity© comme la capacité à transformer des données économiques qualifiées en signaux prospectifs. L'objectif est d'anticiper pénuries, surstocks, tensions de distribution, évolutions de demande et anomalies de marché afin d' aider producteurs, entreprises et institutions à agir plus tôt.

2. De l'observation à l'anticipation

Les tableaux de bord décrivent principalement ce qui s'est produit ou ce qui est observé. La couche prédictive cherche à estimer ce qui pourrait se produire. Cette transition exige des séries temporelles, une couverture suffisante, des modèles validés et une représentation explicite de l'incertitude.

3. Sources de données internes

Les modèles peuvent exploiter, selon les droits, activations, stocks, disponibilités, recherches, ventes, retours, transferts, délais logistiques et autres événements de Deep Authenticity©. Chaque variable conserve sa provenance et son niveau de qualité.

4. Données externes

Des données externes peuvent enrichir les analyses : statistiques publiques, météo, transport, prix, commerce extérieur, calendrier, données sanitaires ou autres sources légitimes. Elles doivent être intégrées dans des rubriques identifiées, documentées et séparées des observations natives de la plateforme.

5. Prévision de la demande

Les modèles peuvent estimer la demande future par référence, catégorie, territoire ou période. Les recherches, ventes historiques, saisonnalité et événements contextuels peuvent contribuer à l' estimation. Une prévision doit toujours préciser horizon, intervalle d'incertitude et date de calcul.

6. Détection précoce des pénuries

Une baisse persistante des stocks combinée à une demande stable ou croissante peut signaler un risque de pénurie. Le système peut produire un indice de tension et une alerte graduée. Cette alerte doit être confirmée par l'analyse du contexte avant toute décision importante.

7. Détection des surstocks

Des stocks élevés associés à une rotation faible ou une demande décroissante peuvent signaler un risque de surstock. L'anticipation permet d'ajuster production, distribution ou stratégie commerciale. Les recommandations doivent respecter les responsabilités propres de l'entreprise.

8. Déséquilibres territoriaux

Deep Authenticity© peut comparer disponibilité et demande agrégées entre zones. Un produit peut être excédentaire dans une région et rare dans une autre. La visualisation de ces écarts peut soutenir redistribution logistique et planification sans exposer les données individuelles des acteurs.

9. Anomalies de marché

Des variations inhabituelles de scans, ventes, retours, disponibilité ou prix lorsqu'ils sont disponibles peuvent déclencher une analyse d'anomalie. Le signal peut refléter fraude, événement réel, erreur de données ou changement de comportement. Il ne doit jamais être assimilé automatiquement à une infraction.

10. Tendances et signaux faibles

La combinaison de plusieurs indicateurs peut révéler des signaux faibles avant qu'ils deviennent visibles dans les statistiques agrégées traditionnelles. Une hausse progressive des recherches associée à une baisse de disponibilité peut, par exemple, justifier une surveillance renforcée.

11. IA et modèles prédictifs

Les modèles peuvent inclure séries temporelles, méthodes statistiques, apprentissage automatique ou architectures plus avancées lorsque justifiées. Le choix du modèle doit dépendre du problème et des données, non d'un effet de mode. Les performances sont évaluées sur des données hors entraînement.

12. Qualité et couverture

Une prédiction fiable exige des données suffisamment représentatives. Une faible adoption de Deep Authenticity© dans un secteur ou territoire limite la portée des conclusions. Le système doit afficher couverture, fraîcheur, données manquantes et changements méthodologiques.

13. Niveaux de confiance

Chaque prévision importante peut être accompagnée d'un niveau de confiance ou intervalle d'incertitude. Les utilisateurs doivent pouvoir distinguer un signal robuste d'une hypothèse fragile. Les seuils d'alerte peuvent varier selon la criticité du secteur.

14. Scénarios prospectifs

Au-delà d'une prévision unique, le système peut présenter plusieurs scénarios : continuité, tension modérée, rupture sévère ou reprise accélérée, selon le cas. Les scénarios rendent visibles les hypothèses et préparent l'intégration avec les jumeaux numériques et la simulation institutionnelle profonde.

15. Producteurs et revendeurs

Les acteurs économiques peuvent utiliser les prévisions pour planifier production, approvisionnement, stocks et distribution. Le tableau de bord doit permettre de comparer prévision antérieure et résultat réel afin d'évaluer progressivement la qualité du modèle.

16. Institutions et politiques publiques

Les institutions habilitées peuvent utiliser des analyses agrégées pour surveiller certaines filières stratégiques, disponibilités ou tensions territoriales. Ces analyses constituent une aide à la décision et non une décision publique automatique. Les statistiques officielles restent gouvernées par les autorités compétentes.

17. Boucle d'apprentissage

Après chaque période, le système compare prédictions et observations. Les erreurs sont mesurées, les dérives détectées et les modèles réévalués. Cette boucle permet d'améliorer la performance tout en conservant l'historique des versions et des décisions méthodologiques.

18. Explicabilité et audit

Pour les usages sensibles, l'utilisateur doit connaître les principaux facteurs ayant contribué à une alerte ou prévision. Les modèles, versions, variables et résultats sont auditables selon les droits. Une décision institutionnelle importante ne doit pas reposer sur un score opaque impossible à examiner.

19. Passage vers les jumeaux numériques

L'intelligence prédictive fournit aux jumeaux numériques une représentation dynamique des tendances et probabilités futures. Le jumeau peut ensuite intégrer contraintes, relations entre secteurs et scénarios de décision. La prévision devient ainsi une composante d'un système de simulation plus large.

20. Critères d'acceptation et conclusion

L'intelligence économique prédictive est cohérente si les données internes et externes sont distinguées ; si demande, pénuries, surstocks, déséquilibres et anomalies peuvent être modélisés ; si les modèles sont validés ; si qualité, couverture et incertitude sont visibles ; si les scénarios rendent les hypothèses explicites ; si producteurs, revendeurs et institutions disposent de vues adaptées ; si la boucle d'apprentissage mesure les erreurs ; et si l'explicabilité prépare les jumeaux numériques.

Deep Authenticity© passe ainsi de la mémoire économique à l'anticipation : l'infrastructure ne se contente plus d'observer les flux authentifiés, elle peut détecter suffisamment tôt certaines tensions pour permettre une action plus informée.

Le Chapitre 21 développera la valeur économique des données agrégées : connaissance des marchés, souveraineté informationnelle, gouvernance, anonymisation et nouveaux services analytiques.

Note de cadrage institutionnel

Les prévisions et alertes de Deep Authenticity© sont des outils d'aide à la décision. Elles ne garantissent pas la réalisation d'un événement futur. Leur qualité dépend de la couverture, de la représentativité et de la fraîcheur des données. Les usages institutionnels ou sectoriels sensibles doivent prévoir validation humaine, audit et mécanismes de recours.

CHAPITRE 21 — VALEUR ÉCONOMIQUE DES DONNÉES AGRÉGÉES : CONNAISSANCE, SOUVERAINETÉ ET GOUVERNANCE

DONNÉES AGRÉGÉES — CONNAISSANCE DES MARCHÉS — SOUVERAINETÉ INFORMATIONNELLE — ANONYMISATION — GOUVERNANCE — ANALYTIQUE — AP BUSINESS — INSTITUTIONS — CONFIDENTIALITÉ — CRÉATION DE VALEUR

1. Objet du chapitre

Ce chapitre définit la valeur économique des données agrégées produites à partir des événements gouvernés de Deep Authenticity©. L'objectif n'est pas de commercialiser indistinctement les données individuelles, mais de transformer des observations qualifiées en connaissances de marché, indicateurs sectoriels et services analytiques compatibles avec la confidentialité, la souveraineté et les droits des acteurs.

2. De la donnée brute à la connaissance économique

Une donnée isolée possède une valeur analytique limitée. Sa mise en contexte avec période, territoire, catégorie, provenance et qualité permet de produire un indicateur. L'agrégation de plusieurs indicateurs peut ensuite révéler tendances, tensions et dynamiques économiques sans exiger l' exposition des dossiers individuels.

3. Catégories de données agrégées

Les agrégats peuvent porter sur volumes d'activation, disponibilité, stocks, recherches, ventes confirmées, retours, transferts, zones de demande ou autres événements autorisés. Chaque agrégat doit préciser population couverte, période, méthode de calcul et éventuelles exclusions.

4. Connaissance des marchés

Les entreprises peuvent utiliser des analyses agrégées pour mieux comprendre demande, distribution, saisonnalité, zones sous-desservies et évolution de certaines catégories. Cette connaissance doit compléter, et non remplacer, les études de marché classiques lorsque la couverture de Deep Authenticity© est partielle.

5. Producteurs et intelligence commerciale

Un producteur peut comparer ses propres indicateurs avec des références sectorielles suffisamment agrégées. Il peut identifier des écarts de disponibilité ou de demande sans accéder aux données confidentielles d'un concurrent. Les benchmarks doivent respecter des seuils empêchant la réidentification.

6. Revendeurs et connaissance territoriale

Les revendeurs peuvent analyser les tendances de recherche et de disponibilité dans leurs zones autorisées. Ces informations peuvent améliorer assortiment et approvisionnement. La plateforme doit distinguer une tendance agrégée d'une donnée individuelle provenant d'un consommateur ou d'un autre commerçant.

7. AP Business comme source de signaux

AP Business peut générer des signaux sur recherches, consultations, disponibilité et interactions commerciales. Ces signaux ont une valeur prospective, mais ne constituent pas des ventes. Les

services analytiques doivent conserver cette distinction afin d'éviter une surestimation artificielle de la demande.

8. Valeur institutionnelle

Les institutions habilitées peuvent exploiter des agrégats sur filières, territoires, disponibilités ou flux afin d'améliorer leur connaissance économique. Ces vues peuvent soutenir planification, surveillance des tensions et politiques publiques, sans transformer automatiquement les données de la plateforme en statistiques officielles.

9. Souveraineté informationnelle

La capacité d'un État ou d'une organisation à comprendre ses propres flux économiques constitue un enjeu de souveraineté. Deep Authenticity© peut permettre de conserver localement les données sensibles tout en produisant des indicateurs agrégés nécessaires à la coordination nationale ou internationale.

10. Principe de minimisation

La création de valeur analytique ne justifie pas la collecte illimitée. Seules les données nécessaires aux finalités définies doivent être collectées et conservées. Lorsque des agrégats suffisent, les données individuelles ne doivent pas être diffusées aux utilisateurs analytiques.

11. Anonymisation et pseudonymisation

La pseudonymisation réduit l'exposition directe de l'identité mais n'équivaut pas nécessairement à une anonymisation irréversible. Les méthodes d'agrégation doivent considérer taille des groupes, rareté des événements, recoupements et risques de réidentification avant toute diffusion.

12. Seuils de confidentialité

Des seuils minimaux peuvent empêcher l'affichage d'un indicateur lorsque le nombre d'acteurs ou d'événements est trop faible. Les catégories rares peuvent être regroupées ou supprimées. Ces règles doivent être cohérentes avec la sensibilité du secteur et du territoire.

13. Gouvernance des finalités

Chaque service analytique doit avoir une finalité documentée : pilotage interne, benchmark, recherche, analyse institutionnelle ou autre usage autorisé. Une donnée collectée pour l'authentification ne doit pas être réutilisée sans gouvernance pour une finalité incompatible.

14. Droits et contrôle des acteurs

Les contrats, politiques et réglementations doivent définir quels acteurs peuvent accéder aux agrégats et dans quelles conditions. Les entreprises doivent connaître les usages analytiques prévus de leurs données. Les mécanismes de consentement ou d'opposition sont appliqués lorsque le droit l'exige.

15. Nouveaux services analytiques

Deep Authenticity© peut proposer des tableaux sectoriels, indices de tension, cartes de disponibilité, analyses de rotation, tendances de recherche ou services prédictifs. La valeur réside dans la qualité de la méthodologie et de la couverture, non dans la simple accumulation de données.

16. Modèle économique des services de données

Certains services analytiques avancés peuvent être intégrés aux offres SaaS, licences institutionnelles ou prestations spécifiques. La facturation doit porter sur le service analytique fourni et ses capacités,

sans créer l'idée que les données personnelles des utilisateurs sont vendues comme une marchandise.

17. Qualité, biais et représentativité

Un agrégat peut être exact pour les données présentes mais non représentatif du marché entier. Les tableaux doivent afficher couverture, fraîcheur et éventuels biais. Les changements d'adoption de la plateforme peuvent eux-mêmes modifier les séries et doivent être pris en compte.

18. Audit et traçabilité analytique

Les formules, sources, versions et transformations utilisées pour produire un indicateur important doivent être auditables. AP Ledger peut ancrer certaines preuves méthodologiques ou empreintes de jeux de résultats. La reproductibilité renforce la confiance dans les services analytiques.

19. Fédération internationale des indicateurs

Des pays ou institutions peuvent partager des indicateurs agrégés via des Corridors de Confiance sans centraliser les bases sources. Des définitions communes permettent des comparaisons tout en maintenant les données détaillées sous gouvernance locale. Cette fédération prépare une connaissance économique mondiale respectueuse des souverainetés.

20. Critères d'acceptation et conclusion

La valorisation des données agrégées est cohérente si données individuelles et agrégats sont distingués ; si les méthodes précisent couverture et période ; si producteurs, revendeurs et institutions reçoivent des vues adaptées ; si AP Business est traité comme source de signaux et non de ventes ; si minimisation, anonymisation et seuils de confidentialité réduisent les risques ; si les finalités et droits d'accès sont gouvernés ; si les services analytiques ont un modèle économique transparent ; et si qualité, biais, audit et souveraineté sont intégrés.

Deep Authenticity© transforme ainsi la donnée de confiance en capital de connaissance sans faire de la surveillance individuelle son modèle économique. La valeur se déplace de la possession des données vers la capacité à produire des indicateurs fiables, gouvernés et utiles.

Le Chapitre 22 développera la souveraineté économique et commerciale : résilience des chaînes, autonomie informationnelle, commerce de confiance et capacité stratégique des États.

Note de cadrage institutionnel

La valorisation analytique doit respecter les réglementations applicables en matière de données personnelles, confidentialité, concurrence, secret des affaires et statistiques. L'agrégation ne garantit pas à elle seule l'anonymat : les risques de réidentification doivent être évalués selon les données, les groupes et les usages.

CHAPITRE 22 — SOUVERAINETÉ ÉCONOMIQUE ET COMMERCIALE : RÉSILIENCE, AUTONOMIE ET COMMERCE DE CONFIANCE

SOUVERAINETÉ ÉCONOMIQUE — COMMERCE — RÉSILIENCE — AUTONOMIE INFORMATIONNELLE — CHAÎNES D'APPROVISIONNEMENT — ÉTATS — CORRIDORS DE CONFIANCE — DONNÉES — TRAÇABILITÉ — CAPACITÉ STRATÉGIQUE

1. Objet du chapitre

Ce chapitre définit la contribution potentielle de Deep Authenticity© à la souveraineté économique et commerciale. L'objectif est de donner aux États, institutions et acteurs économiques une capacité accrue à connaître, sécuriser et analyser leurs chaînes de valeur sans dépendre d'une centralisation extérieure des données critiques.

2. Souveraineté économique et connaissance

La souveraineté économique ne repose pas uniquement sur la production nationale. Elle dépend aussi de la capacité à savoir quels produits circulent, d'où ils proviennent, où apparaissent les tensions et quelles dépendances structurent les chaînes. Une infrastructure de confiance peut améliorer cette connaissance lorsque sa couverture est suffisante.

3. Autonomie informationnelle

Un État doit pouvoir exploiter les informations nécessaires à ses missions sans abandonner la maîtrise de ses données stratégiques. Deep Authenticity© peut fonctionner avec stockage local, contrôle national des accès et échanges limités à des attestations ou agrégats nécessaires.

4. Résilience des chaînes d'approvisionnement

La traçabilité des flux, stocks et disponibilités peut aider à identifier plus tôt des ruptures ou concentrations excessives. Les tableaux de bord et modèles prédictifs permettent d'observer les tensions et de préparer des réponses, sans prétendre éliminer les risques géopolitiques, logistiques ou naturels.

5. Cartographie des dépendances

Les données agrégées peuvent contribuer à cartographier certaines dépendances par produit, catégorie, fournisseur, territoire ou corridor. Les informations sensibles doivent être protégées. La cartographie devient un outil d'aide à la diversification et à la planification stratégique.

6. Produits stratégiques

Les États peuvent définir des catégories nécessitant une surveillance renforcée : médicaments, équipements critiques, alimentation, pièces industrielles ou autres biens selon leurs priorités. Deep Authenticity© peut fournir des vues dédiées, sous contrôle des autorités compétentes.

7. Commerce de confiance

Le commerce de confiance repose sur des identités vérifiables de produits et d'acteurs, des preuves d'événements et des mécanismes d'interopérabilité. Cette couche peut réduire certaines asymétries d'information entre partenaires commerciaux et faciliter les contrôles sans supprimer les obligations douanières ou réglementaires.

8. Trois QR codes et contrôle économique

Dans le domaine physique, les trois QR codes d'Authenticity Plus© restent la fondation anti-contrefaçon : consommateur, revendeur/professionnel et contrôle/douanes. Le troisième canal permet notamment d'inscrire les autorités de contrôle dans une architecture fonctionnellement distincte de l'usage commercial ou consommateur.

9. Douanes et frontières

Les autorités habilitées peuvent utiliser les informations de contrôle pour vérifier des références, lots ou événements autorisés. L'intégration doit respecter leurs systèmes et compétences. Deep Authenticity© enrichit le contexte de contrôle ; elle ne remplace pas les décisions douanières.

10. Corridors de Confiance

Les Corridors de Confiance permettent à plusieurs juridictions d'échanger des attestations vérifiables selon des règles communes. Chaque participant conserve ses bases sensibles, ses clés et sa gouvernance. L'interopérabilité est obtenue par protocoles et preuves plutôt que par une base mondiale unique.

11. Diversification des partenaires

Une meilleure visibilité sur les dépendances peut soutenir la recherche de fournisseurs alternatifs ou de nouveaux débouchés. AP Business et les données agrégées peuvent contribuer à identifier des opportunités, mais la qualification économique et politique des partenaires reste une décision humaine et institutionnelle.

12. PME et souveraineté productive

La souveraineté ne concerne pas uniquement les grandes entreprises. Artisans, agriculteurs, PME et innovateurs constituent une part essentielle du tissu productif. AP Léger et AP Business peuvent renforcer leur visibilité, leur provenance et leur capacité à rejoindre des circuits commerciaux de confiance.

13. Souveraineté des infrastructures

Les déploiements institutionnels peuvent utiliser cloud souverain, infrastructure privée ou architecture hybride. Les clés cryptographiques critiques peuvent rester sous contrôle local. La continuité opérationnelle doit prévoir sauvegarde, reprise, redondance et capacité de fonctionnement en situation dégradée.

14. Souveraineté technologique et interopérabilité

La souveraineté technologique ne signifie pas isolement. Les standards, API et mécanismes fédérés permettent de coopérer tout en maintenant le contrôle des systèmes nationaux. L'objectif est une interdépendance maîtrisée plutôt qu'une dépendance opaque.

15. Données économiques et décision publique

Les indicateurs issus de Deep Authenticity© peuvent compléter les statistiques et systèmes administratifs existants. Ils peuvent apporter davantage de granularité ou de rapidité dans certaines filières. Ils ne deviennent des statistiques officielles que selon les procédures des autorités compétentes.

16. Résilience en situation de crise

En cas de crise sanitaire, logistique, climatique ou commerciale, la connaissance des stocks et flux peut faciliter l'identification des zones de tension. Les modes Online/Offline et architectures distribuées contribuent à maintenir certaines fonctions lorsque les réseaux sont perturbés.

17. Prévention des dépendances numériques

Un État doit éviter qu'une infrastructure critique devienne une dépendance impossible à auditer ou à quitter. Réversibilité, portabilité, standards documentés, gouvernance des clés et continuité des preuves doivent être intégrés aux contrats institutionnels.

18. Gouvernance et contrôle démocratique

Les capacités économiques et analytiques à grande échelle nécessitent des limites claires. Finalités, accès, conservation, audits et mécanismes de recours doivent être gouvernés. La souveraineté de l'État ne doit pas être interprétée comme une autorisation illimitée de surveillance individuelle.

19. Dimension géoéconomique

Une infrastructure de confiance interopérable peut devenir un instrument de coopération économique, de sécurisation des échanges et de reconnaissance mutuelle. Son adoption internationale dépendra toutefois de standards ouverts à l'interopérabilité, d'une gouvernance crédible et de la capacité à respecter les souverainetés partenaires.

20. Critères d'acceptation et conclusion

La contribution à la souveraineté économique est cohérente si les données stratégiques peuvent rester sous contrôle local ; si les chaînes et dépendances sont observables ; si les produits stratégiques disposent de vues adaptées ; si les trois QR codes conservent leur rôle de contrôle physique ; si douanes et Corridors de Confiance sont interopérables ; si PME et acteurs locaux participent à la souveraineté productive ; si infrastructures, clés, réversibilité et modes dégradés sont gouvernés ; et si l'analyse économique respecte les libertés et compétences institutionnelles.

Deep Authenticity© peut ainsi contribuer à une souveraineté économique fondée sur la connaissance et la preuve : savoir ce qui circule, comprendre les dépendances, protéger les chaînes et coopérer internationalement sans renoncer au contrôle des infrastructures critiques.

Le Chapitre 23 développera les Corridors commerciaux de confiance : coopération interétatique, reconnaissance mutuelle, circulation des produits authentifiés et interopérabilité des écosystèmes.

Note de cadrage institutionnel

La souveraineté économique est un objectif de politique publique qui dépend de nombreux facteurs extérieurs à la technologie. Deep Authenticity© peut fournir des outils de connaissance, traçabilité et interopérabilité, mais ne garantit ni autonomie économique ni résilience à elle seule. Les usages publics doivent respecter les cadres constitutionnels, légaux et internationaux applicables.

CHAPITRE 23 — CORRIDORS COMMERCIAUX DE CONFIANCE : COOPÉRATION, RECONNAISSANCE ET INTEROPÉRABILITÉ

CORRIDORS DE CONFIANCE — COMMERCE INTERNATIONAL — COOPÉRATION INTERÉTATIQUE — RECONNAISSANCE MUTUELLE — PRODUITS AUTHENTIFIÉS — DOUANES — INTEROPÉRABILITÉ — SOUVERAINETÉ — AP LEDGER — AP PAY

1. Objet du chapitre

Ce chapitre définit les Corridors commerciaux de confiance de Deep Authenticity© comme des cadres d'interopérabilité permettant à plusieurs États, institutions et acteurs économiques d'échanger des produits et des attestations vérifiables sans imposer une centralisation mondiale des données. Le corridor associe règles techniques, gouvernance, reconnaissance et contrôles.

2. Principe du corridor

Un Corridor de Confiance relie au moins deux écosystèmes qui acceptent un ensemble de protocoles et d'attestations. Chaque participant conserve ses systèmes, bases sensibles et compétences. La coopération repose sur la capacité à vérifier les preuves nécessaires à l'échange.

3. Reconnaissance mutuelle

Les parties peuvent reconnaître certains attributs ou preuves émis par l'autre partie selon un accord défini. La reconnaissance n'est ni automatique ni universelle : elle précise autorités émettrices, types de données, durée, niveaux de confiance et procédures de révocation.

4. Identité du produit

Le produit physique conserve son identité persistante et son Passeport Numérique Universel pendant sa circulation. Les événements de production, exportation, contrôle, importation et distribution peuvent être reliés selon les droits. Les données commerciales sensibles restent compartimentées.

5. Les trois QR codes dans le corridor

Les trois QR codes d'Authenticity Plus© conservent leurs fonctions distinctes : consommateur, revendeur/professionnel et contrôle/douanes. Le corridor n'abolit pas cette architecture ; il permet aux acteurs habilités de vérifier les preuves pertinentes à leur rôle lors du passage entre écosystèmes.

6. Sémantique VERT–JAUNE–ROUGE

Pour les trois QR codes, la sémantique utilisateur reste constante : VERT signifie original ; JAUNE signifie original mais déjà vérifié ou vendu ; ROUGE signifie contrefait ou code inexistant dans Authenticity Plus©. Les règles opérationnelles doivent préserver cette interprétation commune entre juridictions.

7. QR code dynamique

Lorsqu'un QR code dynamique est utilisé, le support visuel peut rester stable tandis que la destination, le jeton ou les informations servies évoluent selon l'état, les droits et les politiques de sécurité. Le dynamisme ne doit pas permettre de réécrire l'historique probant ni de contourner la séparation des trois fonctions.

8. Douanes et autorités de contrôle

Les autorités habilitées peuvent accéder à une vue de contrôle adaptée : identité produit, origine, lot, statut, événements autorisés et attestations nécessaires. Deep Authenticity© complète les systèmes douaniers existants et ne se substitue pas aux décisions souveraines d'admission, saisie ou inspection.

9. Exportation et sortie du territoire

Au départ, les événements d'exportation peuvent être reliés au produit ou au lot. Le corridor vérifie les références attendues et transmet les attestations nécessaires au partenaire. Les informations échangées sont limitées à la finalité du contrôle et du commerce.

10. Importation et entrée

À l'arrivée, l'autorité ou l'acteur habilité peut vérifier la continuité des références et les preuves reconnues. Les contrôles locaux restent applicables. Une attestation étrangère facilite l' interopérabilité mais ne supprime pas les obligations nationales.

11. AP Ledger et chaîne de preuve

AP Ledger peut ancrer les empreintes des attestations, contrôles et transitions critiques. Les parties peuvent vérifier la cohérence d'une séquence sans partager l'intégralité de leurs registres internes. Cette approche favorise l'audit inter-juridictionnel.

12. AP Business et accès aux marchés

AP Business peut permettre aux producteurs et revendeurs autorisés de rendre leurs produits visibles dans les marchés participants. Les recherches et disponibilités restent gouvernées localement. Le corridor peut ainsi relier confiance réglementaire et découverte commerciale.

13. AP Finance et AP Pay

Lorsque le commerce implique un paiement transfrontalier, AP Finance et AP Pay peuvent relier la référence commerciale aux infrastructures financières autorisées. Les corridors commerciaux et financiers peuvent coopérer sans être confondus : produit, paiement et propriété conservent leurs états propres.

14. Standards et API

L'interopérabilité repose sur des formats, identifiants, signatures, API et règles de versionnement documentés. Les interfaces doivent permettre l'évolution sans rompre les preuves anciennes. Les standards externes pertinents peuvent être intégrés lorsque cela améliore la compatibilité.

15. Gouvernance interétatique

Chaque corridor nécessite une gouvernance définissant participants, responsabilités, niveaux de service, sécurité, résolution des incidents et évolution des règles. Les décisions concernant les compétences publiques restent entre les mains des autorités légitimes.

16. Révocation et incidents

Une clé compromise, une autorité révoquée, une erreur de lot ou une attaque doit pouvoir être signalée rapidement. Les participants disposent de mécanismes de révocation et de suspension. Les preuves antérieures restent conservées avec leur contexte historique.

17. Protection des données et secrets commerciaux

Le corridor applique minimisation et contrôle d'accès. Les attestations peuvent confirmer un attribut sans exposer toutes les données sources. Les secrets commerciaux, identités personnelles et informations financières ne doivent pas circuler simplement parce que deux systèmes sont interconnectés.

18. Pilotes bilatéraux et extension progressive

Le déploiement peut commencer par un corridor bilatéral, un secteur ou un type de produit. Les résultats du pilote permettent d'évaluer sécurité, délais, taux d'erreur, adoption et coûts. L'extension à d'autres pays doit être fondée sur des critères d'acceptation mesurés.

19. Dimension géoéconomique

Des corridors interopérables peuvent faciliter lareconnaissance des produits authentifiés et renforcer la confiance entre partenaires commerciaux. Leur crédibilité dépend de la neutralité des protocoles, de la protection des souverainetés et de la capacité à accueillir plusieurs modèles institutionnels.

20. Critères d'acceptation et conclusion

Un Corridor commercial de confiance est cohérent si les participants conservent leurs systèmes souverains ; si la reconnaissance mutuelle est explicitement gouvernée ; si le Passeport Numérique Universel maintient la continuité produit ; si les trois QR codes et la sémantique VERT–JAUNE–ROUGE restent invariants ; si le QR dynamique préserve l'historique ; si douanes, export et import sont interopérables ; si AP Ledger renforce la preuve ; si AP Business, AP Finance et AP Pay peuvent coopérer sans fusionner leurs fonctions ; et si sécurité, révocation, confidentialité et pilotes progressifs sont prévus.

Deep Authenticity© transforme ainsi la frontière d'un point de rupture informationnelle en point de vérification interopérable : les preuves peuvent traverser les juridictions tandis que la souveraineté des données et des décisions demeure locale.

Le Chapitre 24 développera la création de valeur pour les producteurs, revendeurs, consommateurs et États : bénéfices économiques, réduction des frictions, confiance, nouveaux marchés et effets de réseau.

Note de cadrage institutionnel

Les Corridors commerciaux de confiance constituent une architecture conceptuelle de coopération. Leur mise en œuvre exige des accords, des cadres juridiques, des standards techniques et l' autorisation des institutions compétentes. Deep Authenticity© ne confère pas, par elle-même, une reconnaissance douanière ou réglementaire internationale.

CHAPITRE 24 — CRÉATION DE VALEUR POUR LES ACTEURS : CONFIANCE, EFFICACITÉ ET EFFETS DE RÉSEAU

CRÉATION DE VALEUR — PRODUCTEURS — REVENDEURS — CONSOMMATEURS — ÉTATS — CONFIANCE — EFFICACITÉ — NOUVEAUX MARCHÉS — EFFETS DE RÉSEAU — TRAÇABILITÉ — SOUVERAINETÉ

1. Objet du chapitre

Ce chapitre analyse la création de valeur de Deep Authenticity© pour les principaux acteurs de l'écosystème : producteurs, revendeurs, consommateurs, acteurs de seconde main, institutions et États. La valeur ne résulte pas d'une fonction isolée, mais de la continuité entre identité, authenticité, traçabilité, commerce, propriété, paiement et connaissance économique.

2. Principe de valeur partagée

Une infrastructure universelle de confiance ne peut être durable si elle crée de la valeur pour une seule catégorie d'acteurs. Le modèle doit produire des bénéfices complémentaires : protection et visibilité pour le producteur, efficacité pour le revendeur, confiance pour l'acquéreur et capacité d'observation pour les institutions.

3. Valeur pour le producteur

Le producteur peut disposer d'une identité vérifiable pour ses unités, d'une meilleure continuité de distribution, d'alertes et d'indicateurs. L'architecture peut renforcer la protection de la marque, faciliter certains rappels et donner une meilleure visibilité sur la circulation autorisée des produits.

4. Protection contre la contrefaçon

Les trois QR codes d'Authenticity Plus© constituent le mécanisme physique central de différenciation entre produit enregistré et code inexistant ou déjà utilisé. Ils ne suppriment pas toute contrefaçon, mais augmentent la capacité de détection, de signalement et de constitution d'une chaîne de preuve.

5. Valeur commerciale pour le producteur

AP Business peut transformer l'authenticité en visibilité commerciale. Le producteur peut rendre ses références recherchables, orienter l'utilisateur vers des revendeurs reconnus et analyser les zones de demande. La confiance devient ainsi un actif commercial sans se réduire à de la publicité.

6. Valeur pour le revendeur

Le revendeur peut mieux identifier les produits entrant dans son stock, publier leur disponibilité et participer à une chaîne de distribution vérifiable. La Fenêtre Revendeur relie stock authentifié, recherche commerciale, vente et passage vers le premier acquéreur.

7. Réduction des frictions commerciales

L'usage de références communes entre produit, commande, vente, paiement et propriété peut réduire certaines opérations de rapprochement manuel. Les API et ERP permettent d'éviter des ressaisies lorsque les systèmes sont intégrés. Les gains réels doivent être mesurés lors des pilotes.

8. Valeur pour le consommateur

Le consommateur obtient une lecture simple du statut d'authenticité et peut accéder aux informations autorisées du Passeport Numérique Universel. Il peut rechercher un revendeur, suivre certains événements du produit et, lorsqu'il devient propriétaire, disposer d'une continuité patrimoniale.

9. Simplicité VERT–JAUNE–ROUGE

La sémantique VERT = original, JAUNE = original mais déjà vérifié ou vendu, ROUGE = contrefait ou code inexistant dans Authenticity Plus© réduit la complexité de lecture pour l'utilisateur. Cette simplicité doit rester stable même lorsque les mécanismes techniques sous-jacents évoluent.

10. Valeur pour le premier acquéreur

La première acquisition peut relier preuve commerciale, paiement et relation de propriété sans les confondre. L'acquéreur dispose alors d'un produit dont l'identité peut se poursuivre après la vente et servir ultérieurement à la preuve de provenance ou au transfert.

11. Valeur pour la Seconde Main

La continuité du Passeport Numérique Universel permet de conserver l'identité du produit lors de la revente. Le vendeur peut démontrer une provenance autorisée et l'acquéreur peut vérifier le statut avant transfert. Cette continuité peut réduire certaines asymétries d'information du marché d' occasion.

12. Valeur pour artisans et petites structures

AP Léger permet aux artisans, agriculteurs, créateurs, innovateurs et PME d'accéder à une infrastructure autrefois plus facilement disponible aux grands groupes. Provenance, visibilité et recherche commerciale peuvent contribuer à mieux différencier leurs productions.

13. Valeur pour les États

Les États peuvent disposer de vues agrégées sur certaines chaînes, produits stratégiques, tensions et flux. Les fonctions de contrôle peuvent soutenir douanes et autorités selon leurs compétences. Cette valeur institutionnelle repose sur la qualité, la couverture et la gouvernance des données.

14. Valeur pour la souveraineté

Le déploiement souverain permet de conserver données et clés critiques sous contrôle national tout en participant à des Corridors de Confiance. L'État peut ainsi rechercher l'interopérabilité internationale sans transférer nécessairement son infrastructure informationnelle à un acteur extérieur.

15. Nouveaux marchés

La reconnaissance d'identités et d'attestations entre écosystèmes peut faciliter l'accès à de nouveaux circuits commerciaux. Les petits producteurs peuvent bénéficier d'une visibilité accrue et les grands acteurs d'une continuité de preuve. L'accès au marché reste néanmoins soumis aux règles commerciales et réglementaires applicables.

16. Effet de réseau

Plus le nombre d'acteurs, produits et juridictions compatibles augmente, plus la probabilité de trouver une continuité de confiance croît. Cet effet de réseau peut accroître l'utilité de la plateforme. Il doit toutefois être gouverné afin d'éviter dépendance excessive, verrouillage ou concentration abusive.

17. Boucle de valeur

Une boucle positive peut se former : davantage de produits authentifiés améliorent la recherche ; davantage de revendeurs améliorent la disponibilité ; davantage d'utilisateurs enrichissent les signaux agrégés ; de meilleurs indicateurs augmentent l'utilité pour producteurs et institutions, favorisant à leur tour l'adoption.

18. Mesure de la valeur créée

La valeur doit être évaluée par des KPI : taux d'authentification, incidents détectés, délais de rappel, disponibilité, conversion commerciale, réduction des erreurs, taux de transfert, adoption et qualité des données. Les bénéfices économiques doivent être comparés aux coûts de déploiement et d' exploitation.

19. Limites et équité

Les effets de réseau ne doivent pas exclure les acteurs non encore intégrés ni transformer Deep Authenticity© en passage commercial obligatoire sans gouvernance. Interopérabilité, AP Léger, tarification proportionnée, réversibilité et règles de concurrence sont nécessaires pour préserver l' équité de l'écosystème.

20. Critères d'acceptation et conclusion

La création de valeur est cohérente si producteurs, revendeurs, consommateurs, premiers acquéreurs, seconde main, petites structures et États disposent de bénéfices identifiables ; si les trois QR codes et la sémantique VERT–JAUNE–ROUGE restent au cœur de la confiance physique ; si AP Business réduit certaines frictions et ouvre des marchés ; si souveraineté et Corridors de Confiance peuvent coexister ; si les effets de réseau sont mesurés et gouvernés ; et si la valeur créée est comparée aux coûts réels.

Deep Authenticity© devient alors plus qu'un système de vérification : une infrastructure économique où chaque nouvel acteur peut renforcer la valeur collective de la confiance, à condition que cette croissance demeure ouverte, mesurable, interopérable et équitable.

Le Chapitre 25 développera la stratégie d'adoption économique : incitations, pilotes, déploiement progressif, effets de seuil, partenariats et passage à l'échelle.

Note de cadrage institutionnel

Les bénéfices décrits sont des mécanismes potentiels de création de valeur et doivent être vérifiés par des pilotes, études d'impact et indicateurs mesurables. Deep Authenticity© ne garantit pas à elle seule une réduction déterminée de la contrefaçon, une hausse des ventes ou une amélioration macroéconomique.

CHAPITRE 25 — STRATÉGIE D'ADOPTION ÉCONOMIQUE : PILOTES, INCITATIONS ET PASSAGE À L'ÉCHELLE

ADOPTION — PILOTES — INCITATIONS — PARTENARIATS — PASSAGE À L'ÉCHELLE — EFFETS DE SEUIL — AP LÉGER — AP BUSINESS — TRILOGIE DE LA VÉRITÉ — INTEROPÉRABILITÉ — GOUVERNANCE

1. Objet du chapitre

Ce chapitre définit la stratégie d'adoption économique de Deep Authenticity©. Une infrastructure universelle de confiance ne peut être imposée uniquement par sa supériorité technique : elle doit démontrer sa valeur par des pilotes, réduire les frictions d'entrée, créer des incitations pour chaque acteur et organiser un passage progressif de l'expérimentation à l'échelle nationale puis internationale.

2. La Trilogie de la Vérité comme socle d'adoption

Toute stratégie d'adoption doit présenter clairement les trois mécanismes fondamentaux de Deep Authenticity© : les 3 QR Codes pour la vérité du produit physique ; l'Empreinte Cryptographique Native, sésame de l'information et des médias ; et le QR Code Dynamique, sésame du document vérifiable. Cette Trilogie de la Vérité fournit un langage simple permettant aux entreprises, citoyenset institutions de comprendre immédiatement les trois domaines couverts.

3. Adoption par la preuve de valeur

Le déploiement doit commencer par des problèmes concrets et mesurables : contrefaçon, traçabilité insuffisante, difficulté de vérification documentaire, provenance des contenus, visibilité commerciale ou rupture d'information entre acteurs. Chaque pilote définit avant lancement ses indicateurs de succès.

4. Pilotes sectoriels

Des pilotes peuvent être organisés dans des secteurs présentant un besoin élevé de confiance : industrie, pharmacie, agroalimentaire, artisanat, culture, documents administratifs ou médias. Le périmètre doit rester suffisamment limité pour mesurer les résultats tout en représentant un parcours réel de bout en bout.

5. Pilotes territoriaux

Un territoire, une zone industrielle, un port, une commune ou un corridor commercial peut servir de laboratoire opérationnel. Cette approche permet de tester les interactions entre producteurs, revendeurs, consommateurs et autorités avant une extension nationale.

6. Incitation du producteur

Le producteur adopte plus facilement la plateforme si elle combine protection, traçabilité, visibilité commerciale et données utiles. L'intégration doit éviter les doubles saisies grâce aux API et ERP. Les coûts doivent être proportionnés au volume et à la valeur créée.

7. Incitation du revendeur

Le revendeur doit percevoir un bénéfice opérationnel : stock authentifié, meilleure confiance client, recherche par proximité, continuité de vente et gestion simplifiée des retours ou transferts. La Fenêtre Revendeur constitue un levier essentiel d'adoption commerciale.

8. Incitation du consommateur

L'expérience utilisateur doit rester immédiate. Le scan doit fournir une réponse compréhensible et conduire, lorsque pertinent, au Passeport Numérique Universel ou aux services associés. Pour les produits physiques, la lecture VERT–JAUNE–ROUGE demeure le repère fondamental.

9. Incitation documentaire

Pour les administrations, entreprises et citoyens, le QR Code Dynamique permet de vérifier l'état vivant d'un document : valide, expiré, révoqué, remplacé ou autre statut défini. L'adoption documentaire repose sur la simplicité du scan et la capacité de consulter une source de vérité actualisée.

10. Incitation informationnelle et médiatique

Pour les médias, créateurs, institutions et plateformes, l'Empreinte Cryptographique Native permet de rattacher une information ou un contenu à une identité cryptographique et d'en vérifier l'intégrité. Son adoption doit être intégrable aux chaînes de création et de publication sans alourdir excessivement les usages.

11. AP Léger et réduction de la barrière d'entrée

AP Léger permet aux artisans, agriculteurs, créateurs, innovateurs et PME d'entrer dans l'écosystème sans infrastructure informatique lourde. L'adoption universelle exige que la confiance ne soit pas réservée aux organisations disposant de budgets technologiques importants.

12. Partenariats structurants

Les partenariats avec producteurs, distributeurs, institutions, organismes de normalisation, intégrateurs, opérateurs technologiques et acteurs financiers peuvent accélérer le déploiement. Chaque partenariat doit préserver la gouvernance du noyau de confiance et éviter la dépendance exclusive à un acteur.

13. Effets de seuil

La valeur du réseau augmente lorsque suffisamment de producteurs, revendeurs et utilisateurs participent dans une filière ou un territoire. La stratégie doit identifier les seuils minimaux permettant une expérience utile : couverture des produits, densité de revendeurs, disponibilité des contrôles et capacité de vérification.

14. Déploiement par vagues

Le passage à l'échelle peut suivre des vagues : prototype, pilote contrôlé, production limitée, extension sectorielle, extension territoriale, interopérabilité nationale puis Corridors de Confiance internationaux. Chaque vague dispose de critères de passage mesurables.

15. Formation et accompagnement

L'adoption dépend aussi de la compréhension. Producteurs, revendeurs, agents de contrôle et utilisateurs doivent disposer de parcours de formation adaptés. La documentation doit expliquer non seulement comment utiliser le système, mais aussi la signification des preuves et statuts.

16. Interopérabilité plutôt que remplacement brutal

Deep Authenticity© doit s'intégrer aux ERP, systèmes administratifs, infrastructures douanières, plateformes et systèmes financiers existants. Une stratégie de remplacement total créerait des résistances et des coûts élevés. L'interopérabilité permet une transition progressive.

17. Gouvernance de l’adoption

Un programme de déploiement doit suivre adoption, incidents, satisfaction, couverture, coûts, performance et impacts. Les décisions d’extension sont fondées sur ces indicateurs. Les retours des utilisateurs et institutions doivent alimenter les versions suivantes.

18. Modèle économique d’amorçage

Essais, pilotes subventionnés, tarification progressive ou programmes institutionnels peuvent réduire le risque initial. Les conditions temporaires doivent être transparentes et préparer un modèle soutenable. L’objectif est de faciliter l’entrée sans créer une dépendance permanente à la gratuité.

19. Internationalisation

L’expansion internationale doit commencer par des partenaires et corridors où les bénéfices sont clairement identifiables. Standards, localisation linguistique, conformité et souveraineté sont adaptés à chaque juridiction. La Trilogie de la Vérité demeure cependant un socle conceptuel invariant.

20. Critères d’acceptation et conclusion

La stratégie d’adoption est cohérente si la Trilogie de la Vérité est comprise comme socle ; si les pilotes mesurent une valeur réelle ; si producteurs, revendeurs, consommateurs, documents et médias disposent d’incitations propres ; si AP Léger réduit les barrières ; si les partenariats évitent les dépendances exclusives ; si les effets de seuil sont identifiés ; si le déploiement progresse par vagues ; si formation, interopérabilité et gouvernance accompagnent l’expansion ; et si le modèle d’amorçage conduit à une soutenabilité durable.

Deep Authenticity© peut ainsi passer d’une innovation technologique à une infrastructure adoptée : non par une rupture imposée, mais par une succession de preuves de valeur, d’intégrations et de communautés de confiance de plus en plus larges.

Le Chapitre 26 développera la conclusion stratégique du Volume III : synthèse de l’écosystème économique, commercial et financier et articulation avec les volumes suivants.

Note de cadrage institutionnel

La stratégie d’adoption doit être adaptée aux marchés, secteurs et juridictions. Les pilotes ne prouvent une efficacité généralisable que si leurs méthodes, indicateurs et limites sont documentés. Les partenariats publics ou privés doivent respecter les règles de concurrence, marchés publics, données et secteurs réglementés.

CHAPITRE 26 — CONCLUSION STRATÉGIQUE DU VOLUME III : DE LA CONFIANCE À L'ÉCONOMIE VÉRIFIABLE

SYNTHÈSE — ÉCOSYSTÈME ÉCONOMIQUE — COMMERCE — FINANCE — PROPRIÉTÉ — SAAS — LICENCES — ROYALTIES — SOUVERAINETÉ — TRILOGIE DE LA VÉRITÉ — PASSAGE À L'ÉCHELLE

1. Objet de la conclusion

Cette conclusion rassemble les fondations du Volume III de Deep Authenticity©. Le volume a montré comment une infrastructure de vérité peut prolonger l'authentification vers le commerce, la propriété, la finance et l'analyse économique, sans confondre ces fonctions ni leurs responsabilités juridiques.

2. De l'identité à l'économie vérifiable

La chaîne commence par une identité de confiance et se prolonge par des événements vérifiables : production, distribution, vente, paiement, acquisition, transfert, seconde main et analyse. Chaque événement conserve sa nature propre, mais AP Core permet leur rapprochement cohérent.

3. La Trilogie de la Vérité

La doctrine fondamentale de Deep Authenticity© repose désormais sur trois sésames complémentaires : les 3 QR Codes pour la vérité du produit physique ; l'Empreinte Cryptographique Native pour la vérité de l'information et des médias ; le QR Code Dynamique pour la vérité du document vérifiable. Cette Trilogie de la Vérité doit rester une référence transversale dans les volumes suivants.

4. Le produit physique et les trois QR codes

Dans le domaine physique, les trois QR codes — Consommateur, Revendeur/Professionnel et Contrôle/Douanes — demeurent le mécanisme anti-contrefaçon fondateur. Leur séparation fonctionnelle organise les droits et les usages autour d'une même identité produit.

5. La lecture universelle VERT–JAUNE–ROUGE

La lecture VERT = original, JAUNE = original mais déjà vérifié ou vendu, ROUGE = contrefait ou code inexistant dans Authenticity Plus© constitue une interface simple entre la complexité technique et l' utilisateur. Cette sémantique doit rester stable dans l'écosystème physique.

6. Producteur et Revendeur

Le Volume III a placé Producteur et Revendeur au cœur de la chaîne commerciale. Tableaux de bord, stock authentifié, Fenêtre Revendeur, AP Business, ERP et API transforment la confiance en capacité opérationnelle et commerciale.

7. Premier acquéreur et propriété

La première vente peut ouvrir une continuité patrimoniale. Paiement, vente et propriété sont rapprochés sans être fusionnés. Le premier acquéreur devient le point de départ d'une histoire de propriété qui peut se poursuivre pendant toute la vie du produit.

8. Seconde Main

La Seconde Main démontre la valeur de l'identité persistante. Un produit peut changer de propriétaire sans perdre son Passeport Numérique Universel. Provenance, statut et transfert peuvent ainsi accompagner la revente dans un cadre gouverné.

9. Transfert de propriété

Le transfert de propriété constitue un mécanisme structurant de l'économie vérifiable. Il exige identité, droits, consentements et preuves appropriés. Le paiement seul ne suffit pas nécessairement à produire la transition patrimoniale.

10. AP Business

AP Business relie confiance et découverte commerciale : recherche de produits, disponibilité, proximité des revendeurs, B2B/B2C et signaux de demande. La plateforme peut ainsi favoriser des marchés de confiance sans transformer le statut d'authenticité en classement publicitaire.

11. AP Finance et AP Pay

AP Finance structure le contexte financier et AP Pay orchestre les paiements avec des prestataires et infrastructures autorisés. Leur rôle est d'assurer cohérence, interopérabilité et preuve, non de supprimer les obligations réglementaires ou de prétendre remplacer universellement les systèmes financiers existants.

12. Traçabilité produit–transaction–propriété

L'un des acquis majeurs du volume est la distinction de trois continuités : produit, transaction et propriété. Leur rapprochement permet de reconstruire une chaîne économique vérifiable tout en conservant la séparation entre preuve commerciale, preuve financière et relation patrimoniale.

13. SaaS, licences et royalties

Le modèle économique distingue trois leviers : SaaS pour l'accès aux services, licence pour le droit d' usage et royalty pour la rémunération d'une exploitation mesurable. Cette séparation améliore transparence, auditabilité et adaptation sectorielle.

14. Soutenabilité économique

La soutenabilité dépend de revenus diversifiés mais aussi de coûts réels : cloud, cybersécurité, ingénierie, conformité, support, souveraineté et déploiement international. Les projections futures doivent expliciter hypothèses, scénarios et risques.

15. Tableaux de bord et intelligence économique

Les tableaux Producteur, Revendeur et AP Business transforment les événements en indicateurs. L' intelligence prédictive peut ensuite anticiper demande, pénuries, surstocks et anomalies. Observation, alerte, prévision et décision restent des niveaux distincts.

16. Données agrégées et souveraineté informationnelle

La valeur analytique ne repose pas sur la vente indistincte de données personnelles. Elle réside dans des agrégats gouvernés, des indicateurs de qualité et des services analytiques. Les données stratégiques peuvent rester sous contrôle local.

17. Souveraineté économique

Deep Authenticity© peut contribuer à cartographier certaines dépendances, suivre des produits stratégiques et renforcer la résilience informationnelle. La souveraineté recherchée est compatible avec l'interopérabilité : elle protège la maîtrise locale sans imposer l'isolement.

18. Corridors de Confiance et internationalisation

Les Corridors commerciaux et financiers de confiance offrent un modèle fédéré de coopération. Les preuves nécessaires peuvent circuler entre juridictions tandis que bases sensibles, clés et décisions restent sous gouvernance des participants.

19. Adoption et effets de réseau

Le passage à l'échelle repose sur pilotes, AP Léger, intégrations, formation, partenariats et preuves de valeur. Les effets de réseau peuvent renforcer l'utilité collective, mais ils doivent rester ouverts, interopérables, réversibles et compatibles avec les règles de concurrence.

20. Conclusion générale du Volume III

Le Volume III établit que Deep Authenticity© peut constituer un écosystème économique, commercial et financier bâti autour d'une continuité de confiance. Le produit authentifié peut entrer dans un commerce vérifiable, être payé, acquis, transféré, revendu et analysé sans perdre son identité ni effacer son histoire.

La Trilogie de la Vérité donne désormais à cette architecture une doctrine supérieure : vérité du produit par les 3 QR Codes ; vérité de l'information et des médias par l'Empreinte Cryptographique Native ; vérité du document par le QR Code Dynamique. Autour de ces trois sésames, AP Core, AP Ledger, AP Cloud, AP Shield, AP Business, AP Finance, AP Pay et les autres modules constituent les couches opérationnelles de Deep Authenticity©.

Le Volume III ferme ainsi le cycle économique de la confiance. Les volumes suivants pourront étendre cette infrastructure vers les dimensions sectorielles, institutionnelles, prédictives et civilisationnelles de Deep Authenticity© — infrastructure universelle de vérité couvrant le physique, le numérique et l'administratif.

Note de cadrage institutionnel

Cette conclusion synthétise une architecture stratégique et conceptuelle. Les fonctions commerciales, financières, patrimoniales, analytiques et institutionnelles devront être déployées selon les réglementations, autorisations, contrats et validations techniques applicables. Les bénéfices économiques restent à démontrer et mesurer dans les déploiements réels.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV

APPLICATIONS SECTORIELLES

DOCUMENT MAÎTRE CONSOLIDÉ

Livre Blanc 2026 — Authenticity Plus© / Deep Authenticity© — Document Maître Définitif

30 APPLICATIONS — SYNTHÈSE — MATRICE TRANSVERSALE — CONCLUSION

Architecture fonctionnelle consolidée — Édition 2026

NOTE ÉDITORIALE DE CONSOLIDATION

Ce document maître assemble les trente applications sectorielles du Volume IV dans leur ordre officiel. Les versions révisées validées sont retenues pour AP Self — Patrimoine et pour le Chapitre 2 Media / AP Informations. Les textes sectoriels sont conservés sans réécriture de fond ; la consolidation ajoute uniquement la couverture, le sommaire général et l'assemblage éditorial.

SOMMAIRE GÉNÉRAL

01. Industrie — Chapitres 1 à 6
02. Artisanat — Chapitres 1 à 6
03. Agriculture — Chapitres 1 à 6
04. Élevage — Chapitres 1 à 6
05. Pharmacie — Chapitres 1 à 6
06. Santé — Chapitres 1 à 6
07. Automobile — Chapitres 1 à 6
08. Propriété intellectuelle — Chapitres 1 à 6
09. Transport — Chapitres 1 à 6
10. Billetterie — Chapitres 1 à 6
11. Seconde main — Chapitres 1 à 6
12. AP Self — Patrimoine — Chapitres 1 à 6
13. TAXI — Chapitres 1 à 6
14. Logistique — Chapitres 1 à 6
15. Education — Chapitres 1 à 6
16. Food — Chapitres 1 à 6
17. Art et Culture — Chapitres 1 à 6
18. Luxury — Chapitres 1 à 6
19. Construction — Chapitres 1 à 6
20. Smart City — Chapitres 1 à 6
21. Environnement — Chapitres 1 à 6
22. Water — Chapitres 1 à 6
23. Telecom — Chapitres 1 à 6
24. Tourisme — Chapitres 1 à 6
25. Insurance — Chapitres 1 à 6
26. Real Estate / Property — Chapitres 1 à 6
27. Public Administration — Chapitres 1 à 6

28. Defense — Chapitres 1 à 6

29. Media / AP Informations — Chapitres 1 à 6

30. Government — Chapitres 1 à 6

Synthèse générale des 30 applications sectorielles

Matrice transversale des 30 applications sectorielles

MISE À NIVEAU TRANSVERSALE — PASSEPORT NUMÉRIQUE UNIVERSEL

UNE IDENTITÉ PERSISTANTE ADAPTÉE AUX 30 APPLICATIONS SECTORIELLES

Le Passeport Numérique Universel fournit aux applications sectorielles un noyau commun : identité persistante, provenance, statut, événements vérifiables, certifications, droits d'accès et continuité du cycle de vie. Ce noyau n'impose pas un modèle de données uniforme : chaque secteur conserve ses acteurs, autorités, normes, risques et niveaux d'assurance.

Dans l'industrie et les équipements, il peut relier fabrication, série, conformité, installation, maintenance, pièces remplacées, incidents, changements de propriétaire et fin de vie. IoT et NFC peuvent enrichir cette histoire sans remplacer les trois QR Codes lorsque ceux-ci constituent le mécanisme d'authentification physique.

Pour l'artisanat, l'agriculture, l'élevage, l'alimentation, la pharmacie et les biens de consommation, ilpeut relier origine, producteur ou créateur, lots, transformations, certifications, distribution, rappels, interventions et événements de cycle de vie selon les exigences propres au secteur.

Dans la santé, l'éducation, l'identité, les titres, l'immobilier et les autres domaines administratifs, le Passeport Numérique Universel doit respecter l'autorité juridique ou professionnelle de la source. Une infrastructure technique peut vérifier émission, intégrité, statut et chronologie sans se substituer à l' autorité compétente.

Dans les médias, logiciels, créations et propriété intellectuelle, la continuité du Passeport s'articule avec l'Empreinte Cryptographique Native. Dans les documents vérifiables, elle s'articule avec le QR Code Dynamique. Dans le produit physique, elle s'articule avec les trois QR Codes d'Authenticity Plus©.

Le Passeport Numérique Universel constitue ainsi la mémoire structurée de l'actif ou de l'élément sectoriel. Il relie l'état courant à son histoire autorisée sans rendre publiques toutes les données et sans effacer les versions, corrections, révocations ou événements antérieurs.

Règle sectorielle fondamentale : universalité de l'identité ne signifie ni uniformité des données, ni centralisation, ni visibilité universelle. Chaque application sectorielle expose uniquement les informations nécessaires à l'acteur autorisé et au niveau de confiance requis.

Invariant physique : les trois QR Codes — Consommateur, Revendeur/Professionnel et Contrôle/Douanes — restent le mécanisme anti-contrefaçon fondateur. VERT = original ; JAUNE = original mais déjà vérifié ou vendu ; ROUGE = contrefait ou code inexistant dans Authenticity Plus©.

Conclusion générale et clôture officielle du Volume IV

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 1 — INDUSTRIE

CHAPITRE 1 — MISSION, PÉRIMÈTRE ET PRINCIPES FONDATEURS DE L'APPLICATION INDUSTRIELLE

1. Objet du chapitre

Le point 1 — Industrie ouvre le Volume IV — Applications sectorielles. Il décline les capacités Authenticity Plus© / Deep Authenticity© dans les environnements industriels afin d'identifier les objets, relier les événements de production et de circulation, renforcer la traçabilité et fournir des preuves exploitables tout au long du cycle de vie.

2. Mission sectorielle

L'application Industrie vise à établir une continuité de confiance entre l'objet industriel, son identité numérique, son origine, sa fabrication, ses transformations, ses contrôles, sa distribution, son exploitation et sa fin de vie, selon les informations réellement disponibles et autorisées.

3. Objet industriel

Le périmètre peut couvrir un produit fini, un composant, une pièce, un sous-ensemble, un équipement, un lot ou un autre objet industriel identifiable. Chaque objet doit être rattaché au niveau d'identification pertinent sans imposer systématiquement une granularité unitaire.

4. Identité de l'objet

L'identité numérique doit permettre de distinguer l'objet, le lot ou la série concernée et de le corréler aux événements autorisés. L'identifiant ne constitue pas à lui seul une preuve de conformité, d'origine ou d'authenticité : ces affirmations dépendent des preuves et événements associés.

5. Producteur et fabricant

Le producteur ou fabricant constitue un acteur central du parcours industriel. Son identité, son rôle, ses sites ou capacités pertinentes doivent pouvoir être reliés aux objets qu'il déclare ou produit, selon les droits et mécanismes de validation applicables.

6. Sites et unités de production

Les événements peuvent être rattachés à une usine, un atelier, une ligne ou une unité fonctionnelle lorsque cette granularité est utile. La plateforme doit éviter de déduire une localisation ou une responsabilité qui n'a pas été explicitement établie.

7. Matières et composants

Lorsque le cas d'usage l'exige, les matières, composants ou sous-ensembles peuvent être référencés comme éléments d'entrée d'un produit industriel. Leur relation avec le produit final doit rester traçable sans nécessairement exposer l'intégralité des informations confidentielles de fabrication.

8. Lots et séries

Les modèles de production par lot, série ou unité doivent être supportés. Une information applicable à un lot ne doit pas être présentée comme une observation individuelle si aucune preuve au niveau unitaire n'existe.

9. Événements de fabrication

Création, assemblage, transformation, contrôle, conditionnement ou autre événement industriel pertinent peut enrichir le cycle de vie. Chaque événement doit identifier son type, son objet, sa date, son acteur ou système source et son niveau de confiance lorsque cela est nécessaire.

10. Contrôles qualité

Les résultats de contrôle qualité peuvent être associés à l'objet ou au lot selon le périmètre autorisé. Authenticity Plus© ne doit pas transformer un contrôle partiel ou un document fourni par un acteur en certification générale non établie.

11. Conformité et documents

Certificats, rapports, déclarations, notices ou documents techniques peuvent être corrélés aux objets industriels. Leur présence prouve l'existence du document enregistré, mais la plateforme doit distinguer l'intégrité documentaire de la validité juridique ou réglementaire de son contenu.

12. Chaîne d'approvisionnement

Les transferts entre acteurs, sites ou étapes logistiques peuvent enrichir la traçabilité industrielle. Les relations avec Producteur, Revendeur, Transport et autres domaines doivent conserver les responsabilités propres à chacun.

13. Propriété et possession

La possession physique, la garde logistique et la propriété juridique ou fonctionnelle ne doivent pas être confondues. Le domaine Propriété reste responsable des changements de titulaire lorsqu'ils sont représentés dans l'écosystème.

14. Maintenance et réparation

Pour les équipements ou produits durables, les interventions de maintenance, réparation et remplacement de composants peuvent prolonger le dossier de cycle de vie. Les interventions doivent être attribuables à des acteurs ou systèmes autorisés.

15. Pièces de rechange

Une pièce de rechange peut disposer de sa propre identité et être reliée à l'équipement dans lequel elle est installée. Le remplacement doit préserver l'historique de l'ancienne pièce et la date d'entrée en service de la nouvelle.

16. Rappels et incidents

Lorsqu'un fabricant ou une autorité compétente publie un rappel ou une information de sécurité applicable, le système peut relier l'avis aux lots ou objets concernés. Il ne doit pas inventer l' applicabilité lorsque les références ne permettent pas de l'établir.

17. Seconde main et reconditionnement

Un objet industriel peut entrer dans un circuit de revente, de reconditionnement ou de réemploi. Son historique industriel peut accompagner ce nouveau cycle selon les droits d'accès, tandis que la transaction et la propriété suivent les domaines correspondants.

18. Données confidentielles

Les nomenclatures, procédés, paramètres de fabrication, fournisseurs et résultats techniques peuvent constituer des informations sensibles. La traçabilité doit donc être conçue avec des niveaux de visibilité adaptés aux acteurs et aux finalités.

19. Interfaces avec l'écosystème AP

L'application Industrie peut interagir avec Producteur, Revendeur, Propriété, AP Business, AP Finance, AP Pay, SaaS, Licences et Royalties ainsi qu'avec les briques techniques et de preuve des autres volumes. Elle consomme ces capacités sans redéfinir leurs responsabilités.

20. Conclusion

L'application Industrie transpose l'architecture Authenticity Plus© / Deep Authenticity© au cycle de vie des objets industriels. Identité, lots, fabrication, composants, contrôles, documents, maintenance, rappels et circulation constituent les premières fondations d'un dossier industriel traçable et extensible.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 1 — INDUSTRIE

CHAPITRE 2 — IDENTITÉ INDUSTRIELLE, GÉNÉALOGIE PRODUIT, LOTS, SÉRIES ET NOMENCLATURES

1. Objet du chapitre

Ce chapitre structure l'identité industrielle et les relations permettant de reconstruire la généalogie d' un produit, d'un lot, d'une série ou d'un équipement. Il complète les principes fondateurs du chapitre 1 en organisant les liens entre objets industriels sans transformer une relation déclarée en preuve automatique de conformité.

2. Granularité d'identification

Le système doit permettre plusieurs niveaux de granularité : référence de produit, lot, série, unité, composant ou sous-ensemble. Le niveau retenu dépend du cas d'usage, du processus industriel et des preuves réellement disponibles.

3. Identifiant persistant

Chaque objet suivi doit disposer d'une référence suffisamment stable pour être corrélé aux événements de son cycle de vie. Une modification de désignation commerciale ou de localisation ne doit pas créer artificiellement un nouvel objet lorsque l'identité industrielle demeure la même.

4. Référence fabricant

La référence interne ou commerciale du fabricant peut être associée à l'identité AP. Cette relation doit permettre de rapprocher les systèmes industriels existants sans supposer que la référence fabricant est universellement unique.

5. Lot de production

Un lot regroupe des objets ou matières selon une logique de fabrication définie. Les événements appliqués au lot doivent indiquer leur portée afin de ne pas être présentés comme des observations unitaires lorsqu'aucun contrôle individuel n'a été réalisé.

6. Numéro de série

Lorsqu'un suivi unitaire existe, le numéro de série peut être corrélé à l'identité numérique de l'objet. Les doublons, réutilisations ou incohérences de numérotation doivent pouvoir être signalés comme anomalies.

7. Nomenclature

La nomenclature décrit les composants ou sous-ensembles nécessaires à la constitution d'un produit selon le niveau de détail autorisé. Elle peut être versionnée afin de refléter les évolutions de conception ou de fabrication.

8. Version de nomenclature

Un produit fabriqué doit pouvoir être rattaché à la version de nomenclature applicable à sa période ou à son ordre de fabrication. Une version ultérieure ne doit pas réécrire silencieusement la composition historique.

9. Généalogie ascendante

La généalogie ascendante permet d'identifier, selon les données disponibles, les lots, composants ou matières ayant contribué à la fabrication d'un objet. Elle facilite l'analyse d'un incident et la détermination du périmètre potentiellement concerné.

10. Généalogie descendante

La généalogie descendante permet de rechercher les produits ou équipements ayant reçu un composant, un lot ou une matière déterminée. Cette capacité est particulièrement utile pour les rappels et investigations industrielles.

11. Assemblage

Un événement d'assemblage relie des composants à un ensemble ou produit final. Il doit conserver les références nécessaires pour distinguer la composition prévue de la composition effectivement enregistrée lorsque cette information existe.

12. Désassemblage

Lorsqu'un équipement est démonté, reconditionné ou recyclé, les relations entre l'ensemble et ses composants peuvent évoluer. L'historique antérieur doit être conservé afin que le désassemblage ne supprime pas la généalogie passée.

13. Substitution de composant

Une substitution autorisée doit identifier le composant prévu, le composant utilisé et le contexte de la décision lorsque ces informations sont disponibles. Le système ne doit pas qualifier lui-même la substitution de conforme sans preuve ou règle compétente.

14. Transformation

Une transformation industrielle peut faire disparaître l'identité physique d'un intrant au profit d'un nouvel objet ou lot. La relation de provenance doit alors être conservée sans prétendre que l'intrant demeure un composant individualisable.

15. Fusion et fractionnement de lots

Le système doit pouvoir représenter la fusion de plusieurs lots ou le fractionnement d'un lot en sous-lots. Les nouvelles références doivent conserver les relations de provenance afin d'éviter une rupture de traçabilité.

16. Reconditionnement

Un objet reconditionné peut conserver son identité historique ou recevoir un statut ou une identité dérivée selon le processus retenu. Les composants remplacés et interventions pertinentes doivent rester rattachés au dossier.

17. Synchronisation avec les systèmes industriels

Les identités, lots, séries et nomenclatures peuvent provenir d'ERP, MES, PLM, WMS ou autres systèmes autorisés. Les interfaces doivent préserver la source, les références et les règles de corrélation sans supposer que tous les systèmes utilisent le même modèle.

18. Confidentialité de la nomenclature

La généalogie industrielle ne signifie pas que chaque acteur peut consulter toute la nomenclature. Les relations nécessaires à la preuve, au rappel ou à la maintenance peuvent être exposées selon des niveaux de visibilité distincts.

19. Critères d'acceptation

Le modèle est acceptable si un objet peut être relié à son lot ou sa série, à la version de nomenclature applicable et aux composants ou intrants enregistrés, et si les transformations, substitutions, fusions ou fractionnements restent historiquement reconstructibles.

20. Conclusion

Identité, lots, séries, nomenclatures et généalogie constituent le socle de la traçabilité industrielle détaillée. Ils permettent de relier fabrication, composants et transformations tout en préservant le versionnement, la confidentialité et la distinction entre donnée déclarée et preuve établie.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 1 — INDUSTRIE

CHAPITRE 3 — PROCESSUS DE FABRICATION, CONTRÔLES QUALITÉ, CONFORMITÉ ET PREUVES INDUSTRIELLES

1. Objet du chapitre

Ce chapitre organise les événements de fabrication et les preuves qui peuvent être associés à un objet industriel, un lot, une série ou un équipement. Il distingue l'enregistrement d'un processus, le résultat d' un contrôle, l'existence d'un document et l'affirmation de conformité afin d'éviter toute confusion entre traçabilité et certification.

2. Ordre de fabrication

Lorsqu'il existe, l'ordre de fabrication peut servir de référence de corrélation entre produit, lot, nomenclature, opérations et contrôles. Son enregistrement doit préserver la source et la version pertinentes sans faire d'Authenticity Plus© le système maître de planification industrielle.

3. Gamme opératoire

Une gamme ou séquence d'opérations peut décrire les étapes prévues de fabrication. Le système doit distinguer le processus théorique de l'exécution effectivement enregistrée sur un objet ou un lot.

4. Événement de production

Chaque événement de production pertinent peut préciser le type d'opération, l'objet concerné, la date, le site, l'équipement ou le système source et l'acteur lorsque ces informations sont autorisées. L' absence d'une donnée ne doit pas être comblée par une déduction implicite.

5. Début et fin d'opération

Lorsque le processus l'exige, une opération peut conserver ses instants de début et de fin. Ces horodatages permettent d'établir une chronologie sans constituer à eux seuls une preuve que toutes les conditions techniques ont été respectées.

6. Paramètres de procédé

Température, pression, vitesse, dosage, couple, durée ou autres paramètres peuvent être associés à une opération lorsque leur conservation est utile. Les valeurs sensibles doivent être protégées selon leur niveau de confidentialité industrielle.

7. Source machine

Les données peuvent provenir d'un automate, d'une machine, d'un MES, d'un capteur ou d'un autre système autorisé. La plateforme doit conserver la provenance technique afin de distinguer une donnée automatisée d'une saisie humaine ou d'un document importé.

8. Contrôle en cours de fabrication

Des contrôles intermédiaires peuvent être rattachés aux étapes correspondantes. Un contrôle sur échantillon doit être identifié comme tel et ne doit pas être présenté comme une mesure individuelle de chaque unité du lot.

9. Contrôle final

Le contrôle final peut enregistrer des résultats, statuts et références documentaires selon le processus du fabricant. Le statut enregistré doit rester attribuable à la règle ou à l'autorité qui l'a produit.

10. Critères et spécifications

Les contrôles peuvent être évalués par rapport à une spécification ou une version de critères. Le système doit conserver la référence de cette version afin qu'une modification ultérieure ne change pas rétroactivement l'interprétation historique.

11. Résultat conforme ou non conforme

Un résultat peut être qualifié selon les règles du processus compétent. Authenticity Plus© conserve cette qualification et sa provenance mais ne doit pas inventer une conformité réglementaire générale à partir d'un simple statut interne.

12. Non-conformité

Une non-conformité peut être reliée à l'objet, au lot, au contrôle et à l'étape de fabrication concernés. Son ouverture ne signifie pas nécessairement que le produit final sera rejeté : la décision dépend du processus qualité applicable.

13. Dérogation et disposition

Lorsqu'une dérogation, retouche, rebut, acceptation conditionnelle ou autre disposition est décidée, elle doit être attribuable à un rôle ou système compétent et conserver son motif ou sa référence lorsque cela est autorisé.

14. Retouche et reprise

Une opération de retouche ou reprise doit enrichir l'historique plutôt que remplacer l'événement initial. Les nouveaux contrôles réalisés après intervention doivent être corrélés à la séquence correspondante.

15. Certificats et rapports

Certificats d’analyse, rapports d’essai, procès-verbaux ou autres documents peuvent être associés à l’ objet ou au lot. La plateforme peut prouver leur intégrité et leur rattachement sans se substituer à l’ organisme qui en garantit le contenu ou la portée.

16. Signature et validation

Lorsqu’une validation humaine ou électronique est requise, l’identité du valideur, la date, le rôle et la version de l’élément validé doivent pouvoir être conservés selon les mécanismes prévus. Une validation ne doit pas être transférée automatiquement à une version ultérieure.

17. Preuve et AP Ledger

Lorsque l’architecture globale le prévoit, des empreintes, références ou preuves d’intégrité peuvent être ancrées dans AP Ledger. L’application Industrie exploite ce mécanisme pour renforcer la traçabilité sans redéfinir AP Ledger.

18. Rappel et analyse d’impact

Les résultats de contrôle, non-conformités et généalogies peuvent contribuer à déterminer le périmètre d’un rappel ou d’une investigation. Le système doit présenter les objets potentiellement concernés selon les relations établies, sans élargir arbitrairement le périmètre.

19. Critères d’acceptation

Le modèle est acceptable si un événement de fabrication peut être relié à son objet, son processus, sa source et ses contrôles ; si les versions de critères restent identifiables ; et si une preuve documentaire ou technique peut être distinguée de l’affirmation de conformité qu’elle supporte.

20. Conclusion

Processus de fabrication, paramètres, contrôles, non-conformités, reprises et preuves forment la couche d’exécution industrielle du dossier Authenticity Plus©. Leur valeur repose sur la provenance, le versionnement, la chronologie et la distinction stricte entre donnée enregistrée, preuve d’intégrité et décision de conformité.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 1 — INDUSTRIE

CHAPITRE 4 — CHAÎNE D'APPROVISIONNEMENT, LOGISTIQUE, MAINTENANCE ET CYCLE DE VIE INDUSTRIEL

1. Objet du chapitre

Ce chapitre prolonge la traçabilité au-delà de la fabrication afin de couvrir l'approvisionnement, les mouvements logistiques, la mise en service, la maintenance, les réparations, le reconditionnement et la fin de vie. Chaque événement doit rester corrélé à l'objet industriel et à l'acteur ou système qui l'a produit.

2. Approvisionnement

Les matières, composants et sous-ensembles reçus peuvent être reliés à leur fournisseur, lot, référence et documents associés lorsque ces informations sont autorisées. La réception ne constitue pas automatiquement une validation de conformité.

3. Fournisseur

Un fournisseur doit être identifiable dans le contexte de la relation industrielle. Ses déclarations et documents doivent rester attribuables à leur source sans être transformés en garanties générales par la plateforme.

4. Réception industrielle

La réception peut enregistrer date, site, quantité, lot, état et contrôles associés. Les écarts de quantité, dommages ou anomalies doivent pouvoir être conservés sans modifier silencieusement les informations d'expédition.

5. Stockage

Les mouvements d'entrée, sortie et changement d'emplacement peuvent enrichir le dossier lorsque la traçabilité l'exige. Une localisation enregistrée représente un état connu à un instant donné et non une position permanente.

6. Conditions de conservation

Température, humidité, vibration ou autres conditions peuvent être enregistrées pour les produits sensibles. Les données doivent conserver leur source, leur période et leur couverture afin de distinguer une mesure continue d'un contrôle ponctuel.

7. Préparation et expédition

La préparation d'une expédition peut relier objets, lots, quantités, emballages et destination. L' expédition constitue un événement logistique distinct du transfert de propriété et du paiement.

8. Transport

Les informations de transport peuvent être corrélées au domaine sectoriel Transport lorsque celui-ci sera défini. L'application Industrie conserve les références nécessaires sans absorber les responsabilités propres au transporteur ou à la chaîne logistique.

9. Réception par le destinataire

La réception à destination peut confirmer la remise physique ou logistique selon le processus applicable. Elle ne doit pas être interprétée automatiquement comme acceptation commerciale, transfert juridique de propriété ou conformité technique.

10. Mise en service

Pour un équipement durable, la mise en service peut devenir une étape majeure du cycle de vie. Elle peut enregistrer la date, le site, l'installateur, la configuration initiale et les contrôles réalisés selon les droits disponibles.

11. Configuration en exploitation

Les configurations significatives d'un équipement peuvent évoluer après installation. Les versions ou paramètres nécessaires à la traçabilité doivent être conservés lorsque leur modification affecte l' interprétation des événements ultérieurs.

12. Maintenance préventive

Les interventions planifiées peuvent être rattachées à l'équipement, au programme de maintenance et à l'intervenant. Une échéance de maintenance ne signifie pas qu'une intervention a effectivement été réalisée.

13. Maintenance corrective

Une panne ou anomalie peut déclencher une intervention corrective. Diagnostic, pièces remplacées, actions réalisées et résultat peuvent être enregistrés sans transformer le dossier en garantie absolue de remise en état.

14. Pièces remplacées

Le remplacement d'un composant doit préserver la relation avec l'ancienne pièce et identifier la nouvelle lorsqu'elles sont suivies individuellement. La généalogie de l'équipement doit refléter les périodes pendant lesquelles chaque composant était installé.

15. Réparation et reconditionnement

Une réparation ou un reconditionnement doit enrichir l'historique du produit. Les modifications, contrôles et nouvelles conditions de mise sur le marché ou de remise en service doivent rester attribuables aux acteurs compétents.

16. Changement d'exploitant ou de propriétaire

Le changement de détenteur opérationnel, d'exploitant ou de propriétaire doit être distingué. Les transferts de propriété restent gouvernés par le domaine Propriété, tandis que l'application Industrie conserve les événements de cycle de vie autorisés.

17. Rappel et retrait

Un rappel ou retrait peut exploiter la généalogie, les lots et la localisation connue pour identifier les objets potentiellement concernés. Le statut de chaque objet doit refléter les confirmations réellement obtenues et non une simple supposition de récupération.

18. Fin de vie

Mise hors service, démontage, réemploi, recyclage, destruction ou autre disposition de fin de vie peut être enregistrée. Ces événements doivent préserver l'historique antérieur et, lorsque pertinent, créer des relations vers les composants ou matières récupérés.

19. Critères d'acceptation

Le modèle est acceptable si les principales transitions depuis l'approvisionnement jusqu'à la fin de vie sont reconstructibles, si possession, transport, propriété et paiement restent distincts, et si les interventions de maintenance conservent la généalogie des composants.

20. Conclusion

La chaîne d'approvisionnement et le cycle de vie étendent le dossier industriel de la matière reçue jusqu'à la fin d'exploitation. Logistique, conditions de conservation, mise en service, maintenance, pièces remplacées, rappels et fin de vie créent une continuité de traçabilité autour de l'objet industriel.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 1 — INDUSTRIE

CHAPITRE 5 — RAPPELS, INCIDENTS, CONTREFAÇON, AUDIT ET GOUVERNANCE SECTORIELLE

1. Objet du chapitre

Ce chapitre organise la réponse industrielle lorsqu'une anomalie, un incident, un doute d'authenticité ou un rappel affecte un produit, un lot, un composant ou une série. Il définit également les principes d'audit et de gouvernance nécessaires pour que les informations sectorielles restent attribuables, contrôlées et exploitables.

2. Signalement d'incident

Un incident peut provenir d'un fabricant, d'un distributeur, d'un exploitant, d'un système technique ou d'un autre acteur autorisé. Le signalement doit conserver sa source, sa date, l'objet concerné et son statut sans transformer une alerte initiale en conclusion définitive.

3. Qualification

Les incidents peuvent être qualifiés selon leur nature, leur gravité et leur périmètre par les rôles compétents. La plateforme doit conserver les changements de qualification afin de distinguer l'évaluation initiale de la décision finale.

4. Corrélation avec la généalogie

La généalogie ascendante et descendante peut être utilisée pour rechercher les lots, composants ou produits potentiellement liés à un incident. Le résultat représente un périmètre d'investigation fondé sur les relations enregistrées et non une preuve automatique de défaillance.

5. Rappel

Un rappel doit pouvoir être rattaché à l'autorité ou à l'acteur qui l'émet, à sa référence, à sa date et aux critères déterminant les objets concernés. Authenticity Plus© diffuse et corrèle l'information sans se substituer à l'autorité compétente.

6. Périmètre du rappel

Le périmètre peut être défini par produit, lot, série, période, composant ou autre critère disponible. Les objets identifiés doivent pouvoir être classés comme potentiellement concernés, confirmés, exclus ou traités selon les informations réellement obtenues.

7. Suivi du rappel

Les notifications, retours, immobilisations, réparations, remplacements ou destructions peuvent enrichir le suivi. Le système doit distinguer une notification envoyée d'une action effectivement réalisée sur l'objet.

8. Contrefaçon et anomalie d'identité

Une identité dupliquée, incohérente, réutilisée ou associée à des caractéristiques incompatibles peut constituer un signal d'anomalie. La plateforme peut détecter et signaler ces incohérences sans conclure automatiquement à une infraction pénale ou à une contrefaçon juridiquement établie.

9. Vérification de provenance

La provenance peut être renforcée par la continuité des événements, la généalogie, les signatures, les documents et les preuves d'intégrité. Une rupture de chaîne doit être présentée comme une limitation de preuve plutôt que comblée par une supposition.

10. Clonage d'identifiant

Des usages incompatibles d'un même identifiant peuvent déclencher des contrôles supplémentaires : lieux impossibles, chronologies contradictoires, volumes anormaux ou réutilisations non prévues. Les règles de détection doivent rester explicables et auditables.

11. Scoring et signaux

Des scores ou indicateurs de risque peuvent agréger plusieurs signaux. Ils doivent être présentés comme des outils d'aide à l'analyse et non comme des verdicts automatiques, notamment lorsqu'ils reposent sur des données incomplètes.

12. Mise en quarantaine

Un objet ou lot peut être placé dans un statut de quarantaine fonctionnelle selon les droits applicables. Ce statut doit indiquer son origine, sa date et les opérations restreintes sans modifier rétroactivement les événements antérieurs.

13. Levée de quarantaine

La levée doit être effectuée par un acteur ou système autorisé et conserver la justification ou référence pertinente. Une simple disparition du signal initial ne doit pas suffire à effacer l'historique de l'incident.

14. Audit industriel

L'audit doit permettre de reconstruire les principales décisions et événements : création d'identité, changements de nomenclature, contrôles, non-conformités, interventions, rappels, changements de statut et accès privilégiés.

15. Intégrité et AP Ledger

Lorsque l’architecture globale le prévoit, des empreintes ou références critiques peuvent être ancrées dans AP Ledger afin de renforcer l’intégrité et la chronologie. L’application Industrie reste consommatrice de cette capacité.

16. Gouvernance des rôles

Fabricants, fournisseurs, contrôleurs, mainteneurs, distributeurs et autres acteurs ne doivent disposer que des droits nécessaires à leurs responsabilités. Les capacités de modification d’un historique critique doivent être particulièrement limitées.

17. Confidentialité et partage

Un rappel ou une investigation peut nécessiter de partager certaines informations au-delà des frontières habituelles. Ce partage doit rester proportionné au besoin et ne pas exposer automatiquement des secrets industriels, nomenclatures ou données commerciales sans nécessité.

18. Conservation

Les événements, preuves, décisions et documents critiques doivent être conservés selon les politiques applicables au secteur, au produit et au territoire. La plateforme doit permettre des règles différenciées plutôt qu’imposer une durée universelle.

19. Critères d’acceptation

Le modèle est acceptable si un incident peut être relié aux objets potentiellement concernés, si les rappels sont suivis sans confusion entre notification et traitement, si les signaux de contrefaçon restent explicables, et si toute décision critique demeure attribuable et auditée.

20. Conclusion

Rappels, incidents, anomalies d’identité, contrôles de provenance et audit constituent la couche de gouvernance du risque industriel. Ils permettent d’exploiter la traçabilité pour agir rapidement tout en distinguant signal, preuve, décision métier et qualification juridique.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 1 — INDUSTRIE

CHAPITRE 6 — SYNTHÈSE FONCTIONNELLE, CRITÈRES D'ACCEPTATION ET CLÔTURE DE L'APPLICATION INDUSTRIELLE

1. Objet du chapitre

Ce chapitre clôt le Point 1 — Industrie du Volume IV. Il consolide l'identité industrielle, la généalogie produit, la fabrication, les contrôles qualité, la chaîne d'approvisionnement, la maintenance, les rappels, la lutte contre les anomalies d'identité et la gouvernance sectorielle.

2. Mission consolidée

L'application Industrie établit un dossier de cycle de vie permettant de relier un objet industriel à son origine, sa fabrication, ses composants, ses contrôles, sa circulation, son exploitation et sa fin de vie, selon les données et preuves effectivement disponibles.

3. Identité et granularité

Produit, référence, lot, série, unité, composant et sous-ensemble peuvent être identifiés au niveau pertinent. La plateforme ne doit pas présenter une information de lot comme une observation unitaire lorsqu'aucune preuve individuelle n'existe.

4. Généalogie

Les relations ascendantes et descendantes doivent permettre de reconstruire la provenance des intrants et la destination des composants ou lots. Assemblage, transformation, fusion, fractionnement et substitution doivent préserver l'historique.

5. Fabrication

Les événements de production peuvent relier ordre, gamme, site, équipement, paramètres et source technique. La traçabilité d'une opération ne signifie pas automatiquement que celle-ci respecte toutes les exigences de conformité.

6. Qualité et conformité

Contrôles, non-conformités, dérogations, reprises et validations doivent être attribuables et versionnés lorsque nécessaire. Authenticity Plus© distingue l'intégrité de la preuve de la qualification de conformité produite par l'acteur compétent.

7. Documents et preuves

Certificats, rapports et documents techniques peuvent être corrélés à l'objet ou au lot. Leur intégrité et leur rattachement peuvent être renforcés sans transformer la plateforme en autorité émettrice du document.

8. Approvisionnement et logistique

Réception, stockage, préparation, expédition et transport enrichissent la continuité du dossier industriel. Expédition, possession, réception, propriété et paiement restent des événements distincts.

9. Mise en service et exploitation

Pour les équipements durables, installation, configuration, mise en service et changements significatifs peuvent être conservés afin de relier la phase de fabrication à la phase d'exploitation.

10. Maintenance

Maintenance préventive et corrective, diagnostic, réparation et remplacement de composants doivent enrichir l'historique. Une intervention planifiée doit rester distincte d'une intervention effectivement réalisée.

11. Reconditionnement et seconde main

Le reconditionnement et la revente prolongent le cycle de vie de l'objet. Les modifications techniques restent dans le dossier industriel, tandis que transactions et changements de titulaire utilisent les domaines économiques et de Propriété correspondants.

12. Incidents et rappels

Les incidents doivent pouvoir être reliés aux objets potentiellement concernés grâce aux lots et à la généalogie. Le suivi d'un rappel doit distinguer notification, confirmation, traitement et clôture.

13. Authenticité et anomalies

Clonage d'identifiant, chronologies incompatibles, provenance incomplète ou volumes anormaux peuvent produire des signaux. Ces signaux soutiennent l'investigation sans constituer automatiquement une conclusion juridique de contrefaçon.

14. Confidentialité industrielle

Nomenclatures, procédés, paramètres, fournisseurs et résultats techniques peuvent être sensibles. La valeur de la traçabilité ne dépend pas d'une exposition universelle : les niveaux de visibilité doivent être adaptés aux acteurs et finalités.

15. Audit et AP Ledger

Les événements critiques et changements sensibles doivent rester reconstructibles. Lorsque l' architecture globale le prévoit, AP Ledger peut renforcer l'intégrité et la chronologie des références ou preuves sélectionnées.

16. Critère d’acceptation — identité et généalogie

Un objet suivi doit pouvoir être relié au bon niveau d’identité, à son lot ou sa série et, lorsque disponible, à sa composition historique. Les transformations ne doivent pas rompre silencieusement la chaîne de provenance.

17. Critère d’acceptation — exécution et qualité

Les opérations de fabrication et contrôles doivent être attribuables à leurs sources, critères et versions. Les données déclarées, mesures, validations et preuves documentaires doivent rester distinguables.

18. Critère d’acceptation — cycle de vie

Les principales transitions depuis l’approvisionnement jusqu’à la fin de vie doivent être reconstructibles. Maintenance, remplacement, rappel, reconditionnement et fin de vie doivent préserver les événements antérieurs.

19. Critère d’acceptation — gouvernance

Les droits doivent suivre le moindre privilège ; les informations confidentielles doivent rester protégées ; les décisions critiques, accès privilégiés et changements de statut doivent être auditables.

20. Clôture du Point 1 — Industrie

Le Point 1 — Industrie est désormais fonctionnellement défini : identité, généalogie, fabrication, qualité, logistique, maintenance, rappels, authenticité, audit et cycle de vie. Cette architecture sectorielle peut servir de modèle de référence pour les autres applications du Volume IV tout en laissant à chaque secteur ses objets, règles et contraintes propres.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 2 — ARTISANAT

CHAPITRE 1 — MISSION, PÉRIMÈTRE ET PRINCIPES FONDATEURS DE L'APPLICATION ARTISANAT

1. Objet du chapitre

Le Point 2 — Artisanat transpose Authenticity Plus© / Deep Authenticity© aux objets issus d'un savoir-faire artisanal. Il vise à relier une pièce à son artisan, son atelier, ses matières, son processus de création, ses preuves, ses transmissions et ses interventions ultérieures.

2. Mission sectorielle

L'application Artisanat doit créer une continuité de confiance autour de l'origine et de l'histoire d'une pièce sans réduire l'artisanat à un processus industriel. Elle doit préserver la singularité du geste, la diversité des pratiques et la valeur de la provenance.

3. Artisan

L'artisan constitue un acteur central. Son identité numérique peut être reliée à ses créations, déclarations et validations selon les droits applicables, sans que l'inscription dans la plateforme constitue à elle seule une reconnaissance officielle d'un titre professionnel.

4. Atelier

L'atelier peut être identifié comme lieu ou structure de création. Plusieurs artisans peuvent y intervenir et un artisan peut exercer dans plusieurs lieux ; ces relations doivent être explicites plutôt que déduites.

5. Objet artisanal

Le modèle peut couvrir une œuvre, un objet décoratif ou utilitaire, un bijou, un textile, une pièce de mobilier, une céramique ou tout autre objet issu d'un processus artisanal identifiable.

6. Pièce unique

Une pièce unique peut disposer d'une identité propre dès sa création. Cette identité doit préserver la continuité de son histoire même si sa propriété, sa localisation ou son état évoluent.

7. Petite série

Une création produite en petite série peut être identifiée au niveau de la série et, lorsque nécessaire, au niveau de chaque exemplaire. La plateforme doit distinguer les caractéristiques communes de la série des observations propres à une pièce.

8. Matières

Les matières utilisées peuvent être déclarées et, lorsque des preuves existent, reliées à leur provenance, fournisseur, lot ou certification. Une déclaration de matière doit rester distincte d'une preuve indépendante de son origine.

9. Provenance des matières

La provenance peut contribuer fortement à la valeur d'une pièce : origine géographique, filière, récupération, matière ancienne ou autre caractéristique pertinente. Toute affirmation doit conserver sa source et son niveau de preuve.

10. Technique et savoir-faire

La technique employée peut être décrite selon le vocabulaire de l'artisan ou du métier. La plateforme documente cette information sans prétendre évaluer elle-même la maîtrise artistique ou la qualité du geste.

11. Étapes de création

Conception, préparation, façonnage, assemblage, cuisson, finition ou autres étapes peuvent enrichir le dossier lorsqu'elles sont pertinentes. Le niveau de détail reste adapté au métier et à la confidentialité du savoir-faire.

12. Signature et marque d'atelier

Signature, poinçon, marque, estampille ou autre signe peuvent être corrélés à l'identité numérique. Leur présence constitue un élément de provenance mais ne doit pas être utilisée isolément comme preuve absolue d'authenticité.

13. Certificat d'authenticité

Un certificat peut être associé à la pièce et à son émetteur. Authenticity Plus© peut renforcer son intégrité et son rattachement à l'objet sans se substituer à l'auteur ou à l'organisme responsable de l' affirmation.

14. Documentation visuelle

Photographies, vues de détails ou autres éléments visuels peuvent documenter l'état et les caractéristiques d'une pièce à différentes étapes. Ils doivent être datés et attribuables lorsqu'ils servent de preuve.

15. Propriété

La création par l’artisan, la possession physique et la propriété de l’objet sont des notions distinctes. Les changements de titulaire restent gouvernés par le domaine Propriété.

16. Vente et transmission

Première vente, don, succession ou revente peuvent prolonger l’histoire de la pièce. Les événements économiques utilisent les domaines correspondants du Volume III tandis que l’application Artisanat conserve le contexte sectoriel.

17. Réparation et restauration

Une réparation, restauration ou modification doit enrichir l’historique de la pièce et identifier l’ intervenant lorsque possible. L’état d’origine et les interventions ultérieures doivent rester distinguables.

18. Seconde main

La seconde main est particulièrement importante pour les pièces artisanales durables. L’historique de provenance, les certificats, les interventions et les changements de propriété peuvent renforcer la confiance lors d’une revente sans garantir automatiquement la valeur marchande.

19. Confidentialité et droits

Les croquis, procédés, recettes, patrons, techniques ou informations commerciales peuvent être sensibles. Les mécanismes de preuve doivent permettre de protéger le savoir-faire tout en exposant uniquement les éléments nécessaires à l’authenticité et à la traçabilité.

20. Conclusion

L’application Artisanat repose sur l’identité de la pièce, l’identité de l’artisan, la provenance, les matières, le geste, la documentation et la continuité historique. Elle crée un passeport de confiance adapté à la singularité artisanale sans confondre preuve technique, reconnaissance professionnelle, propriété et valeur.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 2 — ARTISANAT

CHAPITRE 2 — IDENTITÉ DE LA PIÈCE, PROVENANCE, MATIÈRES, SAVOIR-FAIRE ET GÉNÉALOGIE ARTISANALE

1. Objet du chapitre

Ce chapitre structure le passeport numérique de la pièce artisanale. Il relie l'objet à son artisan ou atelier, à ses matières, à ses étapes de création et aux preuves de provenance disponibles, tout en respectant la singularité des métiers et la confidentialité du savoir-faire.

2. Identité persistante de la pièce

Chaque pièce suivie doit disposer d'une identité suffisamment stable pour accompagner son cycle de vie. Un changement de propriétaire, de localisation, d'état ou de valeur ne doit pas créer artificiellement une nouvelle identité pour le même objet.

3. Niveau d'identification

Le modèle doit supporter la pièce unique, l'exemplaire numéroté, la petite série, la collection ou le lot lorsque le métier le justifie. Les informations communes à une série doivent rester distinguées des observations propres à chaque exemplaire.

4. Créateur et contributeurs

Une pièce peut être créée par un artisan unique ou résulter de plusieurs contributions. Le modèle doit permettre d'identifier les rôles pertinents — conception, fabrication, décoration, finition ou autre contribution — sans attribuer à un acteur un travail qu'il n'a pas déclaré ou validé.

5. Atelier d'origine

L'atelier peut constituer une référence importante de provenance. La relation entre pièce, artisan et atelier doit être datée ou contextualisée lorsque l'artisan a travaillé dans plusieurs structures ou lieux.

6. Date et période de création

La création peut être associée à une date précise ou à une période lorsque le processus s'étend dans le temps. Une estimation doit être clairement distinguée d'une date documentée.

7. Matières principales

Les matières significatives peuvent être déclarées dans le passeport de la pièce. Leur nature, quantité approximative ou rôle peuvent être enregistrés selon les besoins du métier sans imposer une nomenclature industrielle exhaustive.

8. Matières secondaires et finitions

Pigments, émaux, fils, apprêts, métaux, pierres, essences, vernis ou autres éléments peuvent être documentés lorsqu'ils participent à l'identité ou à la conservation de la pièce.

9. Provenance des matières

Lorsque disponible, la matière peut être reliée à une origine, un fournisseur, un lot, une filière ou un document. Le système doit distinguer provenance déclarée, document justificatif et preuve indépendante.

10. Matières récupérées ou anciennes

Une pièce peut intégrer des matières recyclées, récupérées, anciennes ou provenant d'un autre objet. Cette histoire peut être conservée comme relation de provenance lorsque l'information est suffisamment établie.

11. Savoir-faire

Le passeport peut décrire le métier, la technique ou le savoir-faire mobilisé. Cette description documente le processus mais ne constitue pas automatiquement une certification de compétence, un label officiel ou une protection juridique du savoir-faire.

12. Étapes de création

Les principales étapes peuvent être enregistrées selon le métier : dessin, préparation, façonnage, tissage, sculpture, assemblage, cuisson, gravure, polissage, décoration, finition ou autres opérations pertinentes.

13. Variations artisanales

Les variations entre pièces d'une même série peuvent faire partie de la nature artisanale. Elles doivent pouvoir être documentées sans être systématiquement interprétées comme des défauts ou non-conformités.

14. Signature, poinçon et marque

Les signes physiques portés par la pièce peuvent être enregistrés sous forme descriptive ou visuelle et reliés à leur auteur ou atelier déclaré. Ils constituent des éléments de provenance parmi d'autres.

15. Documentation photographique

Des photographies datées peuvent documenter la pièce achevée, des détails distinctifs, la signature, les matières ou certaines étapes de création. Elles renforcent la continuité documentaire mais ne remplacent pas toutes les autres formes de preuve.

16. Généalogie artisanale

La généalogie relie la pièce à ses créateurs, matières, composants significatifs, documents et étapes. Elle doit rester proportionnée : l'objectif est de reconstruire l'histoire pertinente de la pièce, non d' imposer une modélisation industrielle à chaque geste.

17. Modification ultérieure

Toute transformation significative après création — modification, ajout, remplacement, restauration ou personnalisation — doit pouvoir être distinguée de l'état initial et attribuée à son intervenant lorsque possible.

18. Confidentialité du savoir-faire

Certaines informations de fabrication peuvent constituer le cœur du secret de l'artisan. Le système doit permettre de prouver l'existence ou l'antériorité de certaines informations sans nécessairement révéler recettes, patrons, procédés ou détails techniques.

19. Critères d'acceptation

Le modèle est acceptable si une pièce peut être reliée à son créateur, son atelier, sa période de création, ses matières et ses principales étapes selon les preuves disponibles, tout en distinguant clairement déclarations, documents, observations et informations confidentielles.

20. Conclusion

L'identité et la généalogie artisanales forment le cœur du passeport de la pièce. Elles donnent une continuité numérique à l'auteur, aux matières, au geste et à la provenance tout en respectant la diversité des métiers, les variations naturelles et la protection du savoir-faire.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 2 — ARTISANAT

CHAPITRE 3 — CERTIFICAT D'AUTHENTICITÉ, SIGNATURE, PREUVES, PROPRIÉTÉ INTELLECTUELLE ET PROTECTION CONTRE LA COPIE

1. Objet du chapitre

Ce chapitre définit les mécanismes permettant de relier une pièce artisanale à son créateur, à ses signes distinctifs et aux preuves qui accompagnent son origine. Il organise également l'articulation avec la propriété intellectuelle et les signaux de copie ou d'usurpation, sans transformer la plateforme en autorité judiciaire ou administrative.

2. Déclaration d'authenticité

L'artisan ou l'acteur habilité peut déclarer qu'une pièce est issue de son atelier ou de son processus de création. Cette déclaration doit être datée, attribuable et rattachée à l'identité exacte de la pièce.

3. Certificat d'authenticité

Un certificat d'authenticité peut regrouper l'identité de la pièce, son créateur, sa date ou période de création, ses caractéristiques essentielles et les références de preuve pertinentes. Le certificat doit disposer de sa propre identité et de son état.

4. Émetteur du certificat

L'émetteur doit être identifiable : artisan, atelier, organisme ou autre acteur autorisé. Authenticity Plus© peut garantir la corrélation et l'intégrité du certificat sans se substituer à l'émetteur quant au contenu de son affirmation.

5. Version et révocation

Un certificat corrigé ou remplacé doit conserver la relation avec sa version antérieure. Une révocation doit être visible et motivée selon le processus applicable ; un certificat révoqué ne doit pas disparaître silencieusement de l'historique.

6. Signature de l'artisan

La signature manuscrite, numérique, le poinçon, l'estampille ou la marque d'atelier peuvent être documentés comme signes distinctifs. Leur valeur probante dépend du contexte et des autres éléments de preuve.

7. Liaison physique-numérique

QR code, NFC, puce, étiquette, gravure ou autre support peuvent relier l'objet physique à son passeport numérique. Le support doit être considéré comme un mécanisme de liaison et non comme l' authenticité elle-même.

8. Altération du support

Un support détérioré, remplacé ou détaché doit pouvoir être signalé. La continuité du passeport peut être rétablie selon un parcours contrôlé, avec conservation de l'intervention et des éléments ayant permis la nouvelle liaison.

9. Preuves photographiques

Des images de la pièce, de détails distinctifs, de la signature ou d'étapes de création peuvent compléter le dossier. Leur date, source et contexte doivent être conservés lorsqu'elles contribuent à l' authentification.

10. Preuves documentaires

Factures d'atelier, fiches de création, dessins, attestations, certificats de matière ou autres documents peuvent être référencés. Leur intégrité documentaire doit rester distincte de la vérité matérielle de toutes les affirmations qu'ils contiennent.

11. AP Ledger et antériorité

Lorsque l'architecture globale le prévoit, des empreintes de documents, dessins, photographies ou déclarations peuvent être ancrées dans AP Ledger. Cet ancrage peut renforcer la preuve d'existence et de chronologie sans créer automatiquement un droit de propriété intellectuelle.

12. Propriété intellectuelle

Les droits d'auteur, dessins et modèles, marques, indications géographiques ou autres droits peuvent concerner une création artisanale selon le contexte juridique applicable. L'application Artisanat doit pouvoir référencer ces droits sans prétendre les créer lorsqu'une procédure externe est nécessaire.

13. Auteur et propriétaire de l'objet

Le créateur d'une œuvre et le propriétaire de l'objet physique peuvent être des personnes différentes. Un transfert de propriété matérielle ne doit pas être interprété automatiquement comme un transfert des droits de propriété intellectuelle.

14. Licences d'exploitation

Lorsqu'un artisan autorise la reproduction, l'utilisation d'un motif ou une autre exploitation, cette autorisation peut être reliée au domaine Licences et Royalties. La licence reste distincte de la propriété de la pièce physique.

15. Copie et imitation

La découverte d’une pièce similaire, d’un motif reproduit ou d’une signature imitée peut produire un signal d’investigation. La ressemblance ne doit pas être qualifiée automatiquement de contrefaçon sans analyse et autorité compétentes.

16. Usurpation d’identité

L’utilisation non autorisée de l’identité d’un artisan, de son atelier, d’un certificat ou d’un identifiant AP doit pouvoir être signalée et investiguée. Les éléments suspects doivent être conservés comme preuves potentielles sans altérer le dossier authentique.

17. Détection d’anomalies

Duplications d’identifiants, certificats incohérents, chronologies impossibles, supports réutilisés ou signatures incompatibles peuvent déclencher des alertes. Les règles doivent être explicables et leurs résultats présentés comme signaux.

18. Vérification lors d’une revente

Lors d’une transaction de seconde main, le passeport peut permettre de vérifier l’identité de la pièce, le statut du certificat, les interventions connues et la continuité de provenance. Cette vérification ne constitue pas une estimation de valeur.

19. Critères d’acceptation

Le modèle est acceptable si certificat, émetteur, pièce et preuves restent corrélables ; si les versions et révocations sont visibles ; si la propriété intellectuelle reste distincte de la propriété physique ; et si les signaux de copie ou d’usurpation ne sont pas présentés comme des verdicts automatiques.

20. Conclusion

Certificats, signatures, supports de liaison, preuves et références de propriété intellectuelle renforcent l’identité de la pièce artisanale. Leur combinaison permet une authentification plus robuste tout en conservant une distinction stricte entre preuve d’intégrité, déclaration d’origine, droit juridique et décision sur une éventuelle contrefaçon.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 2 — ARTISANAT

CHAPITRE 4 — VENTE, PROPRIÉTÉ, TRANSMISSION, RESTAURATION, SECONDE MAIN ET CONTINUITÉ DE PROVENANCE

1. Objet du chapitre

Ce chapitre prolonge le passeport artisanal après la création de la pièce. Il organise les événements de vente, transmission, propriété, restauration et seconde main afin que l'histoire de l'objet puisse rester continue sans confondre transaction économique, possession physique, titularité et authenticité.

2. Première mise en circulation

La première remise ou commercialisation d'une pièce constitue une étape importante de son histoire. Elle peut relier l'objet à l'artisan, au vendeur, à l'acquéreur autorisé et aux références de transaction sans exposer inutilement des données personnelles.

3. Première vente

Une première vente peut être corrélée aux domaines Producteur ou Revendeur, AP Finance et AP Pay selon le parcours économique. Le succès du paiement ne doit pas être interprété automatiquement comme un transfert de propriété tant que le parcours de Propriété ne l'a pas établi.

4. Certificat lors de la vente

Le certificat d'authenticité et le passeport numérique peuvent accompagner la pièce lors de sa première transmission. Leur remise au nouvel acquéreur ne doit pas permettre à celui-ci de modifier les déclarations historiques de l'artisan.

5. Propriété de la pièce

Le domaine Propriété gouverne l'identité du titulaire et les changements de titulaire lorsqu'ils sont représentés dans l'écosystème. L'application Artisanat exploite cette information pour maintenir la continuité de provenance.

6. Possession et garde

Une pièce peut être confiée à une galerie, un transporteur, un restaurateur, un musée ou un autre dépositaire sans changement de propriétaire. La garde physique doit donc rester distincte de la propriété.

7. Don et transmission

Une pièce peut être donnée ou transmise sans vente. Le passeport doit pouvoir conserver la continuité du changement de titulaire selon les preuves et règles applicables, sans créer artificiellement une transaction financière.

8. Succession

Lorsqu'une transmission résulte d'une succession, le changement de titulaire doit être enregistré selon le processus autorisé et les justificatifs pertinents. La plateforme ne détermine pas elle-même les droits successoraux.

9. Prêt et exposition

Un prêt temporaire à une exposition, galerie ou institution peut être enregistré comme événement de garde ou de localisation. Il ne doit pas modifier automatiquement la propriété de la pièce.

10. État de conservation

L'état d'une pièce peut être documenté à différents moments par des observations, photographies ou rapports. Chaque constat doit être daté et attribuable afin de distinguer l'état observé de l'état d' origine.

11. Restauration

Une restauration doit identifier, lorsque possible, l'intervenant, la période, la nature de l'intervention et les éléments documentaires correspondants. Elle enrichit l'histoire de la pièce et ne doit pas effacer son état antérieur.

12. Réparation et remplacement

Certaines pièces artisanales utilitaires peuvent faire l'objet de réparations ou de remplacements de composants. Les éléments remplacés et les modifications significatives doivent être documentés lorsqu'ils influencent l'identité, l'usage ou la provenance.

13. Transformation

Une modification importante par un tiers peut changer l'apparence ou la fonction de l'objet. Le passeport doit distinguer la création originale de la transformation ultérieure et identifier l'auteur de cette dernière lorsque l'information est disponible.

14. Réauthentification après intervention

Après une restauration ou modification importante, un artisan, expert ou autre acteur habilité peut produire une nouvelle observation ou attestation. Celle-ci complète le dossier sans remplacer le certificat historique d'origine.

15. Entrée en seconde main

Lorsqu'une pièce est proposée à la revente, le domaine Seconde main peut exploiter les références du passeport, le statut du certificat, la continuité de propriété et les interventions connues afin d'améliorer la confiance dans la transaction.

16. Vérification avant revente

Le vendeur ou la plateforme autorisée peut vérifier que l'identité numérique correspond à la pièce présentée, que le certificat n'est pas révoqué et que les anomalies connues sont visibles. Cette vérification ne constitue pas automatiquement une expertise de valeur.

17. Transfert au nouvel acquéreur

Après réalisation du parcours applicable, le nouveau titulaire peut recevoir l'accès correspondant au passeport sans acquérir le droit de réécrire l'historique de création. Les droits de consultation et d' ajout d'événements doivent rester gouvernés.

18. Royalties éventuelles

Une revente peut générer une rémunération au profit d'un créateur ou d'un autre bénéficiaire uniquement lorsqu'une règle juridique ou contractuelle applicable le prévoit. Le domaine Licences et Royalties gouverne cette règle, AP Finance la conséquence financière et AP Pay le paiement éventuel.

19. Critères d'acceptation

Le modèle est acceptable si la pièce conserve une histoire continue depuis l'artisan jusqu'aux propriétaires successifs, si garde, vente, paiement et propriété restent distincts, et si restaurations, transformations et reventes enrichissent l'historique sans modifier silencieusement les preuves d' origine.

20. Conclusion

La continuité de provenance donne au passeport artisanal sa valeur dans le temps. Vente, transmission, conservation, restauration et seconde main prolongent l'histoire de la pièce tout en préservant l'identité du créateur, les preuves d'origine et la séparation entre objet physique, propriété, transaction et droits intellectuels.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 2 — ARTISANAT

CHAPITRE 5 — GOUVERNANCE, CONTRÔLES, FALSIFICATIONS, AUDIT ET PROTECTION DU PATRIMOINE ARTISANAL

1. Objet du chapitre

Ce chapitre définit les mécanismes de gouvernance et de contrôle nécessaires à la fiabilité du passeport artisanal. Il organise les rôles, les alertes, l'audit, la gestion des falsifications présumées et la préservation documentaire du patrimoine artisanal, sans transformer la plateforme en autorité de certification universelle.

2. Gouvernance des acteurs

Artisans, ateliers, organismes professionnels, experts, restaurateurs, revendeurs et autres acteurs doivent disposer de droits correspondant à leur rôle. La capacité d'ajouter une observation ne doit pas donner automatiquement le droit de modifier les déclarations historiques d'un autre acteur.

3. Validation de l'identité de l'artisan

Lorsque le parcours le prévoit, l'identité déclarée d'un artisan peut être vérifiée par des mécanismes adaptés. Cette vérification doit rester distincte de la reconnaissance d'un diplôme, d'un titre, d'un label ou d'une qualité professionnelle officielle.

4. Gouvernance des ateliers

La création, la fermeture, le changement de responsable ou la relation entre artisan et atelier doivent être historisés lorsque ces informations influencent la provenance des pièces.

5. Contrôle des certificats

Le système doit détecter les certificats révoqués, dupliqués, incohérents ou associés à une identité de pièce incompatible. Une anomalie doit déclencher un signal et non une suppression automatique de la preuve.

6. Contrôle de la liaison physique-numérique

La réutilisation d'un QR, d'une puce ou d'un autre identifiant sur plusieurs objets incompatibles doit pouvoir être détectée. La liaison doit être réévaluable lorsqu'un support est remplacé ou endommagé.

7. Falsification présumée

Une signature imitée, un certificat modifié, un identifiant cloné ou une provenance contradictoire peut être signalé comme suspicion. La qualification définitive relève des acteurs ouautorités compétents.

8. Dossier d'investigation

Une investigation peut regrouper les pièces concernées, observations, photographies, certificats, événements de propriété et autres références autorisées. Les éléments doivent conserver leur source et leur chronologie.

9. Contradictions de provenance

Lorsque deux déclarations ou documents se contredisent, le système doit préserver les deux versions et leur provenance plutôt que choisir silencieusement celle qu'il considère correcte.

10. Expertise

Un expert autorisé peut produire une observation, un rapport ou un avis sur une pièce. L'expertise doit rester attribuable à son auteur et ne doit pas écraser les déclarations antérieures.

11. Contestation

Un artisan, propriétaire ou autre partie autorisée peut contester une information selon le processus prévu. L'ouverture d'une contestation doit être visible et toute décision ultérieure doit rester traçable.

12. Audit du passeport

Les créations et modifications de certificats, changements de propriété, interventions de restauration, remplacements de supports, accès privilégiés et décisions d'investigation doivent être auditables.

13. AP Ledger

Lorsque l'architecture globale le prévoit, les empreintes de certificats, photographies, déclarations ou autres preuves sélectionnées peuvent être ancrées dans AP Ledger afin de renforcer leur intégrité et leur antériorité.

14. Protection des données

Les coordonnées privées des artisans et propriétaires, prix confidentiels, documents contractuels et autres informations sensibles ne doivent pas être rendus publics par défaut. La visibilité doit être gouvernée par finalité et rôle.

15. Patrimoine artisanal

Le passeport peut contribuer à documenter des techniques, traditions, écoles, ateliers et histoires de création. Cette documentation doit respecter les droits des communautés, artisans et détenteurs légitimes des connaissances.

16. Savoir-faire collectif

Certains savoir-faire sont portés par une communauté ou un territoire plutôt que par un auteur individuel. La plateforme doit permettre cette représentation sans attribuer abusivement une tradition collective à une seule personne.

17. Indications et labels

Une indication géographique, un label, une appellation ou une certification peut être référencée lorsque son usage est justifié. Authenticity Plus© ne doit pas attribuer elle-même un statut officiel qui dépend d'une autorité externe.

18. Transmission du savoir-faire

Apprentissage, transmission intergénérationnelle ou relation maître-apprenti peuvent être documentés lorsque les acteurs le souhaitent et que les droits le permettent. Ces relations contribuent à l'histoire du métier sans constituer automatiquement une certification de compétence.

19. Critères d'acceptation

Le modèle est acceptable si les rôles et modifications sensibles sont contrôlés, si les contradictions restent visibles, si les suspicions de falsification sont investigables sans verdict automatique, et si la documentation patrimoniale respecte confidentialité, attribution et droits collectifs.

20. Conclusion

La gouvernance protège simultanément la confiance dans les pièces et la richesse du patrimoine artisanal. Contrôles, audit, investigations, confidentialité et reconnaissance des savoir-faire collectifs permettent de documenter l'authenticité sans effacer la complexité humaine, culturelle et juridique de l'artisanat.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 2 — ARTISANAT

CHAPITRE 6 — SYNTHÈSE FONCTIONNELLE, CRITÈRES D'ACCEPTATION ET CLÔTURE DE L'APPLICATION ARTISANAT

1. Objet du chapitre

Ce chapitre clôt le Point 2 — Artisanat. Il consolide l'identité de la pièce, l'artisan et l'atelier, les matières, la provenance, le savoir-faire, les certificats, la propriété intellectuelle, les transmissions, la restauration, la seconde main, les contrôles et la préservation du patrimoine artisanal.

2. Mission consolidée

L'application Artisanat construit un passeport de confiance autour de la pièce artisanale. Elle doit permettre de relier l'objet à son créateur, son contexte de création et son histoire sans réduire la valeur artisanale à une simple chaîne industrielle de production.

3. Identité de la pièce

Pièce unique, exemplaire numéroté, petite série, collection ou lot peuvent être représentés selon la réalité du métier. L'identité numérique doit rester stable pendant le cycle de vie de l'objet.

4. Artisan, atelier et contributeurs

Créateur, atelier et contributeurs doivent pouvoir être distingués et attribués à leurs rôles réels. La plateforme ne doit ni inventer une contribution ni transformer une identité vérifiée en reconnaissance professionnelle officielle.

5. Matières et provenance

Les matières principales, secondaires, anciennes, recyclées ou récupérées peuvent enrichir le passeport. Les déclarations de provenance doivent rester distinguées des documents justificatifs et des preuves indépendantes.

6. Savoir-faire et création

Techniques, gestes et étapes de création peuvent être documentés de manière proportionnée au métier. Les variations naturelles d'une fabrication artisanale ne doivent pas être automatiquement interprétées comme des défauts.

7. Protection du secret artisanal

Le système doit permettre de documenter l'existence, la chronologie ou l'utilisation d'un savoir-faire sans exiger la publication des recettes, patrons, procédés ou autres informations confidentielles.

8. Certificat et signature

Le certificat d'authenticité, la signature, le poinçon ou la marque d'atelier doivent rester corrélés à leur émetteur et à la pièce concernée. Versions, corrections et révocations doivent être historiquement visibles.

9. Liaison physique-numérique

QR, NFC, puce, gravure ou autre support peut relier l'objet au passeport. Le support est un mécanisme de liaison et non une preuve suffisante d'authenticité à lui seul.

10. Propriété intellectuelle

Auteur, propriétaire de l'objet physique et titulaire de droits intellectuels peuvent être différents. La vente de la pièce ne doit pas transférer implicitement les droits de reproduction ou d'exploitation.

11. Licences et royalties

Les autorisations d'exploitation et rémunérations éventuelles sont gouvernées par Licences et Royalties. L'application Artisanat fournit le contexte sectoriel et les références nécessaires sans redéfinir le contrat.

12. Propriété et transmission

Vente, don, succession, prêt, dépôt et garde doivent être distingués. Le domaine Propriété gouverne les changements de titulaire ; AP Finance et AP Pay gouvernent les conséquences financières et paiements correspondants.

13. Restauration et transformation

Réparation, restauration, modification ou transformation doivent enrichir le passeport sans effacer l' état historique. L'intervenant, la période et la nature de l'intervention doivent être conservés lorsque disponibles.

14. Seconde main

Le passeport doit pouvoir accompagner la revente afin de vérifier identité, certificat, provenance, interventions et continuité de propriété. Cette vérification ne constitue ni une expertise automatique ni une estimation de valeur.

15. Falsification et anomalies

Identifiants clonés, certificats incohérents, signatures suspectes ou contradictions de provenance doivent produire des signaux investigables. La plateforme ne doit pas transformer automatiquement ces signaux en qualification juridique de contrefaçon.

16. Patrimoine artisanal

Le modèle doit pouvoir documenter ateliers, traditions, techniques et transmissions intergénérationnelles. Les savoir-faire collectifs doivent être représentés sans appropriation abusive par un acteur individuel.

17. Critère d’acceptation — authenticité

Une pièce doit pouvoir être reliée à son identité, son créateur, son certificat et ses principales preuves. La plateforme doit indiquer clairement la source et la nature des affirmations qui soutiennent son dossier.

18. Critère d’acceptation — continuité

Les transmissions, changements de propriété, restaurations et reventes doivent préserver la continuité historique. Aucun nouvel acteur ne doit pouvoir réécrire silencieusement les déclarations de création antérieures.

19. Critère d’acceptation — gouvernance

Les droits d’accès, informations confidentielles, contestations, expertises, changements sensibles et interventions privilégiées doivent être contrôlés et auditables, avec AP Ledger lorsque l’architecture globale le prévoit.

20. Clôture du Point 2 — Artisanat

Le Point 2 — Artisanat est désormais fonctionnellement défini : identité de la pièce, artisan, atelier, matières, savoir-faire, certificat, preuves, propriété intellectuelle, propriété physique, restauration, seconde main, gouvernance et patrimoine. Cette architecture est prête à s’articuler avec les autres applications sectorielles du Volume IV.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 3 — AGRICULTURE

CHAPITRE 1 — MISSION, PÉRIMÈTRE ET PRINCIPES FONDATEURS DE L'APPLICATION AGRICULTURE

1. Objet du chapitre

Le Point 3 — Agriculture transpose Authenticity Plus© / Deep Authenticity© aux productions végétales et à leur chaîne de traçabilité. Il vise à relier exploitation, parcelle, campagne, culture, opérations, récolte et lots agricoles jusqu'aux étapes de stockage, conditionnement, transformation et distribution.

2. Mission sectorielle

L'application Agriculture doit établir une continuité de confiance depuis l'origine agricole jusqu'au produit commercialisé. Elle documente les événements, acteurs et preuves disponibles sans se substituer aux autorités, organismes certificateurs, laboratoires ou systèmes réglementaires compétents.

3. Exploitant agricole

L'exploitant constitue un acteur central du parcours. Son identité et son rôle peuvent être reliés aux exploitations, parcelles, campagnes et déclarations dont il est responsable, selon les droits et mécanismes de vérification applicables.

4. Exploitation

Une exploitation peut regrouper plusieurs parcelles, cultures, installations et sites de stockage. Son identité doit rester distincte de celle de l'exploitant afin de préserver l'historique lors d'un changement d'organisation ou de responsable.

5. Parcelle

La parcelle constitue une unité essentielle de provenance. Elle peut être identifiée par une référence, une délimitation ou une autre information autorisée, avec conservation des changements pertinents sans supposer une précision géographique supérieure aux données disponibles.

6. Campagne agricole

Une campagne relie une période de production à une parcelle, une culture et un ensemble d' opérations. Les campagnes successives doivent rester distinctes afin d'éviter qu'une information d' une année soit appliquée automatiquement à une récolte ultérieure.

7. Culture

Le modèle doit identifier l'espèce, la variété ou le type de culture au niveau pertinent. Les informations variétales déclarées doivent conserver leur source et ne pas être présentées comme vérifiées indépendamment lorsqu'aucune preuve correspondante n'existe.

8. Semences et plants

Les semences, plants ou matériels de propagation peuvent être reliés à leur fournisseur, lot, variété, certificat ou autre référence lorsque ces données sont disponibles. Leur utilisation doit pouvoir être corrélée à la campagne concernée.

9. Intrants

Fertilisants, amendements, produits de protection des cultures, eau d'irrigation ou autres intrants pertinents peuvent être enregistrés selon le contexte. La plateforme conserve l'événement et sa source sans décider elle-même de la conformité réglementaire de l'usage.

10. Opérations culturales

Préparation du sol, semis, plantation, irrigation, fertilisation, traitement, taille, désherbage ou autres interventions peuvent enrichir la chronologie de la campagne. Chaque opération doit rester attribuable à son auteur ou système source.

11. Observations et mesures

Des observations de terrain, données météorologiques, mesures de sol, capteurs ou analyses peuvent être associées à la parcelle ou à la culture. Leur provenance, période et couverture doivent être conservées afin de distinguer mesure directe, estimation et donnée externe.

12. Récolte

La récolte constitue le passage de la culture au produit agricole. Elle doit pouvoir être reliée à la parcelle, à la campagne, à la date ou période de récolte, ainsi qu'aux quantités et références pertinentes.

13. Lot agricole

Les produits récoltés peuvent être regroupés en lots. Chaque lot doit conserver sa relation avec la ou les récoltes dont il provient ; les fusions et fractionnements ultérieurs doivent préserver cette généalogie.

14. Stockage

Un lot peut être déplacé vers un silo, entrepôt, chambre froide ou autre installation. Les mouvements et conditions de conservation peuvent être enregistrés lorsque leur suivi contribue à la qualité, à la sécurité ou à la provenance.

15. Conditionnement

Tri, nettoyage, calibrage, emballage ou conditionnement peuvent créer de nouveaux lots ou unités commerciales. Les relations de provenance doivent permettre de remonter vers les lots agricoles sources.

16. Transformation

Lorsqu'un produit agricole est transformé, la relation entre intrants agricoles et produit obtenu doit être conservée au niveau de granularité disponible. La transformation peut relever d'autres applications sectorielles tout en maintenant la chaîne de provenance.

17. Certifications, labels et analyses

Certifications biologiques, indications géographiques, labels, résultats de laboratoire ou autres attestations peuvent être référencés avec leur émetteur, portée et période. Authenticity Plus© renforce leur intégrité et leur rattachement sans attribuer lui-même le statut officiel.

18. Traçabilité bidirectionnelle

Le modèle doit permettre, selon les données disponibles, de remonter d'un produit ou lot commercialisé vers sa récolte, sa campagne et sa parcelle, et inversement de rechercher les lots et produits issus d'une parcelle ou d'une récolte déterminée.

19. Interfaces avec l'écosystème AP

Agriculture peut interagir avec Producteur, Revendeur, Propriété, AP Business, AP Finance, AP Pay, Transport, Licences et Royalties et les couches de preuve de l'écosystème. Chaque domaine conserve ses responsabilités propres.

20. Conclusion

L'application Agriculture établit le socle d'un passeport agricole fondé sur l'exploitation, la parcelle, la campagne, les intrants, les opérations culturales, la récolte et les lots. Cette continuité prépare les contrôles de provenance, de qualité, de stockage, de transformation et de distribution des chapitres suivants.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 3 — AGRICULTURE

CHAPITRE 2 — PARCELLES, CAMPAGNES, SEMENCES, INTRANTS ET OPÉRATIONS CULTURALES

1. Objet du chapitre

Ce chapitre détaille la phase amont de la production agricole. Il structure l'identité des parcelles, les campagnes, les cultures, les semences et plants, les intrants et les opérations culturales afin de construire une chronologie exploitable avant la récolte.

2. Identité de la parcelle

Chaque parcelle suivie doit disposer d'une référence stable dans le contexte de l'exploitation. Son identité peut être reliée à une géométrie, une référence cadastrale ou une autre description autorisée, sans confondre identité fonctionnelle et titre juridique foncier.

3. Évolution du parcellaire

Fusion, division, changement de référence ou réorganisation d'une parcelle doivent préserver les relations historiques. Une nouvelle configuration ne doit pas effacer les campagnes antérieures rattachées à l'ancien découpage.

4. Campagne

La campagne agricole constitue le conteneur temporel des opérations réalisées pour une culture ou une production donnée. Elle doit identifier sa période, sa parcelle, sa culture et son statut.

5. Rotation des cultures

Les cultures successives sur une même parcelle peuvent être conservées afin de reconstruire l' historique agronomique. La plateforme documente cette succession sans produire elle-même une recommandation agronomique.

6. Culture et variété

Espèce, variété, cultivar ou autre niveau pertinent peuvent être enregistrés selon le contexte. Les changements ou mélanges doivent être explicités lorsque leur connaissance influence la traçabilité du produit récolté.

7. Semences et plants

L’utilisation d’un lot de semences ou de plants doit pouvoir être reliée à la campagne concernée. Fournisseur, référence, lot, quantité et documents associés peuvent être conservés lorsque disponibles.

8. Origine et statut des semences

Les informations relatives à l’origine, au traitement, à la certification ou au statut d’un lot de semences doivent conserver leur émetteur et leur preuve. Authenticity Plus© ne doit pas attribuer un statut officiel absent des documents compétents.

9. Préparation du sol

Labour, travail superficiel, amendement, préparation de planches ou autres opérations peuvent être enregistrés avec leur date, leur parcelle et leur auteur ou source technique.

10. Semis et plantation

Le semis ou la plantation constitue un événement structurant reliant la culture à la parcelle et aux semences ou plants utilisés. Les densités, quantités ou modalités peuvent être enregistrées lorsqu’ elles sont pertinentes.

11. Fertilisation

Les apports de fertilisants ou amendements peuvent préciser produit, quantité, date, zone et opérateur. Le système conserve la donnée déclarée et ses références sans conclure automatiquement à sa conformité agronomique ou réglementaire.

12. Irrigation

Les événements d’irrigation peuvent documenter source d’eau, période, volume ou méthode lorsque ces données sont disponibles. Les analyses de l’eau peuvent être rattachées séparément avec leur laboratoire et leur date.

13. Protection des cultures

Les traitements ou autres mesures de protection peuvent être enregistrés avec le produit, la dose, la date, la cible et l’acteur concernés selon les droits applicables. Les autorisations réglementaires restent déterminées par les systèmes et autorités compétents.

14. Désherbage et interventions mécaniques

Les opérations mécaniques, manuelles ou autres interventions culturales peuvent enrichir la chronologie. Le modèle doit rester suffisamment ouvert pour représenter des pratiques conventionnelles, biologiques ou spécifiques à un territoire.

15. Observations de terrain

État végétatif, présence de ravageurs, symptômes, stress hydrique ou autres observations peuvent être enregistrés. Une observation humaine doit rester distinguée d'une mesure instrumentale ou d'une analyse de laboratoire.

16. Capteurs et données externes

Stations météo, sondes, imagerie, données satellitaires ou autres sources peuvent être corrélées à la parcelle. Le système doit conserver la provenance, la résolution et la période afin d'éviter une interprétation excessive de données indirectes.

17. Incidents de campagne

Gel, grêle, sécheresse, inondation, contamination suspectée ou autre incident peut être documenté avec son périmètre et ses conséquences connues. L'événement doit rester distinct d'une estimation automatique de perte ou de conformité.

18. Corrections et traçabilité

Une erreur de saisie ou une information reçue tardivement peut être corrigée selon un mécanisme gouverné. La correction doit préserver la valeur antérieure ou une piste d'audit suffisante lorsque l' information est critique.

19. Critères d'acceptation

Le modèle est acceptable si chaque campagne peut être reliée à sa parcelle, sa culture, ses semences ou plants et ses principales opérations ; si les sources des intrants et observations sont identifiables ; et si les évolutions du parcellaire ne rompent pas l'historique.

20. Conclusion

Parcelles, campagnes, semences, intrants et opérations culturales forment la généalogie amont du produit agricole. Leur chronologie prépare la traçabilité de la récolte et permet d'expliquer l'origine d' un lot sans confondre enregistrement, conseil agronomique, certification et contrôle réglementaire.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 3 — AGRICULTURE

CHAPITRE 3 — RÉCOLTES, LOTS AGRICOLES, ANALYSES, STOCKAGE, CONDITIONNEMENT ET GÉNÉALOGIE POST-RÉCOLTE

1. Objet du chapitre

Ce chapitre organise le passage de la production sur parcelle au produit agricole traçable après récolte. Il structure les événements de récolte, la constitution des lots, les analyses, les mouvements de stockage, les opérations de tri et de conditionnement ainsi que la généalogie permettant de suivre les fusions, fractionnements et transformations.

2. Événement de récolte

Chaque récolte doit pouvoir être reliée à la campagne et à la parcelle concernées. La date ou période, la culture, la quantité et les références opérationnelles pertinentes peuvent être conservées selon le niveau de traçabilité disponible.

3. Récoltes successives

Une même parcelle peut produire plusieurs passages ou cueillettes au cours d'une campagne. Chaque récolte doit pouvoir être distinguée afin de ne pas attribuer automatiquement les mêmes caractéristiques à l'ensemble de la production.

4. Constitution du lot agricole

Après récolte, les produits peuvent être regroupés dans un lot disposant de sa propre identité. Le lot doit conserver la relation avec les récoltes sources et les parcelles correspondantes.

5. Fusion de lots

Plusieurs lots peuvent être regroupés lorsque le processus l'autorise. Le nouveau lot doit conserver la liste ou la relation vers les lots sources afin que la provenance reste reconstructible.

6. Fractionnement

Un lot peut être divisé en sous-lots destinés à différents stockages, clients, traitements ou conditionnements. Chaque sous-lot doit conserver la référence de son lot parent.

7. Quantités et bilans matière

Les quantités d'entrée, de sortie, de perte et de transformation peuvent être enregistrées afin de contrôler la cohérence de la généalogie. Les écarts doivent être explicables sans exiger une égalité parfaite lorsque le processus génère des pertes normales.

8. Échantillonnage

Une analyse peut porter sur un échantillon d'un lot. Le système doit conserver la méthode ou la référence d'échantillonnage disponible et ne pas présenter une mesure d'échantillon comme une mesure individuelle de chaque unité.

9. Analyses de laboratoire

Humidité, résidus, contaminants, caractéristiques physico-chimiques ou autres résultats peuvent être rattachés au lot. Le laboratoire, la date, la méthode ou le rapport doivent être identifiables lorsque ces informations sont fournies.

10. Statut des analyses

Un résultat analytique doit rester attribué au laboratoire ou à l'acteur qui l'a produit. Authenticity Plus© peut préserver son intégrité et son rattachement sans se substituer à l'interprétation réglementaire ou scientifique compétente.

11. Réception en stockage

L'entrée dans un silo, entrepôt, chambre froide ou autre installation peut enregistrer lot, quantité, date, emplacement et état constaté. La réception physique doit rester distincte d'une acceptation commerciale ou réglementaire.

12. Conditions de stockage

Température, humidité, atmosphère, ventilation ou autres paramètres peuvent être suivis lorsqu'ils influencent la conservation. Les mesures doivent conserver leur source, leur période et leur couverture.

13. Mouvements de stock

Transferts entre emplacements, silos ou installations doivent préserver l'identité du lot ou créer les relations nécessaires lorsqu'un mélange ou fractionnement intervient.

14. Tri et calibrage

Les opérations de tri, nettoyage ou calibrage peuvent produire plusieurs catégories ou sous-lots. Les critères utilisés et les relations avec le lot d'origine doivent être conservés lorsque disponibles.

15. Conditionnement

L'emballage ou conditionnement peut créer des unités logistiques ou commerciales identifiables. Ces unités doivent pouvoir être reliées au lot agricole dont elles proviennent.

16. Étiquetage et informations de provenance

Les informations affichées sur un emballage ou un support numérique doivent être dérivées de données autorisées et cohérentes avec le passeport. Une mention commerciale ne doit pas être présentée comme certification officielle si elle ne l'est pas.

17. Transformation primaire

Séchage, mouture, pressage, décorticage ou autre transformation primaire peut créer un nouveau lot. La relation entre intrants et produits obtenus doit être conservée au niveau pertinent.

18. Traçabilité bidirectionnelle post-récolte

Le système doit permettre de remonter d'un lot conditionné vers ses lots agricoles et récoltes sources, et de descendre d'un lot de récolte vers les sous-lots, conditionnements ou produits qui en sont issus.

19. Critères d'acceptation

Le modèle est acceptable si les récoltes peuvent être reliées aux campagnes et parcelles, si les fusions et fractionnements préservent la généalogie, si les analyses restent attribuables et si les mouvements de stockage et conditionnement permettent une traçabilité bidirectionnelle.

20. Conclusion

Récolte, lots, analyses, stockage et conditionnement constituent la généalogie post-récolte. Leur continuité permet de relier le produit agricole commercialisable à son origine tout en distinguant mesures, analyses, décisions de conformité et informations commerciales.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 3 — AGRICULTURE

CHAPITRE 4 — CERTIFICATIONS, LABELS, ORIGINE GÉOGRAPHIQUE, DISTRIBUTION, ALERTES ET RAPPELS AGRICOLES

1. Objet du chapitre

Ce chapitre organise les informations qui accompagnent le produit agricole après sa constitution en lot : certifications et labels, origine géographique, documents de contrôle, distribution, alertes et rappels. Il vise à préserver la continuité entre les preuves agricoles et les informations présentées aux acteurs de la chaîne.

2. Certification

Une certification agricole ou agroalimentaire peut être référencée avec son organisme émetteur, sa portée, sa période de validité et les objets ou exploitations concernés. Authenticity Plus© ne doit pas attribuer lui-même un statut qui relève d'un organisme certificateur.

3. Labels et signes de qualité

Labels, appellations, indications géographiques ou autres signes peuvent être associés aux produits lorsqu'une preuve ou référence compétente existe. Le système doit distinguer une mention marketing d'un statut officiel.

4. Périmètre de certification

Une certification peut concerner une exploitation, une parcelle, une campagne, un produit ou un lot déterminé. Sa présence à un niveau ne doit pas être étendue automatiquement à tous les objets liés.

5. Période de validité

La date d'émission, la période de validité, la suspension ou le retrait éventuel d'un statut doivent être conservés. Une certification expirée ne doit pas être présentée comme active.

6. Origine géographique

L'origine peut être exprimée à différents niveaux : pays, région, territoire, exploitation, parcelle ou autre référence autorisée. Le niveau affiché doit correspondre aux données réellement établies.

7. Provenance et origine

La provenance logistique d'un lot et son origine agricole ne sont pas nécessairement identiques. Un lieu de stockage, de conditionnement ou d'expédition ne doit pas être présenté comme lieu de production.

8. Documents et contrôles

Rapports d'inspection, certificats, résultats de laboratoire ou autres documents peuvent être corrélés au lot. Leur intégrité et leur rattachement doivent rester distincts de l'interprétation réglementaire de leur contenu.

9. Libération du lot

Lorsqu'un processus prévoit une décision de libération, celle-ci doit être attribuée à l'acteur ou système compétent. Authenticity Plus© conserve le statut et sa preuve sans se substituer à l'autorité décisionnaire.

10. Mise en distribution

Le passage d'un lot vers un distributeur, revendeur, transformateur ou autre acteur peut être enregistré avec les références nécessaires. La distribution doit conserver la généalogie du lot et ne pas rompre la remontée vers la récolte.

11. Transport

Les expéditions agricoles peuvent être reliées au domaine Transport. Les conditions de transport pertinentes, notamment pour les produits sensibles, peuvent enrichir le dossier sans confondre responsabilité du transporteur et origine agricole.

12. Chaîne du froid

Lorsque nécessaire, températures et ruptures potentielles de chaîne du froid peuvent être documentées avec leur source et leur période. Une absence de mesure ne doit pas être interprétée comme preuve que les conditions ont été respectées.

13. Réception commerciale

La réception par un acheteur ou un distributeur peut enregistrer quantité, état et anomalies constatées. Elle reste distincte du transfert de propriété, du paiement et de la conformité réglementaire.

14. Alerte

Un résultat analytique, une anomalie de traçabilité, un signal sanitaire ou une information d'un acteur compétent peut déclencher une alerte. L'alerte doit identifier sa source et son périmètre initial.

15. Investigation

La généalogie bidirectionnelle permet de rechercher les parcelles, récoltes, lots et produits potentiellement liés à une alerte. Le périmètre d'investigation doit rester distingué du périmètre définitivement confirmé.

16. Rappel

Lorsqu'un rappel est décidé par l'acteur ou l'autorité compétente, il doit être rattaché aux critères qui déterminent les lots concernés. Notifications, retraits, retours ou destructions peuvent être suivis séparément.

17. Traçabilité descendante

À partir d'une parcelle, d'une récolte ou d'un lot source, le système doit permettre d'identifier les lots, conditionnements, destinations et produits dérivés enregistrés afin de soutenir une action ciblée.

18. Traçabilité ascendante

À partir d'un produit ou lot distribué, le système doit permettre de remonter vers les lots sources, récoltes, campagnes et parcelles lorsque les données existent, en conservant les éventuelles ruptures ou incertitudes.

19. Critères d'acceptation

Le modèle est acceptable si certifications et labels conservent leur portée et leur émetteur, si origine et provenance logistique restent distinctes, si les alertes sont investigables par la généalogie et si un rappel peut être suivi jusqu'aux destinations connues.

20. Conclusion

Certifications, origine, distribution, alertes et rappels relient la traçabilité agricole aux exigences de confiance du marché. La valeur du système repose sur la portée exacte des preuves, la continuité des lots et la capacité à agir dans les deux sens de la chaîne sans transformer une information enregistrée en certification implicite.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 3 — AGRICULTURE

CHAPITRE 5 — GOUVERNANCE, AUDIT, PREUVES, CONTRÔLES DE COHÉRENCE ET LUTTE CONTRE LES FRAUDES DE PROVENANCE

1. Objet du chapitre

Ce chapitre définit les mécanismes de gouvernance nécessaires à la confiance dans le passeport agricole. Il organise les rôles, les contrôles de cohérence, l'audit, les preuves et les signaux de fraude afin que la traçabilité puisse être vérifiée sans transformer automatiquement une anomalie en conclusion juridique.

2. Gouvernance des acteurs

Exploitants, techniciens, coopératives, collecteurs, laboratoires, organismes certificateurs, conditionneurs et distributeurs doivent disposer de droits correspondant à leurs responsabilités. Une capacité de consultation ne doit pas conférer automatiquement un droit de modification.

3. Séparation des responsabilités

La déclaration d'une opération culturale, la production d'une analyse, l'attribution d'une certification, la libération d'un lot et la décision d'un rappel peuvent relever d'acteurs différents. Le système doit préserver cette séparation.

4. Contrôle de cohérence parcelle-campagne

Une campagne doit être cohérente avec la parcelle, la période et la culture enregistrées. Les chevauchements, références incompatibles ou successions impossibles doivent pouvoir produire des alertes explicables.

5. Contrôle des semences et intrants

Les lots de semences, plants et intrants déclarés peuvent être contrôlés par rapport aux références disponibles, aux dates et aux quantités. Une incohérence doit être signalée sans être automatiquement qualifiée d'usage frauduleux.

6. Contrôle chronologique

Semis, opérations culturales, récolte, stockage, conditionnement et distribution doivent respecter une chronologie plausible selon les événements enregistrés. Une date impossible ou contradictoire doit déclencher une investigation.

7. Contrôle des quantités

Les quantités récoltées, fusionnées, fractionnées, stockées, transformées et distribuées peuvent être rapprochées. Les pertes normales, écarts de mesure et transformations doivent être pris en compte avant de qualifier un écart d'anormal.

8. Contrôle de généalogie

Tout lot dérivé doit conserver une relation vers ses lots sources. Une rupture de généalogie, un lot sans origine ou une provenance circulaire doit pouvoir être détecté et rendu visible.

9. Contrôle des certifications

Le système doit vérifier que la certification référencée correspond au bon émetteur, au bon périmètre et à la bonne période. Un certificat expiré, suspendu ou appliqué hors périmètre doit être signalé.

10. Contrôle de l'origine géographique

Les affirmations d'origine doivent être cohérentes avec les parcelles, récoltes et lots enregistrés. Un lieu de stockage ou d'expédition ne doit pas pouvoir remplacer silencieusement le lieu de production.

11. Fraude de provenance présumée

Une origine contradictoire, un lot dupliqué, une quantité incompatible ou un certificat incohérent peut constituer un signal de fraude potentielle. Le système soutient l'investigation mais ne prononce pas lui-même une qualification juridique définitive.

12. Dossier d'investigation

Une investigation peut regrouper événements, lots, documents, analyses, certifications, acteurs et destinations concernés. Chaque élément doit conserver sa source, sa date et son statut.

13. Contestation et correction

Une information peut être contestée par un acteur autorisé. Toute correction doit être traçable et ne doit pas effacer silencieusement la donnée antérieure lorsqu'elle a participé à une décision ou à une preuve.

14. Journal d'audit

Créations et modifications de campagnes, lots, certifications, résultats, décisions de libération, alertes, rappels et interventions privilégiées doivent produire une piste d'audit proportionnée à leur criticité.

15. AP Ledger

Lorsque l'architecture globale le prévoit, des empreintes de certificats, analyses, documents, événements ou autres preuves sélectionnées peuvent être ancrées dans AP Ledger afin de renforcer l'intégrité et la chronologie.

16. Confidentialité

Coordonnées privées, contrats, prix, données agronomiques sensibles, fournisseurs ou résultats commerciaux ne doivent pas être exposés sans nécessité. La transparence de provenance doit rester compatible avec les droits et secrets légitimes des acteurs.

17. Données publiques et données privées

Certaines informations peuvent être destinées au consommateur ou au marché tandis que d'autres restent réservées aux professionnels, certificateurs ou autorités compétentes. Le passeport doit supporter ces niveaux de visibilité.

18. Résilience de la preuve

Une indisponibilité temporaire d'un système source ne doit pas entraîner la perte de l'historique déjà établi. Les références, preuves et synchronisations doivent permettre une reprise contrôlée et éviter les duplications.

19. Critères d'acceptation

Le modèle est acceptable si les incohérences de chronologie, quantité, généalogie, certification et origine peuvent être détectées ; si toute alerte reste explicable ; si les corrections et décisions sont auditables ; et si les informations sensibles restent protégées.

20. Conclusion

La gouvernance agricole transforme la traçabilité en dispositif vérifiable. Contrôles de cohérence, audit, AP Ledger, confidentialité et investigations permettent de renforcer la confiance dans l'origine et les lots tout en maintenant une distinction stricte entre anomalie, preuve, décision métier et qualification juridique.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 3 — AGRICULTURE

CHAPITRE 6 — SYNTHÈSE FONCTIONNELLE, CRITÈRES D'ACCEPTATION ET CLÔTURE DE L'APPLICATION AGRICULTURE

1. Objet du chapitre

Ce chapitre clôt le Point 3 — Agriculture. Il consolide la traçabilité depuis l'exploitation et la parcelle jusqu'aux lots distribués, en intégrant campagnes, semences, intrants, opérations culturales, récoltes, analyses, stockage, certifications, origine, alertes, rappels et gouvernance.

2. Mission consolidée

L'application Agriculture construit un passeport agricole capable de relier un produit à son origine et à son histoire documentée. Elle renforce la continuité de preuve sans se substituer aux exploitants, laboratoires, organismes certificateurs ou autorités compétentes.

3. Exploitation et parcelle

L'exploitation et la parcelle constituent les premiers niveaux de provenance. Leur identité et leurs évolutions doivent rester historiquement reconstructibles sans confondre référence fonctionnelle, localisation et titre juridique foncier.

4. Campagne et culture

Chaque campagne doit être reliée à une période, une parcelle et une culture. Les rotations et campagnes successives doivent rester distinctes afin qu'une information d'une période ne soit pas appliquée automatiquement à une autre.

5. Semences, plants et intrants

Les semences, plants, fertilisants, amendements, traitements et autres intrants pertinents peuvent être rattachés à leurs lots, fournisseurs et documents disponibles. Leur enregistrement ne constitue pas une validation réglementaire automatique.

6. Opérations culturales

Semis, plantation, irrigation, fertilisation, protection, interventions mécaniques et observations forment la chronologie de la campagne. Chaque événement doit rester attribuable à son acteur ou système source.

7. Récolte

La récolte relie la production sur parcelle au produit agricole. Les récoltes successives doivent pouvoir être distinguées et conserver leur relation avec la campagne, la culture et la période correspondantes.

8. Lots et généalogie

Les lots agricoles doivent préserver les relations avec les récoltes sources. Fusion, fractionnement, tri, calibrage, conditionnement et transformation primaire doivent maintenir une généalogie bidirectionnelle.

9. Analyses

Les résultats de laboratoire doivent conserver leur émetteur, date, méthode ou rapport lorsque disponibles. Une mesure sur échantillon ne doit pas être présentée comme une mesure individuelle de chaque unité du lot.

10. Stockage et conservation

Les mouvements de stockage et les conditions pertinentes peuvent enrichir le passeport. La source, la période et la couverture des mesures doivent être explicites, notamment pour la température, l’ humidité ou la chaîne du froid.

11. Certifications et labels

Certifications, labels, indications géographiques et autres signes doivent conserver leur émetteur, leur portée, leur période de validité et leur statut. Authenticity Plus© ne crée pas un statut officiel qui dépend d’un organisme externe.

12. Origine et provenance

L’origine agricole doit rester distinguée de la provenance logistique. Une parcelle ou exploitation de production ne doit pas être remplacée par un lieu de stockage, de conditionnement ou d’expédition dans la présentation de l’origine.

13. Distribution et Transport

Les lots distribués doivent conserver leur généalogie vers les récoltes sources. Les expéditions peuvent s’articuler avec le domaine Transport, sans fusionner responsabilité logistique, propriété, paiement et origine agricole.

14. Alertes et rappels

Une alerte doit conserver sa source et son périmètre initial. La généalogie ascendante et descendante doit permettre d’identifier les objets potentiellement concernés et de suivre un rappel jusqu’aux destinations connues.

15. Fraudes et anomalies

Chronologies impossibles, quantités incohérentes, certifications hors périmètre, lots dupliqués ou origines contradictoires peuvent produire des signaux. Ces signaux soutiennent l'investigation sans constituer automatiquement une qualification juridique de fraude.

16. Audit et AP Ledger

Les changements sensibles, corrections, certifications, analyses, alertes, rappels et décisions critiques doivent être auditables. Lorsque l'architecture globale le prévoit, AP Ledger peut renforcer l'intégrité et l'antériorité de preuves sélectionnées.

17. Critère d'acceptation — traçabilité amont

Pour une récolte donnée, le système doit pouvoir identifier la campagne, la parcelle, la culture et, selon les données disponibles, les semences, intrants et principales opérations qui la précèdent.

18. Critère d'acceptation — traçabilité aval

Pour un lot distribué, le système doit pouvoir remonter vers ses lots et récoltes sources ; inversement, une récolte doit pouvoir être suivie vers les lots, conditionnements, transformations et destinations enregistrés.

19. Critère d'acceptation — gouvernance

Les rôles doivent suivre le moindre privilège, les preuves doivent rester attribuables, les corrections doivent préserver l'historique et les informations sensibles doivent être exposées uniquement selon les finalités et droits applicables.

20. Clôture du Point 3 — Agriculture

Le Point 3 — Agriculture est désormais fonctionnellement défini : exploitation, parcelles, campagnes, cultures, intrants, opérations, récoltes, lots, analyses, stockage, certifications, origine, distribution, alertes, rappels, audit et lutte contre les anomalies de provenance. Cette architecture est prête à s'articuler avec le Point 4 — Élevage et les autres applications du Volume IV.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 4 — ÉLEVAGE

CHAPITRE 1 — MISSION, PÉRIMÈTRE ET PRINCIPES FONDATEURS DE L'APPLICATION ÉLEVAGE

1. Objet du chapitre

Le Point 4 — Élevage transpose Authenticity Plus© / Deep Authenticity© aux filières animales. Il vise à relier exploitation, éleveur, animal ou groupe d'animaux, origine, généalogie, alimentation, mouvements, événements d'élevage, documents sanitaires et productions issues de l'élevage.

2. Mission sectorielle

L'application Élevage construit une continuité de confiance autour de l'animal, du troupeau et des productions associées. Elle documente identité, provenance, chronologie et preuves disponibles sans se substituer aux vétérinaires, autorités sanitaires, organismes certificateurs ou systèmes officiels d' identification.

3. Éleveur

L'éleveur constitue un acteur central du parcours. Son identité et son rôle peuvent être reliés aux exploitations, animaux, troupeaux, déclarations et événements dont il est responsable, selon les droits et mécanismes de vérification applicables.

4. Exploitation d'élevage

Une exploitation peut regrouper plusieurs sites, bâtiments, troupeaux, espèces ou unités de production. Son identité doit rester distincte de celle de l'éleveur afin de préserver la continuité lors d' un changement de responsable ou d'organisation.

5. Granularité d'identification

Le modèle doit supporter l'identification individuelle lorsqu'elle existe, mais aussi les niveaux troupeau, lot, bande ou autre groupe pertinent. La granularité de la preuve commande la granularité de la traçabilité.

6. Animal individuel

Lorsqu'un animal est suivi individuellement, son passeport peut être corrélé à l'identifiant officiel ou professionnel disponible, à son espèce, sa date ou période de naissance, son exploitation d'origine et aux événements ultérieurs.

7. Troupeau, lot ou bande

Lorsque la filière fonctionne principalement au niveau collectif, le groupe doit disposer d'une identité propre et d'une période de composition. Une information enregistrée au niveau du groupe ne doit pas être transformée artificiellement en preuve individuelle.

8. Naissance et entrée

La naissance sur l'exploitation ou l'entrée d'un animal provenant d'un autre acteur constitue un événement structurant. Date, origine, identifiant et documents associés peuvent être conservés selon les données disponibles.

9. Origine et généalogie

Lorsque la filière et les données le permettent, le passeport peut relier l'animal à ses ascendants, son élevage d'origine ou son groupe source. Les informations déclarées et les filiations établies par des systèmes compétents doivent rester distinguées.

10. Espèce, race et caractéristiques

Espèce, race, lignée ou autres caractéristiques pertinentes peuvent être enregistrées avec leur source. Authenticity Plus© ne doit pas transformer une caractéristique déclarée en certification zootechnique officielle sans preuve compétente.

11. Alimentation

Les aliments, fourrages, compléments ou lots d'alimentation peuvent être reliés à l'exploitation, au troupeau ou aux animaux concernés selon la granularité disponible. Fournisseur, lot, période et documents peuvent être conservés lorsque pertinents.

12. Événements d'élevage

Pesées, changements de groupe, reproduction, mise bas, collecte de production ou autres événements non médicaux peuvent enrichir la chronologie. Chaque événement doit rester attribuable à son acteur ou système source.

13. Suivi sanitaire documentaire

Les observations, interventions, analyses, prescriptions, attestations ou autres documents vétérinaires peuvent être rattachés à l'animal ou au groupe selon les droits applicables. La plateforme conserve leur provenance sans produire elle-même de diagnostic.

14. Mouvements

Entrée, sortie, transfert entre sites, regroupement ou séparation peuvent être enregistrés avec date, origine et destination lorsque disponibles. Un mouvement physique doit rester distinct du transfert de propriété et du paiement.

15. Production issue de l'élevage

Lait, œufs, laine ou autres productions peuvent être reliés à l'exploitation, au troupeau ou à l'animal lorsque la granularité de la filière le permet. La plateforme ne doit pas inventer une origine individuelle lorsque la collecte est collective.

16. Constitution des lots de production

Les productions collectées peuvent être regroupées en lots disposant de leur propre identité. Fusion, fractionnement, stockage et conditionnement doivent préserver la relation avec les groupes ou exploitations sources.

17. Traçabilité bidirectionnelle

Le modèle doit permettre, selon les données disponibles, de remonter d'un lot de production vers l' animal, le troupeau ou l'exploitation d'origine, et inversement de rechercher les productions, lots et destinations liés à un animal ou groupe déterminé.

18. Confidentialité et droits

Données personnelles de l'éleveur, informations économiques, données d'exploitation et documents sensibles doivent être protégés selon les rôles et finalités. Les informations sanitaires doivent faire l' objet d'une gouvernance particulièrement rigoureuse.

19. Interfaces avec l'écosystème AP

Élevage peut interagir avec Agriculture pour certains aliments ou fourrages, avec Producteur, Revendeur, Propriété, AP Business, AP Finance, AP Pay, Transport et les couches de preuve de l' écosystème. Chaque domaine conserve ses responsabilités propres.

20. Conclusion

L'application Élevage établit le socle d'un passeport sectoriel fondé sur l'exploitation, l'identité individuelle ou collective, l'origine, la généalogie, l'alimentation, les mouvements, les preuves documentaires et les productions. Elle prépare les chapitres détaillés consacrés à l'identité animale, aux groupes, aux mouvements, à la traçabilité et à la gouvernance.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 4 — ÉLEVAGE

CHAPITRE 2 — IDENTITÉ ANIMALE, NAISSANCES, GÉNÉALOGIE, TROUPEAUX, LOTS ET MOUVEMENTS

1. Objet du chapitre

Ce chapitre détaille l'identité et la généalogie des animaux et groupes suivis dans l'application Élevage. Il organise la naissance ou l'entrée, les relations de filiation, la composition des troupeaux ou lots, les changements de groupe et les mouvements entre exploitations ou sites.

2. Identité persistante

Lorsqu'un animal est suivi individuellement, son identité numérique doit rester stable pendant son cycle de vie. Un changement de détenteur, d'exploitation, de localisation ou de statut ne doit pas créer artificiellement un nouvel animal.

3. Identifiant officiel ou professionnel

Le passeport peut être corrélé à une boucle, puce, numéro officiel ou autre identifiant reconnu dans la filière. Authenticity Plus© conserve cette corrélation sans se substituer au registre officiel qui émet ou gouverne l'identifiant.

4. Identité collective

Lorsqu'une traçabilité individuelle n'existe pas ou n'est pas pertinente, un troupeau, lot, bande ou groupe peut disposer de sa propre identité. La composition et la période de validité du groupe doivent être conservées lorsque les données le permettent.

5. Naissance

Une naissance peut relier l'animal à sa date ou période, son exploitation, sa mère et éventuellement son père ou d'autres références de filiation disponibles. Une filiation déclarée doit rester distincte d' une filiation établie par une preuve ou un registre compétent.

6. Entrée sans historique complet

Un animal peut entrer dans le système avec un historique partiel. Le passeport doit indiquer le point à partir duquel la continuité est établie et ne pas inventer les événements antérieurs manquants.

7. Ascendance

Les relations parentales peuvent construire une généalogie ascendante lorsque la filière le permet. La source de chaque relation doit être identifiable afin de distinguer déclaration, registre, analyse ou autre preuve.

8. Descendance

Le modèle peut également relier un animal à sa descendance enregistrée. Cette capacité soutient la traçabilité zootechnique ou de provenance sans constituer à elle seule une certification génétique.

9. Race, lignée et caractéristiques

Race, lignée ou caractéristiques pertinentes peuvent être associées à l'animal avec leur source. Les résultats issus d'un organisme, d'un registre ou d'une analyse doivent rester attribués à leur émetteur.

10. Création d'un troupeau ou lot

Un groupe peut être créé pour représenter une unité d'élevage, une bande, un lot de production ou une autre organisation pertinente. Sa finalité et sa périodedoivent être explicites.

11. Entrée dans un groupe

L'ajout d'un animal à un troupeau ou lot doit être daté lorsque la traçabilité l'exige. Les informations collectives produites après cette date ne doivent pas être appliquées rétroactivement à l'animal.

12. Sortie d'un groupe

La sortie doit clôturer la période d'appartenance sans supprimer l'historique. Un animal peut rejoindre un autre groupe tout en conservant la succession de ses appartenances.

13. Fusion et séparation de groupes

Deux groupes peuvent être réunis ou un groupe fractionné. Les nouvelles identités collectives doivent conserver les relations vers les groupes sources afin de préserver la généalogie collective.

14. Mouvement interne

Un transfert entre bâtiments, pâtures ou sites d'une même exploitation peut être enregistré lorsque pertinent. Il représente un changement de localisation ou d'unité d'élevage, pas nécessairement un changement de détenteur ou de propriétaire.

15. Mouvement externe

Un déplacement vers une autre exploitation, un marché, un centre ou une autre destination peut conserver date, origine, destination et documents associés selon les droits et obligations applicables.

16. Détention et propriété

Le détenteur opérationnel de l'animal et son propriétaire peuvent être différents. Les changements de propriété relèvent du domaine Propriété ; l'application Élevage conserve les mouvements et événements sectoriels.

17. Transport

Lorsqu'un mouvement nécessite un transport, les références correspondantes peuvent être corrélées au domaine Transport. Le déplacement de l'animal et la prestation logistique restent des événements distincts.

18. Cohérence et anomalies

Identifiants dupliqués, mouvements incompatibles, appartenances simultanées impossibles ou chronologies contradictoires doivent pouvoir produire des signaux d'investigation. Un signal ne constitue pas automatiquement une fraude.

19. Critères d'acceptation

Le modèle est acceptable si l'identité individuelle ou collective reste stable, si naissance ou entrée et filiations conservent leur source, si les changements de groupe sont reconstructibles et si les mouvements préservent la distinction entre localisation, détention, propriété et transport.

20. Conclusion

Identité animale, généalogie, groupes et mouvements constituent le socle de la traçabilité d'élevage. Leur continuité permet de suivre un animal ou une population au fil des exploitations et unités d' élevage sans dépasser la granularité réellement établie par les données.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 4 — ÉLEVAGE

CHAPITRE 3 — ALIMENTATION, ÉVÉNEMENTS D'ÉLEVAGE, SUIVI VÉTÉRINAIRE DOCUMENTAIRE, ANALYSES ET PREUVES SANITAIRES

1. Objet du chapitre

Ce chapitre structure les événements liés à l'alimentation, aux pratiques d'élevage et au suivi sanitaire documentaire. Il organise la provenance des aliments, les observations, interventions et analyses attribuées aux acteurs compétents, sans transformer Authenticity Plus© en système de diagnostic ou de prescription vétérinaire.

2. Lots d'alimentation

Les aliments, fourrages, compléments ou autres apports peuvent être identifiés par fournisseur, référence, lot et période d'utilisation lorsque ces informations sont disponibles. Leur relation avec l' exploitation, le bâtiment, le troupeau ou l'animal doit respecter la granularité réelle des données.

3. Origine des aliments

Lorsque la provenance est documentée, un lot d'alimentation peut être relié à son producteur, son fournisseur, ses matières ou ses documents. Les liens avec l'application Agriculture peuvent être utilisés pour les productions végétales suivies dans l'écosystème.

4. Distribution alimentaire

Une distribution peut enregistrer date ou période, groupe concerné, type d'aliment et quantité lorsque cela est pertinent. Une ration collective ne doit pas être convertie artificiellement en consommation individuelle.

5. Changements de ration

Les modifications significatives de programme alimentaire peuvent être historisées. L'enregistrement décrit le changement et sa période sans constituer une recommandation nutritionnelle produite par la plateforme.

6. Eau et autres apports

Lorsque nécessaire, l'origine ou les analyses de l'eau et d'autres apports peuvent être rattachées à l' exploitation ou au groupe concerné. Les résultats doivent conserver leur laboratoire, leur date et leur portée.

7. Événements d’élevage

Pesée, reproduction, mise bas, changement de groupe, collecte, tonte ou autres événements non médicaux peuvent être enregistrés selon la filière. Chaque événement doit rester attribuable à son auteur ou système source.

8. Observations sanitaires

Une observation relative à l’état d’un animal ou d’un groupe peut être enregistrée par un acteur autorisé. Elle doit être présentée comme une observation et non comme un diagnostic lorsque son auteur ou son contexte ne permet pas cette qualification.

9. Intervention vétérinaire

Une intervention réalisée par un vétérinaire ou un acteur habilité peut être rattachée au passeport avec sa date, son auteur et les documents pertinents. Authenticity Plus© conserve la preuve de l’événement sans déterminer lui-même la conduite médicale.

10. Prescriptions et documents

Les prescriptions, attestations, comptes rendus ou autres documents peuvent être référencés avec leur émetteur et leur période. Les informations sensibles doivent être accessibles uniquement aux rôles autorisés.

11. Traitements enregistrés

Lorsqu’un traitement est documenté par les systèmes ou professionnels compétents, son événement peut être conservé avec les références nécessaires. La plateforme ne doit ni recommander un médicament ni générer une prescription.

12. Analyses de laboratoire

Des analyses réalisées sur un animal, un groupe, un aliment, l’eau ou un autre prélèvement peuvent être rattachées au dossier. Échantillon, laboratoire, date, méthode ou rapport doivent être conservés lorsque disponibles.

13. Portée d’un résultat

Un résultat portant sur un échantillon ou un groupe doit rester présenté à ce niveau. Il ne doit pas être extrapolé automatiquement à chaque animal ou à une période différente.

14. Attestations sanitaires

Une attestation ou un certificat sanitaire peut être relié à l’animal, au groupe, à l’exploitation ou au mouvement concerné. Son statut officiel dépend exclusivement de l’émetteur et du cadre applicable.

15. Périodes et statuts documentaires

Date d’émission, période de validité, remplacement, suspension ou révocation d’un document doivent pouvoir être conservés lorsqu’ils existent. Un document expiré ne doit pas être présenté comme actif.

16. Preuves et AP Ledger

Lorsque l’architecture globale le prévoit, des empreintes de rapports, attestations, analyses ou autres preuves sélectionnées peuvent être ancrées dans AP Ledger afin de renforcer leur intégrité et leur chronologie.

17. Confidentialité renforcée

Les données sanitaires et vétérinaires peuvent être particulièrement sensibles. Leur visibilité doit suivre les rôles, finalités et règles applicables ; la traçabilité de l’accès aux informations critiques doit être prévue.

18. Alertes de cohérence

Des incohérences entre animal, groupe, période, document, analyse ou mouvement peuvent produire des signaux d’investigation. Ces signaux ne doivent pas être transformés automatiquement en conclusion sanitaire.

19. Critères d’acceptation

Le modèle est acceptable si les aliments et événements restent reliés au bon niveau de granularité, si les observations sont distinguées des diagnostics, si les analyses et attestations conservent leur émetteur et leur portée, et si les données sensibles sont gouvernées.

20. Conclusion

Alimentation, événements d’élevage, observations, interventions, analyses et attestations enrichissent le passeport animal ou collectif. Leur valeur repose sur la provenance, la granularité, la chronologie et une séparation stricte entre traçabilité documentaire et décision vétérinaire ou sanitaire.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 4 — ÉLEVAGE

CHAPITRE 4 — PRODUCTIONS ANIMALES, COLLECTE, LOTS, STOCKAGE, TRANSFORMATION, DISTRIBUTION ET TRAÇABILITÉ BIDIRECTIONNELLE

1. Objet du chapitre

Ce chapitre organise le passage de l'animal ou du groupe d'élevage vers les productions qui en sont issues. Il structure la collecte, la constitution des lots, les fusions et fractionnements, le stockage, la transformation et la distribution en maintenant la relation avec l'origine réellement démontrable.

2. Typologie des productions

Le modèle doit pouvoir représenter différentes productions selon la filière, notamment lait, œufs, laine ou autres productions pertinentes. Chaque filière conserve sa granularité, ses cycles et ses documents propres.

3. Origine individuelle ou collective

Une production peut être reliée à un animal individuel lorsque la collecte le permet, ou à un troupeau, lot, bâtiment ou exploitation lorsque la collecte est collective. Le système ne doit jamais inventer une attribution individuelle.

4. Événement de collecte

Chaque collecte pertinente peut enregistrer date ou période, exploitation, groupe ou animal source, quantité et opérateur ou système source. Elle constitue le premier lien entre l'élevage et le lot de production.

5. Collectes successives

Une même exploitation ou un même groupe peut produire plusieurs collectes dans le temps. Chaque collecte doit être distinguable afin de préserver les périodes, conditions et documents qui lui sont propres.

6. Constitution du lot

Plusieurs unités ou collectes peuvent être regroupées dans un lot de production. Le lot doit disposer de sa propre identité tout en conservant les relations vers les collectes et origines qui le composent.

7. Fusion de lots

Lorsque plusieurs lots sont mélangés, le lot résultant doit conserverles relations vers tous les lots sources enregistrés. La fusion réduit éventuellement la granularité de provenance mais ne doit pas effacer les origines connues.

8. Fractionnement

Un lot peut être divisé pour le stockage, le conditionnement, la transformation ou la distribution. Chaque sous-lot doit conserver sa relation avec le lot parent.

9. Bilans de quantité

Les quantités collectées, fusionnées, fractionnées, transformées et distribuées peuvent être rapprochées. Les pertes normales, variations de mesure et rendements de transformation doivent être distingués des incohérences inexpliquées.

10. Analyses du lot

Des analyses de qualité, composition ou autres contrôles peuvent être rattachés au lot avec leur laboratoire, date et portée. Un résultat d'échantillon ne doit pas être présenté comme une mesure individuelle de chaque unité.

11. Stockage

Les lots peuvent être associés à des sites, cuves, chambres, entrepôts ou autres installations de stockage. Les mouvements doivent préserver l'identité ou les relations de généalogie lorsqu'un mélange intervient.

12. Conditions de conservation

Température, durée, humidité ou autres paramètres pertinents peuvent être suivis selon la production. Les mesures doivent conserver leur source et leur période afin de distinguer suivi continu, contrôle ponctuel et absence de donnée.

13. Conditionnement

Le conditionnement peut créer des unités logistiques ou commerciales identifiables. Ces unités doivent pouvoir être reliées au lot de production source et aux informations de provenance autorisées.

14. Transformation

Lorsqu'une production est transformée, un nouveau lot ou produit peut être créé. Les relations entre intrants et produits obtenus doivent être conservées au niveau réellement disponible et peuvent s' articuler avec Industrie ou d'autres applications sectorielles.

15. Distribution

L'expédition vers un transformateur, distributeur, revendeur ou autre acteur doit préserver les références nécessaires à la généalogie. Expédition, réception, propriété et paiement restent des événements distincts.

16. Transport

Les références de déplacement des productions peuvent être corrélées au domaine Transport. Les conditions logistiques pertinentes peuvent enrichir le passeport sans modifier l'origine d'élevage du produit.

17. Traçabilité ascendante

À partir d'un lot conditionné, transformé ou distribué, le système doit permettre de remonter vers les lots, collectes, groupes, animaux ou exploitations sources selon la granularité effectivement enregistrée.

18. Traçabilité descendante

À partir d'un animal, groupe, exploitation, collecte ou lot source, le système doit permettre d'identifier les lots dérivés, conditionnements, transformations et destinations enregistrés afin de soutenir les investigations et rappels.

19. Critères d'acceptation

Le modèle est acceptable si toute production conserve une origine au niveau réellement démontrable, si fusions et fractionnements préservent la généalogie, si analyses et conditions de conservation restent attribuables et si la traçabilité fonctionne dans les deux sens.

20. Conclusion

Productions, collectes, lots, stockage, transformation et distribution prolongent le passeport d'élevage vers le marché. Leur valeur repose sur une généalogie continue et sur le respect strict de la granularité : une origine collective demeure collective tant qu'aucune preuve ne permet de l' individualiser.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 4 — ÉLEVAGE

CHAPITRE 5 — CERTIFICATIONS, CONTRÔLES, ALERTES, RAPPELS, GOUVERNANCE, AUDIT ET LUTTE CONTRE LES FRAUDES DE PROVENANCE

1. Objet du chapitre

Ce chapitre définit la couche de confiance et de gouvernance de l'application Élevage. Il organise les certifications, contrôles de cohérence, alertes, investigations, rappels, audit et signaux de fraude de provenance, tout en préservant les responsabilités des autorités, vétérinaires, organismes certificateurs et autres acteurs compétents.

2. Certifications et attestations

Certifications d'exploitation, de filière, d'origine, de qualité ou autres attestations peuvent être référencées avec leur émetteur, leur portée, leur période et leur statut. Authenticity Plus© ne doit pas attribuer lui-même un statut officiel.

3. Portée de la certification

Une certification peut concerner une exploitation, un site, un troupeau, un animal, une production ou un lot. Le système ne doit pas étendre automatiquement une certification à des objets qui ne figurent pas dans son périmètre.

4. Validité et révocation

Dates d'émission et d'expiration, suspension, remplacement ou révocation doivent pouvoir être historisés. Un document expiré ou révoqué ne doit pas être présenté comme actif.

5. Contrôle d'identité

Les identifiants individuels ou collectifs peuvent être contrôlés pour détecter duplications, réutilisations incompatibles ou références incohérentes. Une anomalie d'identifiant constitue un signal d'investigation.

6. Contrôle de généalogie

Les filiations, groupes sources et relations entre lots doivent conserver une provenance explicite. Une filiation contradictoire ou une rupture de généalogie doit être rendue visible sans être corrigée silencieusement.

7. Contrôle des mouvements

Les mouvements successifs doivent former une chronologie cohérente. Présences simultanées impossibles, destinations incompatibles ou mouvements sans origine connue peuvent déclencher des alertes.

8. Contrôle de l’alimentation

Les lots d’alimentation déclarés peuvent être rapprochés des périodes et groupes concernés. Les incohérences de date, de quantité ou de provenance doivent être signalées selon les données disponibles.

9. Contrôle des productions

Les quantités collectées, fusionnées, fractionnées, transformées et distribuées peuvent être comparées pour identifier des écarts significatifs. Les rendements, pertes normales et incertitudes de mesure doivent être considérés avant toute qualification.

10. Contrôle des documents sanitaires

Attestations, analyses et autres documents doivent être cohérents avec l’animal, le groupe, le lot, la période et l’émetteur concernés. La plateforme contrôle la cohérence documentaire sans produire de conclusion médicale.

11. Alerte

Une anomalie d’identité, de mouvement, de généalogie, de document, d’analyse ou de production peut déclencher une alerte. Celle-ci doit conserver sa source, sa date, son périmètre initial et son statut.

12. Investigation

Le dossier d’investigation peut regrouper animaux, groupes, mouvements, lots, documents, analyses, productions et destinations concernés. Les éléments doivent conserver leur provenance et leur chronologie.

13. Rappel ou retrait

Lorsqu’un rappel ou retrait est décidé par l’acteur ou l’autorité compétente, la généalogie bidirectionnelle doit permettre d’identifier les lots et destinations potentiellement concernés. Notification, récupération, traitement et clôture doivent rester distincts.

14. Fraude de provenance présumée

Identifiants clonés, origines contradictoires, volumes incompatibles, documents incohérents ou ruptures de chaîne peuvent constituer des signaux de fraude potentielle. La plateforme ne prononce pas elle-même une qualification juridique définitive.

15. Contestation et correction

Un acteur autorisé peut contester une information selon le processus prévu. Toute correction d'une donnée critique doit préserver une piste d'audit suffisante et ne pas effacer silencieusement une information ayant participé à une décision.

16. Journal d'audit

Créations et modifications d'identités, groupes, mouvements, certificats, documents, lots, alertes, rappels et interventions privilégiées doivent être auditables selon leur criticité.

17. AP Ledger

Lorsque l'architecture globale le prévoit, des empreintes de certificats, analyses, mouvements, lots, documents ou décisions peuvent être ancrées dans AP Ledger afin de renforcer intégrité, antériorité et non-altération détectable.

18. Confidentialité et accès

Les données d'exploitation, informations économiques et documents sensibles doivent être exposés selon les rôles et finalités. Les informations sanitaires ou vétérinaires doivent bénéficier d'une gouvernance renforcée.

19. Critères d'acceptation

Le modèle est acceptable si certifications et documents conservent leur portée, si les incohérences d' identité, généalogie, mouvements et quantités sont détectables, si les alertes restent explicables, si les rappels exploitent la traçabilité bidirectionnelle et si les décisions critiques sont auditables.

20. Conclusion

Certifications, contrôles, alertes, rappels, audit et investigations constituent la couche de gouvernance du passeport Élevage. Ils transforment la continuité de traçabilité en dispositif vérifiable tout en distinguant strictement anomalie, preuve, décision professionnelle, statut officiel et qualification juridique.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 4 — ÉLEVAGE

CHAPITRE 6 — SYNTHÈSE FONCTIONNELLE, CRITÈRES D'ACCEPTATION ET CLÔTURE DE L'APPLICATION ÉLEVAGE

1. Objet du chapitre

Ce chapitre clôt le Point 4 — Élevage. Il consolide l'identité individuelle et collective, la généalogie, les mouvements, l'alimentation, les événements d'élevage, le suivi vétérinaire documentaire, les productions, les lots, la distribution, les contrôles, les alertes, les rappels et l'audit.

2. Mission consolidée

L'application Élevage construit un passeport de confiance autour de l'animal, du troupeau et des productions associées. Elle relie les événements et preuves disponibles sans se substituer aux systèmes officiels d'identification, aux vétérinaires, aux laboratoires, aux certificateurs ou aux autorités compétentes.

3. Identité et granularité

Le système doit supporter animal individuel, troupeau, lot, bande ou autre groupe pertinent. La granularité de la preuve commande toujours la granularité de la traçabilité ; une donnée collective ne devient jamais artificiellement une preuve individuelle.

4. Naissance et origine

Naissance, entrée dans le système, exploitation d'origine et références disponibles constituent le début de la continuité. Lorsque l'historique antérieur est incomplet, le passeport doit l'indiquer plutôt que reconstruire des événements non établis.

5. Généalogie

Ascendance et descendance peuvent être représentées lorsque les données existent. Chaque relation de filiation doit conserver sa source afin de distinguer déclaration, registre, analyse ou autre mécanisme de preuve.

6. Troupeaux et groupes

Création, composition, fusion, séparation, entrée et sortie d'un groupe doivent rester historiquement reconstructibles. Les événements collectifs ne s'appliquent qu'aux animaux effectivement couverts pendant la période concernée.

7. Mouvements

Transferts internes et externes doivent conserver origine, destination et période lorsque disponibles. Localisation, détention, propriété et transport restent des notions distinctes.

8. Alimentation

Les aliments, fourrages et autres apports peuvent être reliés aux lots, fournisseurs, périodes et groupes concernés. Une distribution collective ne doit pas être convertie en consommation individuelle sans preuve correspondante.

9. Suivi documentaire sanitaire

Observations, interventions, prescriptions, analyses et attestations peuvent enrichir le passeport selon les droits applicables. Leur auteur, portée et période doivent rester explicites ; AP ne produit pas lui-même le diagnostic ou la prescription.

10. Productions animales

Lait, œufs, laine et autres productions peuvent être reliés à l'animal, au groupe ou à l'exploitation selon la granularité réelle de la collecte. La provenance doit rester au niveau effectivement démontrable.

11. Lots et généalogie de production

Collectes, lots, fusions, fractionnements, stockage, conditionnement et transformation doivent préserver une généalogie bidirectionnelle entre les productions et leurs origines.

12. Analyses et conservation

Les résultats de laboratoire et paramètres de conservation doivent conserver leur source, période et portée. Un résultat d'échantillon ou une mesure ponctuelle ne doit pas être généralisé au-delà de ce qu'il établit.

13. Distribution et transport

Les lots distribués doivent conserver leur relation avec les collectes et origines sources. Les références logistiques peuvent s'articuler avec Transport sans confondre déplacement, propriété, paiement et provenance d'élevage.

14. Certifications

Certifications et attestations doivent conserver leur émetteur, leur périmètre, leur validité et leur statut. Authenticity Plus© renforce leur intégrité et leur rattachement sans créer lui-même une certification officielle.

15. Alertes, investigations et rappels

Les incohérences peuvent produire des alertes explicables. La traçabilité ascendante et descendante doit permettre de circonscrire une investigation et de suivre les lots ou destinations concernés lorsqu' un rappel est décidé par l'acteur compétent.

16. Audit et AP Ledger

Les modifications sensibles, documents, mouvements, lots, alertes, rappels et décisions critiques doivent être auditables. AP Ledger peut, lorsque prévu, renforcer l'intégrité et l'antériorité des preuves sélectionnées.

17. Critère d'acceptation — identité

Un animal ou groupe suivi doit conserver une identité stable et une chronologie reconstructible. Les changements de site, détenteur, groupe ou statut ne doivent pas rompre son histoire.

18. Critère d'acceptation — traçabilité

Un lot de production doit pouvoir remonter vers son origine au niveau réellement disponible ; inversement, un animal, groupe ou lot source doit pouvoir être suivi vers les productions et destinations enregistrées.

19. Critère d'acceptation — gouvernance

Les rôles, accès, corrections, documents sensibles et décisions critiques doivent être gouvernés et auditables. Une anomalie ne doit être transformée automatiquement ni en diagnostic, ni en fraude, ni en conclusion juridique.

20. Clôture du Point 4 — Élevage

Le Point 4 — Élevage est désormais fonctionnellement défini : exploitation, identité animale et collective, généalogie, groupes, mouvements, alimentation, suivi documentaire sanitaire, productions, lots, stockage, transformation, distribution, certifications, alertes, rappels, gouvernance et audit. Cette architecture est prête à s'articuler avec le Point 5 — Pharmacie et les autres applications sectorielles du Volume IV.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 5 — PHARMACIE

CHAPITRE 1 — MISSION, PÉRIMÈTRE ET PRINCIPES FONDATEURS DE L'APPLICATION PHARMACIE

1. Objet du chapitre

Le Point 5 — Pharmacie transpose Authenticity Plus© / Deep Authenticity© à la traçabilité et à l'authenticité documentaires des produits pharmaceutiques. Il organise les identités du produit, du fabricant, du site, du lot, du conditionnement et, lorsque applicable, de l'unité sérialisée jusqu'aux acteurs autorisés de la chaîne.

2. Mission sectorielle

L'application Pharmacie vise à renforcer la confiance dans la provenance, l'intégrité des documents et la continuité de distribution. Elle ne se substitue ni aux autorités réglementaires, ni aux fabricants responsables, ni aux pharmaciens, médecins, laboratoires de contrôle ou autres professionnels compétents.

3. Produit pharmaceutique

Le produit doit disposer d'une identité de référence distincte de ses lots et unités physiques. Nom, forme, dosage, présentation ou autres caractéristiques peuvent être représentés selon les données autorisées et les référentiels applicables.

4. Présentation

Une même substance ou marque peut exister sous plusieurs dosages, formes, tailles ou conditionnements. Chaque présentation pertinente doit être distinguée afin d'éviter qu'une information propre à une version soit appliquée à une autre.

5. Fabricant

L'identité du fabricant ou de l'acteur responsable peut être corrélée au produit et aux documents disponibles. Cette relation doit préserver le rôle exact de chaque acteur sans déduire une responsabilité réglementaire qui n'est pas établie par les sources compétentes.

6. Site de fabrication

Un produit peut être fabriqué, conditionné ou contrôlé sur plusieurs sites. Les sites doivent être distingués et reliés aux opérations qu'ils ont effectivement réalisées lorsque l'information est disponible.

7. Références réglementaires

Autorisations, enregistrements, références officielles ou autres statuts peuvent être rattachés au produit avec leur émetteur, territoire, portée, période et statut. Authenticity Plus© ne crée ni ne prolonge une autorisation réglementaire.

8. Lot de fabrication

Chaque lot doit disposer d'une identité distincte du produit de référence. Numéro de lot, dates pertinentes, site, quantité ou autres données peuvent être conservés selon la chaîne documentaire disponible.

9. Contrôles qualité documentaires

Certificats d'analyse, résultats de contrôle ou autres documents qualité peuvent être rattachés au lot avec leur émetteur et leur portée. La plateforme peut préserver leur intégrité sans interpréter elle-même leur conformité scientifique ou réglementaire.

10. Libération du lot

Lorsqu'un processus prévoit une libération du lot, la décision doit être attribuée à l'acteur compétent avec sa date et ses références. Authenticity Plus© conserve la preuve de la décision sans devenir l' autorité qui libère le produit.

11. Conditionnement

Les niveaux de conditionnement primaire, secondaire ou logistique peuvent être représentés lorsque pertinents. Les relations entre lot, unités et emballages doivent préserver la généalogie de distribution.

12. Sérialisation

Lorsqu'une réglementation ou un système de filière prévoit un identifiant unique par unité, celui-ci peut être corrélé au produit, au lot et au conditionnement. L'existence d'un numéro de série ne suffit pas à prouver l'authenticité si sa provenance n'est pas vérifiée.

13. Agrégation

Des unités sérialisées peuvent être regroupées dans des boîtes, cartons, palettes ou autres unités logistiques. Les relations parent-enfant doivent être conservées lorsqu'elles sont disponibles afin de faciliter les mouvements et contrôles.

14. Conditions de conservation

Température, humidité ou autres conditions pertinentes peuvent être associées aux lots et expéditions lorsque des mesures existent. La source, la période et la couverture des mesures doivent rester explicites.

15. Distribution

Les mouvements entre fabricant, dépositaire, grossiste, distributeur, pharmacie ou autre acteur habilité peuvent être enregistrés selon le cadre applicable. Expédition, réception, propriété, paiement et statut réglementaire restent distincts.

16. Vérification

À différents points de la chaîne, un identifiant, lot, document ou statut peut être vérifié contre les références disponibles. Le résultat doit indiquer ce qui a réellement été vérifié et ne pas produire une garantie plus large que la preuve.

17. Traçabilité ascendante

À partir d'une unité ou d'un lot, le système doit pouvoir remonter vers le produit, le lot de fabrication, les sites et documents disponibles selon la granularité enregistrée.

18. Traçabilité descendante

À partir d'un lot, le système doit pouvoir rechercher les unités, agrégations, expéditions et destinations enregistrées afin de soutenir les contrôles, investigations et rappels.

19. Principe de sécurité et critères d'acceptation

Le modèle est acceptable si produit, présentation, lot et unité restent distincts ; si les références réglementaires conservent leur émetteur et leur territoire ; si la libération est attribuable ; et si l'intégrité d'une donnée n'est jamais présentée comme preuve suffisante de qualité pharmaceutique ou d'adéquation médicale.

20. Conclusion

L'application Pharmacie établit un socle de traçabilité fondé sur les identités, lots, documents, conditionnements, sérialisation et mouvements de distribution. Cette architecture prépare les chapitres consacrés à la fabrication, aux contrôles, à la chaîne logistique, à la lutte contre les produits falsifiés et aux rappels.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 5 — PHARMACIE

CHAPITRE 2 — FABRICATION, MATIÈRES ET COMPOSANTS, LOTS, CONTRÔLES QUALITÉ, LIBÉRATION ET GÉNÉALOGIE PHARMACEUTIQUE

1. Objet du chapitre

Ce chapitre détaille la généalogie de fabrication pharmaceutique depuis les matières et composants documentés jusqu'au lot de produit fini. Il organise les relations entre fournisseurs, lots entrants, opérations, contrôles qualité, conditionnement et décision de libération, sans se substituer aux systèmes qualité réglementés.

2. Matières premières

Les matières premières peuvent être identifiées par désignation, fournisseur, fabricant, lot et documents disponibles. Leur rattachement à un lot de fabrication doit conserver la source de l' information et le niveau de preuve réellement disponible.

3. Substances et excipients

Substances actives, excipients et autres composants pertinents doivent pouvoir être distingués selon le modèle de données applicable. Authenticity Plus© documente leur généalogie sans déterminer lui-même leur aptitude pharmaceutique.

4. Articles de conditionnement

Flacons, blisters, bouchons, étiquettes, notices, cartons ou autres articles peuvent être reliés à leurs références et lots lorsque leur traçabilité contribue à l'identité ou à la sécurité du produit.

5. Fournisseurs et fabricants de composants

Le fournisseur commercial et le fabricant d'une matière ou d'un composant peuvent être différents. Le passeport doit préserver les rôles réellement établis et éviter d'attribuer automatiquement la fabrication au fournisseur.

6. Réception des composants

La réception peut enregistrer lot, quantité, date, site et documents associés. Une réception physique ne doit pas être interprétée automatiquement comme acceptation qualité ou autorisation d'utilisation.

7. Statut qualité documentaire

Les statuts disponibles — par exemple en attente, accepté, rejeté ou autre état gouverné — doivent être attribués au système ou acteur compétent. AP conserve la chronologie sans prendre la décision qualité.

8. Ordre ou campagne de fabrication

Le lot de produit peut être relié à une campagne, un ordre ou une autre référence de fabrication. Cette relation structure la généalogie entre composants consommés et produit obtenu.

9. Consommation des lots entrants

Les lots de matières et composants effectivement utilisés doivent pouvoir être reliés au lot fabriqué, avec quantités ou références lorsque disponibles. Une simple disponibilité en stock ne constitue pas une preuve d'utilisation.

10. Étapes de fabrication

Les principales étapes pertinentes peuvent être représentées par événements datés et attribuables. Le passeport de traçabilité ne remplace pas le dossier de lot réglementé ni les instructions opératoires du fabricant.

11. Produits intermédiaires et vrac

Lorsqu'un processus crée un intermédiaire ou un produit vrac, celui-ci peut disposer d'une identité de lot propre. Les transformations successives doivent préserver la généalogie jusqu'au produit fini.

12. Contrôles en cours et qualité

Les résultats ou références de contrôles peuvent être rattachés à l'étape ou au lot concerné. Leur interprétation et les décisions associées restent de la responsabilité des fonctions qualité et des acteurs habilités.

13. Échantillons et analyses

Une analyse doit conserver le lien avec l'échantillon, le lot, le laboratoire, la date et, lorsque disponible, la méthode ou le rapport. Un résultat d'échantillon ne doit pas être généralisé au-delà de sa portée.

14. Déviations et événements qualité

Une déviation, anomalie ou investigation qualité peut être référencée avec son statut et ses liens au lot. Authenticity Plus© conserve la preuve et la chronologie sans décider lui-même de l'impact réglementaire ou de la disposition du lot.

15. Conditionnement du lot

Le conditionnement primaire et secondaire peut créer ou relier des unités, numéros de série et agrégations. Les relations avec le lot de fabrication doivent rester reconstructibles.

16. Sérialisation et agrégation

Lorsque applicable, les identifiants unitaires et les relations d'agrégation doivent être conservés avec leur statut. La duplication, la réutilisation incompatible ou une relation parent-enfant contradictoire doit pouvoir produire un signal.

17. Libération

La décision de libération doit être enregistrée comme décision attribuée à l'acteur habilité, avec date, lot, statut et référence documentaire disponible. L'enregistrement par AP ne constitue pas la décision elle-même.

18. Généalogie ascendante et descendante

Depuis un lot fini, le système doit pouvoir remonter vers les lots entrants et principales références de fabrication disponibles ; depuis un lot de composant, il doit pouvoir rechercher les lots finis enregistrés dans lesquels il a été utilisé.

19. Critères d'acceptation

Le modèle est acceptable si les matières, composants et articles de conditionnement peuvent être reliés aux lots finis ; si réception et acceptation qualité restent distinctes ; si les analyses conservent leur portée ; si les déviations sont historisées ; et si la libération reste attribuée à l'acteur compétent.

20. Conclusion

La généalogie pharmaceutique relie matières, composants, fabrication, contrôles, conditionnement et libération. Authenticity Plus© apporte continuité et intégrité à cette chaîne documentaire sans remplacer le système qualité du fabricant ni les décisions réglementées qui gouvernent la mise à disposition du médicament.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 5 — PHARMACIE

CHAPITRE 3 — SÉRIALISATION, DISTRIBUTION, CHAÎNE DU FROID, VÉRIFICATION, DISPENSATION DOCUMENTAIRE ET LUTTE CONTRE LES PRODUITS FALSIFIÉS

1. Objet du chapitre

Ce chapitre organise la continuité du produit pharmaceutique après libération du lot. Il structure sérialisation, agrégation, expédition, réception, conditions de transport, vérification et événements documentaires de dispensation, avec des mécanismes de détection des anomalies pouvant signaler un produit falsifié ou détourné.

2. Identifiant unitaire

Lorsqu'un système applicable prévoit une sérialisation, chaque unité peut disposer d'un identifiant unique corrélé à sa présentation et à son lot. L'identifiant doit rester distinct des données de produit et du numéro de lot.

3. Statut du numéro de série

Un identifiant peut disposer d'états gouvernés par la filière ou le système compétent. Toute évolution de statut doit conserver sa source et sa chronologie ; AP ne doit pas inventer un statut réglementaire.

4. Agrégation logistique

Les unités peuvent être regroupées en emballages, cartons, caisses ou palettes. Les relations parent-enfant doivent être conservées lorsque disponibles afin de permettre la traçabilité sans scanner nécessairement chaque unité à chaque mouvement.

5. Désagrégation et reconditionnement

L'ouverture d'une agrégation ou un reconditionnement autorisé doit modifier les relations logistiques sans effacer l'historique. Les nouvelles relations doivent rester attribuables à l'acteur qui les a créées.

6. Expédition

Une expédition peut identifier expéditeur, destinataire, lots, unités ou agrégations, date et références logistiques. L'expédition physique reste distincte du transfert de propriété, de la facturation et du paiement.

7. Réception

Le destinataire peut enregistrer la réception et les écarts constatés. Quantité, emballage, identifiants ou état apparent peuvent être contrôlés sans que la réception constitue automatiquement une décision de conformité pharmaceutique.

8. Chaîne du froid

Pour les produits concernés, température et autres conditions peuvent être suivies pendant stockage et transport. Les mesures doivent conserver leur capteur ou système source, leur période et leur couverture.

9. Excursion de température

Une valeur ou période hors des seuils configurés peut produire un signal. L'évaluation de l'impact sur la qualité du médicament relève du fabricant, du pharmacien ou de l'acteur qualité compétent, et non d'Authenticity Plus©.

10. Vérification en chaîne

Fabricants, distributeurs, pharmacies ou autres acteurs habilités peuvent vérifier un lot, une unité ou un document contre les références disponibles. Le résultat doit préciser l'objet et la portée exacte de la vérification.

11. Numéro de série inconnu

Un identifiant absent des références attendues peut être signalé pour investigation. Cette absence ne doit pas être présentée automatiquement comme preuve définitive de falsification, notamment lorsque les systèmes sources sont incomplets ou indisponibles.

12. Duplication ou réutilisation

L'utilisation incompatible d'un même identifiant sur plusieurs unités, lieux ou événements peut constituer un signal fort d'anomalie. Les événements concernés doivent être préservés pour permettre l'investigation.

13. Incohérence lot-produit

Un numéro de série ou conditionnement associé à un lot, une présentation ou une date incompatible doit déclencher un contrôle. La contradiction doit rester visible et ne pas être corrigée silencieusement.

14. Dispensation documentaire

Lorsqu'un cadre applicable permet d'enregistrer un événement de dispensation, le passeport peut conserver un statut ou une référence attribuée au système ou professionnel compétent. AP ne décide pas quel médicament doit être dispensé à une personne.

15. Protection des données lors de la dispensation

La traçabilité du produit doit être conçue de manière à éviter l'exposition inutile d'informations permettant d'identifier un patient. Les données de santé ou de prescription ne doivent pas être rendues publiques dans le passeport produit.

16. Retour et quarantaine

Un produit retourné, suspect ou isolé peut recevoir un statut documentaire de quarantaine ou autre état gouverné par l'acteur compétent. Le système doit préserver l'historique des mouvements et décisions.

17. Produit falsifié présumé

Un identifiant cloné, un emballage incohérent, un lot inexistant ou une chaîne de possession contradictoire peut produire un signal de falsification potentielle. La qualification officielle relève des autorités et professionnels compétents.

18. Investigation et traçabilité bidirectionnelle

L'investigation doit pouvoir remonter d'une unité suspecte vers son lot, ses agrégations et mouvements enregistrés, puis rechercher en sens descendant les autres unités ou destinations potentiellement liées.

19. Critères d'acceptation

Le modèle est acceptable si sérialisation et lot restent distincts, si les agrégations sont reconstructibles, si les conditions de transport conservent leur source, si les anomalies sont explicables et investigables, et si la dispensation documentaire ne révèle pas inutilement de données personnelles ou médicales.

20. Conclusion

Sérialisation, distribution, chaîne du froid et vérification prolongent le passeport pharmaceutique jusqu'aux derniers acteurs de la chaîne. Leur combinaison renforce la détection des détournements et falsifications potentielles tout en maintenant une séparation stricte entre preuve de traçabilité, décision qualité, dispensation et qualification réglementaire.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 5 — PHARMACIE

CHAPITRE 4 — ALERTES QUALITÉ, RETRAITS ET RAPPELS, RETOURS, DESTRUCTION, PHARMACOVIGILANCE DOCUMENTAIRE ET TRAÇABILITÉ D'INVESTIGATION

1. Objet du chapitre

Ce chapitre organise les événements exceptionnels ou correctifs qui peuvent affecter un produit pharmaceutique après fabrication ou distribution : alertes qualité, retraits, rappels, retours, quarantaine et destruction. Il prévoit également la corrélation documentaire avec les systèmes de pharmacovigilance sans transformer Authenticity Plus© en dispositif de diagnostic ou d'évaluation médicale.

2. Origine d'une alerte

Une alerte peut provenir d'un fabricant, d'un laboratoire, d'un distributeur, d'une pharmacie, d'une autorité ou d'un autre acteur habilité. Sa source, sa date, son objet et son périmètre initial doivent être conservés.

3. Alerte qualité

Une déviation, un résultat de contrôle, une anomalie documentaire, une excursion logistique ou une information reçue après libération peut déclencher une alerte qualité. L'alerte ne constitue pas à elle seule une décision de rappel.

4. Périmètre d'investigation

L'investigation peut concerner un produit, une présentation, un lot, certaines unités sérialisées, une période, un site ou des destinations déterminées. Le périmètre suspecté doit rester distinct du périmètre confirmé.

5. Traçabilité ascendante

À partir d'une unité ou d'un lot signalé, le système doit pouvoir rechercher les références de fabrication, composants, documents, contrôles, sites et événements disponibles afin de soutenir l' analyse de l'origine du problème.

6. Traçabilité descendante

À partir d'un lot ou composant concerné, le système doit pouvoir identifier les unités, agrégations, expéditions, destinataires et statuts enregistrés afin de soutenir une action ciblée.

7. Décision de retrait ou rappel

La décision doit être attribuée au fabricant, à l'autorité ou à l'acteur compétent selon le cadre applicable. Authenticity Plus© enregistre la décision, sa portée et ses références sans décider lui-même qu'un médicament doit être rappelé.

8. Notification

Les notifications adressées aux acteurs de la chaîne peuvent être suivies avec leur date, destinataire et statut technique lorsque le système le permet. Une notification enregistrée ne garantit pas à elle seule sa lecture ou son exécution.

9. Blocage et quarantaine

Les unités ou lots concernés peuvent recevoir un statut documentaire de blocage, quarantaine ou autre état gouverné. Le statut doit conserver l'acteur qui l'a posé et les conditions de sa levée.

10. Retour

Un retour depuis un distributeur, une pharmacie ou un autre acteur peut être relié à l'expédition d' origine, au lot ou aux unités concernées. Le retour physique ne signifie pas automatiquement que le produit peut être remis en distribution.

11. Réconciliation du rappel

Les quantités distribuées, localisées, retournées, détruites ou restant non réconciliées peuvent être suivies. Les écarts doivent rester visibles afin de permettre l'analyse et la clôture par l'acteur compétent.

12. Destruction

Une destruction peut être enregistrée avec lot ou unités, quantité, date, opérateur et preuve documentaire disponible. AP conserve l'événement sans certifier lui-même la conformité réglementaire du procédé de destruction.

13. Clôture du rappel

La clôture doit être attribuée à l'acteur compétent et conserver les références disponibles. La plateforme peut calculer ou présenter des indicateurs de suivi, mais ne doit pas conclure seule que toutes les obligations réglementaires ont été satisfaites.

14. Pharmacovigilance documentaire

Lorsqu'une référence à un signal ou dossier de pharmacovigilance doit être corrélée à un produit ou lot, le passeport peut conserver un identifiant ou lien documentaire autorisé. Il ne doit pas exposer publiquement le contenu médical d'un dossier individuel.

15. Séparation des responsabilités

La pharmacovigilance évalue des informations de sécurité selon des processus spécialisés. Authenticity Plus© peut soutenir l'intégrité, la chronologie et la corrélation des références, mais ne produit pas l'évaluation clinique, la causalité ou la décision médicale.

16. Protection des données

Les informations permettant d'identifier un patient, un prescripteur ou des données de santé ne doivent pas être intégrées dans un passeport public de produit. Les accès aux données sensibles doivent suivre des règles strictes de finalité et d'autorisation.

17. Falsification et rappel

Une investigation de falsification présumée peut conduire à un retrait ou rappel décidé par l'acteur compétent. Les identifiants suspects, duplications et mouvements associés doivent être préservés afin de permettre l'analyse de la chaîne.

18. Audit et AP Ledger

Alertes, changements de statut, décisions de rappel, retours, destructions et clôtures doivent être auditables. Des empreintes de documents ou décisions sélectionnées peuvent être ancrées dans AP Ledger lorsque l'architecture globale le prévoit.

19. Critères d'acceptation

Le modèle est acceptable si une alerte conserve sa source, si le périmètre suspecté reste distinct du périmètre confirmé, si les rappels peuvent être suivis jusqu'aux destinations et retours connus, si la destruction est documentée et si aucune donnée médicale individuelle n'est exposée sans autorisation.

20. Conclusion

Alertes, rappels, retours et destructions prolongent la traçabilité pharmaceutique jusque dans les situations critiques. La valeur d'Authenticity Plus© réside dans la continuité, l'intégrité et l'auditabilité de ces événements, tout en laissant les décisions qualité, réglementaires et médicales aux acteurs compétents.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 5 — PHARMACIE

CHAPITRE 5 — GOUVERNANCE, CONFORMITÉ DOCUMENTAIRE, AUDIT, INTEROPÉRABILITÉ RÉGLEMENTAIRE, CYBERSÉCURITÉ DE LA TRAÇABILITÉ ET LUTTE CONTRE LA FRAUDE PHARMACEUTIQUE

1. Objet du chapitre

Ce chapitre définit la couche de gouvernance du passeport pharmaceutique. Il organise les responsabilités, la conformité documentaire, l'audit, l'interopérabilité avec les systèmes réglementaires, la sécurité des identifiants et les investigations liées aux anomalies ou fraudes présumées.

2. Gouvernance des acteurs

Fabricants, sites, fonctions qualité, laboratoires, dépositaires, grossistes, distributeurs, pharmacies et autres acteurs habilités doivent disposer de droits correspondant à leurs responsabilités. Le droit de consulter une donnée ne doit pas conférer automatiquement le droit de la modifier.

3. Séparation des responsabilités

Fabrication, contrôle, libération, distribution, vérification, dispensation documentaire, rappel et décision réglementaire peuvent relever d'acteurs différents. Le modèle doit préserver cette séparation et l' attribution de chaque événement.

4. Conformité documentaire

Autorisations, certificats, analyses, décisions de libération, documents logistiques et autres références doivent conserver leur émetteur, leur portée, leur territoire, leur période et leur statut lorsque ces informations existent.

5. Versions et révocations

Une nouvelle version, correction, suspension ou révocation d'un document critique doit rester liée à son historique. Une version remplacée ne doit pas disparaître silencieusement lorsqu'elle a participé à une décision ou à une transaction.

6. Interopérabilité réglementaire

L'application doit pouvoir corréler des références provenant de systèmes officiels ou sectoriels lorsque les interfaces et droits le permettent. La copie d'une donnée réglementaire dans AP ne doit pas créer un registre officiel parallèle.

7. Référentiels et identifiants

Codes produit, identifiants de présentation, lots, numéros de série, sites et acteurs doivent être reliés aux référentiels pertinents sans supposer qu'un même identifiant possède la même portée dans tous les territoires.

8. Synchronisation et provenance

Toute donnée synchronisée doit conserver, autant que possible, son système source, sa date de récupération ou d'effet et son statut. Une donnée importée ne doit pas être présentée comme créée ou certifiée par Authenticity Plus©.

9. Journal d'audit

Créations, modifications, changements de statut, vérifications, libérations, alertes, rappels, destructions et accès privilégiés doivent produire une piste d'audit proportionnée à leur criticité.

10. AP Ledger

Lorsque l'architecture globale le prévoit, des empreintes de documents, lots, décisions, événements de sérialisation ou autres preuves sélectionnées peuvent être ancrées dans AP Ledger afin de renforcer l'intégrité et l'antériorité.

11. Sécurité des identifiants

Les mécanismes d'émission, importation, vérification et changement de statut des identifiants sensibles doivent être protégés contre les modifications non autorisées, duplications et réutilisations incompatibles.

12. Compromission et révocation technique

Lorsqu'un identifiant, compte, clé ou mécanisme de confiance est compromis, le système doit permettre de suspendre ou révoquer les capacités concernées tout en conservant l'historique des événements antérieurs.

13. Contrôles de cohérence

Chronologies impossibles, lots inexistants, numéros de série dupliqués, agrégations contradictoires, documents hors période ou statuts incompatibles doivent pouvoir produire des signaux explicables.

14. Fraude pharmaceutique présumée

Falsification documentaire, détournement de chaîne, clonage d'identifiants ou substitution de produit peuvent constituer des signaux de fraude potentielle. La plateforme soutient l'investigation mais ne prononce pas elle-même une qualification pénale ou réglementaire.

15. Dossier d'investigation

Une investigation peut regrouper produit, lot, unités, documents, sites, acteurs, mouvements, vérifications et destinations. Chaque élément doit conserver sa source, sa chronologie et son statut.

16. Conservation des preuves

Les éléments utilisés dans une investigation ou une décision critique doivent être protégés contre l' altération non tracée. Les politiques de conservation doivent respecter les obligations et durées applicables au contexte concerné.

17. Confidentialité et minimisation

Les secrets industriels, données commerciales, informations professionnelles sensibles et données personnelles doivent être accessibles uniquement selon la finalité et le rôle. Les données médicales individuelles ne doivent pas être exposées dans le passeport public du produit.

18. Résilience et continuité

Une panne d'un système source ou une interruption de synchronisation ne doit pas conduire à inventer des statuts ou à perdre l'historique déjà établi. Les reprises doivent être contrôlées, auditables et résistantes aux duplications.

19. Critères d'acceptation

Le modèle est acceptable si chaque donnée critique reste attribuable à sa source, si les versions et révocations sont visibles, si l'interopérabilité ne crée pas de faux statut officiel, si les identifiants sensibles sont gouvernés et si les anomalies peuvent être investiguées sans verdict automatique.

20. Conclusion

Gouvernance, conformité documentaire, audit, interopérabilité et sécurité transforment la traçabilité pharmaceutique en infrastructure de confiance. Authenticity Plus© renforce la continuité et l'intégrité des preuves tout en maintenant les décisions qualité, réglementaires, pharmaceutiques et judiciaires dans leurs domaines compétents.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 5 — PHARMACIE

CHAPITRE 6 — SYNTHÈSE FONCTIONNELLE, CRITÈRES D'ACCEPTATION ET CLÔTURE DE L'APPLICATION PHARMACIE

1. Objet du chapitre

Ce chapitre clôt le Point 5 — Pharmacie. Il consolide l'identité du produit, les références réglementaires, la fabrication, les lots, les contrôles documentaires, la libération, la sérialisation, la distribution, la chaîne du froid, les alertes, les rappels, la gouvernance et la lutte contre les falsifications.

2. Mission consolidée

L'application Pharmacie constitue un passeport de confiance destiné à renforcer la provenance, l'intégrité documentaire et la continuité de la chaîne pharmaceutique. Elle ne se substitue ni au système qualité du fabricant, ni aux autorités, ni aux pharmaciens, médecins, laboratoires ou autres professionnels habilités.

3. Identités fondamentales

Produit, présentation, lot, unité sérialisée et agrégation logistique doivent rester des identités distinctes. Une donnée propre à l'un de ces niveaux ne doit pas être étendue automatiquement aux autres.

4. Fabricant et sites

Fabricants, titulaires ou acteurs responsables et sites de fabrication, contrôle ou conditionnement doivent être représentés selon leurs rôles réellement établis. Une relation commerciale ne doit pas être transformée en responsabilité réglementaire implicite.

5. Références réglementaires

Autorisations, enregistrements et statuts doivent conserver leur émetteur, territoire, portée, période et état. Authenticity Plus© peut les corréler mais ne crée pas de registre réglementaire parallèle.

6. Généalogie de fabrication

Matières, substances, excipients, composants et articles de conditionnement peuvent être reliés aux lots finis selon les données disponibles. La réception d'un composant reste distincte de son acceptation qualité et de son utilisation effective.

7. Contrôles et analyses

Analyses, certificats et contrôles doivent conserver laboratoire ou émetteur, date, échantillon et portée lorsque disponibles. L'intégrité d'un rapport ne constitue pas à elle seule une interprétation de conformité.

8. Déviations et décisions qualité

Déviations, investigations et statuts qualité peuvent être historisés. Leur impact et leur résolution restent de la responsabilité des fonctions qualité et acteurs habilités.

9. Libération du lot

La libération doit rester une décision attribuée à l'acteur compétent. AP conserve sa référence, sa date et son statut sans devenir l'autorité qui autorise la mise à disposition du médicament.

10. Sérialisation et agrégation

Lorsque applicable, les unités sérialisées doivent être corrélées au produit et au lot. Les relations d' agrégation et de désagrégation doivent rester reconstructibles et les duplications incompatibles doivent pouvoir être détectées.

11. Distribution

Expéditions et réceptions entre acteurs autorisés doivent préserver les références nécessaires à la traçabilité. Mouvement physique, propriété, facturation, paiement et statut réglementaire restent des événements distincts.

12. Chaîne du froid

Les conditions de stockage et transport peuvent être documentées avec leur source et leur période. Une excursion détectée produit un signal ; l'évaluation de son impact pharmaceutique appartient à l' acteur qualité compétent.

13. Vérification et falsification présumée

Identifiants inconnus ou clonés, lots inexistants, agrégations contradictoires ou chaînes de possession incohérentes peuvent déclencher une investigation. Aucun signal ne doit être présenté automatiquement comme verdict officiel de falsification.

14. Alertes, retraits et rappels

Une alerte doit conserver sa source et son périmètre. Lorsqu'un retrait ou rappel est décidé par l'acteur compétent, la traçabilité descendante doit permettre d'identifier unités, expéditions et destinations enregistrées.

15. Retours, quarantaine et destruction

Retours, blocages, quarantaines et destructions doivent rester attribuables et auditables. Un retour physique ne constitue pas une autorisation automatique de remise en distribution.

16. Pharmacovigilance documentaire

Le système peut corréler des références autorisées à des processus de pharmacovigilance, mais ne doit ni exposer des données médicales individuelles dans le passeport public, ni produire d'évaluation clinique ou de causalité.

17. Audit, cybersécurité et AP Ledger

Les changements critiques, identifiants, documents, décisions, alertes et rappels doivent être protégés et auditables. AP Ledger peut renforcer l'intégrité et l'antériorité de preuves sélectionnées lorsque l' architecture globale le prévoit.

18. Critère d'acceptation — traçabilité

À partir d'une unité ou d'un lot, le système doit pouvoir remonter vers les références de produit, fabrication et documents disponibles ; depuis un lot ou composant, il doit pouvoir rechercher les unités, lots dérivés et destinations enregistrés.

19. Critère d'acceptation — gouvernance

Chaque donnée critique doit rester attribuable à sa source et à son niveau de preuve. Les accès doivent suivre le moindre privilège, les versions et révocations doivent rester visibles et aucune anomalie ne doit produire automatiquement une décision médicale, qualité, réglementaire ou judiciaire.

20. Clôture du Point 5 — Pharmacie

Le Point 5 — Pharmacie est désormais fonctionnellement défini : produit, présentation, fabricant, sites, références réglementaires, matières, fabrication, lots, analyses, libération, conditionnement, sérialisation, distribution, chaîne du froid, vérification, alertes, rappels, pharmacovigilance documentaire, audit, interopérabilité et lutte contre les falsifications. Cette architecture est prête à s' articuler avec le Point 6 — Santé.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 6 — SANTÉ

CHAPITRE 1 — MISSION, PÉRIMÈTRE, IDENTITÉ, CONFIDENTIALITÉ ET PRINCIPES FONDATEURS DE L'APPLICATION SANTÉ

1. Objet du chapitre

Le Point 6 — Santé transpose Authenticity Plus© / Deep Authenticity© à la provenance, à l'intégrité et à la gouvernance des documents et événements d'un parcours de soins. Il structure les identités, établissements, professionnels, épisodes, actes, examens, résultats et documents associés sans se substituer au dossier médical réglementé ni à la décision clinique.

2. Mission sectorielle

L'application Santé vise à rendre vérifiables l'origine, l'auteur, la chronologie et les transformations d' une information de santé. Elle renforce la confiance documentaire tout en maintenant les responsabilités médicales, réglementaires et professionnelles dans leurs systèmes et institutions compétents.

3. Identité de la personne

La personne concernée doit être reliée aux informations de santé par des mécanismes d'identité appropriés, sans rendre son identité publiquement accessible. Les identifiants sensibles doivent être protégés, minimisés et dissociés des couches publiques de preuve.

4. Professionnels de santé

Médecins, pharmaciens, infirmiers, biologistes et autres professionnels peuvent être représentés selon leur rôle et les références autorisées. La plateforme conserve l'attribution d'un document ou événement sans créer elle-même une habilitation professionnelle.

5. Établissements et structures

Hôpitaux, cliniques, laboratoires, cabinets, pharmacies ou autres structures peuvent être reliés aux événements qu'ils émettent ou hébergent. L'identité d'un établissement doit rester distincte de celle du professionnel qui intervient.

6. Épisode ou parcours de soins

Les événements peuvent être regroupés dans un épisode, une prise en charge ou un parcours lorsque le contexte le permet. Cette organisation documentaire ne doit pas produire automatiquement une interprétation clinique de la situation de la personne.

7. Actes et événements

Consultation, admission, examen, prélèvement, intervention ou autre acte peut être référencé avec sa date, son lieu et son auteur ou système source. L'enregistrement atteste la provenance de l' événement, pas son indication médicale.

8. Examens et analyses

Les demandes, prélèvements, analyses et résultats peuvent être corrélés en préservant laboratoire, date, échantillon, méthode ou rapport lorsque disponibles. Un résultat doit conserver sa portée et ne pas être extrapolé automatiquement.

9. Imagerie et comptes rendus

Les références d'examens d'imagerie et leurs comptes rendus peuvent être rattachées au parcours avec leur émetteur et leur chronologie. Authenticity Plus© protège la provenance documentaire sans interpréter les images ni poser de diagnostic.

10. Prescriptions documentaires

Une prescription peut être conservée comme document émis par un professionnel habilité avec son auteur, sa date et son statut lorsque disponibles. La plateforme ne génère pas de prescription et ne recommande pas de traitement.

11. Produits et dispositifs associés

Lorsqu'un parcours implique un médicament, un dispositif médical ou un autre produit traçable, des références peuvent être corrélées aux applications sectorielles correspondantes. La relation documentaire ne constitue pas une recommandation thérapeutique.

12. Consentement et autorisations

Les consentements, autorisations ou bases d'accès applicables doivent pouvoir être représentés avec leur portée et leur période lorsque nécessaire. Un consentement donné pour une finalité ne doit pas être étendu silencieusement à une autre.

13. Contrôle d'accès

Les données de santé doivent suivre un modèle de moindre privilège tenant compte du rôle, de la finalité et du contexte. Les accès sensibles doivent être attribuables et auditables.

14. Accès d'urgence gouverné

Lorsqu'un mécanisme exceptionnel d'accès est prévu par le cadre applicable, son utilisation doit être strictement gouvernée, justifiée, limitée et auditée. L'urgence ne doit pas devenir un mécanisme permanent de contournement des droits.

15. Confidentialité et minimisation

Le système doit limiter l’exposition aux seules données nécessaires à la finalité. Les preuves publiques ou partagées ne doivent pas révéler inutilement identité, diagnostic, prescription, résultat biologique ou autre information médicale personnelle.

16. Intégrité et versionnement

Un document corrigé, complété ou remplacé doit conserver une relation avec ses versions antérieures lorsqu’elles ont participé au parcours ou à une décision. Les modifications critiques ne doivent pas effacer silencieusement l’historique.

17. Audit et AP Ledger

Créations, signatures, transmissions, consultations sensibles, corrections et autres événements critiques doivent pouvoir être audités. Lorsque l’architecture globale le prévoit, AP Ledger peut ancrer des empreintes de preuves sélectionnées sans exposer leur contenu médical.

18. Interopérabilité

L’application doit pouvoir corréler des références provenant de dossiers de santé, laboratoires, établissements, pharmacie ou autres systèmes autorisés. Toute donnée importée doit conserver son système source et ne pas être présentée comme créée par Authenticity Plus©.

19. Critères d’acceptation

Le modèle est acceptable si l’identité de la personne reste protégée, si professionnels et établissements sont attribuables, si chaque document conserve sa source et sa version, si les accès sensibles sont gouvernés et si aucune fonction de provenance documentaire n’est présentée comme diagnostic, prescription ou décision clinique.

20. Conclusion

L’application Santé établit un socle de confiance centré sur provenance, intégrité, confidentialité, consentement, contrôle d’accès et audit. Elle prépare les chapitres consacrés au parcours de soins, aux documents cliniques, aux examens, à l’interopérabilité et à la gouvernance renforcée des données de santé.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 6 — SANTÉ

CHAPITRE 2 — PARCOURS DE SOINS, CONSULTATIONS, ACTES, EXAMENS, ANALYSES, IMAGERIE, COMPTES RENDUS ET CONTINUITÉ DOCUMENTAIRE

1. Objet du chapitre

Ce chapitre structure la continuité documentaire d'un parcours de soins. Il relie consultations, actes, demandes d'examens, prélèvements, analyses, imagerie, comptes rendus et autres documents aux professionnels et établissements qui les ont produits, sans interpréter leur contenu clinique.

2. Parcours de soins

Un parcours peut regrouper plusieurs épisodes, établissements et professionnels. Le système doit préserver les relations chronologiques et documentaires sans imposer une interprétation médicale unique de l'ensemble.

3. Épisode de prise en charge

Une admission, consultation, passage ambulatoire ou autre épisode peut constituer un conteneur fonctionnel d'événements. Son ouverture et sa clôture documentaires restent distinctes d'une conclusion clinique.

4. Consultation

Une consultation peut être enregistrée avec date, professionnel, établissement et références documentaires disponibles. Authenticity Plus© atteste la provenance de l'enregistrement sans certifier le contenu médical de la consultation.

5. Demande d'examen

Une demande d'examen ou d'analyse peut être reliée à son auteur, sa date et son destinataire lorsque disponibles. La plateforme conserve la chaîne documentaire sans décider si l'examen est médicalement indiqué.

6. Prélèvement

Lorsqu'un examen nécessite un prélèvement, celui-ci peut disposer d'un identifiant, d'une date, d'un lieu et d'une chaîne de transmission. La relation entre personne, prélèvement et analyse doit être protégée contre les erreurs d'attribution.

7. Chaîne de possession de l'échantillon

Les transferts d'un échantillon entre prélèvement, transport, réception et laboratoire peuvent être documentés lorsque nécessaire. Une rupture ou incohérence doit pouvoir être signalée sans produire automatiquement une conclusion clinique.

8. Analyse de laboratoire

Le résultat doit conserver laboratoire, date, échantillon, méthode ou rapport lorsque disponibles. La plateforme protège son origine et son intégrité mais ne produit pas l'interprétation médicale du résultat.

9. Corrections de résultats

Lorsqu'un laboratoire corrige ou remplace un résultat, les versions doivent rester reliées et leur statut explicite. Une correction ne doit pas effacer silencieusement la version précédemment communiquée.

10. Imagerie médicale

Les références d'un examen d'imagerie peuvent être reliées à l'établissement, au dispositif ou système source et au professionnel compétent. Les images elles-mêmes doivent rester protégées selon les règles d'accès applicables.

11. Compte rendu d'imagerie

Un compte rendu peut être rattaché à l'examen avec son auteur, sa date et sa version. Authenticity Plus© en sécurise la provenance documentaire sans analyser l'image ni générer une conclusion diagnostique.

12. Actes et interventions

Les actes réalisés peuvent être référencés avec les professionnels, établissements et documents disponibles. La présence d'un événement dans le passeport ne constitue pas une évaluation de sa pertinence clinique ou de son résultat.

13. Documents de sortie et synthèses

Les documents de sortie, lettres, synthèses ou comptes rendus peuvent être reliés à l'épisode concerné. Leur auteur et leur version doivent rester identifiables afin de distinguer document source et copie transmise.

14. Transmission entre professionnels

Un document peut être transmis entre professionnels ou établissements autorisés. L'événement de transmission doit rester distinct de la consultation effective du document par son destinataire.

15. Continuité inter-établissements

Lorsque plusieurs structures participent au parcours, les références peuvent être corrélées sans fusionner les responsabilités. Chaque établissement reste source des données et documents qu'il a effectivement produits.

16. Chronologie

La chronologie doit permettre de distinguer date de l'acte, date de production du document, date de validation, date de transmission et date de consultation lorsque ces événements sont disponibles.

17. Provenance et signature

Les mécanismes de signature ou d'authentification disponibles peuvent être associés aux documents. AP doit indiquer ce qui a été vérifié — identité, signature, intégrité ou provenance — sans étendre la garantie au contenu clinique.

18. Confidentialité et accès

Les examens, résultats, images et comptes rendus sont des données sensibles. Leur accès doit être limité aux acteurs autorisés, avec journalisation des consultations critiques et minimisation des copies inutiles.

19. Critères d'acceptation

Le modèle est acceptable si chaque événement ou document reste attribuable, si prélèvements et résultats conservent leur chaîne documentaire, si les versions corrigées restent visibles, si les transmissions inter-établissements préservent les sources et si aucune fonction de traçabilité ne produit une interprétation clinique automatique.

20. Conclusion

La continuité documentaire du parcours de soins repose sur l'attribution, la chronologie, le versionnement et la confidentialité. Authenticity Plus© relie les preuves produites par les acteurs compétents et rend leur parcours vérifiable, sans devenir un moteur de diagnostic ou de décision thérapeutique.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 6 — SANTÉ

CHAPITRE 3 — PRESCRIPTIONS DOCUMENTAIRES, MÉDICAMENTS, DISPOSITIFS MÉDICAUX, CONSENTEMENTS, AUTORISATIONS ET CONTINUITÉ ENTRE SANTÉ ET PHARMACIE

1. Objet du chapitre

Ce chapitre organise les relations documentaires entre le parcours de soins, les prescriptions émises par des professionnels habilités, les médicaments, les dispositifs médicaux et les autorisations d' accès. Il assure la continuité avec l'application Pharmacie sans transformer Authenticity Plus© en système de prescription ou de décision thérapeutique.

2. Prescription comme document source

Une prescription doit être représentée comme un document attribué à son auteur, avec date, version, statut et contexte lorsque disponibles. AP peut vérifier provenance et intégrité sans déterminer si son contenu est médicalement approprié.

3. Auteuret habilitation

L'identité du professionnel émetteur peut être corrélée aux références professionnelles disponibles. La plateforme ne crée pas elle-même l'habilitation et ne doit pas conclure qu'un acte est autorisé au-delà de ce que les sources compétentes établissent.

4. Versionnement d'une prescription

Modification, remplacement, annulation ou renouvellement documentaire doivent conserver une relation avec les versions antérieures. Une version remplacée ne doit pas être effacée lorsqu'elle a déjà été transmise ou utilisée.

5. Médicament référencé

Le document peut être corrélé à l'identité du produit pharmaceutique ou de sa présentation lorsque les données le permettent. Cette relation doit utiliser les références disponibles sans transformer AP en moteur de choix thérapeutique.

6. Continuité avec Pharmacie

Lorsqu'un médicament est suivi dans le Point 5 — Pharmacie, le parcours Santé peut référencer le produit, la présentation, le lot ou l'événement documentaire pertinent selon les droits applicables. Les deux domaines conservent leurs responsabilités propres.

7. Dispensation documentaire

Un événement de dispensation peut être corrélé à la prescription et au produit lorsque le cadre le permet. AP enregistre la provenance de l'événement mais ne décide ni de la délivrance ni de la substitution pharmaceutique.

8. Lot et unité sérialisée

Lorsque nécessaire et autorisé, le lot ou l'unité sérialisée délivrée peut être corrélé à l'événement de dispensation. Cette information doit bénéficier d'une protection suffisante pour éviter qu'une traçabilité produit ne révèle publiquement le parcours médical d'une personne.

9. Dispositif médical

Un dispositif utilisé, implanté, remis ou associé à un acte peut être référencé avec son fabricant, modèle, lot, numéro de série ou identifiant disponible. L'enregistrement ne constitue pas une évaluation clinique du dispositif.

10. Implant ou dispositif durable

Lorsqu'un dispositif demeure associé à une personne dans le temps, sa relation documentaire peut être conservée afin de soutenir la traçabilité, les alertes ou rappels. Les accès doivent rester strictement gouvernés.

11. Consommables et dispositifs temporaires

Les consommables ou dispositifs temporaires peuvent être corrélés à un acte ou épisode lorsque leur traçabilité est pertinente. Le niveau de détail doit être proportionné à la finalité et aux obligations applicables.

12. Alerte produit

Une alerte provenant du domaine Pharmacie, d'un fabricant ou d'une autorité peut être corrélée aux références de produits ou dispositifs concernés. La plateforme soutient l'identification documentaire sans produire elle-même une recommandation médicale individuelle.

13. Rappel et recherche de corrélation

Lorsqu'un rappel officiel concerne un lot ou dispositif, le système peut rechercher les événements de soins autorisés qui lui sont corrélés. Toute action clinique ultérieure relève des professionnels compétents.

14. Consentement

Un consentement peut être enregistré avec sa finalité, sa portée, sa date et sa durée lorsqu'elles sont applicables. La preuve du consentement doit rester distincte du contenu médical auquel il donne éventuellement accès.

15. Retrait ou évolution du consentement

Le retrait ou la modification d'un consentement doit être historisé et appliqué aux accès futurs selon le cadre applicable. Le retrait ne doit pas effacer les événements qui doivent légalement ou légitimement rester conservés.

16. Autorisations d'accès

Les accès peuvent dépendre du rôle professionnel, de l'établissement, de la relation de soins, du consentement ou d'une autre base autorisée. La plateforme doit pouvoir expliquer la base d'un accès sensible.

17. Délégation et représentation

Lorsque le cadre applicable permet une représentation légale ou une délégation, celle-ci doit être limitée par sa portée, sa période et son fondement. Elle ne doit pas créer un accès général permanent sans justification.

18. Audit et confidentialité

Consultation d'une prescription, corrélation avec un médicament ou dispositif, accès à un consentement et opérations privilégiées doivent être auditables. Les données personnelles et médicales ne doivent jamais être exposées dans les couches publiques de traçabilité.

19. Critères d'acceptation

Le modèle est acceptable si prescriptions et versions restent attribuables, si Santé et Pharmacie restent séparés mais interopérables, si médicaments et dispositifs sont corrélés sans révélation publique du parcours médical, et si consentements et autorisations sont limités, explicables et auditables.

20. Conclusion

Prescriptions, médicaments, dispositifs, consentements et autorisations constituent des points de jonction critiques entre parcours de soins et chaîne pharmaceutique. Authenticity Plus© apporte provenance, continuité et auditabilité tout en maintenant la décision thérapeutique, la dispensation et le suivi clinique sous responsabilité professionnelle.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 6 — SANTÉ

CHAPITRE 4 — IDENTITÉ NUMÉRIQUE DE SANTÉ, PARTAGE SÉCURISÉ, INTEROPÉRABILITÉ, ACCÈS D'URGENCE, JOURNAL D'AUDIT ET SOUVERAINETÉ DES DONNÉES MÉDICALES

1. Objet du chapitre

Ce chapitre définit la gouvernance technique et fonctionnelle des identités et échanges de données dans l'application Santé. Il organise l'identité numérique, le partage sécurisé, l'interopérabilité, les accès exceptionnels, l'audit et la souveraineté des données sans créer un dossier médical public ou universel.

2. Identité numérique de la personne

L'identité utilisée pour relier les événements de santé doit être protégée contre l'usurpation, les collisions et les associations erronées. Les mécanismes techniques doivent limiter l'exposition des identifiants réels aux seuls contextes qui les nécessitent.

3. Identités professionnelles

Les professionnels et organisations doivent disposer d'identités vérifiables adaptées à leurs rôles. Les habilitations, spécialités ou autorisations doivent rester attribuées aux référentiels ou autorités compétentes.

4. Pseudonymisation

Lorsque la finalité le permet, les échanges ou preuves peuvent utiliser des identifiants pseudonymisés afin de réduire l'exposition de l'identité directe. La pseudonymisation ne doit pas être présentée comme anonymisation irréversible.

5. Séparation des espaces

Les données médicales, métadonnées techniques, preuves d'intégrité et informations éventuellement publiques doivent être séparées. Une preuve publique ne doit pas permettre de reconstituer le contenu d'un dossier de santé.

6. Partage sécurisé

Tout partage doit identifier l'émetteur, le destinataire, l'objet, la finalité et, lorsque nécessaire, la période d'accès. Les transferts doivent protéger confidentialité et intégrité pendant le transport et le stockage.

7. Accès par rôle et contexte

Les autorisations doivent tenir compte du rôle professionnel, de l'établissement, de la relation de soins et du contexte. Une fonction administrative ne doit pas ouvrir automatiquement l'accès au contenu clinique complet.

8. Consentement et base d'accès

Lorsqu'un consentement est requis, sa portée et son état doivent être vérifiables. D'autres bases d' accès prévues par le cadre applicable peuvent être représentées sans être artificiellement converties en consentement.

9. Accès temporaire

Un accès peut être limité à une durée, un épisode ou un ensemble de documents. Son expiration doit être appliquée sans supprimer les traces nécessaires à l'audit.

10. Accès d'urgence gouverné

Un mécanisme exceptionnel peut permettre un accès urgent lorsque le cadre applicable l'autorise. Son déclenchement doit être justifié, limité, journalisé et soumis à un contrôle a posteriori afin d'éviter sa banalisation.

11. Journal des consultations

Les accès aux informations sensibles doivent pouvoir enregistrer acteur, date, objet et contexte. Le journal lui-même constitue une donnée protégée et ne doit pas exposer inutilement le contenu consulté.

12. Traçabilité des modifications

Création, correction, remplacement, signature ou suppression logique d'une donnée critique doit produire une piste permettant de comprendre qui a modifié quoi et quand, selon les politiques applicables.

13. Interopérabilité

Les échanges avec dossiers de santé, laboratoires, établissements, pharmacies, dispositifs ou autres systèmes doivent préserver les identifiants, statuts, auteurs et versions nécessaires à la provenance.

14. Donnée source et copie

Une donnée importée ou copiée doit conserver sa référence au système source. La présence d'une copie dans AP ne doit pas être interprétée comme création, validation clinique ou propriété de la donnée par Authenticity Plus©.

15. Résolution des divergences

Lorsque deux systèmes fournissent des informations différentes, le modèle doit préserver les sources et versions plutôt que fusionner silencieusement les valeurs. La résolution métier ou clinique relève des acteurs compétents.

16. Souveraineté et localisation

Les architectures de déploiement doivent permettre de respecter les exigences applicables de localisation, hébergement, transfert et contrôle des données. La couche de preuve doit être conçue pour fonctionner sans publier les données médicales elles-mêmes.

17. Chiffrement et gestion des accès

Les données sensibles doivent être protégées par des mécanismes de sécurité appropriés et une gestion rigoureuse des droits. La perte ou compromission d'un moyen d'accès doit pouvoir entraîner suspension ou révocation sans effacer l'historique.

18. AP Ledger et minimisation

Lorsque AP Ledger est utilisé, il doit privilégier empreintes, références ou preuves minimales plutôt que le contenu médical en clair. L'ancrage doit renforcer l'intégrité sans créer une exposition irréversible de données de santé.

19. Critères d'acceptation

Le modèle est acceptable si l'identité directe est minimisée, si les partages sont gouvernés et attribuables, si l'accès d'urgence est exceptionnel et auditable, si les divergences inter-systèmes restent visibles et si aucune couche publique ou Ledger n'expose le contenu médical personnel.

20. Conclusion

Identité numérique, partage sécurisé, interopérabilité, audit et souveraineté forment l'infrastructure de confiance de l'application Santé. La priorité est de rendre les preuves vérifiables tout en réduisant au minimum la circulation et l'exposition des données médicales elles-mêmes.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 6 — SANTÉ

CHAPITRE 5 — GOUVERNANCE DES DONNÉES DE SANTÉ, QUALITÉ DOCUMENTAIRE, CORRECTIONS, ALERTES, CYBERSÉCURITÉ, RESPONSABILITÉ ET AUDIT DE CONFORMITÉ

1. Objet du chapitre

Ce chapitre définit la gouvernance de confiance de l'application Santé. Il organise qualité documentaire, corrections, alertes, responsabilités, sécurité, audit et gestion des incidents afin que la provenance d'une donnée de santé reste vérifiable sans confondre intégrité technique et validité clinique.

2. Gouvernance des responsabilités

Personne concernée, professionnels, établissements, laboratoires, pharmacies, opérateurs techniques et autres acteurs doivent disposer de responsabilités distinctes. Authenticity Plus© doit conserver l' attribution de chaque événement sans absorber les responsabilités professionnelles ou institutionnelles.

3. Qualité documentaire

Un document doit pouvoir être associé à son auteur ou système source, sa date, son type, sa version et son statut lorsque disponibles. Une donnée complète techniquement n'est pas nécessairement complète médicalement.

4. Donnée déclarée et donnée vérifiée

Le système doit distinguer les informations déclarées, importées, signées, vérifiées ou issues d'un système compétent. Un niveau de confiance technique ne doit pas être présenté comme validation clinique.

5. Corrections

Une erreur documentaire peut être corrigée par un acteur autorisé selon le processus applicable. La correction doit préserver la relation avec la version antérieure et l'identité de l'auteur de la modification.

6. Addendum et complément

Lorsqu'une information nouvelle complète un document existant sans le remplacer, elle doit pouvoir être enregistrée comme addendum ou élément lié. Cette distinction évite de réécrire silencieusement l' historique.

7. Contestation

La personne concernée ou un acteur habilité peut, lorsque le cadre le prévoit, signaler une information contestée. Le statut de contestation doit rester distinct d'une correction médicale ou administrative effectivement validée.

8. Divergences entre sources

Lorsque deux systèmes ou professionnels produisent des informations divergentes, AP doit préserver les deux sources et leur chronologie. Il ne doit pas choisir automatiquement quelle information est médicalement correcte.

9. Alertes documentaires

Une incohérence d'identité, de version, de signature, de chronologie ou de transmission peut déclencher une alerte technique. Celle-ci doit préciser ce qui est incohérent sans se transformer en alerte médicale si aucune autorité clinique ne l'a qualifiée ainsi.

10. Alertes externes

Une alerte provenant d'un établissement, d'un laboratoire, d'un fabricant, d'une autorité ou d'un autre système peut être corrélée au dossier ou aux objets concernés. Sa source et sa portée doivent être explicites.

11. Incident de sécurité

Accès non autorisé, compromission de compte, extraction anormale, altération ou autre événement de sécurité doit pouvoir être enregistré et investigué selon les responsabilités applicables.

12. Révocation des accès

Lorsqu'un compte, rôle, délégation ou moyen d'authentification est compromis ou n'est plus valable, ses capacités doivent pouvoir être suspendues ou révoquées sans effacer les actions antérieures.

13. Journal d'audit

Consultations sensibles, créations, corrections, signatures, transmissions, exports, changements de droits et accès d'urgence doivent produire une piste d'audit proportionnée à leur criticité.

14. Détection des usages anormaux

Des règles peuvent signaler des volumes d'accès inhabituels, des consultations hors contexte ou d' autres comportements atypiques. Un signal technique doit déclencher une investigation et non une accusation automatique.

15. Responsabilité et non-substitution

AP fournit des mécanismes de preuve, d'attribution et de contrôle. Les diagnostics, prescriptions, décisions thérapeutiques, interprétations de résultats et responsabilités professionnelles restent exclusivement dans les domaines compétents.

16. Conservation et suppression

Les durées de conservation, archivages, restrictions et suppressions doivent suivre le cadre applicable et les finalités. Une exigence de traçabilité ne doit pas être utilisée comme justification pour conserver indéfiniment toutes les données médicales.

17. AP Ledger et preuves minimales

Les empreintes de documents, consentements, signatures ou événements critiques peuvent être ancrées lorsque prévu. Les contenus médicaux et identifiants directs doivent rester hors du Ledger lorsque leur inscription créerait une exposition excessive ou irréversible.

18. Audit de conformité

Les contrôles doivent permettre de vérifier attribution des accès, respect des rôles, versionnement, traitement des corrections, usage des accès d'urgence, protection des données et fonctionnement des mécanismes de preuve.

19. Critères d'acceptation

Le modèle est acceptable si corrections et contestations restent historisées, si les divergences ne sont pas fusionnées silencieusement, si les alertes techniques restent distinctes des conclusions médicales, si les accès sont révocables et auditables, et si la conservation des données reste proportionnée.

20. Conclusion

La gouvernance des données de santé exige davantage que l'intégrité cryptographique : elle impose attribution, qualité documentaire, contrôle des accès, capacité de correction, sécurité, audit et respect des responsabilités. Authenticity Plus© fournit cette infrastructure de confiance sans devenir arbitre clinique du contenu médical.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 6 — SANTÉ

CHAPITRE 6 — SYNTHÈSE FONCTIONNELLE, CRITÈRES D'ACCEPTATION ET CLÔTURE DE L'APPLICATION SANTÉ

1. Objet du chapitre

Ce chapitre clôt le Point 6 — Santé. Il consolide identité protégée, professionnels et établissements, parcours de soins, documents, examens, analyses, imagerie, prescriptions documentaires, médicaments et dispositifs associés, consentements, partage sécurisé, interopérabilité, audit et gouvernance.

2. Mission consolidée

L'application Santé fournit une infrastructure de confiance pour vérifier provenance, intégrité, chronologie et accès aux informations de santé. Elle ne remplace ni le dossier médical réglementé, ni le jugement clinique, ni les responsabilités des professionnels et établissements.

3. Identité protégée

La personne concernée doit pouvoir être reliée à son parcours sans exposition publique de son identité ou de ses informations médicales. Identifiants directs, pseudonymes et preuves doivent être séparés selon les finalités.

4. Professionnels et établissements

Chaque document ou événement doit rester attribuable au professionnel, à l'établissement ou au système source concerné. AP ne crée pas lui-même une qualification, spécialité ou habilitation professionnelle.

5. Parcours et épisodes

Consultations, admissions, actes et autres événements peuvent être regroupés en épisodes ou parcours. Cette organisation soutient la continuité documentaire sans produire une interprétation clinique automatique.

6. Examens, prélèvements et analyses

Demandes, prélèvements, chaînes de possession, analyses et résultats doivent conserver leurs relations, auteurs et versions. Un résultat d'échantillon reste limité à sa portée et à son contexte.

7. Imagerie et comptes rendus

Les examens d’imagerie et leurs comptes rendus peuvent être corrélés avec leurs sources et versions. La plateforme protège la provenance documentaire mais ne réalise pas l’interprétation diagnostique.

8. Prescriptions documentaires

Les prescriptions sont représentées comme documents attribués à des professionnels habilités. AP peut vérifier auteur, intégrité et version sans prescrire, modifier un traitement ou recommander un médicament.

9. Continuité Santé–Pharmacie

Lorsque les droits et systèmes le permettent, une prescription ou dispensation peut être corrélée aux références pharmaceutiques pertinentes. Les domaines Santé et Pharmacie restent séparés dans leurs responsabilités et niveaux d’accès.

10. Dispositifs médicaux

Dispositifs, implants et consommables pertinents peuvent être reliés aux actes et événements autorisés. Leur traçabilité soutient notamment les alertes et rappels sans produire d’évaluation clinique.

11. Consentements et autorisations

Consentements, bases d’accès, délégations et représentations doivent conserver leur portée, leur période et leur statut. Une autorisation limitée ne doit jamais devenir un accès général permanent.

12. Partage sécurisé

Tout partage sensible doit être gouverné par le rôle, la finalité, le contexte et les droits applicables. Les transmissions doivent préserver confidentialité, intégrité, source et version.

13. Accès d’urgence

Lorsqu’il existe, l’accès exceptionnel d’urgence doit être limité, justifié, journalisé et contrôlé a posteriori. Il ne doit pas devenir un moyen ordinaire de contourner les autorisations.

14. Interopérabilité et divergences

Les données importées doivent conserver leur système source. En cas de divergence entre sources, AP préserve les versions et ne choisit pas automatiquement quelle information est médicalement correcte.

15. Corrections et contestations

Corrections, addenda, remplacements et contestations doivent être historisés. Une modification critique ne doit pas effacer silencieusement la donnée antérieure lorsqu’elle a participé au parcours.

16. Cybersécurité et audit

Accès sensibles, exports, modifications, signatures, transmissions, changements de droits et incidents doivent être auditables. Les moyens d'accès compromis doivent pouvoir être suspendus ou révoqués sans perte de l'historique.

17. AP Ledger et souveraineté

Lorsque AP Ledger est utilisé, les preuves doivent privilégier empreintes et références minimales. Les données médicales en clair et identifiants directs doivent rester hors des couches publiques ou irréversibles, avec respect des exigences de souveraineté et localisation.

18. Critère d'acceptation — provenance

Chaque information critique doit pouvoir être reliée à son auteur ou système source, sa date, sa version et son statut. Une preuve d'intégrité ne doit jamais être présentée comme validation du contenu clinique.

19. Critère d'acceptation — confidentialité et responsabilité

Les accès doivent suivre le moindre privilège, les données personnelles doivent être minimisées, les accès d'urgence doivent être auditables et aucune fonction AP ne doit être présentée comme diagnostic, prescription, interprétation médicale ou décision thérapeutique.

20. Clôture du Point 6 — Santé

Le Point 6 — Santé est désormais fonctionnellement défini : identité protégée, professionnels, établissements, parcours, consultations, actes, examens, analyses, imagerie, prescriptions documentaires, médicaments et dispositifs associés, consentements, partage, interopérabilité, corrections, cybersécurité, audit, AP Ledger et souveraineté. Cette architecture est prête à s'articuler avec le Point 7 — Automobile.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 7 — AUTOMOBILE

CHAPITRE 1 — MISSION, PÉRIMÈTRE, IDENTITÉ DU VÉHICULE ET PRINCIPES FONDATEURS DE L'APPLICATION AUTOMOBILE

1. Objet du chapitre

Le Point 7 — Automobile transpose Authenticity Plus© / Deep Authenticity© au cycle de vie du véhicule. Il organise l'identité persistante, la provenance documentaire, les événements de fabrication, de circulation, de propriété, d'entretien, de réparation, de contrôle et de transaction afin de constituer un passeport automobile vérifiable.

2. Mission sectorielle

L'application Automobile vise à rendre l'historique d'un véhicule plus vérifiable sans se substituer aux constructeurs, autorités d'immatriculation, organismes de contrôle, assureurs, réparateurs ou autres acteurs compétents. Chaque information conserve son auteur, son système source et son niveau de preuve.

3. Identité persistante du véhicule

Le véhicule doit disposer d'une identité stable pendant son cycle de vie. Le VIN ou tout identifiant applicable peut constituer une référence majeure, mais le modèle doit permettre de conserver les autres identifiants et documents nécessaires sans confondre identité physique et immatriculation.

4. VIN et contrôles de cohérence

Le VIN peut être corrélé au constructeur, au modèle, au site ou à d'autres références disponibles. Duplications, formats incompatibles ou associations contradictoires peuvent produire des signaux d' investigation sans constituer automatiquement une preuve de fraude.

5. Constructeur, marque et modèle

Constructeur, marque, modèle, version, motorisation ou autres caractéristiques peuvent être rattachés à l'identité du véhicule selon les données disponibles. Une information commerciale ne doit pas être présentée comme donnée certifiée lorsqu'elle ne provient pas d'une source compétente.

6. Site et événement de fabrication

Lorsque les données existent, le véhicule peut être relié à un site, une période ou un événement de fabrication. Cette relation constitue le début de sa généalogie industrielle et peut s'articuler avec l' application Industrie.

7. Composants critiques documentés

Moteur, batterie de traction, transmission, modules électroniques ou autres composants significatifs peuvent être reliés au véhicule lorsqu'un identifiant ou une preuve existe. Le remplacement ultérieur doit préserver la relation avec l'ancien et le nouveau composant.

8. Mise en circulation

La première mise en circulation ou un événement équivalent peut être référencé avec sa date, son territoire et sa source. Cette date reste distincte de la date de fabrication, de vente ou de livraison.

9. Immatriculation

Une immatriculation est un attribut administratif susceptible d'évoluer. Un changement de plaque, de territoire ou de certificat ne doit pas créer un nouveau véhicule dans le passeport.

10. Propriété et détention

Propriété juridique, détention, conducteur ou utilisateur peuvent être des notions différentes. Les événements de transfert doivent être représentés selon les données et droits disponibles, avec une protection appropriée des données personnelles.

11. Kilométrage documenté

Les relevés de kilométrage peuvent provenir d'un atelier, d'un contrôle, d'un système embarqué, d'une transaction ou d'une autre source autorisée. Chaque valeur doit conserver date et provenance ; AP ne doit pas transformer une déclaration isolée en kilométrage certifié.

12. Entretien

Les opérations d'entretien peuvent être reliées au véhicule, à l'atelier, à la date, au kilométrage documenté et aux pièces concernées lorsque disponibles. L'enregistrement d'un entretien n'implique pas automatiquement une garantie sur sa qualité technique.

13. Réparations et pièces remplacées

Une réparation peut identifier les composants retirés, réparés ou installés. La provenance des pièces peut être corrélée à l'application Industrie, à la Seconde main ou à d'autres domaines pertinents lorsque les preuves existent.

14. Contrôles techniques et inspections

Les contrôles ou inspections officiels ou privés peuvent être référencés avec leur organisme, date, résultat documentaire et période de validité. Authenticity Plus© conserve la preuve sans se substituer à l'organisme qui réalise ou valide le contrôle.

15. Rappels constructeur

Un rappel ou une campagne technique peut être corrélé au modèle, au VIN ou à un ensemble de véhicules. L'exécution de l'intervention doit rester distincte de l'émission initiale du rappel.

16. Sinistres documentaires

Des références relatives à un sinistre, une expertise ou une réparation peuvent être associées au véhicule lorsque leur partage est autorisé. AP doit distinguer l'existence d'un document de toute conclusion juridique, assurantielle ou technique qui relève de l'acteur compétent.

17. Transaction et seconde main

Lors d'une revente, le passeport peut fournir un historique vérifiable des événements autorisés et faciliter la continuité vers l'application Seconde main. Les données personnelles des anciens propriétaires ne doivent pas être exposées inutilement.

18. Alertes de cohérence et fraude présumée

VIN dupliqué, kilométrages chronologiquement incompatibles, documents contradictoires, pièces non cohérentes ou événements impossibles peuvent déclencher des alertes explicables. Une alerte constitue un signal d'investigation et non une accusation automatique.

19. Critères d'acceptation

Le modèle est acceptable si l'identité du véhicule persiste malgré les changements d'immatriculation ou de propriétaire, si chaque kilométrage conserve sa source, si les remplacements de composants restent historisés, si les documents sont attribuables et si les données personnelles sont protégées.

20. Conclusion

L'application Automobile établit un passeport de cycle de vie centré sur l'identité persistante du véhicule, la provenance des événements et la continuité documentaire. Cette fondation prépare les chapitres consacrés à la fabrication détaillée, à l'entretien, aux pièces, aux contrôles, aux sinistres, aux rappels, à la revente et à la lutte contre la fraude.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 7 — AUTOMOBILE

CHAPITRE 2 — FABRICATION, COMPOSANTS, VIN, CONFIGURATION D'ORIGINE, BATTERIE, PIÈCES CRITIQUES ET GÉNÉALOGIE INDUSTRIELLE DU VÉHICULE

1. Objet du chapitre

Ce chapitre décrit la généalogie industrielle du véhicule depuis sa configuration de référence jusqu'à son assemblage final. Il organise les relations entre VIN, site de fabrication, composants identifiés, lots de pièces, batterie, groupes motopropulseurs et documents de production disponibles.

2. Configuration de référence

Le véhicule peut être relié à une configuration définissant modèle, version, motorisation, transmission, équipements ou autres caractéristiques pertinentes. La configuration documentaire doit rester distincte de l'état réel du véhicule après modifications ultérieures.

3. Attribution du VIN

Lorsque les données sont disponibles, l'attribution du VIN peut être reliée à un événement ou système constructeur. Le passeport conserve cette provenance sans devenir lui-même l'autorité d'émission du VIN.

4. Site d'assemblage

Le véhicule peut être rattaché au site où son assemblage final ou une opération majeure a été réalisé. Les rôles des différents sites doivent rester distingués lorsqu'un véhicule traverse plusieurs installations.

5. Ordre ou dossier de production

Un ordre, dossier ou autre référence de fabrication peut relier la configuration prévue aux composants et opérations effectivement enregistrés. AP conserve la relation documentaire sans remplacer les systèmes industriels du constructeur.

6. Composants sérialisés

Moteur, transmission, batterie, module électronique ou autre composant critique peut disposer d'un numéro de série ou identifiant propre. Ces identités doivent rester distinctes du VIN tout en étant reliées au véhicule concerné.

7. Lots de composants

Lorsque les pièces ne sont pas suivies individuellement, leur lot peut être rattaché à la fabrication du véhicule. La granularité de la généalogie doit rester celle des données réellement disponibles.

8. Origine des pièces

Fabricant, fournisseur, site, lot ou autres références d'origine peuvent être associés aux composants lorsque les preuves existent. Une relation d'approvisionnement ne doit pas être présentée comme preuve de fabrication par le fournisseur commercial.

9. Moteur thermique ou groupe motopropulseur

Pour les véhicules concernés, l'identité du moteur ou du groupe motopropulseur peut être enregistrée et historisée. Un remplacement ultérieur doit préserver la relation avec le composant d'origine et le composant installé.

10. Batterie de traction

Pour un véhicule électrifié, la batterie de traction peut disposer d'un passeport ou d'identifiants propres reliés au véhicule. Fabricant, site, lot, série ou autres références peuvent être corrélés selon les données autorisées.

11. Modules et sous-composants de batterie

Lorsque la granularité le permet, modules ou sous-ensembles peuvent être reliés à la batterie principale. Le modèle ne doit pas inventer une traçabilité unitaire si les preuves ne portent que sur un lot ou un ensemble.

12. Électronique et calculateurs

Les unités électroniques significatives peuvent être identifiées par référence matérielle, série ou version disponible. Les évolutions logicielles ultérieures doivent rester distinguées du remplacement physique d'un calculateur.

13. Logiciels et configuration embarquée

Une version logicielle ou configuration électronique peut être associée à une date ou un événement de production. La plateforme documente la provenance de la version sans évaluer elle-même la sécurité fonctionnelle du logiciel.

14. Contrôles de fin de ligne

Les références de contrôles de production ou de fin de ligne peuvent être rattachées au véhicule avec leur site, date et statut documentaire. AP ne se substitue pas au constructeur pour déclarer la conformité du véhicule.

15. Modification avant livraison

Une modification, campagne, correction ou remplacement intervenant entre production et livraison doit pouvoir être historisé. La configuration de sortie peut ainsi être distinguée de la configuration initialement planifiée.

16. Généalogie ascendante

À partir du VIN, le système doit pouvoir remonter vers les composants sérialisés, lots de pièces, sites et documents disponibles selon la granularité réellement enregistrée.

17. Généalogie descendante

À partir d'un lot de composant ou d'une référence critique, le système doit pouvoir rechercher les véhicules enregistrés dans lesquels cette pièce ou ce lot a été utilisé, afin de soutenir investigations et campagnes ciblées.

18. Anomalies de généalogie

Composant dupliqué, série incompatible, lot hors période, configuration contradictoire ou relation impossible peut déclencher un signal. L'anomalie doit rester explicable et ne constitue pas automatiquement une preuve de fraude ou de défaut.

19. Critères d'acceptation

Le modèle est acceptable si VIN et composants restent des identités distinctes, si la configuration d'origine peut être comparée à l'état ultérieur, si les remplacements ne détruisent pas la généalogie, et si la traçabilité fonctionne du véhicule vers les composants comme des composants vers les véhicules.

20. Conclusion

La généalogie industrielle donne au passeport automobile une profondeur supérieure à un simple historique administratif. En reliant VIN, configuration, sites, composants, lots, batterie et contrôles documentaires, Authenticity Plus© prépare la traçabilité complète des entretiens, réparations, rappels et transactions futures.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 7 — AUTOMOBILE

CHAPITRE 3 — KILOMÉTRAGE, ENTRETIEN, RÉPARATIONS, PIÈCES DE REMPLACEMENT, CONTRÔLES TECHNIQUES, MODIFICATIONS ET HISTORIQUE DE MAINTENANCE

1. Objet du chapitre

Ce chapitre structure l'historique d'usage et de maintenance du véhicule après sa mise en circulation. Il organise les relevés de kilométrage, entretiens, réparations, remplacements de pièces, contrôles techniques et modifications afin de préserver une chronologie vérifiable du cycle de vie.

2. Relevé de kilométrage

Chaque kilométrage enregistré doit conserver sa valeur, sa date et sa source. Atelier, contrôle technique, système embarqué, transaction, expertise ou autre acteur peuvent fournir des relevés dont le niveau de preuve doit rester explicite.

3. Chronologie du kilométrage

Les relevés successifs peuvent être comparés afin d'identifier des évolutions incohérentes. Une baisse ou rupture de chronologie produit un signal d'investigation mais ne constitue pas automatiquement une preuve de manipulation frauduleuse.

4. Sources multiples

Lorsque plusieurs sources fournissent des kilométrages différents à une même période, le système doit préserver chaque valeur et sa provenance. Il ne doit pas fusionner silencieusement les données ni choisir arbitrairement la valeur correcte.

5. Entretien programmé

Les opérations d'entretien périodique peuvent être rattachées au véhicule avec date, kilométrage, atelier et références disponibles. La plateforme documente leur réalisation déclarée ou vérifiée selon la source sans certifier elle-même leur qualité technique.

6. Entretien non programmé

Une intervention déclenchée par une panne, une anomalie ou une autre circonstance peut être enregistrée séparément. Motif déclaré, diagnostic professionnel, intervention et résultat documentaire doivent rester des éléments distincts.

7. Atelier et intervenant

L’identité de l’atelier, du réseau ou du professionnel peut être associée à l’intervention lorsque disponible. Authenticity Plus© conserve l’attribution sans créer lui-même une qualification ou certification professionnelle.

8. Ordre de réparation

Un ordre, devis, facture, rapport ou autre document peut être relié à l’événement de maintenance. Les versions, corrections et pièces justificatives doivent rester attribuables à leur émetteur.

9. Pièces de remplacement

Toute pièce significative remplacée peut être reliée à sa référence, son fabricant, son lot ou son numéro de série lorsque disponibles. La pièce retirée et la pièce installée doivent rester distinguables.

10. Pièces neuves, reconditionnées ou de seconde main

Le statut déclaré d’une pièce — neuve, reconditionnée, remanufacturée ou de seconde main — peut être conservé avec sa source. Lorsque pertinent, la provenance peut s’articuler avec Industrie ou Seconde main.

11. Composants critiques

Moteur, batterie, transmission, calculateurs, systèmes de sécurité ou autres composants critiques doivent bénéficier d’un historique renforcé lorsqu’ils sont remplacés ou modifiés. L’identité du véhicule reste stable malgré ces changements.

12. Batterie et état documentaire

Pour les véhicules électrifiés, interventions, remplacement de batterie ou rapports disponibles peuvent être reliés au passeport. AP conserve la provenance des mesures ou rapports sans produire lui-même une évaluation technique de l’état de santé de la batterie.

13. Logiciels et mises à jour

Les mises à jour logicielles documentées peuvent être enregistrées avec version, date, émetteur ou atelier. Une mise à jour logicielle doit rester distincte d’un remplacement matériel et d’une modification non autorisée.

14. Modifications du véhicule

Transformation, ajout d’équipement, changement de motorisation, modification de carrosserie ou autre évolution significative peut être historisée lorsqu’elle est documentée. Configuration d’origine et état modifié doivent rester comparables.

15. Contrôle technique

Chaque contrôle technique ou inspection équivalente peut être relié à l’organisme, à la date, au kilométrage, au résultat documentaire et à sa période de validité. AP ne se substitue pas à l’organisme de contrôle.

16. Défauts et contre-visites

Les défauts ou observations figurant dans un rapport peuvent être référencés avec leur source. Une contre-visite ou contrôle ultérieur doit rester un événement distinct afin de préserver la chronologie.

17. Preuves de maintenance

Factures, rapports, signatures, références de pièces ou autres preuves peuvent renforcer l'historique. Leur intégrité peut être vérifiée sans que la présence d'un document suffise à certifier la qualité de l' intervention.

18. Alertes de cohérence

Kilométrage décroissant, pièce installée avant sa fabrication documentée, entretien daté hors période, composant sérialisé présent sur plusieurs véhicules ou documents contradictoires peuvent déclencher des signaux explicables.

19. Critères d'acceptation

Le modèle est acceptable si chaque kilométrage conserve sa source, si les interventions sont attribuables, si les pièces retirées et installées restent historisées, si les modifications ne réécrivent pas la configuration d'origine et si les contrôles techniques restent liés à leur organisme émetteur.

20. Conclusion

Kilométrage, maintenance, réparations, pièces et contrôles constituent le cœur de l'historique d'usage du véhicule. Authenticity Plus© transforme ces événements dispersés en une chronologie de provenance vérifiable, particulièrement utile pour les rappels, expertises, transactions et marchés de seconde main.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 7 — AUTOMOBILE

CHAPITRE 4 — SINISTRES, EXPERTISES, ASSURANCES, RAPPELS CONSTRUCTEUR, RÉPARATIONS STRUCTURELLES, SÉCURITÉ ET TRAÇABILITÉ POST-ACCIDENT

1. Objet du chapitre

Ce chapitre organise la provenance documentaire des événements exceptionnels susceptibles d' affecter l'historique, la sécurité ou la valeur d'un véhicule : sinistres, expertises, réparations structurelles, événements assurantiels, rappels constructeur et campagnes techniques. Il distingue strictement l'existence d'une preuve de toute conclusion juridique, assurantielle ou technique.

2. Événement de sinistre

Un sinistre peut être référencé avec date, source, territoire et identifiant de dossier lorsque le partage est autorisé. Le passeport ne doit pas inventer les circonstances ni qualifier la responsabilité des personnes impliquées.

3. Déclaration et source

Une déclaration provenant d'un propriétaire, d'un assureur, d'une autorité, d'un atelier ou d'un autre acteur doit conserver son auteur et son statut. Une déclaration initiale reste distincte d'un fait établi par expertise ou décision compétente.

4. Expertise

Un rapport d'expertise peut être rattaché au véhicule avec expert ou organisme, date, version et références disponibles. Authenticity Plus© garantit la provenance du document sans se substituer à l' expert pour ses conclusions.

5. Photographies et preuves associées

Photographies, rapports, constats ou autres éléments peuvent être référencés avec leur source et leur date. Les métadonnées et droits d'accès doivent être gouvernés afin d'éviter l'exposition inutile de personnes ou d'informations sensibles.

6. Dommages documentés

Les zones ou composants mentionnés comme endommagés peuvent être reliés au dossier d' expertise. AP doit distinguer le dommage déclaré, le dommage constaté et la conclusion technique formelle lorsque ces niveaux existent.

7. Réparation post-sinistre

Une réparation consécutive à un sinistre doit pouvoir être reliée au dossier correspondant, à l'atelier, aux opérations réalisées et aux pièces remplacées lorsque les preuves sont disponibles.

8. Réparation structurelle

Les interventions portant sur châssis, structure, éléments de sécurité ou autres composants critiques doivent bénéficier d'une traçabilité renforcée. Leur présence dans le passeport ne constitue pas à elle seule une évaluation de la sécurité actuelle du véhicule.

9. Pièces remplacées après accident

Les pièces retirées et installées peuvent être reliées à leur référence, provenance, lot ou numéro de série. Les pièces de seconde main ou reconditionnées doivent conserver leur statut déclaré et leur origine lorsque disponible.

10. Contrôle après réparation

Un contrôle, alignement, calibration, inspection ou autre vérification post-réparation peut être référencé avec son émetteur et son résultat documentaire. AP ne se substitue pas au professionnel qui déclare le véhicule conforme ou apte.

11. Événements assurantiels

Référence de dossier, prise en charge, expertise ou autre événement assurantiel peut être corrélé au véhicule lorsque cela est autorisé. Les montants, responsabilités et données personnelles doivent suivre des règles de confidentialité appropriées.

12. Statut économique ou administratif

Lorsqu'un véhicule reçoit un statut particulier après un sinistre selon le cadre applicable, celui-ci doit conserver son émetteur, sa date, son territoire et son évolution. AP ne crée pas lui-même ce statut.

13. Rappel constructeur

Un rappel ou une campagne de sécurité peut être relié à une population de VIN, un composant ou une configuration. L'émission du rappel, la notification et l'exécution de l'intervention doivent rester des événements distincts.

14. Vérification de l'éligibilité

La correspondance d'un VIN avec une campagne peut être vérifiée contre une source disponible. Le résultat doit préciser la source et la date afin d'éviter de présenter une information ancienne comme statut actuel.

15. Exécution d'une campagne

Une intervention de rappel réalisée peut être enregistrée avec atelier, date, kilométrage et référence. Une campagne ouverte ne doit être marquée comme exécutée qu'à partir d'une preuve appropriée.

16. Rappels liés aux composants

Grâce à la généalogie industrielle, un lot de batterie, d'airbag, de module électronique ou autre composant peut être utilisé pour identifier les véhicules potentiellement concernés par une investigation ou campagne.

17. Alertes de sécurité documentaires

Une incohérence entre rappel, composant, réparation, contrôle ou statut peut produire un signal. Le système doit expliquer la contradiction sans générer automatiquement une conclusion sur la sécurité routière du véhicule.

18. Traçabilité post-accident et revente

Lors d'une transaction ultérieure, les événements partageables relatifs aux sinistres et réparations peuvent contribuer à un historique plus transparent. Les données personnelles et les éléments non autorisés doivent rester protégés.

19. Critères d'acceptation

Le modèle est acceptable si déclarations et expertises restent distinguées, si les réparations post-sinistre sont reliées aux preuves disponibles, si les rappels conservent source et statut, si leur exécution est attribuable et si aucune donnée ne produit automatiquement une conclusion juridique ou technique.

20. Conclusion

Sinistres, expertises, réparations structurelles et rappels sont des événements majeurs du cycle de vie automobile. Leur intégration au passeport Authenticity Plus© renforce la transparence et la continuité de preuve, particulièrement lors des contrôles, expertises et transactions de seconde main.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 7 — AUTOMOBILE

CHAPITRE 5 — PROPRIÉTÉ, IMMATRICULATION, IMPORT-EXPORT, VENTE, SECONDE MAIN, VALORISATION DOCUMENTAIRE, FRAUDE ET AUDIT DU PASSEPORT AUTOMOBILE

1. Objet du chapitre

Ce chapitre organise les événements administratifs et transactionnels du véhicule : propriété, détention, immatriculation, importation, exportation, vente et revente. Il définit également les mécanismes de valorisation documentaire, d'alerte, d'investigation et d'audit qui renforcent la confiance dans le passeport automobile.

2. Propriété et détenteur

Le propriétaire juridique, le détenteur, l'utilisateur et le conducteur peuvent être des acteurs différents. Le passeport doit préserver ces distinctions et limiter l'exposition des données personnelles aux seules finalités autorisées.

3. Transfert de propriété

Une vente, donation ou autre transfert peut être enregistré avec date, parties ou références documentaires selon les droits applicables. AP conserve la preuve de l'événement sans se substituer aux formalités légales de transfert.

4. Historique des propriétaires

La continuité de propriété peut être représentée sans rendre publiques les identités des propriétaires successifs. Pour une consultation de seconde main, des indicateurs ou preuves minimisées peuvent suffire à établir la continuité.

5. Immatriculations successives

Plaques, certificats ou autres références administratives peuvent évoluer au cours de la vie du véhicule. Chaque immatriculation doit conserver territoire, période et source sans modifier l'identité persistante du véhicule.

6. Changement de territoire

Un changement de région ou de pays peut produire de nouvelles références administratives. Le système doit conserver la continuité entre ces références lorsque les preuves permettent de relier le même véhicule.

7. Importation

Une importation peut être reliée à des documents douaniers, administratifs, techniques ou logistiques lorsque leur partage est autorisé. Leur présence dans AP ne remplace pas la décision des autorités compétentes.

8. Exportation

Une exportation ou sortie de territoire peut être historisée avec sa date et ses références. L'exportation ne doit pas clôturer artificiellement le passeport si le véhicule poursuit son cycle de vie dans un autre territoire.

9. Continuité transfrontalière

Le passeport doit pouvoir conserver une identité automobile stable malgré les changements de juridiction, d'immatriculation ou de langue documentaire. Les divergences entre référentiels doivent rester visibles et attribuables.

10. Mise en vente

Une mise en vente peut présenter les éléments autorisés du passeport : identité du véhicule, kilométrages documentés, maintenance, contrôles, rappels et autres événements partageables. Les déclarations commerciales doivent rester distinguées des preuves vérifiées.

11. Transaction de seconde main

La vente d'occasion peut être corrélée à l'application Seconde main afin de préserver la continuité du passeport après la transaction. Le nouveau propriétaire reçoit la continuité historique autorisée, non les données personnelles inutiles des précédents propriétaires.

12. Valorisation documentaire

Un historique plus complet, cohérent et vérifiable peut renforcer la transparence d'une transaction. Authenticity Plus© peut produire des indicateurs de complétude ou de provenance, mais ne doit pas imposer lui-même une valeur marchande au véhicule.

13. Indice de complétude

Un indicateur peut signaler la présence ou l'absence de catégories de preuves telles que maintenance, kilométrage, contrôles ou rappels. Cet indice doit mesurer la couverture documentaire et non prétendre mesurer l'état mécanique réel.

14. Fraude au kilométrage présumée

Des relevés chronologiquement incompatibles peuvent déclencher un signal spécifique. L' investigation doit conserver toutes les valeurs et sources concernées ; AP ne doit pas supprimer la donnée discordante ni prononcer automatiquement une fraude.

15. Fraude d'identité présumée

VIN dupliqué, documents associés à plusieurs véhicules, incohérences entre caractéristiques physiques et références disponibles ou réutilisation incompatible d'identifiants peuvent produire une alerte d'identité.

16. Dissimulation d'historique

Une rupture documentaire, une revente sans continuité ou l'absence d'un événement attendu peut être signalée comme manque d'information lorsque pertinent. L'absence de donnée ne doit pas être présentée automatiquement comme preuve de dissimulation volontaire.

17. Dossier d'investigation

Une investigation peut regrouper VIN, immatriculations, kilométrages, pièces, réparations, contrôles, sinistres, documents et transactions. Chaque élément doit conserver sa provenance, sa date, son statut et son niveau de preuve.

18. Audit et AP Ledger

Transferts critiques, changements d'identité administrative, documents, relevés, réparations majeures et autres preuves sélectionnées peuvent être audités. AP Ledger peut renforcer intégrité et antériorité par des empreintes lorsque l'architecture globale le prévoit.

19. Critères d'acceptation

Le modèle est acceptable si le véhicule conserve une identité stable à travers propriétaires et territoires, si les données personnelles sont minimisées, si les transactions distinguent déclarations et preuves, si les indices documentaires ne sont pas présentés comme évaluations mécaniques et si les alertes de fraude restent investigables et non automatiques.

20. Conclusion

Propriété, immatriculation, mobilité transfrontalière et seconde main prolongent le passeport automobile jusqu'au marché. La valeur d'Authenticity Plus© réside dans la continuité vérifiable de l' historique et dans la capacité à révéler les incohérences sans transformer un système de preuve en autorité administrative, expert mécanique ou arbitre de la valeur marchande.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 7 — AUTOMOBILE

CHAPITRE 6 — SYNTHÈSE FONCTIONNELLE, CRITÈRES D'ACCEPTATION ET CLÔTURE DE L'APPLICATION AUTOMOBILE

1. Objet du chapitre

Ce chapitre clôt le Point 7 — Automobile. Il consolide l'identité persistante du véhicule, sa généalogie industrielle, ses composants, son kilométrage, sa maintenance, ses contrôles, ses sinistres, ses rappels, ses changements administratifs et ses transactions de seconde main.

2. Mission consolidée

L'application Automobile constitue un passeport de cycle de vie destiné à rendre l'historique d'un véhicule plus vérifiable. Elle relie des preuves provenant des constructeurs, ateliers, organismes de contrôle, autorités, assureurs et autres acteurs sans se substituer à leurs responsabilités.

3. Identité persistante

Le véhicule doit conserver une identité stable pendant tout son cycle de vie. VIN, immatriculation, propriété et localisation restent des notions distinctes ; un changement de plaque, de propriétaire ou de territoire ne crée pas un nouveau véhicule.

4. Fabrication et configuration d'origine

La configuration initiale, le site de fabrication, l'ordre de production et les contrôles disponibles peuvent constituer le socle industriel du passeport. Les modifications ultérieures doivent rester comparables à cet état d'origine.

5. Composants et généalogie

Moteur, batterie, transmission, électronique et autres composants critiques peuvent être reliés individuellement ou par lot selon les preuves disponibles. La généalogie doit fonctionner du VIN vers les composants et des composants vers les véhicules.

6. Batterie et électrification

Les véhicules électrifiés peuvent conserver des références spécifiques de batterie, modules et interventions. Les mesures ou rapports d'état restent attribués à leur source ; AP ne produit pas lui-même une évaluation technique de santé de la batterie.

7. Kilométrage

Chaque relevé doit conserver valeur, date et provenance. Les divergences ou diminutions chronologiques doivent rester visibles et produire, lorsque pertinent, un signal d'investigation plutôt qu' un verdict automatique.

8. Entretien et réparations

Les interventions doivent être reliées au véhicule, à l'atelier, à la date, au kilométrage et aux preuves disponibles. La présence d'un document d'entretien ne constitue pas une certification automatique de la qualité mécanique.

9. Pièces et remplacements

Pièces retirées et installées doivent pouvoir être distinguées. Les statuts neuf, reconditionné, remanufacturé ou seconde main peuvent être conservés avec leur source, et les composants critiques remplacés ne doivent pas effacer l'historique d'origine.

10. Logiciels et modifications

Mises à jour logicielles, transformations et modifications significatives peuvent être historisées. Une évolution logicielle reste distincte d'un remplacement matériel et la configuration d'origine demeure conservée.

11. Contrôles techniques

Contrôles, inspections, défauts et contre-visites doivent rester liés à leur organisme, leur date, leur kilométrage et leur statut documentaire. AP ne se substitue pas à l'organisme qui émet le résultat.

12. Sinistres et expertises

Déclarations, expertises, dommages documentés, réparations post-sinistre et contrôles ultérieurs doivent être distingués. La plateforme conserve la provenance sans décider de la responsabilité juridique ou de la sécurité actuelle du véhicule.

13. Rappels constructeur

Rappels et campagnes techniques peuvent être reliés au VIN, à une configuration ou à un lot de composant. Émission, éligibilité, notification et exécution doivent rester des événements séparés et attribuables.

14. Propriété et immatriculation

Les changements de propriétaire et d'immatriculation doivent préserver la continuité du passeport tout en minimisant les données personnelles. L'identité administrative ne doit jamais remplacer l' identité persistante du véhicule.

15. Import-export et continuité transfrontalière

Le passeport doit pouvoir suivre un véhicule entre territoires lorsque les preuves permettent d'établir la continuité. Les divergences de référentiels ou documents doivent être conservées plutôt que fusionnées silencieusement.

16. Seconde main et valorisation documentaire

Lors d'une revente, l'historique partageable peut renforcer la transparence. Les indicateurs de complétude mesurent la couverture documentaire et ne doivent pas être présentés comme estimation mécanique ou valeur marchande imposée par AP.

17. Fraudes présumées et investigation

VIN dupliqués, kilométrages incohérents, composants incompatibles, documents contradictoires ou ruptures d'historique peuvent déclencher des alertes. Toute qualification de fraude exige une investigation et, le cas échéant, une décision de l'acteur compétent.

18. Audit et AP Ledger

Événements critiques, documents, changements administratifs, kilométrages, réparations majeures et preuves sélectionnées doivent pouvoir être audités. AP Ledger peut renforcer intégrité et antériorité au moyen d'empreintes lorsque l'architecture globale le prévoit.

19. Critères d'acceptation

Le modèle est acceptable si l'identité persiste à travers tout le cycle de vie, si chaque preuve conserve sa source, si la généalogie industrielle et les remplacements sont reconstructibles, si les données personnelles sont minimisées, et si les alertes restent explicables sans conclusion automatique.

20. Clôture du Point 7 — Automobile

Le Point 7 — Automobile est désormais fonctionnellement défini : identité, VIN, fabrication, configuration, composants, batterie, kilométrage, entretien, réparations, pièces, logiciels, contrôles, sinistres, expertises, rappels, propriété, immatriculation, import-export, seconde main, fraude, audit et AP Ledger. Cette architecture est prête à s'articuler avec le Point 8 — Propriété intellectuelle.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 8 — PROPRIÉTÉ INTELLECTUELLE

CHAPITRE 1 — MISSION, PÉRIMÈTRE, IDENTITÉ DE LA CRÉATION, AUTEURS/TITULAIRES, ANTÉRIORITÉ ET PRINCIPES FONDATEURS

1. Objet du chapitre

Le Point 8 — Propriété intellectuelle transpose Authenticity Plus© / Deep Authenticity© à la provenance et à la chronologie des créations et actifs immatériels. Il organise l'identité de la création, ses versions, ses contributeurs, les revendications de titularité, les dépôts ou enregistrements disponibles, les droits d'exploitation et les preuves associées.

2. Mission sectorielle

L'application vise à renforcer la preuve documentaire autour de la création et de sa chaîne de droits. Elle ne se substitue ni aux offices de propriété intellectuelle, ni aux contrats, ni aux conseils juridiques, ni aux tribunaux compétents pour reconnaître, interpréter ou trancher un droit.

3. Identité de la création

Une œuvre, invention, marque, dessin, logiciel ou autre actif peut disposer d'une identité persistante dans le système. Cette identité doit rester distincte de ses fichiers, versions, dépôts, supports physiques ou exploitations commerciales.

4. Catégorie de propriété intellectuelle

Le modèle peut représenter plusieurs catégories d'actifs tout en conservant leurs différences. Les règles applicables au droit d'auteur, aux marques, brevets, dessins et modèles ou autres droits ne doivent pas être artificiellement fusionnées.

5. Auteur, créateur ou inventeur

Les personnes ayant participé à la création peuvent être reliées à l'actif avec leur rôle déclaré ou documenté. L'enregistrement d'une contribution ne constitue pas à lui seul une décision juridique sur la qualité d'auteur, d'inventeur ou de titulaire.

6. Création collective et contributions

Lorsque plusieurs personnes contribuent à un actif, leurs contributions, périodes ou versions peuvent être documentées selon les preuves disponibles. Le système doit éviter d'attribuer automatiquement l'ensemble de la création à un seul contributeur.

7. Titulaire déclaré

Une personne ou organisation peut être enregistrée comme titulaire déclaré ou comme partie revendiquant un droit. Cette information doit rester distincte d'un titre officiel, d'une cession contractuelle établie ou d'une décision judiciaire.

8. Preuve d'existence

Un fichier, document, dépôt technique ou autre élément peut servir à établir qu'un contenu existait à une date donnée. La preuve d'existence ne démontre pas automatiquement l'originalité, la titularité ou l'étendue juridique des droits.

9. Antériorité

Une chronologie de versions et preuves peut contribuer à documenter l'antériorité d'une création ou d' un élément. Authenticity Plus© doit présenter précisément ce qui est horodaté ou vérifié sans transformer l'antériorité technique en droit exclusif automatique.

10. Versionnement

Chaque évolution significative peut disposer d'une version ou empreinte distincte reliée à ses versions antérieures. Une nouvelle version ne doit pas effacer la preuve de l'état précédent.

11. Dérivations et œuvres liées

Une création dérivée, adaptation, traduction, fork logiciel ou autre actif lié peut référencer l'actif source lorsque cette relation est documentée. Le lien de dérivation ne constitue pas une autorisation juridique d'exploitation.

12. Dépôts et enregistrements

Les références de dépôt ou d'enregistrement auprès d'un office ou organisme peuvent être rattachées à l'actif avec territoire, date, numéro et statut disponibles. AP ne crée, ne renouvelle ni ne prolonge un titre officiel.

13. Territoires et portée

Les droits ou titres peuvent varier selon les territoires, catégories et périodes. Toute représentation doit conserver cette portée afin d'éviter qu'un droit limité soit présenté comme universel.

14. Licences

Une licence peut être référencée avec concédant, licencié, objet, territoire, durée et droits accordés lorsque les documents le permettent. La plateforme conserve la provenance contractuelle sans interpréter elle-même les clauses litigieuses.

15. Cessions et chaîne de titularité

Une cession ou transfert de droits peut être relié aux titulaires successifs et aux documents disponibles. La chaîne doit préserver l'historique et distinguer transfert déclaré, contrat signé, enregistrement officiel et décision compétente.

16. Exploitations autorisées

Une exploitation, publication, distribution ou utilisation peut être corrélée à une licence ou autorisation lorsque les preuves existent. L'absence de corrélation dans AP ne constitue pas automatiquement une preuve de contrefaçon.

17. AP Ledger

Des empreintes de versions, contrats, dépôts ou autres preuves sélectionnées peuvent être ancrées dans AP Ledger afin de renforcer intégrité et antériorité. Le contenu confidentiel peut rester hors Ledger, seule une preuve minimale étant ancrée.

18. Conflits et revendications concurrentes

Dates incompatibles, revendications concurrentes, licences contradictoires ou chaînes de titularité divergentes doivent rester visibles comme conflits documentaires. AP conserve les sources et ne tranche pas automatiquement le différend.

19. Critères d'acceptation

Le modèle est acceptable si identité, version, auteur, titulaire déclaré et titre officiel restent distingués ; si les preuves d'antériorité conservent leur portée ; si licences et cessions sont historisées ; et si aucun ancrage technique n'est présenté comme création automatique d'un droit juridique.

20. Conclusion

L'application Propriété intellectuelle établit un passeport de provenance pour les actifs immatériels. En reliant créations, versions, contributeurs, preuves d'existence, dépôts, droits, licences et cessions, Authenticity Plus© renforce la chaîne de preuve tout en laissant la reconnaissance et le règlement des droits aux institutions et acteurs compétents.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 8 — PROPRIÉTÉ INTELLECTUELLE

CHAPITRE 2 — ŒUVRES, LOGICIELS, INVENTIONS, MARQUES, DESSINS ET MODÈLES : VERSIONS, DÉPÔTS, CONTRIBUTIONS ET CHAÎNE DE PROVENANCE

1. Objet du chapitre

Ce chapitre décline le passeport de propriété intellectuelle selon plusieurs familles d'actifs : œuvres, logiciels, inventions, marques, dessins et modèles. Il organise versions, contributions, dépôts, preuves et relations de provenance sans effacer les différences juridiques entre ces catégories.

2. Principe de spécialisation

Chaque actif doit être associé à sa catégorie et aux métadonnées pertinentes. Une structure commune de provenance peut être partagée, mais les conditions de protection, de dépôt, de durée et de portée doivent rester propres au droit concerné.

3. Œuvres et contenus

Une œuvre textuelle, graphique, audiovisuelle, musicale, photographique ou autre contenu peut disposer d'une identité, d'une empreinte, d'une date de preuve et d'un historique de versions. La plateforme ne décide pas automatiquement si l'œuvre remplit les conditions juridiques de protection.

4. Fichiers et manifestations

Une même création peut exister sous plusieurs fichiers, formats, résolutions, éditions ou supports. L' identité de l'œuvre doit rester distincte de chacune de ses manifestations techniques.

5. Contributions créatives

Les contributions de plusieurs auteurs, artistes, designers, techniciens ou autres participants peuvent être documentées avec leur rôle et leur période lorsque les preuves existent. La contribution enregistrée ne détermine pas à elle seule la répartition juridique des droits.

6. Logiciels

Un logiciel peut être représenté par projet, dépôt, version, release, module ou autre unité pertinente. Code source, binaire, documentation et artefacts de construction doivent pouvoir être reliés sans être confondus.

7. Versions logicielles

Commit, version, release ou build peuvent fournir des repères chronologiques lorsqu'ils sont disponibles. Une empreinte permet de vérifier l'intégrité d'un état donné sans prouver à elle seule l' auteur ou la licéité de tous les composants.

8. Dépendances et composants tiers

Bibliothèques, composants open source ou éléments tiers peuvent être référencés avec leur origine et licence déclarée. La plateforme facilite la traçabilité sans produire automatiquement une analyse juridique complète de compatibilité des licences.

9. Inventions

Une invention peut être reliée à ses inventeurs déclarés, documents techniques, versions, prototypes et preuves d'existence. L'existence d'une preuve antérieure ne constitue pas automatiquement une décision sur brevetabilité ou priorité juridique.

10. Demandes de brevet

Une demande peut être corrélée à son office, numéro, date, territoire, revendication de priorité et statut disponibles. Les données officielles restent celles de l'office ou de la source compétente.

11. Familles et priorités

Lorsque plusieurs demandes sont liées, leurs relations de priorité ou de famille peuvent être représentées selon les références officielles disponibles. AP ne doit pas reconstruire ou affirmer une relation juridique non établie par les sources.

12. Marques

Une marque peut être représentée avec signe, titulaire déclaré, classes, territoire, dépôt, enregistrement et statut disponibles. L'identité du signe reste distincte de chaque titre territorial qui peut le protéger.

13. Usages de marque

Des preuves d'usage peuvent être associées à une période, un territoire, un produit, un service ou une campagne. Elles documentent un usage observé ou déclaré sans déterminer automatiquement ses effets juridiques.

14. Dessins et modèles

Un dessin ou modèle peut être relié à ses représentations, variantes, créateurs, dépôts et territoires. Les versions préparatoires doivent rester distinguées de la version effectivement déposée ou enregistrée.

15. Dépôt et contenu déposé

Pour toute catégorie enregistrable, le système doit distinguer le dossier préparatoire, le contenu effectivement déposé, les modifications ultérieures et le titre éventuellement délivré. Cette séparation est essentielle à la chaîne de preuve.

16. Chaîne de provenance

À partir d'un actif, il doit être possible de reconstruire les versions, contributeurs, fichiers, preuves, dépôts et relations documentées. À partir d'une version ou empreinte, le système doit pouvoir retrouver l'actif et son contexte.

17. Relations entre actifs

Une œuvre peut incorporer un élément tiers, un logiciel dépendre d'une bibliothèque, une marque être utilisée sur un produit ou un dessin être intégré à un objet industriel. Ces relations doivent conserver leur nature et leur source.

18. Anomalies et conflits

Empreintes identiques revendiquées comme créations indépendantes, chronologies incompatibles, dépôts contradictoires ou contributions divergentes peuvent produire des signaux d'investigation. Ils ne constituent pas automatiquement une décision de contrefaçon ou de titularité.

19. Critères d'acceptation

Le modèle est acceptable si chaque catégorie conserve ses spécificités, si œuvre et fichier restent distingués, si logiciel et composants tiers sont traçables, si dépôt préparatoire et dépôt officiel sont séparés, et si la chaîne de provenance permet de remonter des versions aux auteurs, preuves et références disponibles.

20. Conclusion

La propriété intellectuelle regroupe des actifs très différents, mais tous bénéficient d'une provenance rigoureuse. Authenticity Plus© fournit une couche transversale d'identité, de versionnement et de preuve qui respecte les spécificités des œuvres, logiciels, inventions, marques, dessins et modèles.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 8 — PROPRIÉTÉ INTELLECTUELLE

CHAPITRE 3 — TITULARITÉ, COPROPRIÉTÉ, LICENCES, CESSIONS, SOUS-LICENCES, TERRITOIRES, DURÉES, REDEVANCES ET CHAÎNE CONTRACTUELLE DES DROITS

1. Objet du chapitre

Ce chapitre organise la chaîne contractuelle des droits attachés aux actifs de propriété intellectuelle. Il structure titularité déclarée, copropriété, licences, sous-licences, cessions, territoires, durées, droits concédés, redevances documentaires et évolutions contractuelles, tout en préservant la compétence des parties, offices et juridictions.

2. Titularité et source de preuve

Une titularité peut résulter d'un titre, d'un contrat, d'une succession, d'une création ou d'un autre fondement applicable. AP doit conserver la source de la revendication et distinguer titulaire déclaré, titulaire enregistré et titulaire établi par une décision compétente.

3. Copropriété

Lorsqu'un actif comporte plusieurs titulaires, leurs parts, rôles ou droits peuvent être représentés selon les documents disponibles. Le système ne doit pas inventer une répartition lorsqu'elle n'est pas explicitement établie.

4. Chaîne de titularité

Les transferts successifs doivent pouvoir être reconstruits depuis l'origine documentée jusqu'au titulaire actuel déclaré. Chaque maillon conserve date, parties, actif concerné, portée et preuve disponible.

5. Cession

Une cession peut porter sur tout ou partie des droits. Le passeport doit distinguer l'existence du contrat, son objet, sa date, sa portée territoriale et son éventuel enregistrement sans interpréter les clauses litigieuses.

6. Cession partielle

Un transfert peut être limité à certains droits, usages, territoires, classes, produits ou périodes. La plateforme doit éviter qu'une cession partielle soit présentée comme transfert universel de l'actif.

7. Licence

Une licence doit pouvoir identifier concédant, licencié, actif, droits concédés, territoire, durée et éventuelles restrictions documentées. Le droit de propriété sur l'actif reste distinct du droit contractuel d'exploitation.

8. Licence exclusive et non exclusive

Le caractère exclusif ou non exclusif peut être enregistré lorsqu'il ressort du document source. AP ne doit pas déduire l'exclusivité à partir de l'existence d'un seul licencié connu.

9. Sous-licence

Une sous-licence peut être reliée à la licence principale qui l'autorise lorsque les preuves existent. Sa validité ou son étendue ne doit pas dépasser automatiquement celles du droit dont elle dérive.

10. Territoires

Les droits concédés ou transférés peuvent varier selon les pays, régions ou autres périmètres. Chaque relation contractuelle doit conserver son territoire afin d'éviter une représentation mondiale d'un droit local.

11. Durées

Date d'effet, échéance, renouvellement, résiliation ou expiration doivent être historisés lorsque disponibles. Une licence expirée ne doit pas être présentée comme autorisation active.

12. Usages et champs d'exploitation

Reproduction, distribution, adaptation, fabrication, diffusion, commercialisation ou autres usages peuvent être représentés comme champs distincts lorsqu'ils sont définis dans la source. Le modèle ne doit pas étendre un droit au-delà de son libellé documenté.

13. Redevances documentaires

Taux, minimums, échéances ou autres paramètres financiers peuvent être référencés lorsque leur conservation est autorisée. Authenticity Plus© assure provenance et auditabilité mais ne calcule pas automatiquement une dette juridiquement exigible.

14. Déclarations d'exploitation

Les exploitations déclarées par un licencié ou une autre partie peuvent être reliées à la période, au territoire et au contrat concernés. Une déclaration reste distincte d'un audit ou d'une validation par le concédant.

15. Modifications contractuelles

Avenants, renouvellements, extensions ou réductions de portée doivent être reliés au contrat initial. La version active doit être identifiable sans effacer les versions antérieures.

16. Résiliation et révocation

Une résiliation, révocation ou autre fin de droit contractuel doit conserver son auteur, son fondement documentaire, sa date d'effet et son périmètre. AP ne prononce pas lui-même la résiliation.

17. Conflits contractuels

Deux licences incompatibles, une cession contradictoire, un territoire superposé ou une chronologie impossible peuvent produire une alerte. Le système préserve les documents concurrents sans déterminer automatiquement lequel prévaut juridiquement.

18. Confidentialité, audit et AP Ledger

Les contrats et paramètres financiers peuvent être confidentiels. AP Ledger peut ancrer des empreintes, dates et références minimales afin de renforcer l'intégrité sans publier le contenu contractuel.

19. Critères d'acceptation

Le modèle est acceptable si propriété et licence restent distinctes, si cessions partielles conservent leur portée, si sous-licences sont reliées à leur fondement, si territoires et durées sont explicites, si les versions contractuelles sont historisées et si les conflits restent soumis à interprétation compétente.

20. Conclusion

La valeur d'un actif intellectuel dépend aussi de la lisibilité de sa chaîne de droits. Authenticity Plus© permet de reconstruire titularités, cessions, licences, sous-licences, territoires, durées et preuves contractuelles sans transformer la plateforme en juge du contrat ou du droit.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 8 — PROPRIÉTÉ INTELLECTUELLE

CHAPITRE 4 — EXPLOITATION, DIFFUSION, CONTENUS NUMÉRIQUES, PROVENANCE, USAGES AUTORISÉS, CONTREFAÇON PRÉSUMÉE ET GESTION DES CONFLITS DE DROITS

1. Objet du chapitre

Ce chapitre organise la traçabilité des exploitations et diffusions d'un actif de propriété intellectuelle. Il relie publication, reproduction, distribution, adaptation, intégration, diffusion numérique et autres usages aux droits ou autorisations documentés, sans qualifier automatiquement la licéité d'un usage.

2. Événement d'exploitation

Toute exploitation documentée peut être représentée avec l'actif concerné, l'acteur, la date, le territoire, le canal et la référence d'autorisation disponibles. L'événement reste distinct du droit qui l' autorise.

3. Publication et diffusion

Une publication ou diffusion peut être reliée à une édition, version ou manifestation précise. Le passeport doit éviter d'étendre une autorisation portant sur une version à toutes les versions futures ou dérivées.

4. Reproduction et distribution

Les événements de reproduction ou distribution peuvent être corrélés à une licence, un contrat ou un autre fondement documenté. AP conserve la provenance sans décider seul si l'exploitation relève d' une exception ou d'un droit exclusif.

5. Adaptations et dérivations

Traduction, adaptation, remix, fork, transformation ou autre création dérivée peut être reliée à l'actif source. La relation technique de dérivation ne constitue pas à elle seule une autorisation juridique.

6. Contenus numériques

Un actif numérique peut exister sur plusieurs plateformes, services, dépôts ou canaux. Chaque occurrence peut conserver URL ou identifiant de plateforme, version, date et source lorsque ces données sont disponibles et autorisées.

7. Empreintes et correspondances

Des empreintes cryptographiques ou autres mécanismes de correspondance peuvent aider à relier une copie à une version connue. Une correspondance technique doit être présentée avec son niveau de confiance et ne suffit pas à établir une contrefaçon.

8. Provenance des contenus

Auteur déclaré, éditeur, distributeur, plateforme, agence ou autre acteur peut contribuer à la chaîne de provenance. Le système doit distinguer création, publication, hébergement, distribution et simple transmission.

9. Métadonnées de provenance

Les métadonnées intégrées ou externes peuvent être conservées comme éléments de preuve avec leur source. Leur absence ou altération peut être signalée sans conclure automatiquement à une intention frauduleuse.

10. Usages autorisés

Lorsqu'un usage est corrélé à une licence ou autorisation, le système peut vérifier des paramètres documentaires tels que actif, territoire, durée, champ d'exploitation et version. Cette vérification ne remplace pas l'interprétation juridique du contrat.

11. Usages hors périmètre présumés

Un usage observé hors territoire, après expiration ou dans un champ non corrélé peut produire un signal de dépassement potentiel. Le signal doit rester une invitation à vérifier les droits, exceptions et documents applicables.

12. Plateformes et intermédiaires

Les plateformes numériques, diffuseurs, hébergeurs, distributeurs ou autres intermédiaires peuvent être représentés comme acteurs de la chaîne. Leur présence ne détermine pas automatiquement leur responsabilité juridique.

13. Preuves d'exploitation

Captures, rapports, relevés, identifiants de publication ou autres preuves peuvent être rattachés à un événement avec leur date et leur source. Les contenus confidentiels ou personnels doivent bénéficier de protections adaptées.

14. Contrefaçon présumée

Une copie non corrélée à une autorisation connue, une marque utilisée dans un contexte incompatible ou un contenu fortement correspondant peut déclencher une investigation. Authenticity Plus© ne prononce pas lui-même une contrefaçon.

15. Revendication et notification

Une partie peut enregistrer une revendication ou référence de notification concernant un usage contesté. L'existence d'une notification doit rester distincte d'une reconnaissance de violation ou d'une décision de retrait.

16. Réponse et contre-revendication

Une partie concernée peut fournir une réponse, une licence, une preuve de titularité ou une autre justification. Les positions contradictoires doivent être conservées avec leur chronologie sans fusion ni arbitrage automatique.

17. Mesures et décisions externes

Retrait de contenu, blocage, accord amiable, décision d'une plateforme, d'un office ou d'une juridiction peuvent être référencés avec leur source et leur portée. AP enregistre la décision externe sans se l'attribuer.

18. Dossier de conflit et AP Ledger

Un dossier peut regrouper actifs, versions, empreintes, licences, exploitations, revendications et décisions. Des empreintes de preuves sélectionnées peuvent être ancrées dans AP Ledger afin de renforcer intégrité et antériorité sans publier les contenus confidentiels.

19. Critères d'acceptation

Le modèle est acceptable si exploitation et autorisation restent distinctes, si les usages sont évalués selon territoire, durée et champ documentés, si les correspondances techniques ne deviennent pas des verdicts, et si revendications, réponses et décisions externes restent attribuables.

20. Conclusion

La traçabilité des usages prolonge le passeport de propriété intellectuelle au-delà de la création et des contrats. Authenticity Plus© permet de relier contenus, exploitations, autorisations et conflits à leurs preuves, tout en laissant la qualification de contrefaçon et le règlement des différends aux acteurs compétents.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 8 — PROPRIÉTÉ INTELLECTUELLE

CHAPITRE 5 — GOUVERNANCE, CONFIDENTIALITÉ, SECRETS D'AFFAIRES, PREUVES NUMÉRIQUES, INTELLIGENCE ARTIFICIELLE, AUDIT ET INTEROPÉRABILITÉ DES DROITS

1. Objet du chapitre

Ce chapitre définit la gouvernance transversale du passeport de propriété intellectuelle. Il organise confidentialité, secrets d'affaires, preuves numériques, contenus ou contributions assistés par intelligence artificielle, contrôle d'accès, audit, interopérabilité et gestion des incidents sans transformer Authenticity Plus© en autorité juridique.

2. Gouvernance des acteurs

Créateurs, inventeurs, titulaires, employeurs, mandataires, offices, licenciés, plateformes et autres acteurs doivent disposer de rôles distincts. Le droit de consulter une preuve ne confère pas automatiquement le droit de modifier l'actif ou sa chaîne de droits.

3. Classification de confidentialité

Un actif, contrat, prototype, code source, dossier de brevet ou autre élément peut être public, partagé, restreint ou hautement confidentiel selon sa finalité. Les droits d'accès doivent suivre cette classification et son évolution.

4. Secrets d'affaires

Les informations confidentielles à valeur économique peuvent être référencées par des preuves minimales sans exposer leur contenu. Authenticity Plus© doit privilégier empreintes, métadonnées contrôlées et journaux d'accès lorsque la divulgation détruirait la confidentialité recherchée.

5. Preuve d'existence confidentielle

Un document ou fichier confidentiel peut recevoir une preuve d'existence et d'intégrité sans publication de son contenu. L'empreinte technique démontre la correspondance avec un état donné, mais ne révèle ni ne certifie la substance juridique du secret.

6. Contrôle d'accès

Les accès aux actifs sensibles doivent être gouvernés par rôle, organisation, projet, contrat, territoire ou autre contexte pertinent. Les autorisations temporaires doivent pouvoir expirer sans supprimer les traces d'audit nécessaires.

7. Journalisation

Consultations sensibles, téléchargements, exports, modifications, signatures, dépôts de versions et changements de droits doivent pouvoir produire une piste d'audit proportionnée à leur criticité.

8. Preuves numériques

Empreintes, signatures électroniques, horodatages, attestations ou références de systèmes tiers peuvent renforcer la provenance. Chaque mécanisme doit préciser ce qu'il prouve réellement : intégrité, identité, date, émission ou autre propriété vérifiée.

9. Chaîne de conservation

Lorsqu'une preuve est utilisée dans une investigation ou un différend, ses transferts, copies, transformations et conditions de conservation peuvent être documentés. Une copie doit rester distinguée de la source ou de l'original documenté.

10. Intelligence artificielle — principe de provenance

Lorsqu'un actif ou une étape de création implique un système d'intelligence artificielle, cette participation peut être documentée comme élément de provenance. La plateforme ne doit pas déduire automatiquement les conséquences juridiques de cette participation.

11. Contribution humaine et assistance IA

Lorsque les preuves le permettent, le passeport peut distinguer instructions humaines, contributions, sélections, modifications et sorties générées ou assistées. Cette granularité soutient l'analyse ultérieure sans décider qui possède juridiquement les droits.

12. Modèles, outils et versions

Le système ou outil d'IA utilisé peut être référencé avec son fournisseur, nom, version ou date lorsque ces informations sont disponibles et pertinentes. L'absence de ces métadonnées doit être signalée comme limite de provenance plutôt que comblée par supposition.

13. Données et éléments tiers

Lorsqu'un processus créatif incorpore des contenus, bibliothèques, jeux de données ou autres éléments tiers explicitement identifiés, leurs références peuvent être reliées à l'actif. AP ne doit pas affirmer l'origine d'éléments que les preuves ne permettent pas d'identifier.

14. Déclarations relatives à l'IA

Une partie peut déclarer le degré ou la nature d'utilisation d'un système d'IA. Cette déclaration doit conserver son auteur et rester distincte d'une vérification indépendante ou d'une qualification juridique.

15. Interopérabilité avec offices et registres

Les références provenant d'offices, registres, sociétés de gestion, dépôts de code ou autres systèmes peuvent être corrélées lorsque les interfaces et droits le permettent. La donnée importée conserve sa source et AP ne crée pas un registre officiel parallèle.

16. Interopérabilité contractuelle

Les identifiants d'actifs et de droits peuvent être reliés aux contrats, licences, cessions et exploitations. Toute synchronisation doit préserver versions, territoires, périodes et statuts afin d'éviter une autorisation artificiellement élargie.

17. Cybersécurité et révocation

Compte compromis, clé perdue, accès abusif ou altération suspecte doit pouvoir conduire à une suspension ou révocation technique. L'historique antérieur reste conservé afin de permettre l' investigation.

18. AP Ledger

AP Ledger peut ancrer des empreintes de versions, contrats, preuves d'existence ou événements critiques. Les secrets, codes sources, contrats confidentiels et contenus sensibles doivent rester hors de la couche publique ou irréversible lorsque leur exposition serait disproportionnée.

19. Critères d'acceptation

Le modèle est acceptable si les secrets peuvent être prouvés sans être publiés, si les accès sensibles sont gouvernés et auditables, si la participation d'une IA est documentée sans conclusion juridique automatique, si les données externes conservent leur source et si AP Ledger applique une logique de minimisation.

20. Conclusion

La gouvernance de la propriété intellectuelle exige de concilier preuve et confidentialité. Authenticity Plus© / Deep Authenticity© fournit une infrastructure où versions, secrets, contributions humaines ou assistées par IA, contrats et références officielles peuvent être reliés et audités sans exposer inutilement les actifs ni prétendre trancher leur statut juridique.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 8 — PROPRIÉTÉ INTELLECTUELLE

CHAPITRE 6 — SYNTHÈSE FONCTIONNELLE, CRITÈRES D'ACCEPTATION ET CLÔTURE DE L'APPLICATION PROPRIÉTÉ INTELLECTUELLE

1. Objet du chapitre

Ce chapitre clôt le Point 8 — Propriété intellectuelle. Il consolide identité des créations, contributeurs, versions, preuves d'existence, dépôts, titres, titularités, licences, cessions, exploitations, conflits, confidentialité, intelligence artificielle, interopérabilité, audit et AP Ledger.

2. Mission consolidée

L'application Propriété intellectuelle constitue un passeport de provenance et de chaîne de droits pour les actifs immatériels. Elle renforce intégrité, chronologie et auditabilité sans créer elle-même un droit, interpréter définitivement un contrat ou trancher un différend.

3. Identité persistante de l'actif

Une création doit conserver une identité stable à travers fichiers, formats, versions, dépôts et exploitations. L'identité conceptuelle de l'actif reste distincte de ses manifestations techniques et supports.

4. Catégories et spécificités

Œuvres, logiciels, inventions, marques, dessins et modèles peuvent partager une infrastructure de provenance tout en conservant leurs règles, territoires, durées et conditions de protection propres.

5. Auteurs, inventeurs et contributeurs

Les contributions peuvent être attribuées avec leur rôle, période ou version lorsque les preuves existent. Une contribution documentée ne constitue pas automatiquement une décision sur la qualité juridique d'auteur, d'inventeur ou de titulaire.

6. Preuve d'existence et antériorité

Empreintes, signatures, horodatages et autres preuves peuvent établir l'existence d'un état donné à une date donnée. Elles ne démontrent pas automatiquement originalité, brevetabilité, titularité ou droit exclusif.

7. Versionnement et dérivation

Les versions successives doivent rester reliées et les dérivations documentées lorsque connues. Une adaptation ou relation technique avec une œuvre source ne constitue pas à elle seule une autorisation d'exploitation.

8. Dépôts et titres officiels

Demandes, dépôts, enregistrements, priorités et titres peuvent être corrélés aux sources officielles disponibles. AP ne devient ni office d'enregistrement ni registre officiel parallèle.

9. Titularité et chaîne de droits

Titulaire déclaré, titulaire enregistré, copropriété, cession et autres fondements doivent rester distingués. Les transferts successifs doivent pouvoir être reconstruits avec leur portée et leurs preuves.

10. Licences et sous-licences

Les licences doivent conserver concédant, licencié, actif, droits, territoire, durée et restrictions disponibles. Les sous-licences restent reliées au droit dont elles dérivent et ne doivent pas être artificiellement élargies.

11. Exploitations

Publication, reproduction, distribution, adaptation, diffusion ou autres usages peuvent être corrélés à leurs autorisations documentées. L'existence d'un usage sans licence connue dans AP ne constitue pas automatiquement une contrefaçon.

12. Contenus numériques et provenance

Fichiers, plateformes, versions, empreintes et métadonnées peuvent contribuer à la provenance d'un contenu numérique. Une correspondance technique doit rester une preuve de similarité ou d'identité de fichier, non un verdict juridique.

13. Conflits et revendications

Revendications concurrentes, chronologies incompatibles, licences contradictoires ou usages contestés doivent rester visibles avec leurs sources. Réponses, contre-revendications et décisions externes doivent être historisées sans arbitrage automatique.

14. Confidentialité et secrets d'affaires

Les actifs sensibles doivent pouvoir recevoir des preuves d'existence et d'intégrité sans publication de leur contenu. Les contrôles d'accès et journaux doivent préserver la confidentialité tout en permettant l'audit.

15. Intelligence artificielle

La participation d’un système d’IA peut être documentée avec les métadonnées disponibles, contributions humaines et déclarations pertinentes. AP ne déduit pas automatiquement la titularité ou la protection juridique à partir de cette provenance.

16. Interopérabilité

Offices, registres, dépôts de code, plateformes, contrats et autres systèmes peuvent être corrélés lorsque les interfaces et droits le permettent. Toute donnée importée conserve sa source et son statut.

17. Audit et cybersécurité

Accès sensibles, modifications, dépôts de versions, signatures, transferts et changements de droits doivent pouvoir être audités. Les accès compromis doivent pouvoir être révoqués sans effacer l’ historique.

18. AP Ledger

AP Ledger peut renforcer intégrité et antériorité par l’ancrage d’empreintes et références minimales. Les contenus confidentiels, secrets, codes sources et contrats sensibles doivent rester hors des couches publiques ou irréversibles lorsque nécessaire.

19. Critères d’acceptation

Le modèle est acceptable si identité, fichier, version, auteur, titulaire et titre officiel restent distingués ; si la chaîne de droits est reconstructible ; si les autorisations conservent territoire et durée ; si les conflits restent attribuables ; et si aucune preuve technique n’est présentée comme décision juridique automatique.

20. Clôture du Point 8 — Propriété intellectuelle

Le Point 8 — Propriété intellectuelle est désormais fonctionnellement défini : créations, œuvres, logiciels, inventions, marques, dessins et modèles, versions, contributeurs, antériorité, dépôts, titres, titularité, copropriété, licences, cessions, exploitations, contenus numériques, conflits, secrets d’ affaires, IA, interopérabilité, audit et AP Ledger. Cette architecture est prête à s’articuler avec le Point 9 — Transport.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 9 — TRANSPORT

CHAPITRE 1 — MISSION, PÉRIMÈTRE, ACTEURS, MOYENS DE TRANSPORT, UNITÉS LOGISTIQUES ET PRINCIPES FONDATEURS

1. Objet du chapitre

Le Point 9 — Transport transpose Authenticity Plus© / Deep Authenticity© aux flux physiques et documentaires de transport. Il organise acteurs, moyens de transport, marchandises ou unités logistiques, documents, prises en charge, trajets, transbordements, livraisons, incidents et preuves de réception afin de construire une chaîne de provenance multimodale vérifiable.

2. Mission sectorielle

L'application Transport vise à rendre attribuables et chronologiques les événements qui déplacent une marchandise, un colis, une palette, un conteneur ou une autre unité. Elle ne se substitue ni aux transporteurs, ni aux autorités, ni aux systèmes douaniers, portuaires, aéroportuaires ou ferroviaires.

3. Acteurs du transport

Expéditeur, donneur d'ordre, commissionnaire, transporteur, sous-traitant, conducteur, opérateur de terminal, manutentionnaire, destinataire et autres intervenants doivent être représentés selon leur rôle réel dans chaque événement.

4. Identité de l'expédition

Une expédition peut disposer d'un identifiant persistant reliant commande, marchandises, unités logistiques, documents et événements. L'identité de l'expédition reste distincte de celle du véhicule ou du conteneur utilisé.

5. Marchandise et unité logistique

Produit, colis, palette, caisse, conteneur ou autre unité doivent être distingués. Les relations d' agrégation et de désagrégation permettent de savoir quelles marchandises sont contenues dans quelle unité à un moment donné.

6. Moyens de transport

Camion, remorque, train, wagon, navire, aéronef ou autre moyen peut être référencé avec ses identifiants disponibles. Le moyen de transport reste un support de déplacement et ne doit pas être confondu avec l'expédition.

7. Conducteur et équipage

Lorsque nécessaire et autorisé, conducteur, équipage ou opérateur peuvent être associés à une étape. Les données personnelles doivent être minimisées et limitées aux finalités légitimes de traçabilité et de conformité.

8. Document de transport

Lettre de voiture, connaissement, lettre de transport aérien, document ferroviaire ou autre pièce peut être relié à l'expédition avec son émetteur, sa date, sa version et son statut. AP n'émet pas automatiquement un document réglementaire officiel.

9. Prise en charge

La remise d'une unité à un transporteur constitue un événement distinct qui peut conserver lieu, date, acteur, quantité et état documentaire. La prise en charge ne doit pas être confondue avec le transfert de propriété.

10. Départ et arrivée

Les événements de départ et d'arrivée peuvent être enregistrés avec leur source et leur horodatage. Heure planifiée, heure déclarée et heure observée doivent rester distinguées lorsqu'elles proviennent de systèmes différents.

11. Étapes et jalons

Chargement, passage terminal, contrôle, escale, déchargement ou autre jalon peut être ajouté à la chronologie. Le modèle doit permettre un parcours incomplet sans inventer les étapes manquantes.

12. Transbordement

Lorsqu'une unité change de véhicule, de navire, de train ou de mode, le transbordement doit conserver les relations avant et après l'opération. La continuité de l'expédition doit survivre au changement de moyen de transport.

13. Transport multimodal

Une même expédition peut combiner route, rail, mer, air ou autres modes. Chaque segment conserve son transporteur, son moyen, ses documents et ses événements tout en restant relié à la chaîne globale.

14. Scellés et intégrité

Conteneurs, remorques ou unités peuvent être associés à des scellés ou autres mécanismes d' intégrité. Pose, contrôle, rupture et remplacement doivent être historisés lorsque les données existent.

15. Conditions de transport

Température, humidité, choc, position ou autres paramètres peuvent être documentés lorsqu'ils sont pertinents. La plateforme conserve les mesures et leur source sans décider automatiquement de l' acceptabilité commerciale ou réglementaire de la marchandise.

16. Livraison

La livraison constitue un événement distinct pouvant enregistrer lieu, date, destinataire autorisé, quantité et réserves documentaires. Elle ne doit pas être confondue avec la clôture financière de la transaction.

17. Preuve de réception

Signature, scan, photographie, référence système ou autre preuve peut confirmer une réception selon son niveau de fiabilité. AP doit indiquer la nature de la preuve sans étendre sa portée au-delà de ce qu' elle démontre.

18. Incidents et anomalies

Retard, perte, dommage, rupture de scellé, excursion de condition, divergence de quantité ou événement inattendu peut être signalé. Une anomalie déclenche une investigation et ne constitue pas automatiquement une faute du transporteur.

19. Critères d'acceptation

Le modèle est acceptable si expédition, marchandise, unité logistique et moyen de transport restent distincts ; si les changements de mode préservent la continuité ; si chaque événement conserve sa source ; si les preuves de réception sont attribuables ; et si les anomalies restent explicables sans conclusion automatique.

20. Conclusion

L'application Transport établit le socle d'une chaîne de possession et de déplacement vérifiable. En reliant acteurs, unités, moyens, documents, segments, transbordements et réception, Authenticity Plus© prépare une traçabilité multimodale capable de s'articuler avec Industrie, Agriculture, Pharmacie, Automobile et les autres applications sectorielles.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 9 — TRANSPORT

CHAPITRE 2 — DOCUMENTS DE TRANSPORT, CHAÎNE DE POSSESSION, CHARGEMENT, SCELLÉS, GÉOLOCALISATION DOCUMENTAIRE, TRANSBORDEMENTS ET TRAÇABILITÉ MULTIMODALE

1. Objet du chapitre

Ce chapitre approfondit la continuité documentaire et physique d'une expédition. Il structure les documents de transport, les transferts de garde, les opérations de chargement et déchargement, les scellés, les jalons de localisation, les transbordements et les segments multimodaux afin que chaque changement de responsabilité reste attribuable.

2. Dossier de transport

Une expédition peut regrouper plusieurs documents et références : ordre de transport, document principal, instructions, listes de colisage, preuves de prise en charge, documents de terminal et preuves de livraison. Chaque pièce conserve son émetteur, sa version, sa date et son statut.

3. Document principal et documents associés

Le document principal de transport doit rester distinct des annexes et justificatifs. Une correction, substitution ou émission ultérieure doit préserver la relation avec les versions précédentes afin d'éviter une réécriture silencieuse du dossier.

4. Données déclarées et données observées

Poids, quantité, contenu, origine, destination ou autres informations peuvent être déclarés par un acteur puis observés ou contrôlés par un autre. AP doit conserver ces niveaux séparément lorsqu'ils diffèrent.

5. Chaîne de possession

Chaque remise d'une unité logistique peut produire un événement identifiant cédant, receveur, date, lieu et unité concernée. La chaîne de possession documente la garde opérationnelle sans déterminer automatiquement la propriété juridique de la marchandise.

6. Acceptation avec réserves

Lorsqu'un acteur accepte une unité avec réserve, celle-ci doit pouvoir être enregistrée avec son auteur, son horodatage et les éléments justificatifs disponibles. La réserve reste une déclaration documentée jusqu'à son éventuelle résolution.

7. Chargement

Le chargement doit pouvoir relier marchandises, unités logistiques et moyen de transport. Lorsque la granularité le permet, le système conserve les relations d'agrégation entre colis, palettes, conteneurs, remorques ou autres supports.

8. Déchargement

Le déchargement constitue un événement distinct du chargement. Les quantités ou unités déchargées peuvent être comparées aux éléments pris en charge, sans que toute divergence soit automatiquement qualifiée de perte ou de faute.

9. Scellés

La pose d'un scellé peut enregistrer identifiant, unité, acteur, lieu et date. Les contrôles successifs doivent conserver l'état déclaré ou observé du scellé et sa source.

10. Rupture et remplacement de scellé

Toute rupture, ouverture autorisée, contrôle douanier ou remplacement documenté doit préserver l' identifiant précédent et le nouveau. Une rupture inexpliquée peut déclencher une alerte, mais son origine doit faire l'objet d'une investigation.

11. Localisation documentaire

Les événements peuvent être associés à un lieu déclaré, scanné ou enregistré par un système. La localisation documentaire doit rester distinguée d'une position géographique continue ou d'une preuve absolue de présence physique.

12. Données de géolocalisation

Lorsque des données GPS ou télématiques sont autorisées, elles peuvent être reliées aux segments concernés avec leur source et leur précision disponibles. Leur conservation doit respecter la minimisation des données, notamment lorsqu'elles peuvent révéler les déplacements de personnes.

13. Jalons de transport

Entrée ou sortie de terminal, passage frontière, escale, arrivée à quai, départ de dépôt ou autre jalon peut enrichir la chronologie. L'absence d'un jalon attendu constitue un manque documentaire et non la preuve automatique que l'événement n'a pas eu lieu.

14. Transbordement

Un transbordement relie explicitement l'unité quittant un moyen de transport à son chargement sur un autre. L'expédition conserve son identité globale tandis que le segment, le transporteur et le moyen changent.

15. Multimodalité

Route, rail, maritime, aérien ou autres modes peuvent être combinés dans une seule chaîne. Chaque segment possède ses propres documents, acteurs et contraintes, mais doit rester raccordé aux mêmes unités et à la même expédition.

16. Groupage et dégroupage

Une expédition peut être regroupée avec d'autres dans une unité commune puis séparée ultérieurement. Les relations d'agrégation doivent être datées afin de savoir quelles marchandises appartenaient à quelle unité à chaque étape.

17. Passage de frontière et contrôles

Les références de contrôles douaniers, sécuritaires ou administratifs peuvent être associées aux événements lorsque leur partage est autorisé. AP en conserve la provenance sans se substituer aux autorités ni interpréter leur décision.

18. Alertes de continuité

Scellé incohérent, changement de garde non documenté, unité absente d'un transbordement, localisation incompatible ou document contradictoire peut produire un signal d'investigation. Chaque alerte doit exposer les éléments à l'origine du signal.

19. Critères d'acceptation

Le modèle est acceptable si la chaîne de possession peut être reconstruite, si chargement et déchargement restent distincts, si les scellés sont historisés, si la localisation conserve sa source et son niveau de précision, et si la continuité survit aux changements de transporteur, de moyen et de mode.

20. Conclusion

La traçabilité multimodale dépend moins d'un suivi continu que de la qualité des passages de responsabilité. Authenticity Plus© relie documents, unités, scellés, lieux, acteurs et transbordements pour produire une chaîne de possession vérifiable sans transformer les métadonnées logistiques en conclusions automatiques.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 9 — TRANSPORT

CHAPITRE 3 — CONDITIONS DE TRANSPORT, CHAÎNE DU FROID, CAPTEURS, TEMPÉRATURE, INCIDENTS, DOMMAGES, PERTES, RÉSERVES ET PREUVES DE LIVRAISON

1. Objet du chapitre

Ce chapitre organise la preuve des conditions de transport et des incidents susceptibles d'affecter une expédition. Il relie exigences documentées, capteurs, mesures, chaîne du froid, dommages, pertes, réserves et preuves de livraison afin de préserver une chronologie vérifiable sans transformer AP en arbitre automatique de conformité.

2. Conditions contractuelles ou réglementaires

Température, humidité, orientation, exposition, délai ou autres conditions peuvent être associées à une expédition lorsqu'elles proviennent d'un contrat, d'une instruction ou d'une source compétente. Leur origine et leur période d'application doivent rester explicites.

3. Chaîne du froid

Pour les marchandises thermosensibles, les étapes de préparation, chargement, transport, stockage intermédiaire, transbordement et livraison peuvent être reliées à des conditions thermiques documentées. La continuité doit survivre aux changements de transporteur et de mode.

4. Capteurs et enregistreurs

Un capteur ou enregistreur peut être associé à une unité logistique, un conteneur, un véhicule ou une expédition. Son identité, sa période d'utilisation et sa source doivent être conservées lorsque disponibles.

5. Mesures

Chaque mesure pertinente doit pouvoir conserver valeur, unité, date ou période et source. Les données brutes, agrégées ou résumées doivent rester distinguées afin de ne pas présenter un résumé comme l' intégralité de la série.

6. Calibration et qualité métrologique

Lorsqu'une calibration, vérification ou certification du capteur est disponible, elle peut être reliée à l' équipement et à sa période de validité. AP ne doit pas inventer une précision ou une conformité métrologique absente des preuves.

7. Excursion de température

Une mesure hors d'une plage documentée peut produire une alerte d'excursion. L'alerte doit préciser la règle, la durée et les données concernées sans décider automatiquement que la marchandise est inutilisable.

8. Rupture de données

Une absence de mesures, une interruption de capteur ou une perte de connectivité doit être représentée comme lacune documentaire. Elle ne doit pas être assimilée automatiquement à une rupture réelle des conditions de transport.

9. Chocs, inclinaisons et autres événements

Des capteurs peuvent enregistrer choc, vibration, inclinaison, ouverture ou autres paramètres. Chaque événement conserve sa source et son seuil documentaire ; son impact sur la marchandise relève de l'évaluation compétente.

10. Incident de transport

Retard, panne, accident, immobilisation, erreur d'acheminement, rupture de scellé ou autre incident peut être enregistré avec date, lieu, acteur déclarant et documents disponibles.

11. Dommages

Un dommage constaté ou déclaré peut être relié à l'unité, à la marchandise et à l'étape concernée. Déclaration, constat, expertise et conclusion doivent rester des niveaux distincts.

12. Perte et quantité manquante

Une différence entre quantité prise en charge et quantité livrée peut déclencher une investigation. Groupage, dégroupage, livraisons partielles et corrections documentaires doivent être examinés avant toute qualification automatique de perte.

13. Réserves à la livraison

Le destinataire peut, lorsque le processus le prévoit, enregistrer des réserves relatives à l'état, à la quantité ou à d'autres éléments observés. Ces réserves doivent conserver auteur, date et preuve associée.

14. Preuves photographiques et documentaires

Photographies, scans, rapports, signatures ou autres pièces peuvent être rattachés à un incident ou à une livraison. Les métadonnées et données personnelles doivent être protégées selon leur sensibilité.

15. Preuve de livraison

La preuve de livraison peut combiner signature, identité ou rôle du réceptionnaire, horodatage, référence système, scan ou autre élément. AP doit indiquer la nature exacte de la preuve et ne pas lui attribuer une portée supérieure à ce qu'elle démontre.

16. Livraison partielle ou refusée

Une livraison partielle, refusée ou réorientée doit rester un événement distinct. Les unités effectivement remises et celles restant en circulation doivent continuer à être traçables.

17. Dossier d'incident

Un dossier peut regrouper événements, mesures, scellés, documents, réserves, photographies, expertises et réponses des parties. Les versions et positions contradictoires doivent rester historisées.

18. Corrélation sectorielle

Les conditions de transport peuvent être corrélées aux exigences documentées des secteurs Agriculture, Élevage, Pharmacie, Santé ou Industrie. AP conserve cette relation sans déterminer lui-même l'aptitude sanitaire, pharmaceutique ou commerciale du produit.

19. Critères d'acceptation

Le modèle est acceptable si exigences et mesures restent distinctes, si les capteurs sont attribuables, si les lacunes de données sont visibles, si les excursions déclenchent une analyse plutôt qu'un verdict, si les réserves restent attribuées et si la preuve de livraison précise exactement ce qu'elle établit.

20. Conclusion

Conditions, capteurs, incidents et livraison donnent au passeport Transport sa dimension probatoire opérationnelle. Authenticity Plus© permet de reconstruire ce qui a été exigé, mesuré, observé et déclaré tout au long du trajet, tout en laissant l'évaluation de conformité et de responsabilité aux acteurs compétents.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 9 — TRANSPORT

CHAPITRE 4 — TRANSPORT INTERNATIONAL, DOUANES, FRONTIÈRES, PORTS, AÉROPORTS, CORRIDORS LOGISTIQUES, DOCUMENTS RÉGLEMENTAIRES ET CONTINUITÉ TRANSFRONTALIÈRE

1. Objet du chapitre

Ce chapitre étend le passeport Transport aux chaînes internationales. Il organise la continuité documentaire lors des passages de frontière, opérations douanières, escales portuaires ou aéroportuaires, corridors logistiques et changements de juridiction, sans se substituer aux autorités compétentes.

2. Identité transfrontalière de l’expédition

Une expédition doit conserver une identité stable malgré les changements de pays, transporteur, document, terminal ou mode. Les références locales ou réglementaires successives peuvent être reliées sans remplacer l’identité globale du dossier.

3. Exportateur et importateur

Exportateur, importateur, déclarant, représentant ou autre partie peuvent être associés selon leur rôle documenté. La présence d’un acteur dans AP ne constitue pas une validation de son statut réglementaire au-delà des sources disponibles.

4. Documents commerciaux et logistiques

Factures, listes de colisage, certificats, instructions ou autres pièces peuvent être reliés au transport international. Chaque document conserve émetteur, version, date et relation avec l’expédition.

5. Documents douaniers

Déclarations, références de transit, décisions, mainlevées ou autres documents douaniers peuvent être corrélés lorsque leur partage est autorisé. AP ne crée pas lui-même une déclaration douanière officielle ni une décision de dédouanement.

6. Passage de frontière

L’entrée ou sortie d’un territoire peut être représentée comme jalon avec date, lieu et source. Heure prévue, déclarée, observée ou validée doivent rester distinguées.

7. Contrôles

Inspection, scan, pesée, ouverture, contrôle documentaire ou autre intervention d'une autorité peut être référencé avec son résultat documentaire. AP conserve la preuve sans interpréter ou modifier la décision de l'autorité.

8. Ouverture et rescellage

Lorsqu'une unité est ouverte lors d'un contrôle, la rupture du scellé et le nouveau scellé doivent être historisés. Cette continuité permet d'éviter qu'une ouverture autorisée soit confondue avec une rupture inexpliquée.

9. Transit

Une opération de transit peut relier départ, bureaux ou points intermédiaires, garanties ou références disponibles et destination prévue. Les statuts importés restent attribués au système ou à l'autorité source.

10. Ports

Terminal, entrée portuaire, dépôt, chargement à bord, déchargement, transbordement et sortie peuvent constituer des événements distincts. Le conteneur et l'expédition doivent rester traçables malgré les changements de navire ou de terminal.

11. Transport maritime

Navire, voyage, connaissement ou autres références maritimes peuvent être associés aux segments concernés. Les changements de voyage ou de transbordement doivent préserver la continuité des unités logistiques.

12. Aéroports et transport aérien

Acceptation cargo, terminal, vol, escale, transfert et remise peuvent être représentés comme événements distincts. Les références de lettre de transport aérien ou systèmes associés conservent leur source.

13. Rail et corridors terrestres

Train, wagon, terminal ferroviaire, convoi routier ou corridor terrestre peuvent constituer des segments successifs. Les changements d'opérateur ou d'infrastructure ne doivent pas rompre l'identité de l' expédition.

14. Corridors logistiques

Un corridor peut être représenté comme ensemble de points, territoires et segments attendus. Une déviation observée peut être signalée sans être automatiquement qualifiée d'irrégularité.

15. Zones franches et entrepôts

Les passages par zones franches, entrepôts sous contrôle ou autres installations peuvent être documentés avec entrée, sortie, garde et transformations autorisées lorsque les données existent.

16. Changement de juridiction

Les exigences documentaires peuvent varier d'un territoire à l'autre. Le modèle doit conserver les règles ou références applicables sans prétendre harmoniser juridiquement des régimes différents.

17. Divergences entre systèmes

Un port, une douane, un transporteur et un terminal peuvent fournir des horaires ou statuts différents. AP doit préserver chaque source et sa chronologie plutôt que fusionner silencieusement les informations.

18. Alertes transfrontalières

Document manquant, statut contradictoire, scellé incohérent, route inattendue ou rupture de chaîne de garde peut produire un signal d'investigation. L'alerte doit préciser ses sources et ne constitue pas une conclusion de fraude ou d'infraction.

19. Critères d'acceptation

Le modèle est acceptable si l'identité de l'expédition survit aux frontières, si les références douanières restent attribuées, si les ouvertures autorisées sont historisées, si ports, aéroports et corridors peuvent être représentés par événements, et si les divergences inter-systèmes restent visibles.

20. Conclusion

Le transport international multiplie les acteurs, documents et juridictions. Authenticity Plus© assure la continuité entre ces environnements en reliant les preuves sans créer de registre douanier parallèle ni se substituer aux autorités qui contrôlent les frontières et les flux.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 9 — TRANSPORT

CHAPITRE 5 — RESPONSABILITÉS, SOUS-TRAITANCE, ASSURANCES TRANSPORT, RÉCLAMATIONS, PREUVE DE LIVRAISON, FRAUDE DOCUMENTAIRE, CYBERSÉCURITÉ ET AUDIT DE LA CHAÎNE LOGISTIQUE

1. Objet du chapitre

Ce chapitre consolide la dimension de responsabilité et de preuve du passeport Transport. Il organise sous-traitance, assurances, réclamations, preuves de livraison, incidents documentaires, cybersécurité et audit afin que les actions et transferts critiques restent attribuables sans produire automatiquement une conclusion juridique.

2. Attribution des rôles

Donneur d'ordre, commissionnaire, transporteur principal, sous-traitant, conducteur, opérateur de terminal, manutentionnaire, destinataire, assureur et autres acteurs doivent être identifiés selon leur rôle dans chaque événement. La participation à une chaîne ne suffit pas à établir une responsabilité.

3. Ordre et contrat de transport

Un ordre, contrat ou accord peut être relié à l'expédition avec parties, date, périmètre, segments et versions disponibles. AP conserve la provenance documentaire sans interpréter définitivement les obligations contractuelles.

4. Transporteur principal

Le transporteur principal peut être relié aux segments qu'il prend en charge ou organise. Son rôle contractuel doit rester distinct de l'exécution physique lorsqu'un autre opérateur réalise tout ou partie du transport.

5. Sous-traitance

Une sous-traitance doit pouvoir relier donneur d'ordre, exécutant, segment, période et références documentaires. Le changement d'exécutant ne doit jamais rompre l'identité de l'expédition ni sa chaîne de possession.

6. Sous-traitance en cascade

Lorsque plusieurs niveaux de sous-traitance existent, chaque délégation doit rester reconstructible. AP ne doit pas attribuer automatiquement au dernier exécutant les obligations ou responsabilités contractuelles des niveaux précédents.

7. Transfert de garde

Chaque transfert opérationnel doit identifier les unités concernées, le cédant, le receveur, le lieu, la date et les réserves éventuelles. La garde physique reste distincte de la propriété de la marchandise.

8. Incident et déclaration

Retard, dommage, perte, rupture de scellé, excursion de condition ou autre incident peut être déclaré par un acteur. La déclaration initiale doit rester distincte d'un constat, d'une expertise ou d'une décision ultérieure.

9. Réclamation

Une réclamation peut être reliée à l'expédition, au contrat, à l'incident, aux montants réclamés et aux pièces disponibles. Son existence ne constitue pas une reconnaissance de responsabilité ou de dette.

10. Réponse des parties

Acceptation, contestation, demande de complément ou autre réponse doit être historisée avec son auteur et sa date. Les positions contradictoires doivent rester visibles sans fusion ni arbitrage automatique.

11. Expertise

Une expertise ou inspection peut être rattachée au dossier avec expert ou organisme, date, version et conclusions documentaires. Authenticity Plus© garantit la provenance de la pièce sans se substituer à l'expert.

12. Assurance transport

Police, certificat, déclaration de sinistre, référence de dossier, expertise ou décision assurantielle peuvent être corrélés lorsque leur partage est autorisé. AP ne détermine pas lui-même la couverture, l'indemnisation ou la responsabilité.

13. Preuve de livraison renforcée

Signature, identité ou rôle du réceptionnaire, horodatage, scan, photographie, référence système et réserves peuvent être combinés. Le système doit préciser les éléments présents et éviter de présenter une preuve partielle comme confirmation absolue de toutes les conditions de livraison.

14. Fraude documentaire présumée

Documents contradictoires, doublons incompatibles, altérations, dates ou quantités incohérentes, signatures contestées ou références réutilisées peuvent produire un signal d'investigation. Le signal ne constitue pas automatiquement une qualification de fraude.

15. Substitution et rupture de continuité

Changement inexpliqué d'unité logistique, scellé incompatible, disparition d'un maillon de garde ou substitution documentaire peut déclencher une alerte. Les événements autorisés de reconditionnement, contrôle ou transbordement doivent être examinés avant toute conclusion.

16. Cybersécurité

Comptes compromis, modifications anormales, accès non autorisés, extraction massive ou altération suspecte doivent pouvoir être signalés et investigués. Les accès concernés doivent pouvoir être suspendus ou révoqués sans effacer l'historique.

17. Journal d'audit logistique

Créations, modifications, signatures, transmissions, consultations sensibles, téléchargements, changements de droits et événements critiques doivent pouvoir produire une piste d'audit proportionnée à leur importance.

18. AP Ledger et preuves minimales

Empreintes de documents, preuves de livraison, transferts de garde ou autres événements sélectionnés peuvent être ancrées dans AP Ledger. Les contrats, données commerciales confidentielles et informations personnelles doivent rester hors des couches publiques lorsque leur exposition serait disproportionnée.

19. Critères d'acceptation

Le modèle est acceptable si la sous-traitance reste reconstructible, si déclaration, réclamation, expertise et décision restent distinctes, si les preuves de livraison précisent leur portée, si les alertes de fraude restent investigables, et si les actions sensibles sont auditables et révocables.

20. Conclusion

Responsabilité, sous-traitance, assurance et audit donnent au passeport Transport sa capacité à soutenir les investigations et règlements de différends. Authenticity Plus© préserve la chronologie et l'attribution des preuves sans devenir assureur, expert, arbitre contractuel ou autorité judiciaire.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 9 — TRANSPORT

CHAPITRE 6 — SYNTHÈSE FONCTIONNELLE, CRITÈRES D'ACCEPTATION ET CLÔTURE DE L'APPLICATION TRANSPORT

1. Objet du chapitre

Ce chapitre clôt le Point 9 — Transport. Il consolide acteurs, expéditions, marchandises, unités logistiques, moyens de transport, documents, chaîne de possession, conditions, multimodalité, frontières, incidents, sous-traitance, assurances, réclamations, cybersécurité, audit et AP Ledger.

2. Mission consolidée

L'application Transport constitue un passeport de déplacement et de garde destiné à rendre les flux physiques et documentaires plus vérifiables. Elle relie les preuves sans se substituer aux transporteurs, autorités, douanes, assureurs, experts ou juridictions.

3. Identité de l'expédition

L'expédition conserve une identité stable malgré les changements de véhicule, transporteur, terminal, mode ou territoire. Cette identité reste distincte de celles des marchandises, unités logistiques et moyens de transport.

4. Marchandises et unités logistiques

Produits, colis, palettes, caisses, conteneurs et autres unités doivent rester distingués. Les relations de groupage et dégroupage doivent être datées afin de reconstruire leur composition à chaque étape.

5. Acteurs et rôles

Expéditeur, donneur d'ordre, commissionnaire, transporteur, sous-traitant, conducteur, terminal, manutentionnaire et destinataire sont attribués selon leur rôle réel. Leur participation ne détermine pas automatiquement leur responsabilité juridique.

6. Documents de transport

Documents principaux, annexes, listes, instructions et preuves doivent conserver émetteur, date, version et statut. Une correction ou substitution documentaire ne doit pas effacer silencieusement l'état antérieur.

7. Chaîne de possession

Chaque transfert de garde doit pouvoir identifier unité, cédant, receveur, lieu, date et réserves éventuelles. La garde opérationnelle reste distincte de la propriété juridique de la marchandise.

8. Chargement, scellés et transbordements

Chargements, déchargements, poses, ruptures et remplacements de scellés doivent être historisés. La continuité de l'expédition doit survivre aux transbordements et changements de moyen.

9. Multimodalité

Route, rail, mer, air et autres modes peuvent constituer des segments successifs d'une même expédition. Chaque segment conserve ses acteurs, moyens et documents tout en restant raccordé à la chaîne globale.

10. Localisation et jalons

Les lieux déclarés, scans, événements de terminal et données télématiques autorisées peuvent enrichir la chronologie. La localisation documentaire ne doit pas être présentée comme preuve absolue d'une présence physique.

11. Conditions et chaîne du froid

Exigences de température, humidité, choc ou autres conditions doivent rester distinguées des mesures. Une excursion ou une lacune de données déclenche une analyse sans constituer automatiquement un verdict sur la marchandise.

12. Incidents, dommages et réserves

Retards, dommages, pertes, ruptures de scellés et autres incidents doivent conserver leurs déclarations, constats, expertises et réponses séparément. Les réserves à la livraison restent attribuées à leur auteur.

13. Preuve de livraison

Signature, horodatage, scan, photographie ou référence système peuvent constituer des éléments de preuve. Le passeport doit préciser ce qui est effectivement démontré et éviter toute extension automatique de portée.

14. Transport international

Frontières, transit, douanes, ports, aéroports, corridors et changements de juridiction doivent être représentés sans rompre l'identité de l'expédition. Les statuts réglementaires restent attribués à leurs autorités sources.

15. Sous-traitance

Les délégations successives doivent être reconstructibles du transporteur principal jusqu'aux exécutants. La sous-traitance en cascade ne doit ni casser la chaîne de possession ni confondre exécution physique et responsabilité contractuelle.

16. Assurance et réclamations

Déclarations de sinistre, réclamations, expertises, réponses et décisions assurantielles doivent rester des événements distincts. AP conserve les preuves sans déterminer lui-même couverture, indemnisation ou responsabilité.

17. Fraude documentaire et cybersécurité

Documents contradictoires, substitutions, signatures contestées, accès anormaux ou modifications suspectes peuvent déclencher des investigations. Les alertes doivent rester explicables et les accès compromis révocables.

18. Audit et AP Ledger

Les transferts de garde, documents critiques, preuves de livraison, changements de droits et autres événements sélectionnés doivent pouvoir être audités. AP Ledger peut ancrer des empreintes minimales sans publier les informations commerciales ou personnelles sensibles.

19. Critères d'acceptation

Le modèle est acceptable si l'expédition conserve son identité de bout en bout, si chaque événement est attribuable, si la chaîne de garde est reconstructible, si les conditions et mesures restent distinguées, si les changements de mode et de territoire préservent la continuité, et si les alertes ne deviennent pas des verdicts automatiques.

20. Clôture du Point 9 — Transport

Le Point 9 — Transport est désormais fonctionnellement défini : acteurs, expéditions, marchandises, unités, moyens, documents, garde, chargement, scellés, localisation, multimodalité, chaîne du froid, capteurs, incidents, livraison, douanes, frontières, sous-traitance, assurances, réclamations, fraude documentaire, cybersécurité, audit et AP Ledger. Cette architecture est prête à s'articuler avec le Point 10 — Billetterie.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 10 — BILLETTERIE

CHAPITRE 1 — MISSION, PÉRIMÈTRE, ÉVÉNEMENT OU TRAJET, INVENTAIRE, IDENTITÉ DU BILLET ET PRINCIPES FONDATEURS

1. Objet du chapitre

Le Point 10 — Billetterie transpose Authenticity Plus© / Deep Authenticity© à l'émission, la circulation et au contrôle des titres d'accès ou de transport. Il organise organisateurs et opérateurs, événements ou trajets, inventaires, billets, détenteurs, contrôles, transferts, reventes autorisées, annulations et remboursements.

2. Mission sectorielle

L'application Billetterie vise à rendre l'origine, l'état et la chaîne de possession d'un billet plus vérifiables. Elle ne se substitue ni à l'organisateur, ni à l'opérateur de transport, ni au vendeur, ni aux règles contractuelles ou réglementaires applicables.

3. Organisateur ou opérateur

L'entité qui crée l'événement, le service ou le trajet doit pouvoir être reliée à l'offre et à l'inventaire concernés. Son identité reste distincte de celle des distributeurs, plateformes ou revendeurs autorisés.

4. Événement, séance ou trajet

Concert, spectacle, rencontre sportive, musée, conférence, trajet ou autre prestation peut constituer l' objet du billet. Date, horaire, lieu, zone, service ou segment doivent être représentés selon le contexte.

5. Identité de l'offre

Une offre peut relier l'événement ou trajet à une catégorie, un tarif, une zone, une classe ou des conditions d'utilisation. Les évolutions tarifaires ne doivent pas modifier silencieusement les conditions attachées à un billet déjà émis.

6. Inventaire

L'inventaire représente les places, capacités, quotas ou droits d'accès disponibles. Les unités numérotées et les capacités non numérotées doivent être distinguées afin de prévenir la surémission documentaire.

7. Identité persistante du billet

Chaque billet doit disposer d'un identifiant unique et d'un statut évolutif. Son identité doit survivre à un transfert autorisé, à une réémission contrôlée ou à un changement de support sans créer plusieurs droits d'accès actifs.

8. Billet et support

Le droit d'accès doit rester distinct de son support : fichier PDF, billet mobile, carte, QR code, code-barres ou autre représentation. Copier le support ne doit pas créer un nouveau billet légitime.

9. Émission

L'émission relie le billet à l'offre, au vendeur ou système émetteur, à la date et aux conditions applicables. Un billet ne doit être considéré comme authentique que selon les preuves et statuts disponibles.

10. Détenteur et bénéficiaire

Acheteur, détenteur, bénéficiaire et personne autorisée à entrer peuvent être différents. Les données personnelles doivent être minimisées et seules les informations nécessaires au contrôle ou aux obligations applicables doivent être exposées.

11. Billet nominatif

Lorsqu'un billet est nominatif, le lien avec le bénéficiaire doit être protégé et modifiable uniquement selon les règles prévues. Authenticity Plus© ne doit pas rendre publiquement accessible l'identité du détenteur.

12. Statut du billet

Émis, actif, transféré, utilisé, annulé, remboursé, expiré ou autre statut peut être représenté. Les transitions doivent être historisées afin d'éviter qu'un ancien support reste présenté comme actif après un changement.

13. Contrôle d'accès

Le contrôle peut vérifier identité du billet, statut, événement ou trajet, créneau, zone et autres conditions nécessaires. Le résultat du contrôle doit être horodaté et attribué au dispositif ou opérateur concerné.

14. Première utilisation et duplication

Lorsqu'un billet n'autorise qu'une entrée, une utilisation valide doit empêcher la réutilisation du même droit selon les règles du système. Plusieurs copies d'un QR code ne doivent donc pas créer plusieurs accès légitimes.

15. Transfert autorisé

Un billet transférable peut changer de détenteur selon les règles de l'organisateur ou de l'opérateur. Le transfert doit désactiver ou rendre obsolète l'ancien support lorsque cela est nécessaire à la prévention des doublons.

16. Revente autorisée

Une revente peut être représentée comme transaction secondaire lorsqu'elle est permise. Prix, plateforme, limites ou autres conditions restent attribués à leurs sources ; AP ne crée pas lui-même un droit général de revente.

17. Annulation et remboursement

Annulation d'événement, changement de service, remboursement ou avoir peuvent modifier le statut du billet. L'historique doit préserver émission, transaction et décision sans permettre l'utilisation d'un titre remboursé lorsque les règles l'interdisent.

18. Alertes de fraude présumée

Identifiant dupliqué, support présenté plusieurs fois, billet annulé proposé à la vente, incohérence d' inventaire ou chaîne de transfert contradictoire peut déclencher une alerte. Le signal doit rester explicable et ne constitue pas automatiquement une accusation de fraude.

19. Critères d'acceptation

Le modèle est acceptable si billet et support restent distincts, si l'inventaire est relié à l'émission, si un transfert préserve une seule identité active, si les statuts sont historisés, si le contrôle d'accès est attribuable et si les données personnelles sont minimisées.

20. Conclusion

L'application Billetterie établit un passeport du droit d'accès ou de transport. En reliant offre, inventaire, billet, détenteur, statut, contrôle, transfert et remboursement, Authenticity Plus© crée une continuité de preuve capable de réduire duplication, falsification et opacité du marché secondaire.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 10 — BILLETTERIE

CHAPITRE 2 — ÉMISSION, QR CODES ET IDENTIFIANTS DYNAMIQUES, CONTRÔLE D'ACCÈS, VALIDATION HORS LIGNE, ANTI-DUPLICATION ET LUTTE CONTRE LES FAUX BILLETS

1. Objet du chapitre

Ce chapitre définit la couche opérationnelle d'émission et de validation du billet. Il organise identifiants, supports, QR codes ou autres représentations, contrôle d'accès, fonctionnement connecté ou hors ligne, synchronisation, anti-duplication et gestion des billets suspects.

2. Création de l'identité du billet

L'émission doit créer une identité unique reliée à l'offre, à l'inventaire, à l'émetteur et au statut initial. Cette identité logique reste la référence principale même si plusieurs représentations techniques sont successivement produites.

3. Identifiant public et identifiant interne

Lorsque nécessaire, un identifiant présenté au détenteur peut être distinct de l'identifiant interne du billet. Cette séparation peut limiter l'exposition d'informations sensibles et réduire les risques liés à la réutilisation d'un identifiant visible.

4. QR code et code-barres

Un QR code, code-barres ou autre symbole constitue un support de présentation du billet. Il doit être traité comme une représentation vérifiable du droit d'accès et non comme le droit lui-même.

5. Identifiants dynamiques

Lorsque l'architecture le permet, la représentation présentée au contrôle peut évoluer dans le temps ou selon un mécanisme sécurisé. Le changement de représentation ne doit pas créer de nouvelle identité de billet ni altérer son historique.

6. Jetons temporaires

Un jeton temporaire peut être associé à un billet pour une période ou un contexte de contrôle déterminé. Sa durée, son émetteur et son rattachement au billet doivent être vérifiables afin d'éviter qu'un jeton expiré reste interprété comme actif.

7. Émission et signature

Les données critiques d’émission peuvent être signées ou associées à une preuve d’intégrité. Le système de contrôle doit pouvoir distinguer un billet authentiquement émis d’une simple copie visuelle d’un support.

8. Distribution du billet

Le billet peut être remis par application, portefeuille numérique, fichier, impression ou autre canal autorisé. Chaque canal doit préserver l’identité et le statut du même billet sans créer plusieurs droits indépendants.

9. Contrôle en ligne

Lorsque le dispositif est connecté, il peut vérifier en temps utile l’identité, le statut, l’événement ou trajet, le créneau et les conditions pertinentes. La décision de validation doit être journalisée avec le dispositif ou opérateur concerné.

10. Contrôle hors ligne

Lorsque la connectivité est indisponible, un dispositif peut utiliser des données ou preuves préchargées permettant une validation limitée. Le périmètre, la fraîcheur et les limites de cette validation hors ligne doivent être explicites.

11. Risque de double validation hors ligne

Deux dispositifs isolés peuvent ne pas connaître immédiatement les validations effectuées par l’autre. L’architecture doit donc prévoir des règles de réduction du risque et une réconciliation ultérieure, sans prétendre qu’un fonctionnement hors ligne garantit l’absence absolue de duplication.

12. Synchronisation

Après reconnexion, les validations hors ligne doivent être synchronisées avec le registre opérationnel. Les conflits, doubles présentations ou événements incompatibles doivent rester visibles dans l’ historique.

13. Première entrée et réentrée

Les règles peuvent autoriser une entrée unique, plusieurs passages ou une réentrée. Le contrôle doit appliquer le régime attaché au billet et ne pas interpréter automatiquement toute seconde présentation comme fraude.

14. Zones et droits partiels

Un billet peut donner accès à une zone, une classe, un segment, une séance ou un service particulier. Une validation partielle ne doit pas consommer des droits indépendants qui restent encore valables selon l’offre.

15. Anti-duplication

La prévention des doublons repose sur l'identité unique, le statut, l'historique de validation et, lorsque pertinent, des représentations renouvelables. Une copie du support peut être détectée par la contradiction avec l'état du billet.

16. Faux billet présumé

Signature invalide, identifiant inconnu, billet annulé, support modifié ou données incompatibles peuvent déclencher un signal de billet suspect. Le système doit expliquer le motif sans accuser automatiquement la personne qui le présente.

17. Support capturé ou partagé

Une capture d'écran ou copie peut reproduire visuellement un billet. Le contrôle doit donc s'appuyer sur l'état vérifiable du droit et non uniquement sur l'apparence du QR code ou du document.

18. Journal d'accès

Tentatives de validation, succès, refus, réentrées et conflits peuvent être journalisés avec minimisation des données personnelles. Les journaux servent à l'exploitation et à l'audit sans devenir un mécanisme de surveillance disproportionnée.

19. Critères d'acceptation

Le modèle est acceptable si l'identité du billet reste unique malgré ses supports, si les jetons temporaires ont une portée limitée, si le contrôle hors ligne expose ses limites, si la synchronisation préserve les conflits, et si une copie visuelle ne suffit pas à créer un droit d'accès valide.

20. Conclusion

L'anti-fraude en billetterie dépend de la séparation entre droit, identité et support. Authenticity Plus© permet de valider l'état du billet, de gérer les représentations dynamiques et de réconcilier les contrôles connectés ou hors ligne tout en conservant une piste d'audit explicable.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 10 — BILLETTERIE

CHAPITRE 3 — TRANSFERT, REVENTE OFFICIELLE, MARCHÉ SECONDAIRE, PLAFONNEMENT, CHANGEMENT DE DÉTENTEUR, REMBOURSEMENT ET LUTTE CONTRE LE SCALPING ET LES REVENTES FRAUDULEUSES

1. Objet du chapitre

Ce chapitre organise la circulation secondaire du billet après son émission. Il encadre transfert, revente autorisée, changement de détenteur, plafonnement éventuel, remboursement et annulation afin de préserver une seule identité active du billet et une chaîne de provenance vérifiable.

2. Principe de continuité

Un transfert ou une revente ne crée pas un nouveau droit indépendant. L'identité persistante du billet est conservée tandis que son détenteur, son support et certains statuts peuvent évoluer selon les règles applicables.

3. Transfert sans vente

Un détenteur peut, lorsque l'offre l'autorise, transférer le billet à un autre bénéficiaire sans transaction commerciale. L'événement doit conserver l'ancien et le nouveau statut sans exposer inutilement les données personnelles des parties.

4. Changement de détenteur

Le changement de détenteur doit être atomique du point de vue fonctionnel : l'ancien droit de présentation est désactivé ou rendu obsolète au moment où le nouveau devient valide, afin d'éviter deux supports actifs pour le même billet.

5. Réémission du support

Après transfert, un nouveau QR code, jeton ou autre support peut être émis. L'ancien support doit rester lié à l'historique mais ne plus produire un accès lorsque les règles imposent son invalidation.

6. Revente officielle

Une plateforme ou un canal autorisé peut organiser la revente du billet. La transaction secondaire doit rester reliée au billet d'origine, à l'offre, au vendeur, à l'acquéreur et aux règles applicables.

7. Marché secondaire

Le marché secondaire doit conserver la provenance du billet plutôt que recréer une identité opaque. Prix initial, prix de revente et frais peuvent être représentés séparément lorsque leur conservation est autorisée.

8. Plafonnement du prix

Lorsque l'organisateur, l'opérateur ou la réglementation impose un plafond, la règle doit être enregistrée avec sa source, son territoire et sa période d'application. AP peut contrôler la cohérence documentaire sans créer lui-même la règle de prix.

9. Frais et commissions

Frais de service, commission de plateforme ou autres montants doivent être distingués du prix facial et du prix de revente. Cette séparation améliore la transparence du coût total pour l'acquéreur.

10. Scalping et achat automatisé

Des volumes anormaux, comptes multiples, achats rapides ou autres signaux peuvent contribuer à une investigation sur une acquisition abusive. Aucun indicateur isolé ne doit suffire à accuser automatiquement une personne ou organisation.

11. Limites de quantité

Les quotas par compte, identité, moyen de paiement ou autre critère peuvent être appliqués selon les règles de l'émetteur. Leur contrôle doit respecter la minimisation des données et les exigences applicables.

12. Revente hors canal autorisé

Un billet proposé hors d'un canal autorisé peut être signalé lorsque les règles de l'offre le prévoient. L' existence d'une annonce exteme ne suffit pas à déterminer automatiquement la validité juridique de la revente.

13. Détection des doublons de vente

Le même billet proposé simultanément à plusieurs acheteurs, ou un support déjà transféré remis en circulation, peut produire une alerte. L'état central du billet doit permettre de distinguer l'identité valide des copies obsolètes.

14. Billet annulé ou remboursé proposé à la vente

Un billet annulé, remboursé ou expiré ne doit pas retrouver un statut actif par simple copie ou revente du support. Toute tentative contradictoire avec le registre opérationnel doit être signalée au contrôle.

15. Remboursement

Le remboursement peut être total ou partiel selon les règles de l'offre. L'événement doit conserver montant, motif, acteur décisionnaire et statut résultant, sans effacer la transaction initiale.

16. Annulation ou modification de l’événement

Annulation, report, changement de lieu, horaire ou service peut déclencher des droits ou options définis par l’organisateur ou l’opérateur. AP conserve les versions de l’offre et les décisions sans inventer des droits de remboursement.

17. Litiges du marché secondaire

Vendeur, acheteur, plateforme ou organisateur peuvent produire des déclarations et preuves contradictoires. Le dossier doit conserver transactions, statuts, supports, validations et réponses sans arbitrage automatique.

18. Confidentialité et audit

Les données de transaction et d’identité doivent être accessibles uniquement selon les rôles autorisés. Les transferts, changements de statut, remboursements et validations critiques doivent pouvoir être audités.

19. Critères d’acceptation

Le modèle est acceptable si un transfert ne crée jamais deux billets actifs, si l’ancien support devient obsolète lorsque nécessaire, si prix facial, revente et frais restent distingués, si les règles de plafonnement conservent leur source, et si les signaux de scalping ou fraude restent investigables.

20. Conclusion

La circulation secondaire ne doit pas casser l’authenticité du billet. Authenticity Plus© transforme transfert et revente en événements traçables reliés au billet d’origine, ce qui permet de préserver la confiance, de réduire les doublons et d’améliorer la transparence sans imposer lui-même les règles commerciales ou juridiques du marché.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 10 — BILLETTERIE

CHAPITRE 4 — PAIEMENT, RÉSERVATION, ÉMISSION DIFFÉRÉE, ANNULATION, REMBOURSEMENT, CHARGEBACK, LITIGES ET RAPPROCHEMENT FINANCIER DE LA BILLETTERIE

1. Objet du chapitre

Ce chapitre organise la relation entre réservation, paiement et cycle de vie du billet. Il distingue les événements commerciaux et financiers de l'identité du titre afin que paiement, émission, annulation, remboursement, contestation et rapprochement restent traçables sans être confondus.

2. Réservation et billet

Une réservation peut bloquer temporairement une place, un quota ou un droit sans constituer encore un billet définitivement émis. Le système doit distinguer réservation, commande, paiement et émission.

3. Durée de réservation

Une réservation temporaire peut comporter une échéance. À expiration, l'inventaire peut être libéré selon les règles de l'émetteur, avec conservation de la trace de la réservation expirée.

4. Commande

La commande regroupe un ou plusieurs billets, options, frais ou services. Son identifiant et son statut restent distinctsdes identifiants individuels des billets qu'elle peut générer.

5. Paiement

Le paiement peut être initié, autorisé, capturé, refusé, annulé ou remboursé selon les informations fournies par le prestataire concerné. AP conserve ces statuts sans traiter lui-même les données de paiement sensibles au-delà de ce qui est nécessaire.

6. Référence du prestataire de paiement

Les références externes de transaction peuvent être reliées à la commande pour permettre le rapprochement. Les données bancaires complètes ne doivent pas être enregistrées dans le passeport de billetterie.

7. Émission immédiate

Lorsque les règles le permettent, le billet peut être émis après confirmation du paiement ou d'un autre fondement autorisé. L'événement d'émission doit conserver la condition qui l'a déclenché.

8. Émission différée

Certains billets peuvent être émis ultérieurement, par exemple après validation, attribution de place ou ouverture d'une fenêtre de délivrance. La commande payée doit alors rester distincte du billet encore non émis.

9. Paiement sans émission

Un paiement confirmé mais non suivi de l'émission attendue doit pouvoir produire une alerte opérationnelle. Cette incohérence nécessite vérification et ne doit pas être masquée par une création automatique non justifiée du billet.

10. Émission sans paiement

Un billet peut être émis sans paiement dans des cas documentés tels qu'invitation, gratuité, échange ou autre règle autorisée. L'absence de paiement ne constitue donc pas automatiquement une anomalie.

11. Annulation de commande

Une commande peut être annulée avant ou après émission selon les règles applicables. Les billets concernés doivent recevoir les statuts appropriés sans suppression de leur historique.

12. Remboursement

Un remboursement peut concerner tout ou partie d'une commande ou d'un billet. Montant, motif, date, acteur décisionnaire et référence de transaction doivent pouvoir être conservés.

13. Remboursement et validité du billet

Lorsque le remboursement entraîne l'annulation du droit d'accès, le billet doit devenir inutilisable selon les règles applicables. Un support antérieurement délivré ne doit pas pouvoir réactiver un titre remboursé.

14. Chargeback et contestation de paiement

Une contestation initiée auprès d'un prestataire de paiement peut être enregistrée avec son statut et sa référence. L'existence d'un chargeback ne permet pas à AP de conclure automatiquement à une fraude du détenteur ou du vendeur.

15. Billet utilisé puis contesté

Si un billet a été validé avant une contestation financière, les deux événements doivent rester visibles. La plateforme conserve la chronologie afin de soutenir l'analyse sans décider seule du résultat du litige.

16. Litige commercial

Acheteur, vendeur, organisateur, opérateur ou plateforme peuvent fournir des positions et preuves contradictoires. Commande, billet, validations, transferts, remboursements et communications doivent pouvoir être rassemblés dans un dossier d'audit.

17. Rapprochement financier

Les montants de commandes, paiements, remboursements, frais et transactions secondaires peuvent être rapprochés selon les références disponibles. Les écarts doivent être signalés sans être automatiquement qualifiés de détournement ou d'erreur comptable.

18. Confidentialité et sécurité

Les données financières doivent être minimisées, segmentées et accessibles uniquement aux rôles autorisés. Les journaux doivent privilégier identifiants de transaction, montants et statuts nécessaires plutôt que données bancaires sensibles.

19. Critères d'acceptation

Le modèle est acceptable si réservation, commande, paiement et billet restent distincts, si l'émission différée est représentable, si remboursements modifient correctement les statuts, si les chargebacks restent des événements financiers attribués, et si le rapprochement conserve les écarts et leurs sources.

20. Conclusion

La fiabilité de la billetterie dépend autant de la continuité financière que de l'authenticité du billet. Authenticity Plus© relie réservation, commande, paiement, émission, remboursement, contestation et utilisation pour produire une chronologie cohérente sans devenir prestataire de paiement, banque ou arbitre du litige.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 10 — BILLETTERIE

CHAPITRE 5 — GOUVERNANCE DES ORGANISATEURS ET DISTRIBUTEURS, CYBERSÉCURITÉ, FRAUDE, CONFIDENTIALITÉ, CONTRÔLE OPÉRATIONNEL, AUDIT ET AP LEDGER DE LA BILLETTERIE

1. Objet du chapitre

Ce chapitre définit la gouvernance opérationnelle et sécuritaire de l'écosystème Billetterie. Il organise les responsabilités des organisateurs, opérateurs, distributeurs, plateformes secondaires et contrôleurs, ainsi que la cybersécurité, la confidentialité, les investigations de fraude, l'audit et l'usage proportionné d'AP Ledger.

2. Gouvernance des acteurs

Organisateur, opérateur, billetterie primaire, distributeur, revendeur autorisé, prestataire technique et contrôleur doivent disposer de rôles et droits distincts. L'accès à l'inventaire ne doit pas conférer automatiquement le pouvoir de modifier les règles commerciales ou les statuts des billets.

3. Organisateur et source de l'offre

L'organisateur ou l'opérateur responsable de la prestation doit pouvoir être identifié comme source de l'événement, du trajet ou des conditions d'accès. Les distributeurs conservent leur propre rôle sans devenir automatiquement propriétaires de l'inventaire.

4. Distributeurs autorisés

Un distributeur peut recevoir un quota, une période, un canal ou des catégories de billets déterminés. Les émissions doivent rester rattachées à l'inventaire source afin de prévenir les doubles allocations et les surémissions.

5. Gouvernance du marché secondaire

Les plateformes secondaires autorisées peuvent recevoir des droits spécifiques de transfert ou de revente. Leur périmètre doit être explicite afin qu'une plateforme non autorisée ne puisse pas modifier le statut officiel d'un billet.

6. Séparation des privilèges

Création d'événement, gestion d'inventaire, émission, remboursement, modification de prix, contrôle d'accès et administration de sécurité doivent pouvoir relever de privilèges séparés. Cette séparation réduit les risques d'erreur et d'abus internes.

7. Authentification des opérateurs

Les comptes disposant de privilèges sensibles doivent utiliser des mécanismes d'authentification adaptés au risque. Les sessions, appareils ou clés compromis doivent pouvoir être suspendus ou révoqués.

8. Cybersécurité de l'émission

Une compromission du système d'émission peut affecter de nombreux billets. Les opérations de création en masse, changements d'inventaire, réémissions ou modifications de statut doivent donc être particulièrement journalisées et surveillées.

9. Cybersécurité du contrôle

Les terminaux de contrôle doivent être identifiables, administrables et révocables. Un dispositif perdu ou compromis ne doit pas conserver indéfiniment la capacité de valider des billets ou d'accéder aux données sensibles.

10. Fraude interne présumée

Émissions hors quota, remboursements inhabituels, changements répétés de détenteur, validations administratives anormales ou modifications massives peuvent produire des signaux d'investigation. Aucun indicateur isolé ne constitue une preuve automatique de fraude.

11. Fraude externe présumée

Faux sites, supports copiés, identifiants falsifiés, annonces multiples, billets annulés revendus ou tentatives répétées de validation peuvent être corrélés à un dossier d'investigation sans accusation automatique du détenteur.

12. Protection du détenteur

Un acheteur de bonne foi peut présenter un billet devenu invalide à la suite d'une fraude en amont. Le système doit permettre d'expliquer l'état du billet et sa chaîne de provenance sans présumer l'intention de la personne qui le présente.

13. Confidentialité

Identité des détenteurs, transactions, moyens de contact et données de contrôle doivent être minimisés. Les informations accessibles à un contrôleur d'entrée peuvent être plus limitées que celles accessibles au service client ou à l'équipe d'investigation.

14. Conservation des données

Les durées de conservation doivent être proportionnées aux finalités opérationnelles, contractuelles, de sécurité et d'audit. Les données qui ne sont plus nécessaires doivent pouvoir être supprimées ou anonymisées lorsque les obligations applicables le permettent.

15. Continuité opérationnelle

Panne réseau, indisponibilité d'un service, saturation ou incident de cybersécurité ne doit pas nécessairement interrompre tout contrôle. Des modes dégradés peuvent être prévus avec limites explicites, journalisation locale et réconciliation ultérieure.

16. Gestion des incidents

Un incident doit pouvoir conserver date, système concerné, impact, actions de confinement, restauration et éléments de preuve. Les corrections ultérieures ne doivent pas effacer la chronologie initiale.

17. Audit des opérations sensibles

Création ou modification d'inventaire, émissions administratives, transferts, remboursements, annulations, changements de privilèges et validations exceptionnelles doivent pouvoir être audités avec auteur ou système, date et motif disponible.

18. AP Ledger

Des empreintes de lots d'émission, états d'inventaire, règles critiques, transferts ou journaux sélectionnés peuvent être ancrées dans AP Ledger. Les données personnelles, secrets opérationnels et informations financières détaillées doivent rester hors des couches publiques ou irréversibles.

19. Critères d'acceptation

Le modèle est acceptable si les rôles sont séparés, si les quotas des distributeurs restent rattachés à l'inventaire source, si les terminaux compromis sont révocables, si les alertes de fraude restent explicables, si les détenteurs sont protégés contre les présomptions automatiques et si les opérations sensibles sont auditables.

20. Conclusion

La confiance dans la billetterie dépend autant de la gouvernance des opérateurs que de la technologie du billet. Authenticity Plus© relie privilèges, inventaires, émissions, contrôles, incidents et preuves afin de rendre l'écosystème auditable, résilient et moins vulnérable aux manipulations internes ou externes.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 10 — BILLETTERIE

CHAPITRE 6 — SYNTHÈSE FONCTIONNELLE, CRITÈRES D'ACCEPTATION ET CLÔTURE DE L'APPLICATION BILLETTERIE

1. Objet du chapitre

Ce chapitre clôt le Point 10 — Billetterie. Il consolide organisateurs, opérateurs, offres, inventaires, réservations, commandes, paiements, billets, supports, contrôles, transferts, reventes, remboursements, litiges, cybersécurité, audit et AP Ledger.

2. Mission consolidée

L'application Billetterie constitue un passeport du droit d'accès ou de transport. Elle vise à rendre l'origine, le statut, la circulation et l'utilisation d'un billet vérifiables sans se substituer aux organisateurs, opérateurs, distributeurs, prestataires de paiement ou autorités compétentes.

3. Identité persistante du billet

Chaque billet conserve une identité unique pendant tout son cycle de vie. Cette identité survit aux changements de support, de détenteur et aux réémissions contrôlées, sans permettre la coexistence de plusieurs droits actifs lorsque l'offre ne l'autorise pas.

4. Offre et inventaire

Événement, trajet, séance, zone, classe, tarif et capacité doivent rester reliés à l'inventaire source. Les quotas distribués à différents canaux doivent pouvoir être rapprochés afin de limiter surémission et doubles allocations.

5. Réservation, commande et émission

Réservation, commande, paiement et émission sont des événements distincts. Une réservation peut expirer sans billet, et une commande payée peut rester en attente lorsqu'une émission différée est prévue.

6. Billet et support

PDF, billet mobile, QR code, code-barres, carte ou jeton ne sont que des représentations du droit. Copier un support ne crée jamais un second billet légitime.

7. Identifiants dynamiques

Des représentations ou jetons temporaires peuvent renforcer la sécurité lorsque l'architecture le prévoit. Leur renouvellement ne modifie pas l'identité persistante du billet.

8. Contrôle d'accès

Le contrôle doit vérifier les conditions nécessaires selon l'offre et journaliser le résultat. Les dispositifs et opérateurs doivent être attribuables et leurs privilèges révocables.

9. Validation hors ligne

Un mode hors ligne peut assurer une continuité de service avec données préchargées et limites explicites. Il doit être suivi d'une synchronisation et d'une réconciliation des éventuels conflits.

10. Anti-duplication

L'identité unique, le statut, l'historique de validation et les supports obsolètes permettent de détecter les doubles présentations. Une seconde présentation n'est toutefois pas automatiquement frauduleuse lorsque les règles autorisent la réentrée.

11. Transfert

Un transfert autorisé modifie le détenteur du même billet. Lorsque nécessaire, l'ancien support devient obsolète au moment où le nouveau support est activé.

12. Revente et marché secondaire

Une revente autorisée reste rattachée au billet d'origine. Prix facial, prix secondaire, frais, règles de plafonnement et canal doivent pouvoir rester distingués et attribués à leurs sources.

13. Remboursement et annulation

Les remboursements et annulations modifient le statut selon les règles applicables sans effacer l' historique. Un support correspondant à un billet annulé ne doit pas réactiver le droit.

14. Paiements et rapprochement

Les références, montants et statuts financiers nécessaires peuvent être corrélés aux commandes et billets. Les données bancaires sensibles ne doivent pas être intégrées inutilement au passeport.

15. Chargebacks et litiges

Contestations financières, réclamations et positions contradictoires doivent rester historisées avec leurs preuves. AP ne décide pas automatiquement qui a raison ni si une fraude a été commise.

16. Gouvernance et cybersécurité

Création d'événement, inventaire, émission, remboursement, contrôle et administration doivent pouvoir utiliser des privilèges séparés. Les comptes et terminaux compromis doivent pouvoir être suspendus ou révoqués.

17. Protection des détenteurs

La présence d’un faux billet, d’un billet dupliqué ou d’un titre devenu invalide ne doit pas conduire automatiquement à accuser la personne qui le présente. La chaîne de provenance sert précisément à localiser l’origine probable de l’anomalie.

18. Audit et AP Ledger

Émissions, états d’inventaire, transferts, remboursements, changements de privilèges et événements critiques doivent pouvoir être audités. AP Ledger peut ancrer des empreintes minimales sans exposer les données personnelles ou financières détaillées.

19. Critères d’acceptation

Le modèle est acceptable si billet et support restent distincts, si l’inventaire est cohérent avec les émissions, si transfert et revente conservent une identité unique, si le contrôle hors ligne expose ses limites, si les données sensibles sont minimisées et si les alertes restent explicables.

20. Clôture du Point 10 — Billetterie

Le Point 10 — Billetterie est désormais fonctionnellement défini : organisateurs, événements et trajets, offres, inventaires, réservations, commandes, paiements, billets, supports, QR codes, identifiants dynamiques, contrôles, hors ligne, transferts, reventes, remboursements, chargebacks, litiges, gouvernance, cybersécurité, fraude, audit et AP Ledger. Cette architecture est prête à s’articuler avec le Point 11 — Seconde main.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 11 — SECONDE MAIN

CHAPITRE 1 — MISSION, PÉRIMÈTRE, IDENTITÉ DE L'OBJET, PROVENANCE, DÉTENTION, ÉTAT DOCUMENTÉ ET PRINCIPES FONDATEURS

1. Objet du chapitre

Le Point 11 — Seconde main transpose Authenticity Plus© / Deep Authenticity© au cycle de vie des biens revendus. Il organise identité de l'objet, provenance, preuve d'achat, détention, usage documenté, entretien, réparation, état, mise en vente, transaction et transfert afin que l'historique utile survive aux changements de propriétaire.

2. Mission sectorielle

L'application vise à réduire l'asymétrie d'information entre vendeur et acheteur en rendant vérifiables les preuves disponibles. Elle ne garantit pas automatiquement l'état réel d'un objet et ne se substitue ni à l'expertise, ni aux règles de garantie, ni aux autorités compétentes.

3. Périmètre des biens

Le modèle peut s'appliquer à des biens identifiables tels que électronique, mobilier, équipements, outils, articles de mode, objets de collection, produits industriels ou autres biens réutilisables. Les exigences de preuve peuvent varier selon la catégorie.

4. Identité persistante de l'objet

L'objet doit conserver une identité stable de sa première mise en circulation aux reventes successives. Numéro de série, identifiant fabricant, tag AP ou autre référence peuvent contribuer à cette identité sans être automatiquement équivalents.

5. Objet et support d'identification

QR code, NFC, étiquette, certificat ou document n'est qu'un support permettant d'accéder au passeport. Copier le support ne doit pas créer une seconde identité légitime pour un autre objet.

6. Provenance d'origine

Fabricant, artisan, distributeur, vendeur initial ou autre source peut être relié à l'objet lorsque les preuves existent. La provenance doit distinguer déclaration commerciale, document source et vérification indépendante.

7. Preuve d'achat

Facture, reçu, commande, certificat ou autre justificatif peut être rattaché à l'objet. Une preuve d'achat contribue à la chaîne documentaire mais ne démontre pas nécessairement à elle seule la propriété juridique actuelle.

8. Propriétaire, détenteur et utilisateur

Propriétaire, détenteur et utilisateur peuvent être des personnes différentes. Le passeport doit préserver cette distinction et minimiser les données personnelles visibles lors d'une consultation ou d' une revente.

9. Transfert de détention

Prêt, location, dépôt, réparation ou autre remise temporaire ne doit pas être confondu avec un transfert de propriété. Les changements de garde peuvent être historisés lorsqu'ils sont pertinents.

10. Historique de propriété

Les transferts successifs peuvent former une chaîne de propriété documentée. L'acheteur peut recevoir une preuve de continuité sans obtenir l'identité personnelle complète des propriétaires précédents.

11. Usage documenté

Lorsque pertinent, certains événements d'usage peuvent être enregistrés : durée, cycles, kilométrage, heures de fonctionnement ou autres indicateurs adaptés à la catégorie. Ces données conservent leur source et leur niveau de confiance.

12. Entretien

Les opérations d'entretien peuvent être rattachées à l'objet, au prestataire, à la date et aux pièces justificatives. Leur présence ne constitue pas automatiquement une certification de l'état actuel.

13. Réparation

Une réparation doit pouvoir distinguer défaut déclaré, diagnostic, intervention, pièces remplacées et contrôle éventuel. Les conclusions restent attribuées au professionnel ou à la source qui les émet.

14. Pièces remplacées

Lorsqu'un composant identifiable est remplacé, l'objet conserve son identité principale tandis que le composant sortant et le composant entrant peuvent être historisés. Cette logique permet d'éviter l' effacement des transformations importantes.

15. État documenté

L'état peut être décrit par le vendeur, un professionnel, une inspection ou des preuves photographiques. Ces niveaux doivent rester séparés : une déclaration du vendeur n'est pas une expertise indépendante.

16. Défauts connus et réparations antérieures

Les défauts déclarés, dommages documentés ou réparations antérieures peuvent être présentés à l'acheteur selon les règles applicables. L'absence d'un défaut dans AP ne signifie pas automatiquement que l'objet en est exempt.

17. Mise en vente

Une annonce peut être reliée à l'identité du bien et à un sous-ensemble autorisé de son passeport. Description, prix, état déclaré et vendeur restent des données de l'annonce et ne doivent pas écraser l'historique antérieur.

18. Signaux d'anomalie

Numéro de série incohérent, passeport dupliqué, historique contradictoire, objet signalé, preuve d'achat incompatible ou plusieurs ventes simultanées peuvent produire une alerte. Celle-ci déclenche une vérification et ne constitue pas automatiquement une accusation.

19. Critères d'acceptation

Le modèle est acceptable si l'identité de l'objet survit aux reventes, si propriétaire et détenteur restent distincts, si déclaration d'état et expertise sont séparées, si réparations et composants sont historisés, si les données personnelles sont minimisées et si les anomalies restent explicables.

20. Conclusion

L'application Seconde main transforme la revente en continuité de provenance plutôt qu'en rupture d'historique. Authenticity Plus© permet à un objet de conserver les preuves utiles de son origine, de ses transformations et de ses transactions successives, afin d'améliorer la confiance sans promettre une certitude que les sources ne permettent pas d'établir.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 11 — SECONDE MAIN

CHAPITRE 2 — AUTHENTIFICATION AVANT REVENTE, ÉTAT ET GRADING, INSPECTION, RÉPARATIONS, RECONDITIONNEMENT, PIÈCES REMPLACÉES ET VALORISATION DOCUMENTAIRE

1. Objet du chapitre

Ce chapitre organise l'évaluation documentaire d'un bien avant sa revente. Il relie identité, authenticité, inspection, état déclaré ou observé, grading, réparations, reconditionnement, composants remplacés et complétude du passeport afin d'améliorer la transparence sans transformer Authenticity Plus© en expert universel de l'état du bien.

2. Vérification de l'identité avant revente

Avant publication d'une annonce, le vendeur ou un professionnel peut vérifier les identifiants disponibles : numéro de série, référence fabricant, tag AP, certificat ou autres éléments. Les divergences doivent rester visibles et peuvent déclencher une investigation.

3. Authentification documentaire

Facture d'origine, certificat, emballage, historique de service ou autres pièces peuvent contribuer à l' authentification. La présence d'un document ne suffit pas à garantir son authenticité ; sa provenance et son intégrité doivent être considérées séparément.

4. Authentification physique ou experte

Pour certaines catégories, une inspection physique ou l'avis d'un spécialiste peut compléter les preuves numériques. La conclusion doit rester attribuée à l'expert, au professionnel ou à l'organisme qui l'émet.

5. État déclaré par le vendeur

Le vendeur peut décrire l'état, les défauts connus, l'usure ou les accessoires inclus. Cette déclaration doit être identifiée comme telle et ne pas être présentée comme une expertise indépendante.

6. Inspection structurée

Une inspection peut utiliser une grille adaptée à la catégorie : fonctionnement, aspect, sécurité, accessoires, pièces manquantes ou autres critères. Date, inspecteur, méthode et limites doivent pouvoir être conservés.

7. Grading

Un grade peut synthétiser un état selon une échelle définie par une plateforme, un professionnel ou un standard. La source et la définition du grade doivent être accessibles afin d'éviter qu'un même terme soit interprété différemment selon les acteurs.

8. Grade et preuve sous-jacente

Le grade ne doit pas remplacer les observations qui l'ont produit. Photographies, mesures, tests ou remarques peuvent rester reliés au résultat afin de rendre l'évaluation explicable.

9. Usure normale et dommage

Lorsque la grille le permet, usure d'usage, défaut esthétique, dommage fonctionnel et dommage structurel doivent être distingués. La qualification reste attribuée à la source qui l'a réalisée.

10. Réparations antérieures

Les réparations connues doivent pouvoir être présentées avec date, prestataire, nature de l' intervention et justificatifs disponibles. Une réparation correctement documentée ne doit pas être assimilée automatiquement à une dégradation de valeur.

11. Reconditionnement

Un bien reconditionné doit pouvoir être relié au reconditionneur, au processus déclaré, aux tests réalisés et aux composants remplacés. Le terme reconditionné ne doit pas être utilisé comme synonyme automatique de neuf.

12. Niveaux de reconditionnement

Des catégories ou grades de reconditionnement peuvent exister selon les acteurs. Le passeport doit conserver la définition appliquée, les contrôles réalisés et la source du classement.

13. Pièces remplacées

Batterie, écran, moteur, carte électronique, mécanisme, boîtier ou autre composant identifiable peut être historisé lorsqu'il est remplacé. L'objet principal conserve son identité tandis que l'historique de transformation reste accessible.

14. Origine des pièces

Lorsqu'elle est connue, l'origine d'une pièce peut être documentée : fabricant, référence, neuve, reconditionnée, remanufacturée ou seconde main. AP ne doit pas inventer une origine ou une qualité absente des preuves.

15. Tests après intervention

Des tests fonctionnels ou contrôles post-réparation peuvent être reliés à l'intervention. Leur présence démontre qu'un test documenté a été effectué, non que l'objet restera exempt de panne future.

16. Photographies et preuves visuelles

Des images datées peuvent documenter l'état avant mise en vente, avant réparation ou après reconditionnement. Elles doivent être reliées à leur auteur ou système source et ne pas être présentées comme preuve absolue de tous les aspects non visibles.

17. Indice de complétude documentaire

Le passeport peut produire un indicateur de couverture : identité, origine, achats, entretien, réparations, inspections et transferts. Cet indice mesure la quantité ou la qualité documentaire disponible, pas l' état matériel réel du bien.

18. Valorisation documentaire

Un historique cohérent, des interventions traçables et une inspection récente peuvent soutenir la confiance et contribuer à la valorisation commerciale. Authenticity Plus© ne fixe toutefois pas automatiquement le prix de marché ni la valeur financière du bien.

19. Critères d'acceptation

Le modèle est acceptable si déclaration vendeur, inspection et expertise restent distinguées ; si tout grade possède une définition et une source ; si le reconditionnement conserve ses opérations et pièces ; si la complétude documentaire n'est pas confondue avec l'état matériel ; et si les divergences d'identité restent investigables.

20. Conclusion

L'authentification avant revente ne consiste pas à produire une note opaque, mais à rendre les preuves lisibles. Authenticity Plus© relie identité, inspection, grading, réparations, reconditionnement et pièces remplacées afin que l'acheteur puisse comprendre l'histoire documentée du bien avant la transaction.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 11 — SECONDE MAIN

CHAPITRE 3 — MISE EN VENTE, VENDEUR, ANNONCE AUTHENTIFIÉE, TRANSACTION, PAIEMENT, TRANSFERT DE PROPRIÉTÉ, LIVRAISON ET CONTINUITÉ DU PASSEPORT

1. Objet du chapitre

Ce chapitre organise le passage d'un bien documenté vers une transaction de seconde main. Il relie vendeur, annonce, objet, état, prix, transaction, paiement, livraison, réception et transfert de propriété afin que le passeport survive au changement d'acquéreur sans effacer l'historique antérieur.

2. Vérification du vendeur

Le vendeur peut être identifié ou vérifié selon le niveau de risque, la plateforme et les obligations applicables. Les données personnelles nécessaires à cette vérification ne doivent pas devenir publiques dans le passeport de l'objet.

3. Droit de mise en vente

La plateforme peut demander des éléments permettant d'établir que le vendeur est autorisé à proposer le bien. Cette vérification documentaire ne constitue pas automatiquement une décision définitive de propriété juridique.

4. Liaison entre annonce et objet

Une annonce authentifiée doit être reliée à une identité d'objet précise. Un même passeport ne doit pas être utilisé simultanément pour présenter plusieurs objets distincts comme s'ils étaient le même bien.

5. Contenu de l'annonce

Description, photographies, état déclaré, prix, accessoires, conditions de vente et informations de livraison doivent rester attribués au vendeur ou à la plateforme qui les fournit.

6. Données issues du passeport

L'annonce peut réutiliser certaines données vérifiées du passeport : référence, origine, réparations, inspection ou grade. Les données historiques ne doivent pas pouvoir être modifiées par le vendeur simplement pour améliorer l'annonce.

7. Différence entre déclaration et donnée vérifiée

Les informations déclarées par le vendeur doivent être visuellement ou structurellement distinguées des données provenant d'un fabricant, d'un réparateur, d'un expert ou d'une autre source indépendante.

8. Prix de vente

Le prix demandé et le prix effectivement convenu doivent pouvoir être distingués. Authenticity Plus© ne détermine pas automatiquement la valeur de marché ni le caractère équitable du prix.

9. Réservation de l'objet

Lorsqu'un acheteur réserve le bien, le statut de l'annonce peut évoluer afin de limiter les ventes simultanées. Une réservation ne constitue pas nécessairement un transfert de propriété.

10. Transaction

La transaction doit relier l'objet, le vendeur, l'acquéreur, la date, le prix ou les références commerciales disponibles et le statut de l'opération. Les données sensibles sont minimisées.

11. Paiement

Le paiement peut être référencé par identifiant de transaction, montant et statut provenant du prestataire concerné. Les données bancaires complètes ne doivent pas être intégrées au passeport.

12. Paiement conditionnel ou séquestre

Lorsqu'un intermédiaire ou mécanisme de séquestre est utilisé, les étapes d'autorisation, blocage, libération ou remboursement peuvent être reliées à la transaction. AP ne devient pas lui-même établissement de paiement ou dépositaire des fonds.

13. Livraison ou remise en main propre

Expédition, point relais, livraison ou remise directe peuvent constituer des modalités distinctes. Les preuves disponibles doivent être reliées à la transaction sans confondre livraison matérielle et transfert juridique de propriété.

14. Preuve de réception

Signature, scan, confirmation dans une application ou autre preuve peut documenter la réception. Sanature et sa source doivent rester explicites ; une confirmation technique ne prouve pas automatiquement l'absence de défaut.

15. Contestation à réception

L'acquéreur peut signaler non-réception, objet différent, dommage ou autre divergence. La déclaration, les photographies, les réponses du vendeur et les éventuelles expertises doivent rester séparées.

16. Transfert de propriété documenté

Lorsque les règles et preuves permettent de documenter le transfert, le passeport peut enregistrer le changement de propriétaire avec date et fondement. AP ne crée pas lui-même le transfert juridique si celui-ci dépend de règles externes.

17. Transmission du passeport

Après transfert, le nouvel acquéreur reçoit les droits nécessaires pour administrer la continuité du passeport. L'ancien propriétaire perd les privilèges de gestion correspondants tout en restant représenté de manière minimisée dans l'historique.

18. Vente multiple et anomalies

Plusieurs transactions actives pour le même objet, annonce réutilisée après vente, paiement contradictoire ou transfert impossible peuvent produire une alerte. Celle-ci déclenche une investigation et non une accusation automatique.

19. Critères d'acceptation

Le modèle est acceptable si annonce et objet sont reliés, si données déclarées et vérifiées restent distinctes, si réservation, paiement, livraison et propriété ne sont pas confondus, si le passeport est transmis sans rupture et si les ventes multiples sont détectables.

20. Conclusion

La transaction de seconde main devient ainsi un événement de continuité plutôt qu'une rupture documentaire. Authenticity Plus© relie annonce, vendeur, acquéreur, paiement, livraison et transfert afin que le nouvel acquéreur hérite d'un historique vérifiable sans obtenir inutilement les données privées des propriétaires précédents.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 11 — SECONDE MAIN

CHAPITRE 4 — OBJETS VOLÉS OU SIGNALÉS, CONTREFAÇON PRÉSUMÉE, PASSEPORTS CLONÉS, NUMÉROS DE SÉRIE INCOHÉRENTS, FRAUDE À LA REVENTE, LITIGES ET RÉCUPÉRATION DE PROVENANCE

1. Objet du chapitre

Ce chapitre organise la gestion des anomalies graves susceptibles d'affecter la confiance dans un bien de seconde main. Il couvre signalements, objets potentiellement volés, contrefaçon présumée, clonage de passeport, incohérences d'identifiants, fraude documentaire, litiges et reconstruction de provenance, tout en maintenant une stricte distinction entre signalement, suspicion et décision compétente.

2. Principe de non-accusation automatique

Une anomalie technique ou documentaire ne suffit jamais à qualifier automatiquement une personne de fraudeur, voleur ou contrefacteur. Authenticity Plus© produit des signaux, conserve les preuves et facilite l'investigation ; la qualification juridique appartient aux acteurs ou autorités compétents.

3. Objet signalé

Un bien peut recevoir un statut de signalement lorsqu'une source autorisée déclare une perte, un vol présumé, une contestation de propriété ou une autre situation pertinente. Le statut doit conserver source, date, portée et état de traitement.

4. Confidentialité du signalement

L'existence d'une restriction peut être communiquée sans exposer publiquement l'identité du déclarant, de l'ancien propriétaire ou les détails sensibles d'une enquête. Les informations détaillées restent accessibles uniquement aux rôles autorisés.

5. Vérification avant transaction

Lorsqu'un objet est signalé ou présente une anomalie forte, une transaction peut nécessiter une vérification supplémentaire selon les règles de la plateforme. Toute suspension préventive doit rester proportionnée, traçable et réversible.

6. Numéro de série incohérent

Un numéro absent, altéré, dupliqué ou incompatible avec les références documentées peut produire une alerte. L'incohérence doit être examinée en tenant compte des réparations, remplacements de composants, erreurs de saisie ou autres explications possibles.

7. Identifiants multiples

Un objet peut légitimement posséder plusieurs identifiants : fabricant, composant, plateforme, certificat ou tag AP. Le système doit modéliser leurs relations afin de ne pas interpréter automatiquement leur différence comme une fraude.

8. Passeport cloné

Lorsqu'un même identifiant ou support semble être utilisé pour plusieurs objets distincts, le système peut détecter une contradiction de provenance. Le passeport authentique ne doit pas être déterminé uniquement par la première copie présentée.

9. QR, NFC et support copié

La copie d'un QR code, d'une puce ou d'une étiquette ne crée pas une seconde identité légitime. La vérification doit s'appuyer sur l'état du passeport, les preuves associées et, lorsque pertinent, les caractéristiques propres à l'objet.

10. Contrefaçon présumée

Différences de fabrication, identifiants incompatibles, certificat suspect, provenance impossible ou expertise défavorable peuvent contribuer à une investigation. AP ne prononce pas automatiquement qu'un bien est contrefait.

11. Fraude documentaire présumée

Facture modifiée, certificat incohérent, historique artificiellement créé, photographies réutilisées ou pièces contradictoires peuvent produire des alertes explicables. Les documents originaux et leurs versions doivent rester historisés.

12. Vente multiple

Plusieurs annonces ou transactions incompatibles pour le même objet peuvent signaler un risque de vente multiple. Les réservations, annulations et échecs de paiement doivent être considérés avant toute conclusion.

13. Dossier d'investigation

Un dossier peut regrouper identifiants, signalements, annonces, transactions, photographies, factures, inspections, expertises, messages de statut et autres preuves autorisées. Chaque élément conserve son auteur ou sa source et sa chronologie.

14. Contestation

Vendeur, acquéreur, ancien propriétaire, plateforme, fabricant ou autre partie peut contester un signalement ou une conclusion. Les positions contradictoires doivent rester visibles et ne pas être fusionnées en une vérité artificielle.

15. Vérification externe

Fabricant, expert, assureur, plateforme, autorité ou autre organisme compétent peut fournir une vérification ou décision. AP conserve son origine et sa portée sans l'étendre au-delà de ce que le document établit.

16. Résolution

Selon les éléments reçus, une restriction peut être levée, maintenue ou modifiée par l'acteur compétent. L'historique doit conserver le signalement initial, les vérifications et la résolution afin d' éviter une réécriture du passé.

17. Récupération de provenance

Lorsqu'un passeport est perdu, inaccessible ou absent, un processus de récupération peut reconstruire progressivement l'historique à partir de factures, certificats, réparations, photographies, identifiants, transactions et autres preuves attribuables.

18. Provenance partielle

Une provenance reconstruite doit indiquer clairement ses lacunes. Les périodes ou propriétaires inconnus restent inconnus ; Authenticity Plus© ne crée pas artificiellement les maillons manquants.

19. Critères d'acceptation

Le modèle est acceptable si signalement et décision restent distincts, si les données sensibles sont protégées, si un clone de support ne crée pas une identité valide, si les parties peuvent contester, si les résolutions restent historisées et si la provenance récupérée expose explicitement ses lacunes.

20. Conclusion

La confiance dans la seconde main exige de pouvoir traiter les anomalies sans transformer un signal en verdict. Authenticity Plus© relie identité, signalements, preuves, contestations et décisions externes afin de protéger acheteurs et propriétaires légitimes tout en permettant la récupération progressive d' un historique incomplet.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 11 — SECONDE MAIN

CHAPITRE 5 — GARANTIES, SAV, RÉPARABILITÉ, ÉCONOMIE CIRCULAIRE, RÉEMPLOI, RECYCLAGE, FIN DE VIE, GOUVERNANCE, AUDIT ET AP LEDGER

1. Objet du chapitre

Ce chapitre étend le passeport Seconde main au service après-vente et à la circularité. Il organise garanties documentées, interventions SAV, réparabilité, disponibilité des pièces, réemploi, reconditionnement, réaffectation, recyclage, fin de vie, gouvernance, audit et AP Ledger afin que l'historique utile accompagne le bien jusqu'à sa sortie du cycle d'usage.

2. Garantie d'origine

Une garantie commerciale, fabricant ou autre garantie documentée peut être reliée au bien avec émetteur, période, territoire et conditions disponibles. Authenticity Plus© conserve la preuve et son statut sans créer lui-même un droit de garantie.

3. Garantie transférable

Lorsqu'une garantie est transférable à un acquéreur de seconde main, le passeport peut documenter cette continuité. Si le transfert dépend de conditions externes, celles-ci restent attribuées à leur source et ne sont pas présumées satisfaites.

4. Garantie liée au reconditionnement

Un reconditionneur ou vendeur professionnel peut fournir une garantie propre à son intervention ou à la revente. Cette garantie doit rester distincte de la garantie initiale du fabricant.

5. Service après-vente

Demande SAV, diagnostic, prise en charge, intervention, restitution et clôture peuvent former une chronologie reliée au bien. Chaque étape conserve son acteur, sa date et les justificatifs disponibles.

6. Réparation sous garantie

Une réparation effectuée dans le cadre d'une garantie peut être reliée à la garantie invoquée et à la décision du prestataire. AP ne décide pas lui-même si une panne devait juridiquement être couverte.

7. Réparabilité

Le passeport peut documenter des informations de réparabilité provenant de fabricants, professionnels, standards ou autres sources identifiées. Un indice ou une appréciation doit conserver sa méthode, sa date et sa source.

8. Disponibilité des pièces

Références de composants, compatibilités documentées, disponibilité déclarée et alternatives autorisées peuvent être associées au bien. L'absence d'une pièce dans AP ne démontre pas qu'elle est indisponible sur le marché.

9. Documentation technique

Notices, schémas, instructions de maintenance ou références techniques peuvent être reliés au passeport selon les droits d'accès applicables. Les informations confidentielles ou protégées ne doivent pas être rendues publiques sans autorisation.

10. Réemploi

Un bien encore fonctionnel peut entrer dans un nouveau cycle d'usage par revente, don, réaffectation ou autre forme de réemploi. Son identité et son historique doivent être conservés lorsque cela est pertinent.

11. Réaffectation

Lorsqu'un bien change d'usage ou de contexte, l'événement peut être documenté sans prétendre que la nouvelle utilisation est automatiquement conforme à toutes les exigences applicables.

12. Réutilisation de composants

Lorsqu'un objet ne peut plus être utilisé comme ensemble, certains composants peuvent être récupérés et réutilisés. Les composants identifiables peuvent recevoir ou conserver une provenance liée à l'objet donneur.

13. Remanufacturation et reconditionnement

Une opération industrielle ou professionnelle de remise en état peut créer un nouvel état documenté du bien. Les pièces remplacées, tests et acteur responsable doivent rester reliés à l'identité historique.

14. Orientation vers recyclage

Lorsqu'un bien est orienté vers une filière de recyclage, l'événement peut enregistrer collecteur, opérateur, date et référence documentaire. L'orientation ne signifie pas automatiquement que le recyclage final a effectivement été réalisé.

15. Recyclage documenté

Une preuve émise par un opérateur compétent peut documenter réception, traitement, matières récupérées ou autre résultat disponible. AP conserve la déclaration ou preuve de l'opérateur sans inventer des taux de recyclage non fournis.

16. Fin de vie

La fin de vie peut correspondre à destruction, recyclage, démantèlement, récupération de composants ou autre sortie documentée. Le passeport principal peut être clôturé tout en conservant les relations avec les composants ou matières poursuivant un nouveau cycle.

17. Gouvernance des acteurs circulaires

Fabricants, réparateurs, reconditionneurs, plateformes, collecteurs et recycleurs doivent disposer de rôles distincts. Chaque acteur ne peut modifier que les événements ou données relevant de son périmètre autorisé.

18. Audit et AP Ledger

Garanties, interventions critiques, changements de composants, transferts, reconditionnements et preuves de fin de vie peuvent être audités. AP Ledger peut ancrer des empreintes minimales de ces événements sans publier les données personnelles, commerciales ou techniques sensibles.

19. Critères d’acceptation

Le modèle est acceptable si garanties d’origine et de reconditionnement restent distinctes, si les interventions SAV sont historisées, si réparabilité et disponibilité conservent leurs sources, si réemploi et recyclage restent des événements vérifiables, et si la fin de vie ne détruit pas la provenance des composants réutilisés.

20. Conclusion

La seconde main s’inscrit dans un cycle plus large que la seule revente. Authenticity Plus© permet au passeport d’accompagner garantie, réparation, réemploi, reconditionnement, récupération de composants et recyclage, donnant à l’économie circulaire une continuité documentaire vérifiable jusqu’à la fin de vie.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 11 — SECONDE MAIN

CHAPITRE 6 — SYNTHÈSE FONCTIONNELLE, CRITÈRES D'ACCEPTATION ET CLÔTURE DE L'APPLICATION SECONDE MAIN

1. Objet du chapitre

Ce chapitre clôt le Point 11 — Seconde main. Il consolide identité du bien, provenance, propriété et détention, état, inspection, réparations, reconditionnement, mise en vente, transaction, transfert, anomalies, garanties, réemploi, recyclage, gouvernance, audit et AP Ledger.

2. Mission consolidée

L'application Seconde main constitue un passeport de continuité pour les biens qui changent de détenteur ou de propriétaire. Elle réduit l'asymétrie d'information en reliant les preuves disponibles sans promettre une certitude supérieure à celle des sources.

3. Identité persistante du bien

L'objet conserve une identité stable pendant ses cycles d'usage, de réparation et de revente. Numéro de série, identifiant fabricant, tag AP ou autre référence restent des éléments d'identification dont la source et la portée doivent être distinguées.

4. Provenance

Fabricant, artisan, distributeur, achat initial, certificats et autres sources peuvent constituer la provenance documentée. Les déclarations, documents et vérifications indépendantes restent des niveaux distincts.

5. Propriété, détention et usage

Propriétaire, détenteur et utilisateur ne doivent jamais être automatiquement confondus. Prêt, location, dépôt ou réparation peuvent modifier la garde sans constituer un transfert de propriété.

6. État et inspection

État déclaré par le vendeur, inspection professionnelle, expertise et grading doivent rester attribués à leurs sources. Un grade ne remplace pas les observations et preuves qui le justifient.

7. Réparations et composants

Entretien, réparation, pièces remplacées et tests doivent pouvoir être historisés. L'objet principal conserve son identité malgré les transformations, tandis que les composants identifiables peuvent conserver leur propre provenance.

8. Reconditionnement

Le reconditionnement doit documenter acteur, opérations, pièces et contrôles disponibles. Le terme ne doit pas être assimilé automatiquement à un état neuf ni à une qualité uniforme entre opérateurs.

9. Mise en vente

L'annonce doit être reliée à l'objet réel et distinguer données du passeport et déclarations du vendeur. Une annonce ne doit pas pouvoir réécrire l'historique du bien.

10. Transaction et paiement

Réservation, transaction, paiement, livraison et réception sont des événements distincts. Les références financières utiles peuvent être corrélées sans intégrer inutilement les données bancaires sensibles.

11. Transfert de propriété et du passeport

Lorsque le transfert est documenté, le nouvel acquéreur reçoit les droits nécessaires à la continuité du passeport. L'ancien propriétaire perd les privilèges de gestion correspondants sans être effacé de l' historique minimisé.

12. Objets signalés

Perte, vol présumé, contestation de propriété ou autre signalement doit conserver source, date et statut. Un signalement ne constitue pas automatiquement une décision juridique.

13. Contrefaçon et fraude présumées

Identifiants incompatibles, documents suspects, passeports clonés ou historiques contradictoires peuvent déclencher une investigation. AP ne qualifie pas automatiquement le bien ou la personne de frauduleux ou contrefaisant.

14. Contestations et décisions externes

Vendeur, acheteur, propriétaire antérieur, fabricant, expert, plateforme ou autorité peuvent fournir des positions ou décisions. Elles doivent rester attribuées, datées et historisées.

15. Récupération de provenance

Un passeport absent ou incomplet peut être reconstruit progressivement à partir de preuves attribuables. Les périodes inconnues restent explicitement inconnues et ne sont jamais comblées artificiellement.

16. Garanties et SAV

Garanties d’origine, garanties de reconditionnement, demandes SAV, diagnostics et réparations peuvent suivre le bien lorsque les conditions le permettent. AP conserve ces éléments sans créer lui-même les droits de garantie.

17. Économie circulaire

Réemploi, réaffectation, récupération de composants, remanufacturation, reconditionnement et recyclage prolongent la chaîne de provenance au-delà d’une simple succession de ventes.

18. Fin de vie, audit et AP Ledger

La clôture d’un objet peut conserver les relations avec les composants ou matières poursuivant un nouveau cycle. Les événements critiques peuvent être audités et leurs empreintes minimales ancrées dans AP Ledger sans publier les données sensibles.

19. Critères d’acceptation

Le modèle est acceptable si l’identité survit aux reventes, si les rôles de propriété et de garde restent distincts, si les états et grades sont sourcés, si les transformations sont historisées, si les signalements ne deviennent pas des verdicts, si la provenance incomplète reste explicite et si la circularité préserve les liens utiles.

20. Clôture du Point 11 — Seconde main

Le Point 11 — Seconde main est désormais fonctionnellement défini : identité, provenance, achats, propriété, détention, usage, entretien, réparation, inspection, grading, reconditionnement, mise en vente, transaction, paiement, livraison, transfert, signalements, contrefaçon présumée, passeports clonés, récupération de provenance, garanties, SAV, réparabilité, réemploi, recyclage, fin de vie, gouvernance, audit et AP Ledger.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 12 — AP SELF — PATRIMOINE

CHAPITRE 1 RÉVISÉ — MISSION, INVENTAIRE PATRIMONIAL, CERTIFICATION NUMÉRIQUE, IDENTITÉ DES BIENS, PREUVE DE PROPRIÉTÉ, TRAÇABILITÉ ET SOUVERAINETÉ

1. Objet du chapitre

Ce chapitre révisé intègre le document de référence AP Self – Patrimoine au Point 12 du Volume IV. AP Self – Patrimoine vise à structurer l'inventaire numérique du patrimoine individuel et familial en reliant les biens à des identités, documents, photographies, preuves, événements et mécanismes de vérification.

2. Vision fondatrice

AP Self – Patrimoine répond au constat que de nombreux objets de valeur, équipements, documents et biens hérités existent sans traçabilité numérique structurée. Le système permet de commencer une chaîne de preuve à partir des éléments réellement disponibles, puis de l'enrichir au cours du temps.

3. Inventaire patrimonial numérique

Le titulaire peut enregistrer ses biens dans un inventaire sécurisé et organisé par catégories. Cet inventaire décrit les biens effectivement enrôlés dans AP Self – Patrimoine ; il ne doit pas être présenté comme une déclaration exhaustive de toute la richesse ou de l'ensemble du patrimoine réel d'une personne.

4. Identité numérique du bien

Chaque bien enrôlé peut recevoir une identité numérique persistante reliant description, photographies, caractéristiques, numéros ou références disponibles, documents et événements successifs. L'identité numérique du bien reste distincte de la détermination juridique définitive de sa propriété.

5. Enregistrement avec ou sans documents

Facture, certificat, acte, reçu ou autre justificatif peut accompagner l'enrôlement. Lorsqu'aucun document historique n'existe, l'utilisateur peut néanmoins enregistrer le bien, le photographier et déclarer ce qu'il sait. Le système commence alors la preuve à la date réelle d'enrôlement sans fabriquer une histoire antérieure.

6. Certification numérique

AP Self – Patrimoine peut associer au dossier des empreintes, horodatages, signatures ou attestations permettant de vérifier l'existence et l'intégrité d'éléments documentés. La certification doit préciser exactement ce qui est certifié et ne transforme pas automatiquement une déclaration personnelle en titre officiel de propriété.

7. QR Code sécurisé et dynamique

Un QR Code sécurisé peut être associé au passeport du bien afin d'en permettre la vérification contrôlée. Les informations visibles dépendent des droits et du statut du bien ; les données patrimoniales privées ne doivent pas être exposées publiquement par défaut.

8. Propriété, détention et usage

Propriétaire déclaré, propriétaire documenté, titulaire d'un registre officiel, détenteur et utilisateur peuvent être représentés séparément. Prêt, location, dépôt, garde ou mise à disposition ne doivent jamais être assimilés automatiquement à un transfert de propriété.

9. Preuve de propriété

AP Self – Patrimoine agrège les preuves disponibles relatives à la propriété : facture, acte, contrat, certificat, historique de transfert ou autre source. Il renforce la capacité à documenter une revendication de propriété, mais la portée juridique définitive dépend des documents, registres et autorités compétentes.

10. Traçabilité des biens

Les événements importants du cycle de vie peuvent être enregistrés : acquisition, transfert, entretien, expertise, assurance, perte déclarée, vol présumé, récupération, donation ou transmission. Chaque événement conserve sa date, sa source et son statut.

11. Protection contre le vol et la fraude

La traçabilité et le marquage numérique peuvent faciliter l'identification d'un bien déclaré perdu ou volé et compliquer sa revente comme bien d'origine inconnue. Le statut AP constitue un signal vérifiable ; il ne remplace ni une déclaration officielle ni une procédure des autorités compétentes.

12. Assurance

Le passeport peut relier un bien à des factures, photographies, expertises, valeurs déclarées et références d'assurance. Ces éléments peuvent faciliter la constitution d'un dossier de sinistre et contribuer à réduire certaines fraudes, sans préjuger de la décision d'indemnisation de l'assureur.

13. Valeur patrimoniale documentée

Prix d'acquisition, estimation, expertise, valeur assurée et valeur déclarée restent des notions distinctes. Toute valeur conserve sa date, sa devise, sa nature et sa source. AP Self – Patrimoine ne calcule pas automatiquement la richesse réelle d'un citoyen.

14. Transmission et héritage

Le passeport peut préserver la mémoire documentaire d'un bien lors d'une donation, succession ou transmission familiale. Les nouveaux documents enrichissent la provenance sans antidater la preuve. AP Self – Patrimoine ne se substitue ni au testament, ni au notaire, ni aux règles successorales applicables.

15. Transactions et services futurs

Une identité patrimoniale mieux documentée peut soutenir, lorsque le cadre juridique et les partenaires compétents le permettent, des services liés à l'assurance, à la transmission, à la vente ou à d'autres transactions. Toute utilisation financière ou garantie de crédit exige des règles et validations propres au service concerné.

16. Intégration institutionnelle

Le document AP Self – Patrimoine envisage une intégration progressive avec services publics, assurances et administrations. Cette interopérabilité doit fonctionner par échanges autorisés et finalisés, sans créer un accès général de l'État, des assureurs ou de tiers au coffre patrimonial privé.

17. Confidentialité et contrôle du citoyen

Le patrimoine individuel est une donnée particulièrement sensible. Le coffre reste privé par défaut, avec chiffrement approprié, minimisation, accès granulaires, partage volontaire et journalisation. La connaissance agrégée de l'économie ne doit pas devenir un registre public nominatif de richesse.

18. Souveraineté et standard national

AP Self – Patrimoine peut constituer une infrastructure souveraine de preuve et de traçabilité des biens et, dans une démarche progressive, contribuer à un standard national de certification patrimoniale. Toute reconnaissance officielle ou valeur juridique doit résulter du cadre légal et institutionnel applicable.

19. Deep Authenticity© et AP Ledger

Deep Authenticity© peut confronter identités, documents, photographies, numéros, chronologies et événements afin de signaler des incohérences. AP Ledger peut ancrer des empreintes minimales prouvant l'existence ou l'intégrité d'éléments à un moment donné ; les documents complets et données personnelles restent hors des couches publiques ou irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si AP Self – Patrimoine permet l'inventaire et la traçabilité sans inventer le passé ; si identité numérique, détention et propriété juridique restent distinguées ; si le QR permet une vérification contrôlée ; si assurances, transmissions et transactions reposent sur des preuves attribuées ; si l'intégration institutionnelle respecte le consentement, les droits et la confidentialité ; et si la souveraineté numérique n'aboutit pas à un registre public du patrimoine personnel. AP Self – Patrimoine devient ainsi une infrastructure de continuité patrimoniale et de preuve, centrée sur le citoyen.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 12 — AP SELF — PATRIMOINE

CHAPITRE 2 RÉVISÉ — ENRÔLEMENT PATRIMONIAL, BIENS AVEC OU SANS DOCUMENTS, CAPTURE PHOTOGRAPHIQUE, CERTIFICATION NUMÉRIQUE, QR CODE SÉCURISÉ, PERTE, VOL PRÉSUMÉ, BLOCAGE ET RÉCUPÉRATION

1. Objet du chapitre

Ce chapitre révisé définit l'enrôlement concret d'un bien dans AP Self – Patrimoine. Il combine l' architecture existante du Point 12 avec les fonctions du document AP Self – Patrimoine : inventaire sécurisé, certification numérique, QR Code, traçabilité, statut de perte ou vol et mécanismes de récupération.

2. Cas d'usage fondateur

Une personne peut posséder une montre héritée, un bijou, une œuvre, un équipement, un objet de collection ou un autre bien sans facture ni certificat historique. AP Self – Patrimoine permet de commencer aujourd'hui sa chaîne documentaire sans prétendre reconstruire artificiellement le passé.

3. Principe : ne pas inventer le passé

Toute information antérieure non prouvée reste une déclaration attribuée à son auteur. Une mention telle que « héritée de mon grand-père » peut être enregistrée comme provenance déclarée, mais elle ne devient pas une provenance historiquement vérifiée sans preuve indépendante.

4. Création de l'identité patrimoniale

L'enrôlement crée une identité numérique persistante du bien reliant informations déclarées, photographies, caractéristiques visibles, identifiants disponibles, documents et futurs événements. Cette identité numérique n'est pas, à elle seule, un titre juridique de propriété.

5. Capture photographique initiale

Plusieurs photographies peuvent documenter l'état observé : vues générales, détails distinctifs, inscriptions, gravures, numéros visibles, accessoires ou marques particulières. Les images sont datées et reliées à l'enrôlement sans constituer automatiquement une expertise d'authenticité.

6. Description et caractéristiques

Marque déclarée, modèle présumé, matériau, dimensions, couleur, inscriptions, numéro de série ou autres caractéristiques peuvent être enregistrés. Chaque donnée conserve son origine : observation, lecture sur l'objet, document ou vérification professionnelle.

7. Biens avec justificatifs

Facture, certificat, acte, reçu, expertise ou autre document peut être associé au passeport. Le document conserve émetteur disponible, date, référence, version et relation avec le bien.

8. Biens sans justificatifs

L'absence de document ne bloque pas l'enrôlement. Le passeport affiche clairement le niveau de preuve disponible, par exemple « provenance déclarée — documents historiques indisponibles », afin d'éviter toute confusion entre déclaration et preuve indépendante.

9. Certification numérique

Empreinte, horodatage, signature ou attestation disponible peut fixer l'état documentaire du bien à une date donnée. La certification prouve ce qui a été enregistré ou signé selon le mécanisme utilisé ; elle ne garantit pas automatiquement l'authenticité matérielle du bien.

10. QR Code sécurisé et dynamique

Un QR Code peut permettre une vérification contrôlée du passeport : identité du bien, statut, informations publiques autorisées et validité de certaines preuves. Les données privées, documents sensibles et informations personnelles restent protégés.

11. Association physique et numérique

Lorsque cela est approprié, un marquage ou identifiant peut relier physiquement le bien à son passeport. La conception doit limiter les risques de copie, substitution ou réutilisation d'un identifiant sur un autre objet.

12. Enrichissement progressif

Le passeport peut recevoir ultérieurement facture retrouvée, expertise, réparation, photographie, assurance ou autre preuve. Chaque nouvel élément conserve sa date réelle d'ajout et ne modifie pas rétroactivement le niveau de preuve qui existait auparavant.

13. Déclaration de perte

Le titulaire peut déclarer un bien perdu. Le passeport conserve la date, le déclarant, le statut et les informations nécessaires. Une déclaration dans AP Self – Patrimoine ne remplace pas une déclaration officielle lorsqu'une procédure externe est requise.

14. Vol présumé

Le titulaire peut signaler un vol présumé et joindre, lorsqu'elle existe, une référence de déclaration auprès de l'autorité compétente. AP distingue le signalement du titulaire de la qualification juridique ou de l'enquête officielle.

15. Blocage du passeport

Un statut de blocage peut limiter transfert, modification ou certaines opérations sur le passeport lorsqu'un bien est déclaré perdu ou volé. Le blocage numérique ne constitue pas une saisie juridique du bien.

16. Vérification lors d'une transaction

Avant une transaction, un acteur autorisé peut vérifier le statut publiable du passeport. Un statut perdu, vol présumé, bloqué ou incohérent peut déclencher une vérification renforcée sans établir automatiquement la responsabilité d'une personne.

17. Récupération

Lorsqu'un bien est retrouvé, la récupération peut être documentée avec date, acteur, justificatifs disponibles et changement de statut. La clôture d'un signalement officiel externe reste sous l'autorité du service compétent.

18. Deep Authenticity©

Deep Authenticity© peut confronter photographies, identifiants, documents, empreintes, déclarations et chronologies pour signaler duplications, substitutions ou incohérences. Un signal nécessite une vérification adaptée et ne constitue pas à lui seul une accusation de fraude.

19. AP Ledger et confidentialité

Des empreintes minimales de création, certification, blocage, changement de statut ou récupération peuvent être ancrées dans AP Ledger. Photographies privées, factures, adresses, identités complètes et autres données patrimoniales sensibles restent hors des couches publiques ou irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si un bien peut être enrôlé avec ou sans documents ; si le passé non prouvé reste déclaré comme tel ; si photographies et caractéristiques documentent sans prétendre expertiser ; si le QR vérifie sans exposer le coffre privé ; si perte, vol présumé, blocage et récupération restent des statuts distincts ; et si chaque enrichissement conserve sa date réelle. AP Self – Patrimoine crée ainsi une chaîne de provenance à partir du présent, progressivement renforcée par les preuves futures.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 12 — AP SELF — PATRIMOINE

CHAPITRE 3 RÉVISÉ — ASSURANCES, EXPERTISES, VALEURS PATRIMONIALES, SINISTRES, TRANSACTIONS, PROFESSIONNELS ET CHAÎNE DE PREUVE

1. Objet du chapitre

Ce chapitre révisé organise l'usage du Passeport AP Self – Patrimoine avec les assureurs, experts, professionnels et acteurs de transaction. Il exploite l'inventaire certifié, les preuves disponibles et la traçabilité sans transférer à Authenticity Plus© les décisions juridiques, assurantielles ou commerciales.

2. Dossier patrimonial assurable

Le passeport peut rassembler identité du bien, photographies, factures, certificats, expertises, réparations, historique et valeurs documentées. Le titulaire choisit les éléments nécessaires à partager avec l'assureur.

3. Souscription d'assurance

Lors d'une souscription, AP Self – Patrimoine peut faciliter la présentation structurée des biens et justificatifs. L'existence d'un passeport ne crée pas automatiquement une couverture et ne remplace pas l'acceptation du risque par l'assureur.

4. Preuves pour l'assurance

Facture, photographie, certificat, expertise, numéro de série et historique peuvent renforcer le dossier documentaire. Chaque preuve conserve sa source et sa date afin de distinguer document original, copie, déclaration et expertise.

5. Valeur d'acquisition

Le prix d'acquisition documenté correspond à une transaction identifiée et datée. Il reste distinct de la valeur actuelle, de la valeur assurée, de la valeur d'expertise et du prix potentiel de revente.

6. Valeur déclarée

Le titulaire peut déclarer une valeur lorsqu'aucune évaluation indépendante n'est disponible. Cette valeur reste explicitement attribuée au déclarant et ne devient pas automatiquement une expertise.

7. Expertise professionnelle

Une expertise peut être reliée à l'expert ou à l'organisme, à la date, au périmètre, aux méthodes déclarées et à la valeur ou conclusion produite. AP authentifie la provenance du rapport sans se substituer à l'expert.

8. Réévaluations

Un bien peut recevoir plusieurs évaluations au cours du temps. Les valeurs antérieures restent historisées avec leur date et leur source afin d'éviter qu'une nouvelle estimation ne réécrive silencieusement l'historique.

9. Valeur assurée

La valeur retenue dans un contrat d'assurance reste une donnée contractuelle attribuée à la police ou à l'assureur concerné. Elle ne doit pas être présentée comme une valeur universelle du bien.

10. Déclaration de sinistre

En cas de perte, dommage ou vol présumé, le titulaire peut constituer un dossier reliant bien, statut, photographies, documents, déclaration et références externes disponibles. Le dossier AP ne remplace pas les formalités exigées par l'assureur ou les autorités.

11. Instruction du sinistre

Demande, réception, expertise, demande de complément, décision et indemnisation restent des étapes distinctes. AP Self – Patrimoine peut tracer les pièces et statuts sans décider du droit à indemnisation.

12. Prévention de la fraude

La comparaison des identités de biens, documents, photographies, numéros et chronologies peut aider à détecter doublons ou incohérences. Un signal technique déclenche une vérification et ne constitue pas à lui seul une preuve de fraude.

13. Transaction entre particuliers

Lors d'une vente ou d'un transfert, le titulaire peut partager une vue limitée du passeport permettant de vérifier identité du bien, provenance disponible et statut. Le partage n'expose pas l'ensemble du coffre patrimonial.

14. Professionnels du marché

Commerçants, maisons de vente, experts, réparateurs ou autres professionnels autorisés peuvent ajouter ou vérifier des événements selon leur rôle. Chaque contribution reste attribuée à son auteur ou organisme.

15. Transfert du passeport

Lorsqu'un transfert de bien est documenté, les droits d'administration du passeport peuvent évoluer tout en conservant l'historique antérieur. Le transfert technique du passeport ne remplace pas les formalités juridiques requises pour le bien concerné.

16. Biens gagés ou financés

Lorsqu'un service financier autorisé s'appuie sur un bien, le passeport peut documenter les preuves nécessaires et un statut contractuel approprié. AP Self – Patrimoine ne crée pas seul un gage, une sûreté ou un droit de préférence.

17. Interopérabilité avec assureurs et professionnels

Les échanges doivent être limités aux données nécessaires, avec consentement ou autre base autorisée, durée et finalité déterminées. Aucun partenaire ne reçoit un accès général au patrimoine du titulaire.

18. Deep Authenticity©

Deep Authenticity© confronte preuves, photographies, expertises, valeurs, transactions et chronologies afin de signaler incohérences ou substitutions. Ses résultats restent explicables et soumis à la vérification des acteurs compétents.

19. AP Ledger et confidentialité

Des empreintes minimales d'expertises, changements de statut, transactions ou événements critiques peuvent être ancrées dans AP Ledger. Valeurs patrimoniales détaillées, contrats, dossiers de sinistre et données personnelles restent hors des couches publiques ou irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si les différentes valeurs restent distinctes et sourcées ; si le passeport facilite l'assurance sans créer la couverture ; si AP ne décide pas de l'indemnisation ; si les signaux de fraude ne deviennent pas des accusations automatiques ; si les transactions conservent provenance et historique ; et si assureurs et professionnels n'accèdent qu'aux informations nécessaires. AP Self – Patrimoine devient ainsi un dossier patrimonial vérifiable utilisable dans les relations assurantielles et professionnelles.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 12 — AP SELF — PATRIMOINE

CHAPITRE 4 RÉVISÉ — TRANSMISSION FAMILIALE, DONATION, SUCCESSION, HÉRITAGE, COFFRE D'URGENCE, PERSONNES AUTORISÉES ET CONTINUITÉ DU PASSEPORT PATRIMONIAL

1. Objet du chapitre

Ce chapitre révisé organise la continuité d'AP Self – Patrimoine lors d'une donation, d'une transmission familiale, d'une succession, d'une incapacité ou du décès du titulaire. Il préserve les passeports, documents et preuves sans transformer Authenticity Plus© en notaire, registre successoral ou autorité déterminant les héritiers.

2. Principe de continuité patrimoniale

La disparition, l'incapacité ou le changement de titulaire ne doit pas entraîner la disparition de la mémoire documentaire des biens. Les passeports conservent leur identité et leur chronologie tandis que les droits d'administration évoluent selon les preuves et procédures autorisées.

3. Transmission volontaire du vivant

Le titulaire peut préparer ou documenter le transfert d'un bien vers un bénéficiaire. Vente, donation, remise, prêt ou autre mécanisme restent distingués et conservent leurs justificatifs disponibles.

4. Donation

Une donation peut relier le bien, le donateur, le bénéficiaire, la date et les documents disponibles. AP Self – Patrimoine documente l'événement sans déclarer automatiquement que toutes les conditions civiles, fiscales ou formelles ont été satisfaites.

5. Héritage familial déclaré

Un bien transmis familialement sans documents historiques peut conserver une origine déclarée, par exemple « hérité d'un grand-parent ». Cette déclaration est datée et attribuée ; elle n'est pas transformée rétroactivement en preuve indépendante.

6. Préparation successorale documentaire

Le titulaire peut organiser les biens, contrats, assurances, documents et contacts qu'il souhaite rendre retrouvables par des personnes autorisées. Cette préparation documentaire ne remplace pas un testament, un acte notarié ou les règles successorales applicables.

7. Personnes de confiance

Le titulaire peut désigner une ou plusieurs personnes de confiance pour certaines fonctions de récupération, notification ou continuité. Une désignation technique dans AP Self – Patrimoine ne détermine pas juridiquement la qualité d'héritier.

8. Coffre d'urgence

Un coffre d'urgence peut contenir ou référencer les informations strictement nécessaires pour retrouver les passeports patrimoniaux, assurances, contacts professionnels et documents essentiels. Son accès est renforcé et limité à des circonstances et rôles définis.

9. Déclenchement de la continuité

Une procédure de continuité peut être initiée à partir de preuves ou événements autorisés. AP Self – Patrimoine ne doit pas déduire seul un décès, une incapacité ou un droit successoral à partir d'une simple absence d'activité.

10. Vérification des justificatifs

Les actes, certificats, décisions, documents successoraux ou autres justificatifs fournis conservent leur source, date et statut. Leur portée reste déterminée par les autorités et professionnels compétents.

11. Gel de protection

Lorsqu'une situation successorale ou de sécurité l'exige, certaines modifications ou transferts techniques peuvent être temporairement gelés afin de préserver l'intégrité du dossier. Ce gel numérique n'équivaut pas à une mesure judiciaire sur le bien.

12. Accès gradué

Les personnes autorisées n'accèdent qu'aux informations nécessaires : inventaire limité, coordonnées d'un assureur, existence d'un document ou procédure de récupération. Le coffre complet n'est pas automatiquement ouvert.

13. Continuité des assurances et contrats

Les références d'assurance, garanties, expertises ou contrats peuvent être rendues accessibles aux personnes autorisées lorsque nécessaire. AP facilite leur découverte mais ne modifie ni bénéficiaire, ni police, ni contrat.

14. Transfert des droits d'administration

Après validation des preuves requises, les droits techniques d'administration d'un passeport peuvent être transférés ou partagés. Ce transfert conserve l'ancien titulaire, la date, la base documentaire et le nouvel administrateur.

15. Conservation de la provenance

La transmission d’un bien ne recommence pas son histoire numérique à zéro. Les propriétaires ou détenteurs successifs, documents, expertises et événements autorisés restent reliés dans la chaîne de provenance.

16. Protection contre l’appropriation abusive

Toute demande de récupération ou de transfert sensible peut nécessiter plusieurs contrôles, délais ou validations. Une personne disposant d’un accès d’urgence ne devient pas automatiquement propriétaire ou administrateur permanent.

17. Interopérabilité avec professionnels

Notaires, assureurs, administrations ou autres professionnels compétents peuvent recevoir ou fournir des preuves selon des échanges autorisés. Aucun partenaire ne reçoit un accès général au patrimoine familial.

18. Deep Authenticity©

Deep Authenticity© peut confronter identités, documents, désignations, chronologies et transferts afin de signaler incohérences ou substitutions. Le résultat reste un signal de vérification et non une décision successorale.

19. AP Ledger et confidentialité

Des empreintes minimales de désignation, gel, validation, transfert ou changement de statut peuvent être ancrées dans AP Ledger. Testaments, actes complets, inventaires détaillés, valeurs et données familiales restent hors des couches publiques ou irréversibles.

20. Critères d’acceptation et conclusion

Le modèle est acceptable si la continuité documentaire survit au changement de titulaire ; si personne de confiance et héritier juridique restent distingués ; si le coffre d’urgence est limité ; si les justificatifs restent attribués aux autorités compétentes ; si le transfert technique ne remplace pas la transmission juridique ; et si l’historique du bien est conservé. AP Self – Patrimoine devient ainsi une mémoire patrimoniale transmissible sans se substituer au droit successoral.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 12 — AP SELF — PATRIMOINE

CHAPITRE 5 RÉVISÉ — CONFIDENTIALITÉ PATRIMONIALE, COFFRE NUMÉRIQUE, CONSENTEMENT, PARTAGE SÉLECTIF, INTEROPÉRABILITÉ, SOUVERAINETÉ, CYBERSÉCURITÉ, DEEP AUTHENTICITY© ET GOUVERNANCE

1. Objet du chapitre

Ce chapitre révisé définit la gouvernance de sécurité d'AP Self – Patrimoine. Il organise le coffre patrimonial, la confidentialité, le consentement, le partage sélectif, l'interopérabilité avec les acteurs autorisés, la souveraineté, la cybersécurité et les mécanismes de vérification.

2. Principe de confidentialité par défaut

L'inventaire patrimonial est privé par défaut. L'enrôlement d'un bien ne doit pas créer automatiquement une publication de sa possession, de sa valeur, de son emplacement ou de l'identité de son titulaire.

3. Coffre numérique patrimonial

Le coffre peut regrouper passeports de biens, photographies, factures, certificats, expertises, contrats, assurances et autres documents. Les données sont organisées par actif et par niveau d'accès afin d' éviter qu'un partage ponctuel n'ouvre l'ensemble du patrimoine.

4. Contrôle du titulaire

Le titulaire conserve, dans les limites du cadre applicable, le contrôle des accès et partages volontaires. Il peut autoriser un acteur à consulter une preuve déterminée sans lui donner accès à l' inventaire complet.

5. Consentement et finalité

Tout partage volontaire précise destinataire, finalité, périmètre, durée et informations concernées. Le consentement à une vérification d'un bien ne vaut pas consentement général à l'analyse du patrimoine.

6. Partage sélectif

Une vue limitée peut présenter identité du bien, statut, preuve d'existence, provenance disponible ou document précis. Les valeurs, autres biens, adresses et informations familiales restent masqués lorsqu'ils ne sont pas nécessaires.

7. QR Code et vue publique

Le QR sécurisé ou dynamique ne doit restituer que les informations publiables et nécessaires à la vérification. Une personne scannant un QR ne reçoit pas automatiquement l'identité complète du titulaire ni l'accès au coffre.

8. Interopérabilité avec les assurances

Un assureur peut recevoir, avec autorisation ou autre base applicable, les preuves nécessaires à une souscription ou un sinistre. L'intégration ne crée pas un accès permanent à tous les actifs du client.

9. Interopérabilité avec les autorités

Dans les situations prévues par le cadre applicable, certaines preuves relatives à un bien perdu, volé ou récupéré peuvent être échangées avec les autorités compétentes. AP Self – Patrimoine ne crée pas un accès policier généralisé au patrimoine privé.

10. Interopérabilité avec les administrations

Des administrations autorisées peuvent vérifier certains documents ou statuts lorsque leur mission l' exige. Les échanges restent limités par la compétence, la finalité et le niveau de données strictement nécessaire.

11. Professionnels et tiers

Notaires, experts, réparateurs, maisons de vente, commerçants ou autres professionnels peuvent recevoir des droits limités à leur intervention. Leurs consultations et contributions sensibles peuvent être journalisées.

12. Révocation des accès

Un accès temporaire ou permanent doit pouvoir être suspendu ou révoqué lorsque le rôle ou la finalité disparaît. La révocation empêche les accès futurs sans effacer les preuves des actions antérieures.

13. Cybersécurité

Comptes, sessions, API, certificats, QR, clés et systèmes de stockage sont protégés par des mécanismes adaptés d'authentification, chiffrement, segmentation, journalisation et révocation. Aucun secret d'accès n'est placé dans une couche publique.

14. Protection contre l'usurpation

Les opérations sensibles telles que transfert d'administration, changement d'identité du bien, récupération de compte ou ouverture du coffre d'urgence peuvent nécessiter des contrôles renforcés et plusieurs facteurs de vérification.

15. Minimisation des données

AP Self – Patrimoine conserve et expose uniquement les données nécessaires aux fonctions utilisées. La preuve d'existence d'un bien peut, selon le cas, être fournie sans révéler sa valeur, son emplacement ou l'ensemble de ses documents.

16. Souveraineté patrimoniale

Le titulaire et les autorités compétentes doivent pouvoir connaître et gouverner les conditions de stockage, conservation, transfert, archivage et suppression applicables. Une infrastructure nationale éventuelle doit préserver la maîtrise des données et les droits des citoyens.

17. Deep Authenticity©

Deep Authenticity© confronte identités, documents, photographies, accès, changements de statut et chronologies afin de signaler incohérences, substitutions ou usages suspects. Ses résultats sont des signaux de vérification et non des décisions automatiques sur la propriété ou la fraude.

18. Audit et traçabilité

Les opérations sensibles peuvent être auditées : création, partage, consultation privilégiée, modification, blocage, transfert et révocation. L'auditeur n'obtient que les informations nécessaires à sa mission et ne reçoit pas automatiquement le coffre complet.

19. AP Ledger

Des empreintes minimales de certifications, changements de statut, autorisations, révocations ou transferts critiques peuvent être ancrées dans AP Ledger. Inventaires complets, valeurs, photographies privées, contrats, adresses, identités et documents sensibles restent hors des couches publiques ou irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si le coffre reste privé par défaut ; si chaque partage est limité par finalité ; si le QR n'expose pas le patrimoine ; si assureurs, autorités, administrations et professionnels n'accèdent qu'aux preuves nécessaires ; si les accès sont révocables et auditables ; si la souveraineté est préservée ; et si Deep Authenticity© reste un mécanisme de vérification. AP Self – Patrimoine peut ainsi devenir une infrastructure de confiance sans devenir un registre public de richesse individuelle.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 12 — AP SELF — PATRIMOINE

CHAPITRE 6 RÉVISÉ — SYNTHÈSE FONCTIONNELLE, ARCHITECTURE AP SELF PATRIMOINE, CRITÈRES D'ACCEPTATION ET CLÔTURE DÉFINITIVE DU POINT 12

1. Objet du chapitre

Ce chapitre clôt la révision du Point 12 — AP Self Patrimoine. Il consolide l'inventaire patrimonial, l'enrôlement des biens, la certification numérique, les assurances, les expertises, les transactions, la transmission familiale, le coffre numérique, l'interopérabilité, Deep Authenticity© et AP Ledger.

2. Mission consolidée

AP Self Patrimoine fournit au citoyen une infrastructure de continuité documentaire permettant d'identifier, documenter, protéger et transmettre les biens enrôlés. Le système renforce la preuve disponible sans se substituer aux titres, registres, professionnels ou autorités compétents.

3. Inventaire patrimonial

L'inventaire regroupe les biens volontairement enrôlés et leurs preuves. Il n'est pas nécessairement exhaustif et ne doit pas être interprété comme une mesure automatique de la richesse totale d'une personne ou d'une famille.

4. Identité numérique des biens

Chaque bien peut conserver une identité persistante reliant photographies, caractéristiques, documents, numéros disponibles, certifications et événements. Identité numérique, détention, usage et propriété juridique restent distincts.

5. Enrôlement avec ou sans documents

Un bien peut être enregistré avec facture, certificat, acte ou autre justificatif, mais aussi sans document historique. Dans ce dernier cas, AP Self Patrimoine commence la chaîne de provenance à la date réelle d'enrôlement et conserve les éléments antérieurs comme déclarations lorsqu'ils ne sont pas indépendamment prouvés.

6. Certification et QR sécurisé

Empreinte, horodatage, signature ou attestation peut fixer l'état documentaire d'un bien. Un QR sécurisé ou dynamique permet une vérification contrôlée du statut et des preuves publiables sans ouvrir le coffre patrimonial privé.

7. Provenance et cycle de vie

Acquisition, entretien, expertise, assurance, transfert, perte, vol présumé, blocage, récupération, donation et transmission peuvent être historisés. Chaque événement conserve date, source, acteur et statut.

8. Perte, vol et récupération

Déclaration de perte, vol présumé, blocage numérique et récupération restent des événements distincts. AP peut contribuer à identifier un bien et à documenter son statut sans remplacer les déclarations officielles, enquêtes ou décisions des autorités compétentes.

9. Assurances et sinistres

Le passeport peut structurer photographies, factures, expertises, valeurs et références nécessaires à l'assurance ou à un sinistre. Existence d'un passeport, couverture, instruction et indemnisation restent distinctes.

10. Valeurs patrimoniales

Prix d'acquisition, valeur déclarée, estimation professionnelle, valeur assurée et prix de revente restent séparés, datés et attribués à leur source. AP Self Patrimoine ne calcule pas automatiquement une valeur patrimoniale universelle.

11. Transactions et professionnels

Lors d'une transaction ou intervention, une vue limitée peut être partagée avec l'acteur autorisé. Experts, réparateurs, commerçants, maisons de vente, assureurs ou autres professionnels contribuent uniquement dans le périmètre de leur rôle.

12. Transmission familiale

Donation, héritage déclaré, succession et transfert technique du passeport conservent leurs preuves et chronologies. Personne de confiance, bénéficiaire désigné et héritier juridique restent des notions distinctes.

13. Coffre d'urgence et continuité

Le coffre d'urgence permet de rendre retrouvables les informations essentielles dans des circonstances définies. Il ne crée ni accès permanent au patrimoine, ni droit de propriété, ni qualité successorale.

14. Confidentialité par défaut

Inventaire, valeurs, documents, adresses, photographies privées et données familiales sont protégés par défaut. L'enrôlement d'un bien ne signifie pas sa publication ni l'exposition de sa possession.

15. Consentement et partage sélectif

Chaque partage est limité par destinataire, finalité, durée et données nécessaires. Une autorisation portant sur un bien ou une preuve ne constitue jamais une autorisation générale d'explorer l'ensemble du patrimoine.

16. Interopérabilité institutionnelle

Assureurs, autorités, administrations, notaires et autres acteurs compétents peuvent échanger des preuves lorsque le cadre applicable le permet. Cette interopérabilité ne crée pas un registre ouvert ni un accès transversal au patrimoine privé.

17. Deep Authenticity©

Deep Authenticity© confronte identités, photographies, documents, expertises, valeurs, accès, transferts et chronologies afin de signaler incohérences, duplications ou substitutions. Ses résultats restent des signaux de vérification et non des décisions automatiques de propriété, fraude ou succession.

18. Souveraineté, cybersécurité et audit

Stockage, conservation, transfert, révocation et archivage sont gouvernés selon les droits et règles applicables. Les accès sensibles sont protégés et auditables ; l'auditeur reçoit uniquement les informations nécessaires à sa mission.

19. AP Ledger et critères d'acceptation

AP Ledger reçoit seulement des empreintes minimales d'événements critiques autorisés. Le modèle est acceptable si le passé non prouvé n'est pas inventé ; si propriété, détention et identité numérique restent distinctes ; si les valeurs sont sourcées ; si les transferts techniques ne remplacent pas les actes juridiques ; si les partages sont minimisés ; et si aucune donnée patrimoniale sensible n'est placée dans une couche publique ou irréversible.

20. Clôture définitive du Point 12 — AP Self Patrimoine

Le Point 12 est désormais révisé et fonctionnellement défini autour d'AP Self Patrimoine : inventaire, identité des biens, enrôlement avec ou sans documents, photographies, certification, QR sécurisé, provenance, perte et vol présumé, récupération, assurances, expertises, valeurs, transactions, transmission familiale, coffre d'urgence, confidentialité, interopérabilité, souveraineté, Deep Authenticity©, audit et AP Ledger. AP Self Patrimoine constitue ainsi une infrastructure centrée sur le citoyen pour préserver et renforcer la mémoire probatoire de son patrimoine sans devenir un registre public de richesse ni se substituer aux autorités juridiques compétentes.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 13 — TAXI

CHAPITRE 1 — MISSION, CHAUFFEUR, VÉHICULE, LICENCE OU AUTORISATION, IDENTITÉ DU TAXI, PRISE EN CHARGE, COURSE, PASSAGER ET PRINCIPES FONDATEURS

1. Objet du chapitre

Le Point 13 — TAXI transpose Authenticity Plus© / Deep Authenticity© au transport individuel professionnel. Il relie chauffeur, véhicule, licence ou autorisation, prise en charge, course, tarification, paiement, preuve de service et événements opérationnels afin de créer une continuité de confiance entre passager et professionnel.

2. Mission sectorielle

L'application TAXI vise à permettre au passager de vérifier qu'un véhicule, un chauffeur et une autorisation correspondent aux informations déclarées dans l'écosystème. Elle ne se substitue ni aux autorités de transport, ni aux licences officielles, ni aux règles locales de tarification ou de sécurité.

3. Identité du chauffeur

Le chauffeur dispose d'une identité professionnelle vérifiable selon les données autorisées. Le passager ne doit accéder qu'aux informations nécessaires à la confiance et au service ; les documents personnels complets restent protégés.

4. Identité du véhicule

Le véhicule peut être relié à marque, modèle, immatriculation ou autres références pertinentes, ainsi qu'à son statut opérationnel. Les données affichées doivent permettre au passager de reconnaître le véhicule sans exposer des informations administratives inutiles.

5. Relation chauffeur-véhicule

Un chauffeur peut utiliser différents véhicules et un véhicule peut être exploité par plusieurs chauffeurs selon les règles applicables. Chaque période d'affectation doit être historisée afin d'éviter de présenter une association ancienne comme actuelle.

6. Licence ou autorisation

Licence, carte professionnelle, agrément ou autre autorisation peut être référencé avec autorité émettrice, identifiant, période et statut disponibles. Authenticity Plus© restitue la preuve et sa source sans devenir l'autorité qui délivre ou renouvelle l'autorisation.

7. Identité numérique du taxi

Le couple opérationnel chauffeur-véhicule-autorisation peut produire une identité de service vérifiable pour une période donnée. Cette identité permet de confirmer que les éléments présentés au passager sont cohérents au moment de la prise en charge.

8. QR Code dynamique

Un QR Code dynamique affiché dans le véhicule ou présenté par le chauffeur peut ouvrir une fiche de vérification minimale : véhicule, chauffeur professionnel, statut de l'identité TAXI et informations de course autorisées. Le QR ne doit pas exposer l'adresse privée ou les documents personnels du chauffeur.

9. Vérification avant montée

Avant ou au début de la course, le passager peut vérifier que le QR, le véhicule et le chauffeur correspondent. Une divergence importante peut produire un message de vigilance sans transformer automatiquement l'anomalie en accusation de fraude.

10. Création de la course

Chaque course peut recevoir un identifiant distinct relié au chauffeur et au véhicule actifs. Heure de prise en charge, zone ou point de départ autorisé, destination ou zone d'arrivée et autres éléments nécessaires peuvent être associés selon les règles de confidentialité.

11. Passager

L'identité complète du passager n'est pas nécessaire dans tous les cas. Le système doit privilégier la minimisation et peut utiliser un identifiant de course ou un compte pseudonymisé lorsque l'identité civile n'est pas requise.

12. Prise en charge

La prise en charge constitue un événement horodaté reliant course, chauffeur, véhicule et contexte de départ. Elle ne doit pas être créée rétroactivement sans conserver l'origine et la nature de la correction.

13. Course en cours

Le statut de la course peut évoluer de demandée ou acceptée à prise en charge, en cours, terminée, annulée ou contestée. Les transitions importantes doivent être historisées.

14. Trajet et confidentialité

Les données de trajet peuvent être sensibles car elles révèlent les déplacements du passager et du chauffeur. Leur collecte, leur précision, leur conservation et leur partage doivent être limités aux finalités légitimes du service, de la sécurité et de l'audit.

15. Tarification

Compteur, tarif réglementé, forfait, supplément ou autre mécanisme peut être documenté selon le contexte. TAXI conserve la source et les paramètres disponibles sans inventer le tarif ni se substituer à l'autorité compétente.

16. Fin de course

La fin de course peut enregistrer heure, statut, montant et références nécessaires à la preuve de service. Les données doivent rester proportionnées et ne pas exposer publiquement l'historique des déplacements.

17. Paiement et reçu

Paiement en espèces, carte, application ou autre moyen peut être référencé avec montant et statut. Un reçu numérique peut être associé à la course sans intégrer inutilement les données bancaires sensibles.

18. Signalement d'anomalie

Chauffeur différent, véhicule différent, QR invalide, autorisation expirée, montant contesté ou autre divergence peut être signalé. Le système conserve les faits déclarés et les réponses sans produire automatiquement une conclusion juridique.

19. Critères d'acceptation

Le modèle est acceptable si chauffeur, véhicule et autorisation restent des identités distinctes ; si leur association est datée ; si le QR dynamique permet une vérification minimale ; si chaque course possède sa propre identité ; si les trajets sont protégés ; et si les anomalies restent investigables sans accusation automatique.

20. Conclusion

L'application TAXI établit un passeport de confiance pour la course professionnelle. Authenticity Plus© relie le bon chauffeur, le bon véhicule, l'autorisation pertinente et la bonne course au moment du service, tout en préservant la confidentialité des déplacements et la compétence des autorités de transport.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 13 — TAXI

CHAPITRE 2 — QR CODE DYNAMIQUE TAXI, VÉRIFICATION INSTANTANÉE DU CHAUFFEUR ET DU VÉHICULE, LICENCE, COMPTEUR, DÉBUT ET FIN DE COURSE, REÇU NUMÉRIQUE ET PREUVE DE TRAJET

1. Objet du chapitre

Ce chapitre définit la couche opérationnelle de vérification d'une course TAXI. Il organise QR Code dynamique, identité professionnelle, correspondance chauffeur-véhicule, autorisation, compteur ou tarification, début et fin de course, reçu numérique et preuve de service.

2. QR Code dynamique TAXI

Chaque identité TAXI active peut disposer d'un QR Code dynamique relié au passeport opérationnel. Le code constitue un point de vérification et non une licence officielle en lui-même. Sa réponse peut évoluer selon le statut du chauffeur, du véhicule, de l'autorisation ou de la course.

3. Emplacement et présentation

Le QR peut être présenté dans le véhicule, sur un support professionnel ou dans une interface numérique autorisée. Le passager doit pouvoir l'identifier facilement sans que le support révèle des informations personnelles inutiles.

4. Vérification du chauffeur

Le scan peut confirmer des éléments minimaux permettant de reconnaître le chauffeur professionnel : identité ou nom professionnel selon le cadre applicable, photographie de référence lorsque autorisée, statut actif et autres données nécessaires.

5. Vérification du véhicule

La fiche peut afficher les caractéristiques nécessaires pour reconnaître le véhicule, par exemple marque, modèle, immatriculation partielle ou complète selon les règles applicables, et statut opérationnel.

6. Correspondance chauffeur-véhicule

La vérification doit confirmer que le chauffeur et le véhicule sont actuellement associés dans l'écosystème AP. Une association expirée ou différente doit produire une vigilance plutôt que présenter des données anciennes comme valides.

7. Vérification de la licence ou autorisation

Le système peut restituer le statut documenté d'une licence, carte professionnelle, agrément ou autre autorisation avec sa source et sa période. AP ne doit jamais présenter comme valide une autorisation dont le statut n'est pas connu ou vérifiable.

8. Protection contre le QR copié

Une photographie ou copie du QR ne doit pas suffire à créer une identité TAXI légitime. La réponse dynamique doit dépendre de l'état du passeport et des associations actives, ce qui permet de rendre un support copié obsolète ou suspect.

9. Création de l'identité de course

Au début d'un service, une course peut recevoir un identifiant unique relié au chauffeur, au véhicule, à l' heure et aux paramètres nécessaires. L'identité de course reste distincte de l'identité permanente du taxi.

10. Début de course

Le démarrage peut être confirmé par le chauffeur, le système de réservation, le compteur ou un autre événement autorisé. La source du déclenchement doit être conservée afin de rendre la chronologie explicable.

11. Compteur et tarification

Lorsque le taxi utilise un compteur, les données nécessaires peuvent être reliées à la course selon les capacités et règles applicables. Tarif réglementé, forfait, suppléments et autres composantes doivent rester distingués et attribués à leurs sources.

12. État du compteur

Lorsque cette information est disponible, début, fin, référence de contrôle ou statut technique du compteur peuvent contribuer à la preuve de tarification. Authenticity Plus© ne certifie pas lui-même la conformité métrologique de l'appareil.

13. Trajet

Le trajet peut être représenté avec le niveau de précision strictement nécessaire. Les points exacts de départ et d'arrivée constituent des données sensibles et ne doivent pas être rendus publics ni conservés sans finalité légitime.

14. Preuve de trajet

Horodatages, distance déclarée ou mesurée, événements de prise en charge et de fin, et données autorisées peuvent constituer une preuve de service. Une trace GPS ne doit pas être présentée comme infaillible ou exhaustive lorsqu'elle comporte des lacunes.

15. Fin de course

La fin de course clôt la période de service et peut fixer les données finales disponibles : durée, distance, tarif, suppléments et statut. Toute correction ultérieure doit être historisée.

16. Reçu numérique

Un reçu peut relier identifiant de course, date, montant, composantes tarifaires, chauffeur ou opérateur professionnel et moyen de paiement selon les informations autorisées. Il ne doit pas exposer les données bancaires sensibles.

17. Vérification du reçu

Un QR ou identifiant de reçu peut permettre de vérifier que celui-ci correspond à une course enregistrée et qu'il n'a pas été modifié depuis son émission, selon les preuves disponibles.

18. Course contestée

Montant, trajet, chauffeur, véhicule ou horaire peuvent être contestés par une partie. Le dossier doit conserver le reçu, les événements de course, les données disponibles et les déclarations contradictoires sans arbitrage automatique.

19. Critères d'acceptation

Le modèle est acceptable si un QR copié ne crée pas une identité TAXI valide ; si chauffeur, véhicule et autorisation sont vérifiés comme association actuelle ; si la course possède un identifiant propre ; si compteur et tarif restent sourcés ; si le reçu est vérifiable ; et si les données de trajet restent protégées.

20. Conclusion

Le QR Code dynamique transforme la vérification TAXI en contrôle simple avant et pendant le service. Authenticity Plus© permet au passager de vérifier l'identité opérationnelle de la course, puis de conserver un reçu et une preuve cohérente du service, tout en protégeant les déplacements et sans se substituer aux autorités de transport ou de métrologie.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 13 — TAXI

CHAPITRE 3 — SÉCURITÉ DU PASSAGER ET DU CHAUFFEUR, ALERTE D'URGENCE, PARTAGE TEMPORAIRE DE COURSE, INCIDENTS, OBJETS OUBLIÉS, RÉCLAMATIONS ET PROTECTION DES DONNÉES DE DÉPLACEMENT

1. Objet du chapitre

Ce chapitre définit les mécanismes de sécurité et de continuité de preuve associés à une course TAXI. Il organise alerte d'urgence, partage temporaire, incidents, objets oubliés, réclamations et protection des données de déplacement, sans transformer Authenticity Plus© en service de secours ou en système de surveillance permanente.

2. Sécurité symétrique

L'architecture doit protéger à la fois le passager et le chauffeur. Les mécanismes de signalement, de preuve et de contestation doivent rester accessibles aux deux parties et ne pas présumer automatiquement laquelle est responsable d'un incident.

3. Identité de course comme point de référence

Chaque événement de sécurité doit être relié à l'identité unique de la course, au chauffeur et au véhicule actifs, ainsi qu'aux horodatages pertinents. Cette liaison permet d'éviter qu'un incident soit attribué à une course différente.

4. Alerte d'urgence

Une fonction d'alerte peut permettre au passager ou au chauffeur de déclencher un événement de sécurité pendant une course. Le système doit enregistrer l'heure, la course et le contexte technique disponible tout en limitant les informations aux besoins de protection.

5. Limite de l'alerte

Authenticity Plus© ne doit jamais laisser croire qu'un déclenchement garantit l'intervention des secours. Une transmission vers un service d'urgence, une centrale ou un tiers n'est présentée comme effective que lorsqu'une intégration opérationnelle réelle existe et confirme la prise en charge.

6. Destinataires autorisés

Selon le service, une alerte peut être transmise à une centrale, une plateforme, une personne de confiance ou un service effectivement intégré. Les destinataires, conditions et limites doivent être clairement définis.

7. Partage temporaire de course

Le passager ou le chauffeur peut partager temporairement un lien ou un statut de course avec une personne autorisée. Ce partage doit expirer automatiquement ou à la fin de la course et ne pas ouvrir un accès permanent à l'historique des déplacements.

8. Données partagées

Le partage peut être limité au statut de la course, à l'identité professionnelle du taxi et, si nécessaire, à une position ou progression temporaire. Les informations non nécessaires, notamment les historiques antérieurs, restent privées.

9. Incident pendant la course

Accident, panne, conflit, interruption ou autre événement peut être déclaré et horodaté. Les déclarations des différentes parties restent distinctes, et les preuves disponibles peuvent être ajoutées au dossier sans conclusion automatique.

10. Incident après la course

Une réclamation peut être ouverte après la fin du service en utilisant l'identifiant de course et le reçu numérique. Cette continuité évite de dépendre uniquement d'un souvenir, d'une plaque notée manuellement ou d'une capture isolée.

11. Objet oublié

Le passager peut déclarer qu'un objet a été oublié dans le véhicule en sélectionnant la course concernée et en fournissant une description minimale. Le chauffeur peut confirmer la découverte sans recevoir inutilement des informations personnelles supplémentaires.

12. Passeport d'un objet retrouvé

Si l'objet dispose déjà d'un Passeport Numérique compatible AP, son identifiant ou QR peut faciliter le rapprochement avec son titulaire selon les autorisations. Le chauffeur ou le tiers ne doit pas obtenir automatiquement l'accès au patrimoine ou aux coordonnées privées du propriétaire.

13. Restitution d'un objet

La restitution peut être documentée par un événement horodaté reliant objet, course et statut de remise. Une preuve de restitution peut être conservée sans exposer publiquement l'identité complète des parties.

14. Réclamation tarifaire

Un passager peut contester montant, supplément, compteur ou autre composante. Le dossier peut réunir reçu, paramètres documentés, événements de course et déclarations des parties, sans que TAXI tranche automatiquement le litige.

15. Réclamation du chauffeur

Le chauffeur peut également signaler non-paiement, dommage, comportement problématique ou autre incident. Le système conserve la déclaration et les preuves autorisées sans créer de notation punitive automatique ou de présomption de culpabilité.

16. Conservation proportionnée

Les données de trajet et de sécurité ne doivent pas êtreconservées indéfiniment par défaut. Leur durée doit correspondre aux finalités légitimes : preuve de course, règlement d'un litige, obligations applicables ou sécurité.

17. Protection de la localisation

Les adresses de départ et d'arrivée, trajets réguliers et positions en temps réel peuvent révéler domicile, école, travail ou habitudes. L'accès doit être strictement limité, journalisé et protégé contre l' usage secondaire non autorisé.

18. Journal d'accès

Les consultations sensibles d'un trajet, d'une alerte ou d'un dossier d'incident doivent pouvoir être auditées. Un acteur disposant d'un accès professionnel ne doit pas pouvoir consulter librement les déplacements sans justification.

19. AP Ledger et minimisation

Des empreintes minimales d'événements critiques peuvent être ancrées dans AP Ledger afin de protéger leur intégrité et leur chronologie. Les coordonnées précises, conversations, identités privées et détails sensibles des incidents restent hors des couches publiques ou irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si l'alerte ne promet pas un secours non intégré ; si le partage de course est temporaire ; si passager et chauffeur disposent de voies de signalement ; si les objets oubliés peuvent être restitués sans exposition excessive ; si les réclamations restent contradictoires et traçables ; et si les déplacements sont protégés par minimisation, durée limitée et contrôle d'accès. TAXI devient ainsi un passeport de sécurité de la course sans devenir un outil de surveillance.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 13 — TAXI

CHAPITRE 4 — FAUX TAXIS, CHAUFFEURS USURPÉS, QR CODES CLONÉS, LICENCES SUSPENDUES OU EXPIRÉES, FRAUDE TARIFAIRE, FAUSSES COURSES, LITIGES ET INVESTIGATION

1. Objet du chapitre

Ce chapitre organise la détection et le traitement des anomalies susceptibles d'affecter l'identité ou la confiance d'une course TAXI. Il couvre faux taxis présumés, usurpation de chauffeur, QR Codes clonés, autorisations incohérentes, anomalies tarifaires, fausses courses, litiges et investigation.

2. Principe de non-accusation automatique

Une anomalie technique, documentaire ou tarifaire ne constitue pas à elle seule une preuve de fraude. Authenticity Plus© produit des signaux, conserve les éléments disponibles et facilite la vérification ; les qualifications juridiques relèvent des acteurs et autorités compétents.

3. Faux taxi présumé

Un véhicule peut être signalé comme potentiellement non conforme lorsqu'il présente une identité TAXI absente, invalide ou incompatible avec les informations affichées. Le système doit indiquer la nature de l'incohérence sans affirmer automatiquement que le véhicule est un faux taxi.

4. Usurpation de chauffeur

Si la personne présente ne correspond pas au chauffeur professionnel associé à l'identité TAXI active, une alerte peut être déclenchée. Des remplacements légitimes, erreurs de données ou changements autorisés doivent pouvoir être vérifiés avant toute conclusion.

5. Véhicule substitué

Un chauffeur légitime utilisant un véhicule différent de celui actuellement associé au passeport doit pouvoir être distingué d'une usurpation complète. L'association chauffeur-véhicule doit être mise à jour par une procédure autorisée avant d'être présentée comme valide.

6. QR Code cloné

La copie photographique ou imprimée d'un QR Code légitime ne doit pas reproduire l'identité opérationnelle du taxi. La réponse dynamique dépend du statut actuel du passeport, de l'association chauffeur-véhicule et, lorsque pertinent, de la course active.

7. Détection d’utilisations incompatibles

Des scans géographiquement ou temporellement incompatibles, plusieurs véhicules utilisant le même identifiant ou des associations contradictoires peuvent produire une alerte de clonage. Les limites des données de localisation doivent être prises en compte.

8. Licence expirée

Lorsqu’une autorisation documentée arrive à expiration, le passeport ne doit plus la présenter comme valide. Un statut tel que « expiration constatée — vérification requise » peut être utilisé lorsque le renouvellement n’est pas encore connu.

9. Licence suspendue ou révoquée

Lorsqu’une source compétente fournit un statut de suspension ou de révocation, l’identité TAXI peut être restreinte selon les règles applicables. La source, la date et la portée de la décision doivent être conservées.

10. Absence de donnée à jour

L’impossibilité de vérifier en temps réel une autorisation ne doit pas être traduite automatiquement par « invalide ». Le système doit distinguer valide, expirée, suspendue, révoquée, inconnue ou vérification indisponible selon les informations réellement disponibles.

11. Anomalie tarifaire

Écart entre tarif documenté, compteur, forfait annoncé, suppléments ou reçu peut produire une alerte ou une contestation. Une anomalie peut provenir d’une erreur, d’une règle locale, d’un problème technique ou d’une pratique abusive ; l’investigation doit préserver ces possibilités.

12. Manipulation présumée du compteur

Des données incohérentes peuvent déclencher une vérification du compteur ou de la tarification. AP ne certifie pas la conformité métrologique et ne conclut pas à une manipulation sans éléments provenant des acteurs compétents.

13. Fausse course

Une course créée sans prise en charge réelle, dupliquée, artificiellement prolongée ou attribuée à de mauvaises identités peut être signalée. Les événements de début, fin, paiement et preuve de service servent à reconstruire la chronologie.

14. Reçu falsifié ou modifié

Un reçu dont les données ne correspondent pas à l’enregistrement de course peut être marqué comme incohérent. Un identifiant ou QR de reçu vérifiable permet de contrôler son intégrité sans exposer les données bancaires.

15. Dossier d’investigation

Le dossier peut regrouper identité TAXI, chauffeur, véhicule, autorisation, scans, événements de course, compteur, reçu, paiements référencés, déclarations et autres preuves autorisées. Chaque élément conserve sa source et son horodatage.

16. Contestation contradictoire

Chauffeur, passager, opérateur ou autre partie peut fournir une version différente des faits. Le système conserve les positions séparément et ne fusionne pas artificiellement les déclarations contradictoires.

17. Restriction préventive

Une anomalie grave peut justifier une restriction temporaire de certaines fonctions AP selon les règles de gouvernance. La mesure doit être proportionnée, attribuable, réversible et accompagnée d'un mécanisme de réexamen.

18. Vérification externe et résolution

Autorité de transport, opérateur, organisme de contrôle ou autre acteur compétent peut confirmer, corriger ou invalider certains éléments. La résolution est historisée avec sa source sans effacer l'alerte initiale.

19. Audit et AP Ledger

Les événements critiques d'identité, restrictions, changements d'autorisation et résolutions peuvent produire une piste d'audit et des empreintes minimales dans AP Ledger. Les trajets précis, identités privées et détails de litiges restent hors des couches publiques ou irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si un QR copié ne reproduit pas une identité active ; si chauffeur, véhicule et autorisation peuvent être vérifiés séparément ; si l'absence de donnée n'est pas assimilée à une invalidité ; si les anomalies tarifaires restent investigables ; si les parties peuvent contester ; et si toute restriction est traçable et réversible. TAXI transforme ainsi les incohérences en signaux vérifiables plutôt qu'en accusations automatiques.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 13 — TAXI

CHAPITRE 5 — GOUVERNANCE DES OPÉRATEURS, MAINTENANCE ET CONFORMITÉ DU VÉHICULE, ASSURANCE PROFESSIONNELLE, CYBERSÉCURITÉ, CONTRÔLE DES ACCÈS, CONFIDENTIALITÉ, AUDIT ET AP LEDGER

1. Objet du chapitre

Ce chapitre définit la gouvernance opérationnelle et technique de l’application TAXI. Il relie opérateurs, chauffeurs, véhicules, maintenance, contrôles documentés, assurance professionnelle, habilitations, cybersécurité, confidentialité, audit et AP Ledger afin que la confiance créée au moment de la course repose sur des données administrées de manière contrôlée.

2. Gouvernance des acteurs

Autorité de transport, opérateur, centrale, chauffeur, propriétaire ou exploitant du véhicule, atelier, assureur et autres acteurs doivent conserver des rôles distincts. Authenticity Plus© ne doit pas permettre à un acteur de modifier les données relevant d’une autre source sans habilitation.

3. Séparation des privilèges

Création d’une identité TAXI, rattachement d’un chauffeur, affectation d’un véhicule, ajout d’un document, changement de statut et administration système peuvent nécessiter des privilèges différents. Cette séparation limite l’impact d’une erreur ou d’un compte compromis.

4. Cycle de vie du chauffeur

Activation, renouvellement documentaire, suspension, changement d’opérateur et fin d’activité peuvent être historisés. Les anciennes périodes restent visibles dans l’audit sans être présentées comme des habilitations actuelles.

5. Cycle de vie du véhicule

Entrée en service, affectations successives, immobilisation, maintenance, contrôle, changement d’ exploitant et sortie de service peuvent être reliés au passeport du véhicule. Le statut opérationnel doit refléter les informations réellement disponibles.

6. Maintenance

Révision, réparation, pneumatiques, freinage, éclairage, équipements de sécurité ou autres interventions pertinentes peuvent être documentés par date, prestataire et justificatifs disponibles. Leur présence ne garantit pas automatiquement l’état futur du véhicule.

7. Contrôle technique ou réglementaire

Un contrôle officiel ou professionnel peut être référencé avec organisme, date, résultat et période de validité lorsque ces données sont disponibles. AP restitue le document et sa source sans devenir organisme de contrôle.

8. Conformité et absence de donnée

Une preuve expirée, une preuve absente et une vérification temporairement indisponible sont trois situations différentes. Le système ne doit pas déduire une non-conformité lorsque l'information disponible ne permet pas cette conclusion.

9. Assurance professionnelle

Police ou attestation d'assurance peut être reliée au véhicule, au chauffeur ou à l'exploitant selon le cadre applicable. Référence, période et statut documenté peuvent être conservés sans exposer les données contractuelles inutiles.

10. Sinistre et assurance

Un accident ou sinistre lié à une course peut être relié à l'identité de course, au véhicule et aux documents d'assurance pertinents. Déclaration, expertise, décision et indemnisation restent des événements distincts attribués à leurs sources.

11. Gestion des terminaux

Téléphones professionnels, tablettes, terminaux embarqués, lecteurs ou systèmes de caisse peuvent accéder à certaines fonctions TAXI. Chaque terminal autorisé doit pouvoir être identifié, limité et révoqué.

12. Authentification renforcée

Les opérations sensibles, notamment changement d'affectation, modification de documents, levée de restriction ou administration, peuvent exiger une authentification renforcée et des contrôles additionnels proportionnés au risque.

13. Compte compromis

En cas de compromission présumée, sessions et terminaux peuvent être révoqués et certaines opérations temporairement restreintes. La récupération du compte doit préserver l'historique et ne pas permettre d'effacer les traces de l'incident.

14. Protection du QR dynamique

La gestion du QR doit empêcher qu'un ancien état mis en cache ou une copie statique soit présenté comme une vérification actuelle. Le résultat affiché doit indiquer suffisamment clairement la fraîcheur ou le statut de la vérification.

15. Confidentialité du chauffeur

Documents d’identité, adresse privée, informations bancaires, contrats et données personnelles non nécessaires restent hors de la fiche publique TAXI. Le passager accède uniquement aux éléments nécessaires à la reconnaissance et à la confiance.

16. Confidentialité du passager

Identité, coordonnées, lieux de départ et d’arrivée, historique de courses et moyens de paiement sont protégés par défaut. Leur accès doit être limité aux finalités du service, de la sécurité, du litige ou aux obligations applicables.

17. Conservation et suppression

Les durées de conservation doivent être adaptées aux catégories de données et aux obligations pertinentes. La suppression ou anonymisation des données personnelles arrivées en fin de nécessité doit rester compatible avec la conservation d’empreintes minimales d’intégrité lorsqu’elle est légitime.

18. Journal d’audit

Créations et modifications d’identités, affectations chauffeur-véhicule, changements d’autorisation, restrictions, consultations sensibles et opérations administratives critiques doivent pouvoir être journalisés avec acteur et horodatage.

19. AP Ledger

AP Ledger peut ancrer des empreintes minimales de licences ou statuts documentés, affectations, événements critiques et résolutions. Il ne doit pas devenir un registre public des déplacements, des identités civiles, des paiements ou des dossiers complets de chauffeurs et passagers.

20. Critères d’acceptation et conclusion

Le modèle est acceptable si les rôles et privilèges sont séparés ; si maintenance, contrôle, assurance et autorisation conservent leurs sources ; si les terminaux compromis sont révocables ; si les QR reflètent un état actuel ; si les données de chauffeur et de passager restent minimisées ; et si l’audit garantit la traçabilité sans transformer AP Ledger en base publique de surveillance. Cette gouvernance fournit le socle nécessaire à la clôture fonctionnelle de l’application TAXI.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 13 — TAXI

CHAPITRE 6 — SYNTHÈSE FONCTIONNELLE, VÉRIFICATION PHYSIQUE ET NUMÉRIQUE, MODE OFFLINE, CRITÈRES D'ACCEPTATION ET CLÔTURE DE L'APPLICATION TAXI

1. Objet du chapitre

Ce chapitre clôt le Point 13 — TAXI. Il consolide l'identité du chauffeur, du véhicule et de l'autorisation, le QR Code dynamique, la vérification avant montée, la concordance spatio-temporelle smartphone-véhicule, le mode Offline sécurisé, la course, la tarification, la sécurité, les incidents, la lutte contre les faux taxis, la gouvernance, l'audit et AP Ledger.

2. Mission consolidée

L'application TAXI constitue un passeport de confiance de la course professionnelle. Sa fonction emblématique est simple : permettre au voyageur, avant de monter, de vérifier que le taxi présent devant lui correspond réellement au chauffeur, au véhicule et à l'autorisation actifs dans l'écosystème Authenticity Plus© / Deep Authenticity©.

3. QR Code dynamique extérieur

Un QR Code dynamique TAXI de référence peut être apposé sur la lunette arrière du véhicule dans un format physique standardisé, notamment un carré d'environ 5 cm × 5 cm lorsque le support et les règles locales le permettent. Il doit être suffisamment visible et accessible au scan avant l'entrée du passager dans le véhicule.

4. Le QR comme point d'accès et non comme identité

Le QR Code n'est ni la licence, ni l'identité du taxi, ni la preuve unique de conformité. Il constitue une porte d'accès sécurisée au Passeport Numérique TAXI. Copier, photographier ou imprimer le QR ne doit pas permettre de reproduire l'identité active du véhicule légitime.

5. Fiche de vérification du voyageur

Après scan, le voyageur peut recevoir les informations nécessaires à la vérification : photographie du chauffeur actuellement affecté, identité ou nom professionnel autorisé, marque et modèle du véhicule, immatriculation selon le niveau publiable, référence professionnelle, statut documenté de l' autorisation et état du Passeport TAXI.

6. Photographie du chauffeur

La photographie affichée doit correspondre au chauffeur actuellement associé au véhicule dans le système. Le voyageur peut ainsi comparer la personne au volant avec la photographie de référence, sans accéder aux documents personnels complets du professionnel.

7. Association chauffeur-véhicule-autorisation

Le niveau de confiance principal repose sur la concordance simultanée entre trois identités distinctes : chauffeur, véhicule et autorisation. Leur relation doit être active, datée et provenant des sources autorisées au moment de la vérification.

8. Vérification spatio-temporelle

Deep Authenticity© peut renforcer la vérification en comparant, lorsque les données sont disponibles et autorisées, la position du smartphone effectuant le scan avec une position récente et fiable du véhicule associé au Passeport TAXI. La vérification porte sur une proximité réaliste et une cohérence temporelle, non sur des coordonnées strictement identiques.

9. Tolérance de proximité

La précision GPS varie selon les appareils, l'environnement urbain, les bâtiments et les conditions de réception. Le système doit donc appliquer une zone de tolérance contextualisée et afficher un niveau de proximité ou de confiance plutôt qu'exiger une égalité parfaite des positions.

10. Lutte contre le clonage physique

Si un QR Code copié d'un taxi légitime est collé sur un autre véhicule situé ailleurs, la concordance entre smartphone, véhicule déclaré, chauffeur affecté et données de présence peut échouer. Le système doit alors refuser le statut complet « TAXI VÉRIFIÉ » et expliquer l'élément non concordant.

11. Résultat de vérification

Lorsque les éléments nécessaires concordent, l'interface peut afficher un statut clair de type « TAXI VÉRIFIÉ ». En cas d'écart, elle doit utiliser des messages factuels tels que « chauffeur non associé », « véhicule non concordant », « autorisation expirée », « proximité non vérifiée » ou « vérification indisponible », selon le fait réellement établi.

12. Principe de non-fausse négative

L'absence de réseau, une localisation indisponible ou une source momentanément inaccessible ne doit pas transformer automatiquement le taxi en véhicule invalide. Le système doit distinguer l'échec de vérification technique d'une incohérence effectivement constatée.

13. Mode Offline sécurisé

En l'absence de connectivité, l'application peut passer en mode Offline sécurisé. Elle utilise alors des preuves locales signées et limitées dans le temps : identité du véhicule, photographie du chauffeur, association chauffeur-véhicule, statut connu de l'autorisation, certificat temporaire et autres données minimales préchargées.

14. Géolocalisation en mode Offline

Le GPS du smartphone peut continuer à fournir une position sans connexion Internet. La comparaison avec le véhicule n'est possible hors ligne que si le véhicule ou son terminal professionnel dispose lui aussi d'une preuve locale récente et vérifiable de présence ou de proximité. Sans cette preuve, la géolocalisation doit être indiquée comme non vérifiée.

15. Affichage Offline

Le voyageur doit pouvoir distinguer clairement une vérification en ligne d'une vérification hors ligne. L' interface peut afficher « TAXI VÉRIFIÉ — MODE HORS LIGNE » lorsque les preuves locales sont suffisamment récentes et cohérentes, avec l'heure de dernière synchronisation. Si elles sont insuffisantes : « Vérification partielle — connexion requise ».

16. Resynchronisation

Au retour de la connectivité, les événements Offline sont réconciliés avec AP Core et les sources disponibles. Le système vérifie si, pendant la coupure, une autorisation a été suspendue, un chauffeur remplacé, un véhicule signalé ou un passeport restreint. Les conflits restent visibles et auditables.

17. Identité de course et reçu

Après vérification, chaque course peut recevoir une identité propre reliée au chauffeur et au véhicule actifs. Début, fin, tarification documentée, paiement référencé et reçu numérique peuvent former une preuve de service cohérente sans exposer les données bancaires ou l'historique complet du voyageur.

18. Sécurité, incidents et confidentialité

Partage temporaire de course, alertes de sécurité, objets oubliés, réclamations et dossiers d'incident doivent protéger les deux parties. Les positions précises, habitudes de déplacement, identités privées et données sensibles restent privées par défaut, avec accès limité et journalisé.

19. Critères d'acceptation

Le modèle est acceptable si le voyageur peut scanner avant de monter ; si le QR dynamique de 5 cm × 5 cm n'est qu'un accès au passeport ; si la photo du chauffeur et le véhicule correspondent aux associations actives ; si la proximité smartphone-véhicule est vérifiée avec tolérance lorsqu'elle est disponible ; si le mode Offline expose clairement son niveau de fraîcheur ; si une copie du QR ne suffit pas à reproduire un taxi vérifié ; et si les données de déplacement restent protégées.

20. Clôture du Point 13 — TAXI

Le Point 13 — TAXI est désormais fonctionnellement défini : chauffeur, véhicule, autorisation, identité TAXI, QR Code dynamique extérieur, photographie du chauffeur, concordance chauffeur-véhicule-autorisation, proximité smartphone-véhicule, mode Online et Offline sécurisé, resynchronisation, course, compteur et tarification, reçu, sécurité, objets oubliés, faux taxis, QR clonés, licences expirées ou suspendues, investigations, maintenance, assurance, cybersécurité,

confidentialité, audit et AP Ledger. La fonction emblématique de l’application peut se résumer ainsi : « Avant de monter, je scanne et je vérifie que c’est le vrai taxi. »

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 14 — LOGISTIQUE

CHAPITRE 1 — MISSION, IDENTITÉ DES MARCHANDISES, COLIS, PALETTES ET CONTENEURS, ACTEURS LOGISTIQUES, CHAÎNE DE POSSESSION, PROVENANCE, EXPÉDITION, TRANSPORT, RÉCEPTION ET PRINCIPES FONDATEURS

1. Objet du chapitre

Le Point 14 — Logistique transpose Authenticity Plus© / Deep Authenticity© aux flux physiques de marchandises. Il vise à relier l'objet transporté, son conditionnement, les acteurs successifs, les événements de prise en charge et les preuves disponibles afin de créer une continuité vérifiable de l' expédition à la réception.

2. Mission sectorielle

Le Passeport Numérique Logistique doit permettre de répondre à une question simple : quel bien ou lot est transporté, par qui, sous quelle responsabilité opérationnelle, à quel moment et selon quelles preuves ? Il ne remplace ni les documents douaniers officiels, ni les contrats de transport, ni les autorités compétentes.

3. Identité de la marchandise

Une unité logistique peut représenter un produit, un lot, une pièce, un équipement ou une autre marchandise identifiable. Référence fabricant, numéro de série, lot, SKU, identifiant AP ou autre identifiant peuvent contribuer à son identité tout en conservant leur source.

4. Colis

Le colis possède une identité logistique distincte du contenu qu'il transporte. Un même colis peut contenir plusieurs objets ou lots, et le passeport doit conserver la relation contenu-contenant sans les confondre.

5. Palette

Une palette peut regrouper plusieurs colis et recevoir sa propre identité. La composition doit pouvoir évoluer lors de consolidation ou dégroupage, chaque changement étant horodaté et attribué.

6. Conteneur

Un conteneur peut regrouper palettes, colis ou marchandises en vrac. Son numéro, son scellé et ses événements de chargement ou déchargement constituent des éléments de traçabilité distincts de l' identité des marchandises.

7. Hiérarchie logistique

L’architecture doit permettre la relation produit → colis → palette → conteneur → véhicule ou moyen de transport. Une modification à un niveau ne doit pas réécrire silencieusement l’identité des autres niveaux.

8. Acteurs logistiques

Expéditeur, fabricant, entrepôt, commissionnaire, transporteur, chauffeur, opérateur portuaire ou aéroportuaire, douane, dernier kilomètre et destinataire peuvent intervenir successivement. Chaque acteur ne doit pouvoir attester que les événements relevant de son rôle.

9. Chaîne de possession

La chaîne de possession documente qui a la garde opérationnelle de l’unité logistique à un instant donné. Elle reste distincte de la propriété commerciale ou juridique de la marchandise.

10. Provenance

La provenance peut relier fabricant, site de production, lot, documents d’origine et événements antérieurs disponibles. Les maillons inconnus restent explicitement inconnus plutôt que reconstruits artificiellement.

11. Préparation de l’expédition

Avant départ, le dossier peut réunir identité des unités, quantité, poids documenté, conditionnement, destination, transporteur prévu et documents associés. Chaque donnée conserve sa source.

12. Scellés et intégrité

Un scellé physique, électronique ou autre mécanisme peut être relié au conteneur ou au colis. Son statut contribue à l’intégrité de la chaîne sans prouver à lui seul que le contenu n’a subi aucune modification.

13. Prise en charge

La remise de la marchandise à un transporteur constitue un événement horodaté. Expéditeur et transporteur peuvent disposer de preuves distinctes de remise et d’acceptation, ce qui permet de conserver les divergences éventuelles.

14. Transport multimodal

Route, rail, mer, air ou autres modes peuvent se succéder dans une même expédition. Le Passeport Logistique conserve les segments et transferts plutôt que de réduire le parcours à un seul transporteur.

15. Événements de transit

Arrivée en hub, départ, transbordement, contrôle, attente, changement de véhicule, rupture de charge ou autre événement peut enrichir la chronologie selon les données disponibles.

16. Géolocalisation et proportionnalité

La position d'un véhicule ou d'une unité peut contribuer à la preuve de transit lorsqu'elle est disponible et autorisée. Elle doit être utilisée avec une précision et une durée adaptées, sans devenir un mécanisme de surveillance inutile des personnes.

17. Réception

À destination, la réception peut documenter date, destinataire autorisé, état apparent, quantité et réserves éventuelles. La réception physique ne signifie pas automatiquement acceptation sans réserve de toutes les obligations contractuelles.

18. Anomalies initiales

Colis manquant, scellé incohérent, quantité différente, retard, dommage apparent ou identité incompatible peut produire une alerte. Le système conserve le fait observé et sa source sans déterminer automatiquement la responsabilité.

19. AP Ledger et continuité

Les événements critiques de création d'identité, composition, transfert de garde, scellé, départ et réception peuvent produire des empreintes minimales dans AP Ledger. Les documents commerciaux complets, données personnelles et informations sensibles restent hors des couches publiques ou irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si marchandise, colis, palette et conteneur possèdent des identités distinctes mais reliées ; si garde et propriété ne sont pas confondues ; si chaque transfert est attribuable et horodaté ; si le multimodal conserve la continuité ; si les anomalies restent investigables ; et si AP Ledger protège l'intégrité sans exposer les données sensibles. Le Passeport Numérique Logistique devient ainsi la mémoire vérifiable du déplacement physique d'un bien.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 14 — LOGISTIQUE

CHAPITRE 2 — QR CODES DYNAMIQUES, SCANS LOGISTIQUES, SCELLÉS INTELLIGENTS, GÉOLOCALISATION, CHAÎNE DE POSSESSION EN TEMPS RÉEL, ONLINE/OFFLINE ET PREUVE DE LIVRAISON

1. Objet du chapitre

Ce chapitre définit la couche opérationnelle du Passeport Numérique Logistique. Il organise l' identification par QR Code dynamique, les scans successifs, les scellés, la géolocalisation, les transferts de garde, le fonctionnement Online/Offline et la preuve de livraison.

2. QR Code dynamique logistique

Colis, palette, conteneur ou autre unité logistique peut recevoir un QR Code dynamique relié à son identité AP. Le QR constitue un point d'accès au passeport et non la marchandise elle-même ; une copie visuelle du code ne doit pas suffire à reproduire un statut logistique légitime.

3. Scan au départ

Lors de la préparation ou de l'expédition, un scan peut confirmer l'unité, son état documentaire, son rattachement à l'expédition et l'acteur qui réalise l'opération. Le scan est horodaté et attribué à un terminal ou compte autorisé.

4. Scan de prise en charge

Au transfert vers un transporteur, les parties peuvent enregistrer remise et acceptation. Lorsque les deux événements existent, leur concordance renforce la chaîne de possession ; une divergence reste visible.

5. Scans de transit

Hub, entrepôt, port, aéroport, plateforme ou point de transbordement peuvent produire des événements de passage. L'absence d'un scan attendu déclenche une anomalie potentielle sans prouver automatiquement une perte.

6. Anti-clonage du QR

Deep Authenticity© peut comparer identité du QR, unité physique, terminal, localisation, séquence logistique et fraîcheur du statut. Deux scans incompatibles du même identifiant peuvent produire une alerte de duplication ou de clonage.

7. Scellé intelligent

Un scellé numéroté, électronique ou connecté peut être lié à un colis ou conteneur. Pose, activation, ouverture, rupture ou remplacement sont des événements distincts. Un scellé intact contribue à l'intégrité sans garantir à lui seul l'intégralité du contenu.

8. Remplacement du scellé

Lorsqu'un contrôle autorisé impose l'ouverture, l'ancien scellé est clôturé et le nouveau est enregistré avec motif, acteur, date et référence disponibles. La chaîne ne doit jamais masquer une ouverture légitime.

9. Géolocalisation

Une position du véhicule, du terminal ou de l'unité connectée peut renforcer la preuve de transit. Le système doit distinguer position mesurée, position déclarée et position déduite, ainsi que leur fraîcheur.

10. Concordance spatio-temporelle

Deep Authenticity© peut vérifier qu'un scan est cohérent avec le lieu et le moment attendus de l'événement. Une tolérance adaptée est nécessaire car GPS, réseaux et infrastructures peuvent produire des imprécisions.

11. Chaîne de possession en temps réel

Chaque prise en charge et remise peut faire évoluer le détenteur opérationnel courant. L'historique conserve les détenteurs précédents, les périodes et les preuves sans confondre garde physique et propriété commerciale.

12. Online

En mode connecté, le terminal vérifie le statut actuel du passeport, les restrictions, la composition logistique et les événements récents avant d'enregistrer une opération critique.

13. Offline sécurisé

Dans une zone sans réseau, un terminal autorisé peut utiliser des preuves locales signées, limitées dans le temps, ainsi qu'un contexte logistique préchargé. Les opérations Offline sont identifiées comme telles et ne doivent pas être présentées comme ayant bénéficié d'une vérification temps réel.

14. Limites Offline

Une preuve locale expirée, une unité inconnue ou une incohérence critique peut empêcher la validation complète. L'interface doit distinguer « vérifié hors ligne », « vérification partielle » et « connexion requise » selon les preuves réellement disponibles.

15. Resynchronisation

Au retour du réseau, les événements Offline sont transmis, ordonnés et confrontés à l'état central. Doubles prises en charge, restrictions intervenues pendant la coupure ou séquences contradictoires produisent une réconciliation et, si nécessaire, une investigation.

16. Livraison

À destination, un scan peut relier unité, course ou expédition, destinataire autorisé, heure et état apparent. La livraison peut être confirmée par différents mécanismes selon le contexte sans imposer une seule technologie.

17. Preuve de livraison

Signature, code temporaire, scan du destinataire, photographie autorisée, terminal professionnel ou autre preuve peut contribuer à la livraison. Chaque mécanisme conserve sa nature et sa source ; aucun n'est présenté comme infaillible.

18. Livraison partielle ou avec réserves

Quantité manquante, dommage apparent, scellé différent ou refus partiel doivent être enregistrés au moment de la réception lorsque possible. Le passeport conserve les réserves sans conclure automatiquement sur la responsabilité.

19. AP Ledger

Empreintes minimales de scans critiques, transferts de garde, changements de scellés et preuve de livraison peuvent être ancrées dans AP Ledger. Positions détaillées, signatures, documents commerciaux et données personnelles restent hors des couches publiques ou irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si un QR copié ne suffit pas à créer une unité légitime ; si les scans sont attribuables et ordonnés ; si scellés et changements restent historisés ; si la géolocalisation est utilisée avec tolérance ; si le mode Offline est explicite et réconcilié ; et si la livraison peut être prouvée sans surexposer le destinataire. Deep Authenticity© transforme ainsi chaque passage logistique en événement vérifiable d'une chaîne de possession continue.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 14 — LOGISTIQUE

CHAPITRE 3 — IoT ET CAPTEURS, CHAÎNE DU FROID, TEMPÉRATURE, HUMIDITÉ, CHOCS, OUVERTURE, CONDITIONS DE TRANSPORT, ALERTES ET PREUVES ENVIRONNEMENTALES

1. Objet du chapitre

Ce chapitre définit l'intégration des capteurs et données environnementales au Passeport Numérique Logistique. Il couvre température, humidité, chocs, inclinaison, ouverture, lumière, localisation et autres mesures utiles afin de documenter les conditions subies par une marchandise pendant son transport.

2. Principe de preuve environnementale

Une donnée de capteur constitue une observation technique produite par un dispositif identifié. Elle ne doit pas être confondue avec une conclusion automatique sur la qualité, la sécurité ou la conformité finale de la marchandise.

3. Identité du capteur

Chaque capteur ou dispositif connecté peut disposer d'un identifiant, d'un fabricant, d'un modèle, d' une configuration et d'un statut. Les données doivent rester reliées au dispositif qui les a produites.

4. Association capteur-unité logistique

Le capteur peut être associé à un produit, colis, palette, conteneur ou véhicule pour une période donnée. Début et fin d'association doivent être historisés afin de savoir à quelle unité les mesures se rapportent.

5. Température

Pour les flux thermosensibles, la température peut être mesurée selon une fréquence définie. Les valeurs, unités, horodatages et éventuelles lacunes doivent être conservés sans résumer abusivement une série complète par une seule valeur.

6. Chaîne du froid

Le Passeport Logistique peut documenter la continuité thermique depuis la préparation jusqu'à la réception. Une excursion hors plage peut être signalée avec durée et amplitude disponibles, sans conclure automatiquement que le produit est impropre.

7. Seuils

Les plages acceptables doivent provenir d'une source identifiée : fabricant, réglementation, protocole, contrat ou autre référence autorisée. Authenticity Plus© ne doit pas inventer un seuil générique lorsqu'il dépend du produit.

8. Humidité

L'humidité peut être pertinente pour médicaments, aliments, électronique, œuvres, matériaux ou autres marchandises. Comme pour la température, les mesures doivent conserver leur contexte et la qualité connue du capteur.

9. Chocs et vibrations

Accéléromètres ou indicateurs peuvent enregistrer choc, vibration ou chute. Un dépassement déclenche un événement à examiner ; il ne prouve pas automatiquement que le contenu est endommagé.

10. Inclinaison et orientation

Pour les marchandises devant rester verticales ou dans une orientation donnée, un capteur peut signaler une inclinaison ou un retournement. La durée et l'intensité de l'événement contribuent à l'analyse.

11. Ouverture et lumière

Un capteur d'ouverture, de rupture ou de lumière peut indiquer qu'un colis ou conteneur a été ouvert ou exposé. Une ouverture peut être légitime, par exemple lors d'un contrôle, et doit être rapprochée des événements autorisés de la chaîne.

12. Géolocalisation du capteur

Lorsque le dispositif dispose d'une position, celle-ci peut être comparée aux scans, au véhicule et au parcours attendu. Une incohérence spatio-temporelle peut produire une alerte sans devenir automatiquement une preuve de détournement.

13. Qualité et calibration

La confiance dans une mesure dépend du dispositif, de son état, de sa calibration lorsqu'elle est requise, de son horloge et de la continuité des données. Une calibration expirée ou inconnue doit être visible.

14. Pannes et données manquantes

Batterie faible, perte de signal, panne, saturation mémoire ou défaut de synchronisation peuvent créer des trous de mesure. Le système doit afficher ces lacunes plutôt que reconstruire artificiellement des valeurs absentes.

15. Mode Offline des capteurs

Les capteurs peuvent continuer à enregistrer localement pendant une absence de réseau. Les données sont synchronisées ultérieurement avec leurs horodatages et indicateurs d'intégrité, sans prétendre qu'elles ont été vérifiées en temps réel.

16. Alertes

Dépassement de seuil, rupture de chaîne du froid, choc important, ouverture inattendue ou perte prolongée de données peut générer une alerte vers les acteurs autorisés. L'alerte conserve sa règle de déclenchement et son contexte.

17. Réaction à une alerte

Transporteur, entrepôt, qualité, destinataire ou autre acteur peut enregistrer inspection, mise en quarantaine, changement de conditionnement ou autre action. L'action corrective reste distincte de l' alerte qui l'a déclenchée.

18. Réception et analyse

À la réception, les données environnementales peuvent compléter l'état apparent et les réserves. Une décision d'acceptation, de quarantaine, d'expertise ou de refus reste attribuée à l'acteur compétent.

19. AP Ledger et volumétrie

Les séries complètes de capteurs peuvent être volumineuses et sensibles. AP Ledger doit privilégier des empreintes d'intégrité, résumés signés ou événements critiques plutôt que publier toutes les mesures brutes sur une couche irréversible.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si chaque mesure reste reliée à son capteur et à l'unité concernée ; si les seuils sont sourcés ; si excursions, chocs et ouvertures restent des observations et non des verdicts ; si les données manquantes sont visibles ; si l'Offline est resynchronisé ; et si AP Ledger protège l' intégrité sans stocker inutilement toutes les séries. Deep Authenticity© étend ainsi la provenance logistique à l'environnement réellement subi par la marchandise.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 14 — LOGISTIQUE

CHAPITRE 4 — PERTE, VOL, DÉTOURNEMENT, SUBSTITUTION DE MARCHANDISES, COLIS OUVERTS, FAUX SCANS, QR CLONÉS, ANOMALIES DE LIVRAISON, LITIGES ET INVESTIGATION LOGISTIQUE

1. Objet du chapitre

Ce chapitre organise la détection et le traitement des anomalies affectant une chaîne logistique : perte, vol présumé, détournement, substitution, ouverture inattendue, faux scans, QR clonés, livraison incohérente et litiges. L'objectif est de préserver les preuves et reconstruire la chronologie sans transformer automatiquement une anomalie en accusation.

2. Principe de non-accusation

Un retard, un scan manquant, une rupture de scellé ou une incohérence de localisation peut avoir plusieurs causes. Authenticity Plus© / Deep Authenticity© produit des signaux de vigilance et facilite l' investigation ; la responsabilité juridique ou contractuelle reste déterminée par les acteurs compétents.

3. Perte présumée

Une unité qui ne réapparaît pas à l'étape attendue peut recevoir un statut de recherche ou perte présumée. Le dernier événement fiable, le dernier détenteur opérationnel connu et les données disponibles sont conservés.

4. Vol présumé

Lorsqu'un vol est déclaré, le passeport peut être restreint et le signalement horodaté. Une référence à une déclaration externe peut être ajoutée sans exposer publiquement les détails sensibles.

5. Détournement de parcours

Une divergence importante entre parcours attendu et positions disponibles peut déclencher une alerte. Déviation routière, changement opérationnel, erreur GPS ou incident légitime doivent rester des hypothèses possibles jusqu'à vérification.

6. Substitution de marchandise

Une unité présentant un numéro, une apparence, un poids, un lot ou d'autres caractéristiques incompatibles avec son passeport peut être signalée comme substitution présumée. Le système conserve les observations et preuves de comparaison.

7. Substitution de contenu

Un colis ou conteneur peut conserver son enveloppe ou son identifiant alors que son contenu a changé. Les relations contenu-contenant, scellés, poids documentés et inspections successives contribuent à détecter cette situation.

8. Colis ou conteneur ouvert

Une ouverture inattendue, un scellé rompu ou un remplacement non documenté produit une alerte d'intégrité. Une ouverture officielle ou opérationnelle peut ensuite être rapprochée de l'événement et expliquée.

9. Faux scan

Un scan peut être suspect lorsqu'il provient d'un terminal non autorisé, d'un lieu incompatible, d'une séquence impossible ou d'un compte compromis. Le scan reste conservé comme événement contesté plutôt que supprimé.

10. QR Code cloné

Deux unités physiques utilisant le même identifiant ou des scans simultanés incompatibles peuvent indiquer un clonage. Deep Authenticity© combine contexte, terminal, localisation, caractéristiques physiques et chronologie pour renforcer la détection.

11. Fausse preuve de livraison

Une livraison peut être contestée lorsque signature, code, photographie, lieu, heure ou destinataire ne concordent pas. Chaque preuve conserve sa nature et sa source afin de permettre une analyse contradictoire.

12. Livraison au mauvais destinataire

Si une unité est remise à une personne ou un site différent de la destination documentée, le passeport peut signaler l'écart. Une redirection autorisée doit pouvoir être ajoutée et historisée.

13. Quantité manquante ou dommage

À réception, différence de quantité, dommage apparent ou conditionnement altéré peut être enregistré avec réserves, photographies et autres éléments autorisés. L'événement ne détermine pas automatiquement à quel moment le dommage s'est produit.

14. Gel ou restriction du passeport

Une anomalie grave peut entraîner une restriction temporaire des transferts ou validations AP. Cette mesure doit être proportionnée, attribuable, réversible et accompagnée d'une procédure de réexamen.

15. Dossier d'investigation

Le dossier peut réunir scans, transferts de garde, scellés, positions, données capteurs, documents, photographies, déclarations et preuves de livraison. Chaque élément conserve sa source, son horodatage et son niveau de confiance.

16. Reconstruction de chronologie

L'investigation cherche à établir la dernière étape cohérente, la première anomalie observée et les événements intermédiaires disponibles. Les périodes sans données restent explicitement inconnues.

17. Contradiction entre acteurs

Expéditeur, transporteur, entrepôt, destinataire ou autre acteur peut présenter une version différente. Le système conserve les déclarations séparément et ne fusionne pas artificiellement des récits contradictoires.

18. Résolution

Retrouvé, livré, remplacé, erreur corrigée, réclamation acceptée ou autre résolution peut clôturer l' incident opérationnel. L'alerte initiale et la résolution restent toutes deux dans l'historique.

19. Audit et AP Ledger

Signalements critiques, restrictions, changements de scellé, événements contestés et résolutions peuvent produire des empreintes minimales dans AP Ledger. Les dossiers complets d'enquête, positions précises et informations commerciales sensibles restent protégés.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si perte et vol présumé restent distincts ; si les détournements et substitutions sont des signaux investigables ; si les faux scans ne sont pas effacés ; si un QR cloné peut être détecté par contexte ; si les litiges conservent les versions contradictoires ; et si toute restriction est traçable et réversible. Deep Authenticity© transforme ainsi l'anomalie logistique en dossier de preuve structuré plutôt qu'en accusation automatique.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 14 — LOGISTIQUE

CHAPITRE 5 — DOUANES, DOCUMENTS DE TRANSPORT, CONFORMITÉ, ASSURANCES CARGO, RESPONSABILITÉS, INTEROPÉRABILITÉ, CYBERSÉCURITÉ, GOUVERNANCE, AUDIT ET AP LEDGER

1. Objet du chapitre

Ce chapitre définit la couche institutionnelle, documentaire et de gouvernance du Passeport Numérique Logistique. Il organise les relations avec les documents de transport, les formalités douanières, la conformité, l'assurance cargo, les responsabilités, l'interopérabilité entre systèmes, la cybersécurité, l'audit et AP Ledger.

2. Principe de complémentarité

Authenticity Plus© / Deep Authenticity© ne remplace ni les documents réglementaires, ni les déclarations douanières, ni les contrats de transport, ni les systèmes officiels. Le passeport relie ces sources et leurs événements afin d'améliorer la continuité et la vérifiabilité.

3. Documents de transport

Lettre de voiture, connaissement, lettre de transport aérien, bordereau, manifeste ou autre document peut être relié à une expédition. Chaque document conserve son émetteur, sa référence, sa version, sa date et son statut lorsque disponibles.

4. Document et marchandise

Le document de transport reste distinct de la marchandise, du colis, de la palette et du conteneur. Une correction documentaire ne doit pas modifier silencieusement l'identité physique de l'unité logistique.

5. Douanes

Déclaration, référence de dossier, contrôle, mainlevée, inspection ou autre événement douanier peut être référencé lorsqu'il est disponible et autorisé. AP restitue le statut documenté sans se substituer à l'administration douanière.

6. Contrôle douanier et ouverture

Lorsqu'une autorité ouvre un colis ou un conteneur, l'événement peut expliquer une rupture ou un remplacement de scellé. Le nouveau scellé et les références disponibles doivent pouvoir rejoindre la chronologie.

7. Conformité documentaire

Certificats, licences, attestations, origine, documents sanitaires, phytosanitaires ou autres pièces applicables peuvent être reliés au lot ou à l'expédition. Leur validité reste déterminée par leurs émetteurs et règles propres.

8. Marchandises réglementées

Certaines marchandises imposent des conditions particulières de transport, stockage, documentation ou manipulation. Le passeport peut signaler les exigences documentées sans fournir lui-même une autorisation de transporter.

9. Assurance cargo

Police, certificat, couverture déclarée, période, assuré et références de l'expédition peuvent être associés au passeport. La présence d'une assurance ne signifie pas automatiquement qu'un sinistre particulier est couvert ou indemnisable.

10. Sinistre cargo

Perte, dommage, vol présumé, rupture de chaîne du froid ou autre sinistre peut être relié aux preuves de transport, capteurs, réserves et documents d'assurance. Déclaration, expertise et décision d' indemnisation restent des événements distincts.

11. Responsabilités

Expéditeur, transporteur, commissionnaire, entrepôt, sous-traitant et destinataire peuvent avoir des obligations différentes. Le Passeport Logistique documente les transferts de garde et les événements sans déterminer automatiquement la responsabilité juridique.

12. Sous-traitance

Un transporteur peut confier un segment à un autre opérateur. Chaque sous-traitance ou changement de détenteur opérationnel doit pouvoir être enregistré afin que la chaîne ne perde pas la visibilité sur l' acteur effectivement responsable de la garde.

13. Interopérabilité

Le passeport doit pouvoir échanger des données avec ERP, WMS, TMS, systèmes portuaires, plateformes de transport, IoT ou autres infrastructures autorisées. Les mappings doivent préserver l' identité, la source, les unités, les horodatages et le sens des statuts.

14. Identifiants externes

Numéros de suivi, références de conteneur, lots, commandes, expéditions et autres identifiants peuvent coexister. AP doit les relier sans supposer qu'un identifiant externe est universel ou permanent.

15. Gouvernance des accès

Expéditeur, transporteur, douane, assureur, destinataire et auditeur ne doivent pas disposer des mêmes droits. Consultation, ajout de preuve, changement de garde, modification documentaire et administration doivent être séparés.

16. Cybersécurité des terminaux et API

Terminaux de scan, passerelles IoT, comptes professionnels et API constituent des points sensibles. Authentification, révocation, limitation des privilèges, journalisation et gestion des secrets doivent protéger les opérations critiques.

17. Compte ou terminal compromis

Un terminal volé ou un compte compromis doit pouvoir être révoqué rapidement. Les événements suspects produits avant révocation restent conservés et peuvent être marqués pour investigation plutôt qu'effacés.

18. Audit

Création d'identité, composition d'unités, transferts de garde, changements de scellés, accès sensibles, modifications documentaires, restrictions et résolutions doivent pouvoir produire une piste d'audit attribuable et horodatée.

19. AP Ledger et confidentialité commerciale

AP Ledger peut ancrer des empreintes minimales d'événements et documents critiques. Prix, contrats, itinéraires détaillés, documents douaniers complets, secrets commerciaux et données personnelles restent hors des couches publiques ou irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si AP complète sans remplacer les systèmes officiels ; si documents et marchandises restent distincts ; si les contrôles expliquent les ruptures de scellé ; si assurance et responsabilité ne sont pas déduites automatiquement ; si les sous-traitants restent visibles ; si l'interopérabilité conserve la provenance des données ; et si cybersécurité, audit et AP Ledger protègent la chaîne sans exposer les informations commerciales sensibles.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 14 — LOGISTIQUE

CHAPITRE 6 — SYNTHÈSE FONCTIONNELLE, CRITÈRES D'ACCEPTATION ET CLÔTURE DE L'APPLICATION LOGISTIQUE

1. Objet du chapitre

Ce chapitre clôt le Point 14 — Logistique. Il consolide l'identité des marchandises et unités logistiques, la chaîne de possession, les QR Codes dynamiques, les scans, scellés, géolocalisation, modes Online/Offline, capteurs IoT, anomalies, douanes, assurances, interopérabilité, cybersécurité, audit et AP Ledger.

2. Mission consolidée

Le Passeport Numérique Logistique constitue la mémoire vérifiable du déplacement physique d'un bien. Il permet de savoir quelle unité est concernée, dans quel contenant elle se trouve, quel acteur en a la garde, quels événements ont été observés et quelles preuves les soutiennent.

3. Hiérarchie d'identité

Marchandise, produit, lot, colis, palette, conteneur et moyen de transport restent des identités distinctes mais reliées. Consolidation, dégroupage ou changement de contenant modifie les relations sans réécrire l'identité historique des unités.

4. Garde et propriété

La chaîne de possession documente la garde opérationnelle sans être confondue avec la propriété commerciale ou juridique. Chaque transfert de garde doit pouvoir être attribué, daté et relié aux preuves disponibles.

5. QR Code dynamique et scans

Le QR dynamique donne accès au passeport courant. Les scans de départ, prise en charge, transit et réception enrichissent la chronologie. Une copie visuelle du QR ne doit pas suffire à reproduire une identité logistique légitime.

6. Deep Authenticity© et anti-clonage

Identité, terminal, caractéristiques physiques, séquence, localisation et fraîcheur peuvent être combinés pour détecter des utilisations incompatibles. Deux unités utilisant le même identifiant peuvent ainsi déclencher une investigation de clonage.

7. Scellés

Pose, activation, rupture, ouverture autorisée et remplacement d'un scellé restent des événements distincts. Un scellé intact renforce l'intégrité du conditionnement sans garantir à lui seul l'identité ou l'état complet du contenu.

8. Géolocalisation et cohérence

Les positions disponibles peuvent être comparées aux scans, au parcours et aux acteurs attendus. Deep Authenticity© utilise une cohérence spatio-temporelle avec tolérance adaptée plutôt qu'une égalité irréaliste des coordonnées.

9. Online et Offline

En mode Online, l'état courant peut être vérifié avant une opération critique. En mode Offline sécurisé, des preuves locales signées et limitées dans le temps permettent une continuité contrôlée. La reconnexion déclenche la resynchronisation et la réconciliation.

10. IoT et conditions de transport

Température, humidité, chocs, vibrations, inclinaison, ouverture, lumière et autres mesures peuvent documenter l'environnement subi par la marchandise. Chaque donnée reste reliée à son capteur, à sa période d'association et à sa qualité connue.

11. Chaîne du froid

Les excursions thermiques sont documentées avec les seuils provenant de sources identifiées. Une excursion constitue une observation et une alerte ; elle ne devient pas automatiquement une décision sur la sécurité ou la qualité du produit.

12. Données manquantes

Panne, batterie faible, perte réseau ou défaut de synchronisation peuvent produire des lacunes. Les valeurs absentes restent absentes : le système ne reconstruit pas artificiellement une continuité qui n'a pas été mesurée.

13. Anomalies et investigations

Perte, vol présumé, détournement, substitution, ouverture, faux scan, QR cloné, dommage ou livraison contestée peuvent ouvrir un dossier structuré. L'anomalie est un signal investigable et non une accusation automatique.

14. Reconstruction chronologique

L'investigation conserve la dernière étape cohérente, la première anomalie observée, les preuves intermédiaires et les périodes inconnues. Les déclarations contradictoires des acteurs restent séparées.

15. Livraison et preuve

La réception peut être documentée par scan, signature, code, photographie autorisée ou autre mécanisme. Livraison physique, réserves et acceptation contractuelle restent des notions distinctes.

16. Douanes et conformité

Documents de transport, contrôles douaniers, licences, certificats et autres preuves réglementaires peuvent rejoindre le passeport. AP les relie et en protège la provenance sans remplacer les autorités ou systèmes officiels.

17. Assurance et responsabilités

Assurance cargo, sinistre, expertise et décision d'indemnisation restent attribués à leurs acteurs. Les transferts de garde facilitent l'analyse mais ne déterminent pas automatiquement la responsabilité juridique.

18. Interopérabilité, cybersécurité et gouvernance

ERP, WMS, TMS, IoT et plateformes externes peuvent échanger avec AP en préservant identités, sources, unités et horodatages. Comptes, terminaux et API sont soumis à des droits minimaux, révocation et journalisation.

19. AP Ledger et critères d'acceptation

AP Ledger conserve des empreintes minimales des événements critiques sans publier itinéraires détaillés, contrats, positions, documents douaniers complets ou données personnelles. Le modèle est acceptable si les identités restent distinctes, la garde est traçable, l'Offline est explicite, les capteurs sont sourcés, les anomalies restent investigables et les systèmes officiels conservent leur autorité.

20. Clôture du Point 14 — Logistique

Le Point 14 — Logistique est désormais fonctionnellement défini : marchandises, colis, palettes, conteneurs, acteurs, chaîne de possession, provenance, QR dynamiques, scans, scellés, géolocalisation, Online/Offline, IoT, chaîne du froid, preuves environnementales, perte, vol présumé, détournement, substitution, faux scans, QR clonés, livraison, douanes, conformité, assurance cargo, interopérabilité, cybersécurité, gouvernance, audit et AP Ledger. Le Volume IV peut désormais poursuivre avec le Point 15 — Education.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 15 — EDUCATION

CHAPITRE 1 — IDENTITÉ ACADÉMIQUE, ÉTABLISSEMENT, APPRENANT, ENSEIGNANT, INSCRIPTION, CURSUS, DIPLÔMES, CERTIFICATS, COMPÉTENCES ET PASSEPORT NUMÉRIQUE ÉDUCATIF

1. Objet du chapitre

Le Point 15 — Education transpose Authenticity Plus© / Deep Authenticity© à la continuité des preuves éducatives. Il relie établissements, apprenants, enseignants, inscriptions, cursus, résultats, diplômes, certificats et compétences dans un Passeport Numérique Éducatif vérifiable.

2. Mission sectorielle

La mission est de permettre à une personne de conserver et présenter des preuves éducatives vérifiables tout au long de son parcours, y compris lorsqu'elle change d'établissement ou de pays. AP ne remplace ni l'établissement, ni le ministère, ni l'autorité d'accréditation.

3. Identité académique de l'apprenant

Le Passeport Éducatif doit relier les preuves à la bonne personne sans rendre son dossier scolaire public. L'identité civile, l'identité de compte et les identifiants propres aux établissements restent distingués.

4. Mineurs et protection renforcée

Lorsque l'apprenant est mineur, confidentialité, contrôle d'accès, représentation légale et minimisation doivent être renforcés. Le passeport ne doit pas devenir un profil public permanent retraçant l'enfance ou les difficultés scolaires.

5. Établissement

École, université, centre de formation ou autre organisme dispose d'une identité institutionnelle distincte. Statut, accréditation et habilitations peuvent être reliés à des sources compétentes sans être créés par Authenticity Plus©.

6. Enseignant et personnel habilité

Un enseignant ou agent peut être relié à un établissement et à certaines fonctions pour une période donnée. Son rôle doit déterminer ce qu'il peut attester, consulter ou modifier.

7. Inscription

L’inscription constitue un événement documenté reliant apprenant, établissement, programme et période. Préinscription, admission, inscription administrative et présence effective peuvent rester des états distincts.

8. Cursus

Le cursus peut représenter programme, niveau, spécialité, modules, unités d’enseignement et périodes suivies. Les modifications de programme doivent être historisées plutôt que réécrire rétroactivement le parcours.

9. Résultats académiques

Notes, validations, crédits, appréciations ou décisions peuvent être reliés à leur établissement, session et source. Les données détaillées restent privées et ne doivent être exposées qu’avec une finalité et une autorisation appropriées.

10. Diplôme

Un diplôme peut recevoir une référence vérifiable reliée à l’établissement émetteur, au titulaire, à l’intitulé, à la date et au statut. Le Passeport Éducatif facilite la vérification sans devenir lui-même l’autorité qui délivre le diplôme.

11. Certificat

Certificat de formation, attestation, micro-certification ou autre credential peut rejoindre le passeport. Chaque preuve conserve son émetteur, son périmètre et, lorsqu’elle existe, sa période de validité.

12. Compétences

Une compétence peut être déclarée, enseignée, évaluée ou certifiée. Ces niveaux doivent rester distincts : avoir suivi un cours ne signifie pas automatiquement maîtriser ou être certifié dans une compétence.

13. Portfolio

Projets, travaux, réalisations ou expériences peuvent être reliés au passeport avec leurs auteurs, dates et validations disponibles. Un portfolio complète les titres officiels sans les remplacer.

14. Provenance des preuves

Chaque diplôme, note, certificat ou compétence vérifiée doit conserver sa provenance : établissement, enseignant habilité, organisme certificateur ou autre source. Une pièce téléchargée par l’utilisateur reste distinguée d’une preuve transmise directement par l’émetteur.

15. QR Code dynamique

Un diplôme, certificat ou profil de partage peut utiliser un QR Code dynamique permettant à un tiers autorisé de vérifier l’émetteur, le titulaire, le statut et les informations consenties sans accéder au dossier scolaire complet.

16. Partage contrôlé

L’apprenant peut partager une sélection de diplômes ou compétences avec une université, un employeur ou autre organisme. Le partage doit être limité aux informations nécessaires et, lorsque pertinent, à une durée déterminée.

17. Portabilité

Le passeport doit préserver les preuves lors d’un changement d’école, d’université, de plateforme ou de pays. La portabilité ne signifie pas qu’un nouvel établissement est obligé de reconnaître académiquement toutes les preuves.

18. Corrections et révisions

Erreur de nom, note rectifiée, diplôme corrigé ou décision modifiée doit produire une nouvelle version ou un événement de correction. L’historique d’intégrité reste auditable sans exposer publiquement les anciennes données sensibles.

19. AP Ledger

Des empreintes minimales de diplômes, certificats et événements critiques peuvent être ancrées dans AP Ledger pour renforcer l’intégrité et la vérification. Notes détaillées, dossiers disciplinaires, données personnelles et travaux privés restent hors des couches publiques ou irréversibles.

20. Critères d’acceptation et conclusion

Le modèle est acceptable si l’identité académique reste privée ; si les établissements conservent l’ autorité d’émission ; si diplôme, certificat et compétence restent distincts ; si le QR permet une vérification minimale ; si l’apprenant contrôle le partage ; si les corrections sont historisées ; et si les mineurs bénéficient d’une protection renforcée. Le Passeport Numérique Éducatif devient ainsi une mémoire portable et vérifiable du parcours sans créer un dossier scolaire public permanent.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 15 — EDUCATION

CHAPITRE 2 — DIPLÔMES VÉRIFIABLES, QR CODES DYNAMIQUES, VÉRIFICATION PAR UNIVERSITÉS ET EMPLOYEURS, FAUX DIPLÔMES, RÉVOCATION, CORRECTIONS, ÉQUIVALENCES ET RECONNAISSANCE INTERNATIONALE

1. Objet du chapitre

Ce chapitre définit la couche de vérification des diplômes, certificats et autres preuves éducatives. Il organise l'émission, le QR Code dynamique, la consultation autorisée, la détection des incohérences, les corrections, la révocation, les équivalences et la reconnaissance internationale.

2. Principe de vérifiabilité

Un diplôme vérifiable doit permettre de confirmer au minimum l'émetteur, le titulaire selon les droits de consultation, l'intitulé, la date, la référence et le statut documenté. Authenticity Plus© protège la preuve sans devenir l'autorité académique qui délivre le titre.

3. Émission par l'établissement

L'établissement ou l'autorité habilitée émet la preuve depuis un compte et un rôle autorisés. L'événement d'émission est horodaté et relié à l'identité institutionnelle de l'émetteur.

4. Empreinte d'intégrité

Le document ou jeu de données peut produire une empreinte cryptographique permettant de détecter une modification ultérieure. L'empreinte protège l'intégrité du contenu enregistré mais ne prouve pas, à elle seule, la légitimité de l'émetteur.

5. QR Code dynamique du diplôme

Le diplôme ou certificat peut comporter un QR Code dynamique ouvrant une fiche de vérification. Le QR n'embarque pas nécessairement toutes les données personnelles ; il donne accès au statut courant et aux informations autorisées.

6. Vérification par une université

Une université recevant une candidature peut vérifier que le titre présenté correspond à une preuve émise par l'établissement identifié. Elle conserve toutefois ses propres règles d'admission, d'équivalence et de reconnaissance.

7. Vérification par un employeur

Un employeur peut vérifier un diplôme ou une compétence partagée par le titulaire sans obtenir l'ensemble du dossier scolaire. Le principe de minimisation limite la consultation aux informations nécessaires.

8. Consentement et partage

Le titulaire peut autoriser un partage ciblé, temporaire ou permanent selon le contexte. Les journaux de partage doivent permettre de savoir quelle preuve a été rendue accessible et selon quelles conditions.

9. Faux diplôme

Un document dont l'émetteur, la référence, le contenu ou le statut ne correspond pas aux données vérifiables peut être signalé comme incohérent ou non vérifié. Le système ne doit pas transformer automatiquement cette incohérence en accusation pénale.

10. Copie ou QR cloné

La reproduction graphique d'un diplôme ou de son QR Code ne doit pas suffire à créer un titre valide. Le scan interroge le Passeport Éducatif et le statut actuel de la preuve plutôt que de faire confiance à l'apparence du document.

11. Diplôme ancien ou non numérisé

Un diplôme historique peut être ajouté par son titulaire ou numérisé par un établissement. Une copie fournie par l'utilisateur reste distinguée d'une preuve confirmée directement par l'émetteur.

12. Correction

Erreur de nom, intitulé, date ou autre donnée peut être corrigée par l'acteur habilité. La version corrigée devient la référence active tandis que l'existence de la correction reste auditable.

13. Révocation ou retrait

Lorsqu'une autorité habilitée retire ou révoque officiellement une preuve, le passeport peut refléter ce statut avec sa source et sa date. Une révocation ne doit jamais être créée par AP sans décision provenant de l'acteur compétent.

14. Suspension ou vérification en cours

Lorsque le statut fait l'objet d'un contrôle, un état intermédiaire peut être utilisé afin d'éviter de présenter comme valide ou révoquée une preuve dont la situation n'est pas encore déterminée.

15. Équivalence

Une équivalence académique constitue une décision distincte du diplôme d'origine. Elle doit identifier l'organisme qui l'accorde, le système éducatif concerné, la portée et la date de la décision.

16. Reconnaissance internationale

Le Passeport Éducatif facilite la transmission et la compréhension des preuves entre pays grâce à la provenance, aux métadonnées et aux traductions autorisées. Il ne garantit pas qu'un diplôme sera juridiquement ou académiquement reconnu dans tous les pays.

17. Traductions

Une traduction officielle, certifiée ou informative doit conserver son statut et son auteur ou organisme. La traduction ne remplace jamais le document source et doit rester reliée à celui-ci.

18. Interopérabilité

Les preuves peuvent être échangées avec systèmes universitaires, plateformes de candidature ou autres infrastructures autorisées. L'interopérabilité doit préserver l'émetteur, le titulaire, le statut, la version et l'intégrité de la preuve.

19. AP Ledger et confidentialité

Des empreintes minimales d'émission, correction, révocation ou statut peuvent être ancrées dans AP Ledger. Notes détaillées, dossiers scolaires, adresses, identifiants sensibles et documents privés restent hors des couches publiques ou irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si un tiers peut vérifier une preuve sans accéder au dossier complet ; si un QR copié ne crée pas un diplôme valide ; si corrections et révocations proviennent d'acteurs habilités ; si diplôme et équivalence restent distincts ; si la reconnaissance internationale n'est jamais promise automatiquement ; et si le titulaire conserve le contrôle du partage. Deep Authenticity© transforme ainsi le diplôme statique en preuve éducative vérifiable, évolutive et portable.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 15 — EDUCATION

CHAPITRE 3 — EXAMENS, ÉVALUATIONS, IDENTITÉ DU CANDIDAT, PRÉSENCE, TRAVAUX, USAGE DE L'IA, PLAGIAT, INTÉGRITÉ ACADÉMIQUE ET TRAÇABILITÉ DES RÉSULTATS

1. Objet du chapitre

Ce chapitre définit la couche de confiance applicable aux examens, évaluations et travaux académiques. Il relie identité du candidat, session, présence, épreuve, remise de travail, correction, usage déclaré ou autorisé de l'IA, contrôles d'intégrité et publication des résultats.

2. Principe fondamental

Deep Authenticity© doit permettre d'établir qui a participé à quelle évaluation, dans quel contexte et selon quelles preuves, sans prétendre déduire automatiquement l'honnêteté, l'intention ou la culpabilité d'un apprenant.

3. Identité du candidat

Avant une évaluation, l'établissement peut vérifier que le candidat correspond à l'identité académique inscrite. Les méthodes de vérification doivent rester proportionnées et éviter de diffuser ou conserver inutilement des données biométriques ou documents d'identité.

4. Inscription à l'épreuve

L'inscription à un examen constitue un événement distinct de l'inscription au cursus. Elle relie candidat, matière, session, établissement, date et règles applicables.

5. Présence

La présence peut être documentée par émargement, carte institutionnelle, QR dynamique, terminal autorisé ou autre mécanisme. Une preuve de présence indique la participation ou l'accès à la session, pas automatiquement l'auteur de chaque réponse.

6. QR Code de session

Une session peut disposer d'un QR Code dynamique ou d'un identifiant temporaire permettant de confirmer le lieu, l'horaire et l'épreuve. Un code copié ou utilisé hors du contexte prévu peut produire une incohérence.

7. Épreuve et version

Sujet, version, barème et consignes doivent être identifiables. Lorsqu'il existe plusieurs versions, le passeport d'évaluation conserve celle attribuée au candidat afin d'éviter les confusions lors de la correction ou d'une contestation.

8. Remise d'un travail

Devoir, mémoire, projet, fichier ou autre production peut recevoir une preuve de dépôt avec auteur déclaré, date, version et établissement destinataire. Une nouvelle remise ne doit pas effacer silencieusement la précédente.

9. Intégrité du fichier

Une empreinte cryptographique peut permettre de vérifier qu'un fichier remis n'a pas été modifié après le dépôt enregistré. Elle ne prouve pas à elle seule que le contenu a été entièrement créé par le candidat.

10. Usage de l'intelligence artificielle

L'usage d'outils d'IA doit être interprété selon les règles de l'établissement et de l'épreuve. Le système peut conserver une déclaration d'usage, une autorisation, une restriction ou des éléments de processus lorsque cela est prévu, sans inventer une règle académique universelle.

11. IA autorisée

Lorsque l'IA est permise, l'établissement peut demander de déclarer le type d'assistance utilisé, par exemple recherche, reformulation, traduction, génération d'idées ou aide technique. Cette déclaration reste distincte de l'évaluation académique du travail.

12. Détection automatisée et prudence

Un détecteur de texte généré par IA, de similarité ou d'anomalie ne doit jamais constituer à lui seul une preuve définitive de fraude. Les résultats automatisés sont des signaux à examiner avec leur méthode, leurs limites et le contexte académique.

13. Plagiat et similarité

Un taux de similarité n'est pas automatiquement un taux de plagiat. Citations, bibliographie, expressions communes et contenus autorisés peuvent produire des correspondances. La qualification académique relève d'une analyse humaine selon les règles applicables.

14. Sources et citations

Lorsque l'épreuve l'exige, références, citations et sources peuvent être associées au travail. Deep Authenticity© peut aider à préserver la provenance des éléments sans juger automatiquement la qualité intellectuelle de leur utilisation.

15. Correction

La correction doit rester reliée au correcteur ou au processus habilité, au barème, à la version de l’ épreuve et à la copie concernée. Correction initiale, seconde correction et révision sont des événements distincts.

16. Résultat

Note, mention, validation ou décision est publiée par l’établissement ou l’acteur habilité. Le Passeport Éducatif en conserve la provenance et la version sans devenir lui-même l’autorité qui attribue la note.

17. Contestation et recours

Le candidat peut contester un résultat ou un signalement selon les procédures de l’établissement. Copie, barème, événements, analyses automatisées et décisions successives peuvent être réunis dans un dossier contradictoire.

18. Confidentialité

Copies, notes, commentaires, signalements d’intégrité et procédures disciplinaires sont des données sensibles. Leur accès doit être limité aux personnes habilitées ; elles ne doivent pas devenir des informations publiques du Passeport Éducatif.

19. Audit et AP Ledger

Dépôt, empreinte du travail, publication d’un résultat, correction officielle ou décision finale peuvent produire des empreintes minimales dans AP Ledger. Les copies complètes, prompts, conversations, notes détaillées et dossiers disciplinaires restent hors des couches publiques ou irréversibles.

20. Critères d’acceptation et conclusion

Le modèle est acceptable si identité, présence et auteur déclaré restent des preuves distinctes ; si les versions des travaux sont conservées ; si l’usage de l’IA dépend des règles de l’épreuve ; si aucun détecteur automatisé ne produit seul un verdict de fraude ; si similarité et plagiat ne sont pas confondus ; si les recours restent possibles ; et si les résultats demeurent privés. Deep Authenticity© renforce ainsi l’intégrité académique par la provenance et la traçabilité plutôt que par une surveillance ou une accusation automatique.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 15 — EDUCATION

CHAPITRE 4 — FAUX DIPLÔMES, USURPATION D'IDENTITÉ ACADÉMIQUE, FALSIFICATION DES NOTES ET CERTIFICATS, FRAUDE AUX EXAMENS, COMPTES COMPROMIS, LITIGES ET INVESTIGATION

1. Objet du chapitre

Ce chapitre organise la détection, la qualification prudente et l'investigation des anomalies affectant les preuves éducatives : faux diplômes présumés, usurpation d'identité académique, falsification de notes ou certificats, irrégularités d'examen, comptes compromis et litiges.

2. Principe de non-accusation automatique

Une incohérence documentaire, technique ou comportementale constitue un signal à vérifier, non une preuve automatique de fraude. Authenticity Plus© / Deep Authenticity© conserve les faits, leurs sources et les versions contradictoires ; les décisions disciplinaires, administratives ou judiciaires relèvent des autorités compétentes.

3. Faux diplôme présumé

Un document peut être signalé lorsqu'il ne correspond pas à l'émetteur, à la référence, au titulaire, à l' intitulé, à la date ou au statut enregistrés. L'absence d'un diplôme ancien dans un système numérique ne suffit cependant pas à conclure qu'il est faux.

4. Diplôme ou certificat modifié

Une différence entre l'empreinte d'un document vérifiable et celle du fichier présenté peut révéler une modification. Le système doit identifier l'incohérence sans prétendre déterminer automatiquement qui l'a créée ni pourquoi.

5. QR Code copié ou détourné

La copie du QR d'un titre légitime sur un autre document ne doit pas permettre de valider ce dernier. La fiche de vérification doit afficher les données de référence afin que le tiers puisse comparer le document présenté au passeport actif.

6. Usurpation d'identité académique

Une preuve authentique peut être présentée par une personne qui n'en est pas le titulaire. Les mécanismes de partage et de vérification doivent donc confirmer la relation entre la preuve et le titulaire autorisé, avec minimisation des données personnelles.

7. Compte étudiant compromis

Un compte compromis peut permettre des dépôts, demandes de documents ou partages non autorisés. Sessions, terminaux et jetons d'accès doivent pouvoir être révoqués, tandis que les événements suspects restent conservés pour investigation.

8. Compte institutionnel compromis

La compromission d'un compte d'établissement ou d'un agent habilité présente un risque plus élevé d' émissions ou modifications frauduleuses. Les opérations sensibles doivent être protégées par séparation des rôles, authentification renforcée et journalisation.

9. Falsification de notes

Une note présentée différemment du résultat officiel peut être signalée comme incohérente. Correction légitime, recours, seconde session et décision de jury doivent rester des événements distincts afin d'éviter de confondre une révision officielle avec une falsification.

10. Faux certificat

Un certificat peut être fabriqué, altéré ou attribué à tort. La vérification doit porter sur l'émetteur, le titulaire, le programme, la date, le statut et, lorsqu'elle existe, la période de validité.

11. Irrégularité d'examen

Substitution de candidat, accès non autorisé, communication interdite ou autre irrégularité peut être signalée selon les règles de l'établissement. Les preuves techniques ou humaines restent attribuées à leurs sources et soumises à examen contradictoire.

12. Limites des détections automatisées

Reconnaissance faciale, analyse comportementale, détection d'IA, similarité ou autres systèmes automatisés peuvent produire des erreurs. Aucun signal automatisé ne doit, à lui seul, entraîner une conclusion définitive de fraude académique.

13. Dossier d'investigation

Le dossier peut réunir identité académique, inscription, session, présence, copies, versions, empreintes, journaux d'accès, déclarations, décisions et autres preuves autorisées. Les données non nécessaires doivent rester exclues.

14. Chaîne de preuve

Chaque élément d'investigation conserve son origine, sa date, son intégrité connue et les personnes ou systèmes qui l'ont fourni. Une capture d'écran ou une déclaration reste distinguée d'une donnée institutionnelle directement vérifiée.

15. Contradiction et droit de réponse

L’apprenant, l’enseignant, l’établissement ou un tiers concerné peut contester un élément. Les versions contradictoires doivent être conservées séparément afin que le processus de décision reste explicable.

16. Restriction préventive

En cas de risque sérieux, un établissement peut restreindre temporairement certaines opérations, par exemple l’émission ou le partage d’une preuve, selon ses règles. La restriction doit être attribuable, proportionnée, réexaminable et ne pas être confondue avec une sanction définitive.

17. Correction et réhabilitation

Lorsqu’une suspicion est levée ou une erreur corrigée, le statut actif doit refléter la résolution. L’ historique d’audit peut conserver l’existence de l’incident avec accès limité, sans maintenir publiquement une suspicion devenue infondée.

18. Protection des mineurs et données sensibles

Les investigations concernant des mineurs exigent une confidentialité renforcée. Dossiers disciplinaires, accusations, copies, données biométriques éventuelles et éléments comportementaux ne doivent pas être inscrits dans un registre public ou irréversible.

19. Audit et AP Ledger

Empreintes minimales d’émission, correction, révocation, restrictions institutionnelles ou décisions finales peuvent être ancrées dans AP Ledger lorsque cela est légitime. Les dossiers d’enquête complets et données disciplinaires restent hors des couches publiques.

20. Critères d’acceptation et conclusion

Le modèle est acceptable si l’absence de donnée n’est pas assimilée à un faux diplôme ; si un QR copié ne valide pas un document différent ; si comptes compromis et opérations suspectes sont révocables et auditables ; si les détections automatisées restent des signaux ; si le droit de réponse et la correction sont préservés ; et si les données disciplinaires restent privées. Deep Authenticity© transforme ainsi les anomalies éducatives en dossiers de preuve vérifiables plutôt qu’en accusations automatiques.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 15 — EDUCATION

CHAPITRE 5 — GOUVERNANCE DES ÉTABLISSEMENTS, ACCRÉDITATIONS, IDENTITÉ DES ENSEIGNANTS, CYBERSÉCURITÉ, CONFIDENTIALITÉ, INTEROPÉRABILITÉ, CONSERVATION, AUDIT ET AP LEDGER

1. Objet du chapitre

Ce chapitre définit la gouvernance institutionnelle et technique du Passeport Numérique Éducatif. Il organise l'identité des établissements et enseignants, les accréditations, les habilitations, la cybersécurité, la confidentialité, l'interopérabilité, la conservation des données, l'audit et AP Ledger.

2. Identité institutionnelle

Chaque école, université, centre de formation ou organisme certificateur dispose d'une identité distincte. Nom, statut, références institutionnelles et sources disponibles doivent être versionnés afin de préserver l'historique en cas de changement.

3. Accréditation

Une accréditation ou habilitation est une preuve émise par une autorité compétente. Authenticity Plus© peut en restituer l'émetteur, le périmètre, la période et le statut documenté sans devenir lui-même organisme d'accréditation.

4. Programme accrédité

L'accréditation d'un établissement ne signifie pas nécessairement que tous ses programmes disposent du même statut. Le passeport doit pouvoir relier une accréditation à l'établissement, au programme, au niveau et à la période réellement concernés.

5. Identité professionnelle de l'enseignant

Un enseignant ou agent habilité peut disposer d'une identité professionnelle reliée à un établissement pour une période donnée. Les données personnelles non nécessaires restent privées.

6. Habilitations

Enseigner, saisir une note, corriger une épreuve, valider un jury, émettre un certificat ou administrer un système sont des fonctions différentes. Les droits numériques doivent refléter cette séparation des responsabilités.

7. Changement d'établissement

Lorsqu'un enseignant change d'établissement ou de fonction, ses anciennes habilitations doivent pouvoir être clôturées sans effacer l'historique des actes qu'il a légitimement accomplis.

8. Gouvernance des émissions

L'émission de diplômes, certificats et attestations doit provenir de rôles habilités. Pour les opérations à fort impact, des validations multiples ou contrôles supplémentaires peuvent être prévus selon la gouvernance de l'établissement.

9. Cybersécurité des comptes

Comptes étudiants, enseignants et administrateurs présentent des niveaux de risque différents. Authentification renforcée, gestion des sessions, révocation, limitation des privilèges et détection d' activités anormales doivent protéger les fonctions sensibles.

10. Cybersécurité des systèmes

Systèmes d'information étudiants, plateformes d'apprentissage, outils d'examen, API et services de délivrance de diplômes doivent être intégrés selon des interfaces contrôlées. Une compromission d'un système source doit pouvoir être isolée et investiguée.

11. Confidentialité par défaut

Notes, absences, appréciations, besoins éducatifs, dossiers disciplinaires et autres données scolaires sont privées par défaut. Le Passeport Éducatif ne doit exposer publiquement que les informations explicitement prévues pour la vérification.

12. Protection des mineurs

Les données concernant les mineurs exigent une gouvernance renforcée : droits adaptés, représentation légale lorsqu'elle est requise, partage limité, durée de conservation proportionnée et absence de profilage public durable.

13. Interopérabilité

Le Passeport Éducatif peut échanger avec systèmes scolaires, universitaires, plateformes de formation, services de candidature et organismes certificateurs. Les échanges doivent préserver l' émetteur, le titulaire, la version, le statut et la provenance.

14. Portabilité internationale

Formats et métadonnées peuvent faciliter la présentation de preuves dans d'autres systèmes éducatifs. Cette portabilité technique ne doit pas être confondue avec une reconnaissance juridique ou académique automatique.

15. Conservation

Les durées de conservation diffèrent selon la nature des données. Un diplôme ou une preuve d'émission peut nécessiter une conservation longue, tandis que journaux techniques, données de session ou éléments disciplinaires peuvent relever d'autres règles.

16. Rectification et droits

Les mécanismes de rectification doivent permettre de corriger des données erronées tout en protégeant l'intégrité des preuves institutionnelles. Une demande de modification ne doit pas permettre de réécrire arbitrairement une décision académique officielle.

17. Continuité institutionnelle

Fusion, changement de nom, fermeture ou transformation d'un établissement ne doit pas rendre les anciennes preuves invérifiables. La gouvernance doit prévoir la continuité de vérification et la succession des autorités de conservation lorsque cela est possible.

18. Audit

Émissions, corrections, révocations, changements d'habilitation, consultations sensibles et opérations administratives critiques doivent être attribuables et horodatés. Les journaux doivent eux-mêmes être protégés contre les altérations non autorisées.

19. AP Ledger

AP Ledger peut ancrer des empreintes minimales d'identités institutionnelles, accréditations, diplômes et événements critiques. Les dossiers scolaires complets, notes, données de mineurs et informations disciplinaires restent hors des couches publiques ou irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si établissement, programme et accréditation restent distincts ; si les habilitations reflètent les rôles réels ; si les anciennes preuves survivent aux changements institutionnels ; si les mineurs et données scolaires restent protégés ; si l'interopérabilité préserve la provenance ; et si l'audit renforce l'intégrité sans créer un registre public de la vie scolaire. Cette gouvernance fournit le socle nécessaire à la clôture fonctionnelle de l'application Education.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 15 — EDUCATION

CHAPITRE 6 — SYNTHÈSE FONCTIONNELLE, CRITÈRES D'ACCEPTATION ET CLÔTURE DE L'APPLICATION EDUCATION

1. Objet du chapitre

Ce chapitre clôt le Point 15 — Education. Il consolide l'identité académique, les établissements, enseignants et apprenants, les cursus, diplômes, certificats et compétences, les examens et travaux, la vérification par QR Code dynamique, l'intégrité académique, la gouvernance, la cybersécurité, la confidentialité, l'interopérabilité, l'audit et AP Ledger.

2. Mission consolidée

Le Passeport Numérique Éducatif constitue une mémoire portable et vérifiable du parcours d'apprentissage. Il permet au titulaire de conserver et présenter des preuves provenant d'émetteurs identifiés, tout en laissant aux établissements et autorités compétentes leurs pouvoirs d'émission, d'évaluation, d'équivalence et de reconnaissance.

3. Identité académique

Identité civile, compte numérique, identifiants institutionnels et identité académique restent reliés mais distincts. La vérification doit confirmer la bonne personne sans rendre son dossier scolaire public.

4. Établissements et accréditations

Établissement, programme et accréditation sont trois objets distincts. Chaque accréditation conserve son autorité émettrice, son périmètre, sa période et son statut documenté.

5. Cursus et résultats

Inscription, programme, unités d'enseignement, évaluations, crédits, notes et décisions successives composent la chronologie académique. Une correction ou un recours produit une nouvelle étape sans effacer silencieusement la précédente.

6. Diplômes et certificats

Diplômes, certificats, attestations et micro-certifications restent reliés à leurs émetteurs et à leurs titulaires. Authenticity Plus© renforce leur vérifiabilité sans devenir l'autorité qui les délivre.

7. Compétences

Compétence déclarée, enseignée, évaluée et certifiée constituent des niveaux différents. Le Passeport Éducatif conserve cette distinction afin de ne pas transformer automatiquement la participation à une formation en certification de maîtrise.

8. QR Code dynamique

Un QR Code dynamique peut permettre à une université, un employeur ou un autre tiers autorisé de vérifier une preuve et son statut courant sans accéder à l'ensemble du dossier académique.

9. Anti-falsification

Une photocopie, un fichier modifié ou un QR copié ne doit pas suffire à reproduire un diplôme valide. Émetteur, référence, empreinte d'intégrité, titulaire, version et statut courant contribuent à la vérification.

10. Examens et présence

Identité du candidat, inscription à l'épreuve, présence, sujet, version et remise du travail sont des preuves distinctes. La présence à une session ne prouve pas automatiquement l'auteur de chaque réponse.

11. Travaux et versions

Devoirs, mémoires et projets peuvent recevoir une preuve de dépôt, une empreinte d'intégrité et une chronologie de versions. Une nouvelle remise ne doit pas effacer la précédente.

12. Intelligence artificielle et intégrité académique

L'usage de l'IA dépend des règles de l'établissement et de l'épreuve. Une déclaration d'usage, une autorisation ou une restriction peut être conservée, mais aucun détecteur automatisé ne doit produire à lui seul un verdict définitif de fraude.

13. Plagiat et similarité

Un taux de similarité n'est pas automatiquement un taux de plagiat. Les résultats automatisés constituent des signaux à interpréter avec les sources, citations, règles de l'épreuve et analyse humaine.

14. Fraudes et investigations

Faux diplôme présumé, usurpation, note falsifiée, compte compromis ou irrégularité d'examen peut ouvrir un dossier d'investigation. Les faits, preuves, déclarations contradictoires et décisions restent séparés et attribuables.

15. Corrections, révocations et recours

Correction, révocation, suspension, réhabilitation et recours sont des événements distincts provenant d'acteurs habilités. Le statut actif doit refléter la décision courante tout en préservant un audit approprié.

16. Reconnaissance et portabilité internationale

Le passeport facilite la transmission, la traduction et la compréhension des preuves entre systèmes et pays. La portabilité technique ne constitue jamais une garantie automatique d'équivalence ou de reconnaissance académique ou juridique.

17. Protection des mineurs

Pour les mineurs, confidentialité, minimisation, représentation légale lorsque requise, durée de conservation et contrôle des accès sont renforcés. Notes, difficultés scolaires, incidents et dossiers disciplinaires ne doivent pas devenir un profil public permanent.

18. Gouvernance, cybersécurité et continuité

Les habilitations reflètent les rôles réels des enseignants et administrateurs. Comptes, systèmes, API et opérations sensibles sont protégés par authentification, séparation des privilèges, révocation et audit. Fusion ou fermeture d'un établissement doit autant que possible préserver la vérifiabilité des preuves anciennes.

19. AP Ledger et critères d'acceptation

AP Ledger peut recevoir des empreintes minimales d'émission, correction, révocation, accréditation ou autres événements critiques. Le modèle est acceptable si le titulaire contrôle le partage, si les émetteurs conservent leur autorité, si les signaux automatisés ne deviennent pas des verdicts et si les données scolaires sensibles restent hors des couches publiques ou irréversibles.

20. Clôture du Point 15 — Education

Le Point 15 — Education est désormais fonctionnellement défini : identité académique, établissements, enseignants, inscriptions, cursus, résultats, diplômes, certificats, compétences, portfolio, QR Codes dynamiques, vérification par universités et employeurs, examens, travaux, IA, intégrité académique, faux diplômes, usurpation, investigations, accréditations, cybersécurité, confidentialité, interopérabilité, portabilité, audit et AP Ledger. Le Volume IV peut désormais poursuivre avec le Point 16 — Food.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 16 — FOOD

CHAPITRE 1 — IDENTITÉ ALIMENTAIRE, PRODUCTEUR, ORIGINE, LOTS, INGRÉDIENTS, TRANSFORMATION, CONDITIONNEMENT, DISTRIBUTION ET PASSEPORT NUMÉRIQUE FOOD

1. Objet du chapitre

Le Point 16 — Food transpose Authenticity Plus© / Deep Authenticity© à la chaîne alimentaire. Il relie produit, lot, ingrédients, producteurs, transformateurs, conditionnement, distribution et preuves disponibles afin de créer un Passeport Numérique Food vérifiable.

2. Mission sectorielle

La mission est de permettre de répondre à des questions simples : quel produit alimentaire est présenté, d'où provient-il, de quel lot relève-t-il, quels acteurs documentés sont intervenus et quelles preuves soutiennent son histoire ? AP complète les contrôles et systèmes officiels sans se substituer aux autorités sanitaires.

3. Identité du produit alimentaire

Un produit peut disposer d'une identité propre reliée à sa dénomination, marque, fabricant ou transformateur, catégorie, format et autres références disponibles. L'identité commerciale reste distincte de l'identité d'un lot précis.

4. Lot

Le lot constitue une unité essentielle de traçabilité. Numéro de lot, date de production, site, quantité et autres informations peuvent être reliés à la preuve source. Deux lots d'un même produit conservent des histoires distinctes.

5. Producteur primaire

Agriculteur, éleveur, pêcheur, coopérative ou autre producteur primaire peut être identifié comme source d'une matière première lorsque cette information est disponible et autorisée.

6. Origine

Pays, région, exploitation, zone de pêche ou autre origine peut être documentée avec sa source. Authenticity Plus© doit distinguer origine déclarée, origine vérifiée par un tiers et origine provenant d' une autorité ou certification.

7. Ingrédients

Le Passeport Food peut relier le produit fini à ses ingrédients et, lorsque possible, aux lots d’ ingrédients utilisés. Une recette commerciale confidentielle ne doit pas être rendue publique au-delà des obligations et consentements applicables.

8. Transformation

Nettoyage, découpe, cuisson, mélange, fermentation, raffinage, pasteurisation ou autre étape peut devenir un événement documenté. Chaque transformation relie les entrées aux sorties sans prétendre reconstruire une donnée absente.

9. Composition de lot

Lorsqu’un lot fini résulte de plusieurs lots de matières premières, la relation doit être conservée. Inversement, un lot de matière première peut alimenter plusieurs lots finis, ce qui facilite la traçabilité ascendante et descendante.

10. Conditionnement

Emballage primaire, secondaire ou logistique peut recevoir ses propres références. Date de conditionnement, site, ligne et identifiant de conditionnement peuvent contribuer à la traçabilité du lot.

11. Étiquetage

Dénomination, ingrédients, allergènes déclarés, quantité, dates et informations réglementaires restent reliés à la version de l’étiquette applicable au lot. Une modification d’étiquette ne doit pas réécrire rétroactivement les lots déjà distribués.

12. Dates

Date de production, conditionnement, durabilité minimale, limite de consommation ou autre date doivent conserver leur signification propre. Le système ne doit pas transformer automatiquement une date en conclusion générale sur la sécurité du produit.

13. Allergènes

Les allergènes déclarés constituent une information critique provenant du fabricant ou d’une source compétente. Toute modification ou alerte doit être versionnée et propagée selon les règles applicables.

14. Certifications et allégations

Bio, origine, qualité, commerce équitable, halal, casher ou autre certification ou allégation ne doit être affichée comme vérifiée que si une preuve et un émetteur identifiables la soutiennent. AP ne crée pas lui-même ces certifications.

15. Distribution

Grossiste, entrepôt, transporteur, distributeur, commerce ou restauration peuvent constituer des étapes successives. Les transferts documentés permettent de suivre le lot sans rendre publiques les informations commerciales confidentielles.

16. QR Code dynamique consommateur

Un QR Code dynamique sur le produit ou son emballage peut donner accès à une fiche Food adaptée au consommateur : identité, lot, origine documentée, ingrédients et allergènes publiables, certifications vérifiables, statut de rappel et autres informations autorisées.

17. QR Code professionnel

Les acteurs autorisés peuvent accéder à une vue plus détaillée : références de lots, chaîne de possession, documents, contrôles ou événements opérationnels. Les droits professionnels restent séparés de la vue consommateur.

18. Provenance et niveaux de preuve

Une donnée saisie par un producteur, confirmée par un laboratoire, issue d'un certificateur ou provenant d'une autorité ne possède pas le même niveau de preuve. Le Passeport Food doit préserver ces différences.

19. AP Ledger et confidentialité

Empreintes minimales d'identité de lot, transformations critiques, certificats ou événements importants peuvent être ancrées dans AP Ledger. Recettes confidentielles, contrats, volumes, prix, données personnelles et documents sensibles restent hors des couches publiques ou irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si produit et lot restent distincts ; si les ingrédients peuvent être reliés aux lots disponibles ; si origine déclarée et vérifiée ne sont pas confondues ; si les certifications restent attribuées à leurs émetteurs ; si le QR consommateur n'expose pas les secrets commerciaux ; et si la traçabilité peut fonctionner dans les deux sens. Le Passeport Numérique Food devient ainsi la mémoire vérifiable du parcours alimentaire, de l'origine documentée au produit présenté au consommateur.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 16 — FOOD

CHAPITRE 2 — TRAÇABILITÉ DE LA FERME À L'ASSIETTE, QR CODE DYNAMIQUE, CHAÎNE DU FROID, TRANSPORT, STOCKAGE, RESTAURATION, ONLINE/OFFLINE ET VÉRIFICATION CONSOMMATEUR

1. Objet du chapitre

Ce chapitre définit la continuité opérationnelle du Passeport Numérique Food depuis la production primaire jusqu'au consommateur. Il organise scans, transferts, chaîne du froid, transport, stockage, transformation, restauration, QR Code dynamique et fonctionnement Online/Offline.

2. Principe « de la ferme à l'assiette »

La traçabilité Food doit permettre de remonter du produit ou du plat vers les lots et acteurs documentés, et de descendre d'un lot de matière première vers les produits finis concernés. Les maillons absents restent explicitement inconnus.

3. Création du lot primaire

À la production, un lot peut recevoir un identifiant relié au producteur, au lieu ou à la zone documentée, à la date, à la quantité et aux preuves disponibles. Une déclaration du producteur reste distinguée d' une certification indépendante.

4. QR Code ou identifiant logistique

Lot, caisse, palette ou autre unité peut recevoir un QR Code ou identifiant relié au Passeport Food. Une copie visuelle du code ne doit pas suffire à reproduire le statut courant du lot.

5. Collecte et regroupement

Plusieurs lots peuvent être regroupés lors de collecte ou consolidation. Le système conserve les relations entre lots sources et unité regroupée afin de préserver la traçabilité ascendante.

6. Transport

Chaque transfert documenté peut relier expéditeur, transporteur, unité, heure, destination et preuves disponibles. La garde opérationnelle reste distincte de la propriété commerciale.

7. Chaîne du froid

Pour les produits thermosensibles, température et autres paramètres peuvent être associés au lot pendant transport et stockage. Les seuils doivent provenir d'une source identifiée et non être inventés par AP.

8. Excursion de température

Une excursion hors plage produit un événement documenté avec durée, amplitude et source disponibles. Elle déclenche une alerte ou une analyse mais ne constitue pas automatiquement un verdict de dangerosité.

9. Stockage

Entrepôt, chambre froide, plateforme ou commerce peut enregistrer réception, emplacement, conditions, sortie et transfert. Les événements restent attribuables aux acteurs ou systèmes qui les produisent.

10. Transformation intermédiaire

Lorsqu'une matière première est découpée, mélangée, cuite ou transformée, les lots d'entrée sont reliés aux lots de sortie. Cette généalogie permet de suivre l'impact potentiel d'une anomalie.

11. Distribution et commerce

Distributeur, magasin, marché ou plateforme peut recevoir et céder des lots. Le consommateur n'a pas besoin d'accéder aux contrats, prix d'achat ou données commerciales confidentielles pour vérifier l'identité du produit.

12. Restauration

Restaurant, cantine ou autre établissement peut relier certains ingrédients ou lots à une préparation lorsque le niveau de traçabilité disponible le permet. Le système ne doit pas prétendre connaître un lot précis si l'établissement ne l'a pas enregistré.

13. Plat et provenance

Un plat peut disposer d'une fiche de provenance documentant les ingrédients ou fournisseurs vérifiables. Cette fiche reste différente d'une certification sanitaire du plat et ne remplace pas les obligations de l'établissement.

14. QR Code consommateur

Le consommateur peut scanner un QR Code dynamique sur l'emballage, l'étiquette, le rayon ou un support autorisé afin d'accéder aux informations publiables du produit et au statut courant du lot.

15. Vérification Deep Authenticity©

Le scan peut confronter identifiant, lot, produit, version d'étiquette, statut de rappel, certification et contexte disponible. Une incohérence produit une information de vérification ou une alerte sans accusation automatique.

16. Online

En mode connecté, l'application consulte le statut courant : lot actif, rappel éventuel, informations publiables, certifications et dernières mises à jour autorisées.

17. Offline sécurisé

En absence de réseau, l'application peut utiliser des données signées et mises en cache avec date de dernière synchronisation. Elle doit indiquer clairement qu'il s'agit d'une vérification hors ligne et ne pas présenter comme temps réel un statut ancien.

18. Resynchronisation

Au retour du réseau, le statut est actualisé et les événements Offline sont réconciliés. Un rappel ou changement intervenu pendant la coupure doit remplacer l'ancien état dès que la synchronisation réussit.

19. Confidentialité et AP Ledger

Les événements critiques peuvent produire des empreintes minimales dans AP Ledger. Positions détaillées, recettes, prix, volumes, contrats et données personnelles restent protégés. La vue consommateur applique la minimisation.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si la traçabilité fonctionne dans les deux sens ; si les regroupements conservent les lots sources ; si la chaîne du froid documente sans rendre de verdict automatique ; si le restaurant n'affirme que ce qu'il peut sourcer ; si le QR dynamique donne le statut courant ; et si l' Offline affiche sa fraîcheur. Deep Authenticity© relie ainsi la chaîne alimentaire physique à une continuité numérique vérifiable de la production à la consommation.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 16 — FOOD

CHAPITRE 3 — SÉCURITÉ ALIMENTAIRE, ANALYSES DE LABORATOIRE, CONTAMINANTS, ALLERGÈNES, CHAÎNE DU FROID, DATES, CONTRÔLES SANITAIRES, CERTIFICATIONS ET PREUVES DE CONFORMITÉ

1. Objet du chapitre

Ce chapitre définit la couche de preuve relative à la sécurité et à la conformité alimentaires. Il relie analyses de laboratoire, contaminants recherchés, allergènes, conditions de conservation, dates, contrôles sanitaires, certifications et décisions provenant des acteurs compétents.

2. Principe de prudence

Authenticity Plus© / Deep Authenticity© organise et vérifie la provenance des preuves ; il ne remplace ni le laboratoire, ni le professionnel compétent, ni l'autorité sanitaire. Une donnée technique ou une alerte ne doit pas être transformée automatiquement en diagnostic de sécurité alimentaire.

3. Identité de l'échantillon

Toute analyse doit rester reliée à un échantillon identifié, lui-même associé lorsque possible au produit, au lot, au lieu, à la date et à la méthode de prélèvement. Une analyse d'un échantillon ne doit pas être étendue sans justification à des lots différents.

4. Laboratoire

Le laboratoire conserve son identité, son rôle, ses références et, lorsqu'elles sont disponibles, ses accréditations pertinentes. AP ne déduit pas une compétence analytique simplement du nom d'un laboratoire.

5. Rapport d'analyse

Le rapport peut être relié à l'échantillon, à la méthode, à la date, aux résultats et à la version du document. Une empreinte d'intégrité permet de détecter une modification du fichier de référence.

6. Contaminants

Micro-organismes, résidus, substances chimiques, corps étrangers ou autres contaminants peuvent faire l'objet de recherches selon le produit et le contexte. Le Passeport Food conserve ce qui a réellement été analysé plutôt que d'affirmer que tout contaminant possible a été exclu.

7. Résultat négatif

Un résultat indiquant qu'un élément n'a pas été détecté doit rester lié à la méthode, à la limite analytique et à l'échantillon concernés. Il ne constitue pas une garantie absolue d'absence dans toute la production.

8. Seuils et références

Lorsqu'un résultat est comparé à une limite ou spécification, la référence utilisée doit être identifiée : réglementation applicable, cahier des charges, norme, exigence contractuelle ou autre source compétente.

9. Allergènes déclarés

Les allergènes présents ou susceptibles d'être présents selon les informations du fabricant doivent être accessibles dans la vue consommateur lorsque cela est applicable. La source et la version de l' information restent conservées.

10. Changement de recette ou d'allergène

Une modification de formulation, de fournisseur ou de risque de contamination croisée peut modifier l' information allergène. Les versions doivent être rattachées aux lots concernés afin d'éviter qu'une nouvelle étiquette réécrive l'historique.

11. Chaîne du froid

Température, durée, capteurs et excursions éventuelles peuvent compléter la preuve sanitaire. Les mesures restent des observations techniques ; la décision d'accepter, bloquer ou retirer un lot relève des règles et acteurs compétents.

12. Dates alimentaires

Date de production, conditionnement, durabilité minimale et limite de consommation doivent être distinguées. Le Passeport Food restitue leur nature et leur source sans inventer une prolongation ou réduction de durée de vie.

13. Contrôle sanitaire

Inspection, prélèvement, contrôle documentaire ou autre intervention officielle peut être référencé avec l'autorité, la date et le statut disponibles. AP ne transforme pas l'absence de contrôle enregistré en non-conformité.

14. Non-conformité documentée

Lorsqu'un laboratoire, un fabricant ou une autorité compétente documente une non-conformité, le lot peut recevoir un statut adapté et déclencher les procédures prévues. Source, portée et date de la décision doivent être conservées.

15. Certification

Certification biologique, qualité, origine ou autre schéma peut être reliée au produit ou à l'acteur. Organisme certificateur, périmètre, période et statut sont nécessaires pour éviter qu'un logo seul soit traité comme une preuve suffisante.

16. Preuve de conformité

Une preuve de conformité peut provenir d'un rapport, d'un certificat, d'une déclaration réglementaire ou d'un contrôle officiel. Ces preuves conservent des niveaux d'autorité différents et ne doivent pas être fusionnées en un statut opaque.

17. QR Code et consommateur

Le QR dynamique peut afficher les informations de sécurité publiables : allergènes, statut de rappel, certifications vérifiables et éventuellement références de contrôles ou analyses lorsque leur publication est appropriée. Les rapports techniques complets restent protégés si nécessaire.

18. Mise à jour et propagation

Une nouvelle analyse, correction d'étiquette ou décision officielle doit être propagée aux vues concernées. Les anciennes informations restent historisées pour les lots auxquels elles s'appliquaient.

19. AP Ledger et confidentialité

Empreintes minimales de rapports, certificats, décisions de non-conformité ou changements critiques peuvent être ancrées dans AP Ledger. Données de laboratoire détaillées, secrets industriels, dossiers d'inspection complets et informations personnelles restent protégés.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si l'analyse reste liée à son échantillon ; si un résultat négatif n'est pas présenté comme garantie absolue ; si les seuils sont sourcés ; si allergènes et versions de recette sont reliés aux bons lots ; si les contrôles restent attribués aux autorités compétentes ; et si le QR consommateur privilégie une information claire sans exposer les données techniques sensibles. Deep Authenticity© renforce ainsi la confiance alimentaire par la provenance vérifiable des preuves de sécurité et de conformité.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 16 — FOOD

CHAPITRE 4 — CONTAMINATION, FRAUDE ALIMENTAIRE, SUBSTITUTION, FAUSSE ORIGINE, FAUX LABELS, QR CLONÉS, RAPPELS DE LOTS, RETRAIT DU MARCHÉ, ALERTES CONSOMMATEURS ET INVESTIGATION

1. Objet du chapitre

Ce chapitre organise la détection et le traitement des anomalies graves de la chaîne Food : contamination documentée ou suspectée, fraude alimentaire présumée, substitution, fausse origine, faux labels, QR Codes clonés, rappels de lots, retraits du marché et investigations. L'objectif est de réduire le temps entre détection, identification des lots concernés et information des acteurs autorisés.

2. Principe de non-accusation automatique

Une incohérence de lot, d'origine, d'étiquette, de composition ou de QR Code constitue un signal à examiner. Authenticity Plus© / Deep Authenticity© conserve les faits et leurs sources ; la qualification de fraude, les sanctions et les responsabilités restent du ressort des acteurs et autorités compétents.

3. Contamination suspectée

Un signal de laboratoire, une alerte sanitaire, une plainte documentée ou une anomalie de processus peut conduire à placer un lot sous vérification. Le statut doit distinguer suspicion, analyse en cours et contamination confirmée par une source compétente.

4. Contamination confirmée

Lorsqu'une autorité, un laboratoire habilité ou un acteur compétent confirme une non-conformité selon le cadre applicable, le Passeport Food peut relier la décision aux lots concernés, aux preuves, à la date et à la portée documentée.

5. Traçabilité ascendante

À partir d'un produit ou lot concerné, le système doit permettre de remonter vers les ingrédients, lots sources, producteurs, fournisseurs et transformations documentés. Les maillons inconnus restent explicitement inconnus.

6. Traçabilité descendante

À partir d'un ingrédient ou lot source, le système doit identifier les lots finis, expéditions, distributeurs ou autres destinations documentées susceptibles d'être concernés. Cette fonction réduit le périmètre d'un rappel lorsque les données le permettent.

7. Substitution alimentaire

Un ingrédient, une espèce, une qualité ou une matière première différente de celle déclarée peut produire une alerte de substitution présumée lorsqu'une preuve fiable révèle l'incohérence. Le système conserve l'observation sans attribuer automatiquement l'intention.

8. Fausse origine

Une origine affichée qui ne correspond pas aux preuves disponibles peut être signalée comme incohérente. Origine déclarée, certification d'origine et résultat d'une investigation restent des niveaux de preuve distincts.

9. Faux labels et certifications

Un logo ou une mention de certification ne doit pas suffire à établir sa validité. Organisme émetteur, périmètre, période, produit ou lot concerné et statut doivent être vérifiables lorsque la certification est présentée comme telle.

10. Falsification d'étiquette

Modification d'ingrédients, allergènes, dates, lot, origine ou autres informations peut être détectée par comparaison avec la version de référence du lot. Une différence peut également provenir d'une correction légitime et doit être investiguée.

11. QR Code cloné

La copie du QR Code d'un produit légitime sur un produit différent ne doit pas reproduire son authenticité. Deep Authenticity© peut confronter identifiant, lot, produit, version d'étiquette, lieu, séquence de scans et statut courant afin de détecter des usages incompatibles.

12. Signalement consommateur

Le consommateur peut signaler une incohérence, un emballage suspect ou autre problème depuis la fiche Food, sans que son signalement devienne automatiquement une preuve de fraude. Les informations personnelles du déclarant restent protégées.

13. Mise en quarantaine

Un fabricant, distributeur ou acteur habilité peut bloquer temporairement un lot dans son périmètre pendant une vérification. La quarantaine est distincte d'un rappel officiel et doit conserver son auteur, son motif, sa date et son statut.

14. Rappel de lot

Lorsqu'un rappel est décidé par l'acteur ou l'autorité compétente, le Passeport Food doit permettre d'identifier précisément les lots concernés, la portée, la date et les instructions officielles associées. AP ne crée pas lui-même un rappel sanitaire.

15. Retrait du marché

Le retrait des points de vente ou circuits professionnels peut être suivi comme une série d'événements : notification, localisation des stocks documentés, blocage, collecte, retour, destruction ou autre destination autorisée.

16. Alerte consommateur

Le scan d'un QR dynamique appartenant à un lot faisant l'objet d'un rappel documenté doit afficher prioritairement une alerte claire et le statut courant. Les instructions doivent provenir de la source compétente et ne pas être improvisées par AP.

17. Offline et rappels

En mode Offline, une information de rappel mise en cache peut être affichée avec sa date de dernière synchronisation. L'absence de rappel dans un cache ancien ne doit jamais être présentée comme une garantie de statut actuel ; la reconnexion doit actualiser la fiche en priorité.

18. Dossier d'investigation

Le dossier peut réunir généalogie des lots, scans, étiquettes, certificats, analyses, capteurs, transferts, signalements et décisions. Chaque élément conserve son origine, sa date et son niveau de preuve afin de reconstruire la chronologie.

19. AP Ledger, audit et confidentialité

Empreintes minimales des rappels, restrictions, décisions critiques et preuves essentielles peuvent être ancrées dans AP Ledger. Dossiers complets d'enquête, données commerciales, recettes, positions détaillées et informations personnelles restent protégés.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si suspicion et contamination confirmée restent distinctes ; si la traçabilité fonctionne en amont et en aval ; si substitution, fausse origine et faux labels restent investigables ; si un QR cloné ne reproduit pas le statut légitime ; si un rappel documenté est propagé rapidement au consommateur ; si l'Offline expose la fraîcheur de l'information ; et si AP ne se substitue jamais à l'autorité sanitaire. Deep Authenticity© transforme ainsi une alerte alimentaire en chaîne de preuve et d'action traçable.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 16 — FOOD

CHAPITRE 5 — PRODUCTEURS, TRANSFORMATEURS, RESTAURANTS, AUTORITÉS SANITAIRES, LABORATOIRES, CERTIFICATIONS, GOUVERNANCE, CYBERSÉCURITÉ, CONFIDENTIALITÉ, INTEROPÉRABILITÉ, AUDIT ET AP LEDGER

1. Objet du chapitre

Ce chapitre définit la gouvernance institutionnelle et technique du Passeport Numérique Food. Il organise les rôles des producteurs, transformateurs, distributeurs, restaurants, laboratoires, certificateurs et autorités, ainsi que les habilitations, la cybersécurité, la confidentialité, l'interopérabilité, l'audit et AP Ledger.

2. Identité des acteurs

Chaque acteur professionnel dispose d'une identité distincte reliée, lorsque disponible, à ses références officielles et à ses sites d'activité. L'identité d'une entreprise, d'un établissement, d'un site et d'un utilisateur professionnel ne doit pas être confondue.

3. Producteur primaire

Le producteur peut créer ou documenter des lots de matières premières et leur origine déclarée. Les certifications, contrôles et validations provenant de tiers restent attribués à ces tiers.

4. Transformateur

Le transformateur relie les lots entrants aux lots sortants, documente les étapes pertinentes, le conditionnement et les versions d'étiquetage. Les recettes et paramètres industriels confidentiels restent protégés.

5. Distributeur et commerce

Les acteurs de distribution peuvent documenter réception, stockage, transfert, mise en rayon, blocage et retrait. Ils ne doivent pas pouvoir modifier rétroactivement l'identité ou l'origine émises par les acteurs amont sans événement de correction attribuable.

6. Restaurant et restauration collective

Le restaurant ou la cantine peut publier les informations qu'il est réellement capable de sourcer : fournisseurs, ingrédients, allergènes, certifications ou lots lorsque disponibles. L'absence de granularité doit être indiquée plutôt que comblée artificiellement.

7. Laboratoire

Le laboratoire transmet ou atteste des résultats reliés à des échantillons identifiés. Méthode, date, rapport et statut d'accréditation disponible restent attachés à la preuve afin d'éviter qu'un résultat soit sorti de son contexte.

8. Organisme certificateur

Le certificateur conserve l'autorité sur la certification qu'il émet. Produit, site, acteur, périmètre, période et statut doivent être explicitement reliés afin qu'un logo seul ne serve pas de preuve.

9. Autorité sanitaire

Une autorité compétente peut être source d'inspections, alertes, décisions, rappels ou autres statuts officiels. Authenticity Plus© les restitue et les propage selon les droits et interfaces disponibles sans créer lui-même une décision sanitaire.

10. Séparation des rôles

Créer un lot, modifier une fiche, publier une étiquette, joindre un rapport, déclarer un rappel ou administrer les droits sont des opérations différentes. Les habilitations doivent appliquer le principe du moindre privilège.

11. Gouvernance des corrections

Toute correction d'origine, lot, ingrédient, allergène, date, certificat ou autre donnée critique doit conserver son auteur, sa justification, sa date et sa version. Les corrections légitimes ne doivent pas devenir des réécritures silencieuses.

12. Cybersécurité des comptes

Comptes professionnels et administrateurs doivent être protégés par des mécanismes adaptés au niveau de risque : authentification renforcée, gestion des sessions, révocation, séparation des privilèges et journalisation.

13. Terminaux, QR et IoT

Terminaux de scan, imprimantes d'étiquettes, passerelles IoT et capteurs peuvent devenir des points d'attaque. Leur identité, association, révocation et historique doivent être gérés afin de limiter faux scans, faux lots ou données injectées.

14. API et systèmes externes

ERP, WMS, TMS, systèmes de laboratoire, plateformes de certification et systèmes officiels peuvent échanger avec AP. Chaque donnée importée conserve sa source, son horodatage, son unité et son statut afin d'éviter une fusion opaque.

15. Confidentialité commerciale

Recettes, volumes, prix, contrats, marges, fournisseurs confidentiels et paramètres industriels ne sont pas destinés à la vue consommateur. La transparence alimentaire doit être conciliée avec la protection légitime des secrets commerciaux.

16. Données personnelles

Coordonnées individuelles, comptes utilisateurs, signalements consommateurs et autres données personnelles sont minimisés et protégés. Le Passeport Food porte principalement sur les produits, lots, acteurs professionnels et preuves nécessaires.

17. Interopérabilité et standards

L'interopérabilité doit permettre de relier identifiants de produits, lots, unités logistiques, certificats, rapports et événements provenant de systèmes différents. Les mappings doivent préserver le sens des données et leur provenance.

18. Continuité et résilience

Une panne, une perte de réseau ou l'indisponibilité temporaire d'un partenaire ne doit pas conduire à inventer un statut. Les mécanismes Offline, files d'attente, reprises et réconciliations doivent conserver la fraîcheur et les conflits éventuels.

19. Audit et AP Ledger

Créations de lots, transformations critiques, corrections, certifications, rapports, restrictions et rappels peuvent produire des traces d'audit et des empreintes minimales dans AP Ledger. Les contenus sensibles complets restent hors des couches publiques ou irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si chaque acteur reste limité à son rôle ; si laboratoire, certificateur et autorité conservent leur propre autorité ; si les corrections sont versionnées ; si les secrets commerciaux restent protégés ; si l'interopérabilité conserve la provenance ; et si la cybersécurité couvre comptes, terminaux, IoT et API. Cette gouvernance fournit le socle nécessaire à la clôture fonctionnelle de l'application Food.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 16 — FOOD

CHAPITRE 6 — SYNTHÈSE FONCTIONNELLE, CRITÈRES D'ACCEPTATION ET CLÔTURE DE L'APPLICATION FOOD

1. Objet du chapitre

Ce chapitre clôt le Point 16 — Food. Il consolide l'identité alimentaire, les lots, producteurs, ingrédients, transformations, conditionnements, distribution, traçabilité de la ferme à l'assiette, chaîne du froid, sécurité alimentaire, analyses, rappels, gouvernance, cybersécurité, interopérabilité et AP Ledger.

2. Mission consolidée

Le Passeport Numérique Food constitue la mémoire vérifiable d'un produit ou d'un lot alimentaire. Il relie les preuves disponibles depuis l'origine documentée jusqu'au consommateur, sans se substituer aux producteurs, laboratoires, certificateurs, professionnels ou autorités sanitaires.

3. Produit et lot

L'identité commerciale du produit reste distincte du lot physique. Chaque lot conserve sa propre chronologie, ses ingrédients documentés, ses transformations, ses contrôles et ses destinations.

4. Origine et producteurs

Origine déclarée, origine vérifiée et certification d'origine restent distinguées. Producteurs, exploitations, zones ou autres sources sont reliés uniquement lorsque des données et preuves appropriées existent.

5. Ingrédients et généalogie

Les lots d'ingrédients peuvent être reliés aux lots finis. La traçabilité doit fonctionner en amont pour retrouver les sources et en aval pour identifier les produits ou destinations potentiellement concernés.

6. Transformation et conditionnement

Chaque transformation relie entrées et sorties. Conditionnement, version d'étiquette, dates, ingrédients et allergènes applicables restent rattachés aux lots correspondants sans réécriture rétroactive.

7. QR Code dynamique consommateur

Le QR dynamique fournit une vue claire et minimisée : produit, lot, origine documentée, ingrédients et allergènes publiables, certifications vérifiables, statut de rappel et autres informations autorisées.

8. QR professionnel

Les acteurs habilités disposent d'une vue plus riche comprenant généalogie des lots, documents, transferts, analyses, contrôles et événements opérationnels. Les secrets commerciaux restent protégés.

9. De la ferme à l'assiette

Collecte, regroupement, transport, stockage, transformation, distribution, commerce et restauration peuvent former une chaîne continue. Les étapes non documentées restent explicitement inconnues.

10. Chaîne du froid

Température et autres mesures IoT peuvent documenter les conditions subies par un lot. Une excursion constitue une observation et une alerte, non un verdict automatique sur la sécurité ou la qualité.

11. Analyses de laboratoire

Chaque résultat reste relié à l'échantillon, à la méthode, au laboratoire et aux limites analytiques. « Non détecté » ne signifie pas absence absolue dans l'ensemble de la production.

12. Allergènes et sécurité

Les informations allergènes et leurs versions sont rattachées aux lots concernés. Une modification de recette, fournisseur ou risque documenté doit être propagée sans modifier rétroactivement les anciennes versions.

13. Certifications et contrôles

Laboratoire, organisme certificateur et autorité sanitaire conservent chacun leur propre autorité. Authenticity Plus© / Deep Authenticity© vérifie la provenance des preuves sans créer lui-même certification ou décision sanitaire.

14. Fraude et anomalies

Substitution, fausse origine, faux label, étiquette falsifiée ou QR cloné produit un signal investigable. L' incohérence n'est jamais automatiquement transformée en accusation de fraude.

15. Rappels et retraits

Quarantaine, rappel officiel, retrait du marché et résolution sont des statuts distincts. Un rappel documenté doit être propagé rapidement aux acteurs concernés et devenir prioritaire lors d'un scan consommateur.

16. Online et Offline

Online permet la consultation du statut courant. Offline sécurisé affiche des données signées ou mises en cache avec leur date de dernière synchronisation ; un ancien cache ne doit jamais être présenté comme garantie d'absence de rappel actuel.

17. Gouvernance et confidentialité

Producteur, transformateur, distributeur, restaurant, laboratoire, certificateur et autorité disposent de droits distincts. Recettes, prix, volumes, contrats, données personnelles et informations industrielles sensibles restent protégés.

18. Cybersécurité et interopérabilité

Comptes, terminaux, imprimantes d'étiquettes, QR, IoT, API, ERP, WMS, TMS et systèmes de laboratoire doivent préserver identité, provenance, horodatage et révocabilité. Les conflits de synchronisation restent visibles et auditables.

19. AP Ledger et critères d'acceptation

AP Ledger peut ancrer des empreintes minimales de lots, transformations critiques, certificats, rapports, restrictions et rappels. Le modèle est acceptable si la traçabilité est bidirectionnelle, si les niveaux de preuve restent distincts, si le QR expose le statut courant et si les données sensibles restent hors des couches publiques ou irréversibles.

20. Clôture du Point 16 — Food

Le Point 16 — Food est désormais fonctionnellement défini : identité alimentaire, producteurs, origines, lots, ingrédients, transformations, conditionnement, distribution, QR Codes dynamiques, ferme à l' assiette, chaîne du froid, Online/Offline, analyses, allergènes, contrôles, certifications, contamination, fraude présumée, rappels, retraits, gouvernance, cybersécurité, interopérabilité, audit et AP Ledger. Le Volume IV peut désormais poursuivre avec le Point 17 — Art et Culture.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 17 — ART ET CULTURE

CHAPITRE 1 — IDENTITÉ DE L'ŒUVRE, ARTISTE, CRÉATEUR, PROVENANCE, CERTIFICAT D' AUTHENTICITÉ, QR CODE DYNAMIQUE ET PASSEPORT NUMÉRIQUE ART&CULTURE

1. Objet du chapitre

Le Point 17 — Art et Culture transpose Authenticity Plus© / Deep Authenticity© aux œuvres d'art, objets culturels et créations patrimoniales. Il établit un Passeport Numérique Art&Culture reliant l'objet physique ou numérique à son identité, sa provenance documentée, ses créateurs, ses certificats et son historique.

2. Mission sectorielle

La mission est de rendre vérifiable ce qui peut l'être : identité de l'œuvre, auteur ou attribution, provenance, expositions, restaurations, transferts documentés et certificats. AP ne se substitue ni à l' artiste, ni à l'expert, ni au musée, ni aux autorités patrimoniales.

3. Identité de l'œuvre

Une œuvre reçoit une identité distincte comportant, selon les données disponibles, titre, type, technique, dimensions, date ou période, signature, numéro d'inventaire, édition et caractéristiques descriptives. Les champs inconnus restent inconnus.

4. Artiste ou créateur

L'identité du créateur peut être reliée à l'œuvre avec son niveau de preuve. Œuvre signée, attribuée, atelier de, école de ou auteur inconnu ne doivent pas être confondus.

5. Attribution

Une attribution est une opinion ou conclusion provenant d'une source identifiée et peut évoluer avec la recherche. Une nouvelle attribution ne doit pas effacer les attributions historiques ; chaque version conserve auteur, date et justification disponible.

6. Œuvre unique et édition

Une œuvre unique, un multiple, une photographie, une sculpture éditée ou une estampe nécessitent des modèles distincts. Numéro d'exemplaire, taille d'édition, épreuves et variantes peuvent être reliés au passeport.

7. Photographies de référence

Des photographies de l'œuvre, de la signature, du revers, du cadre, des marques, étiquettes et détails peuvent constituer une empreinte visuelle de référence. Elles documentent l'état observé à une date donnée sans constituer seules une expertise d'authenticité.

8. Provenance

La provenance est une chronologie de détenteurs, collections, galeries, ventes, donations, successions ou autres événements documentés. Une période sans preuve doit être représentée comme lacune plutôt que reconstruite artificiellement.

9. Propriété, garde et exposition

Propriété juridique, possession physique, dépôt, prêt et exposition sont des relations distinctes. Une œuvre prêtée à un musée ne change pas nécessairement de propriétaire.

10. Certificat d'authenticité

Un certificat peut être relié à l'œuvre avec son émetteur, sa date, sa référence, son contenu et son statut. Authenticity Plus© vérifie la provenance et l'intégrité du certificat mais ne transforme pas un certificat contesté en vérité absolue.

11. Experts et comités

Expert, fondation, comité d'artiste, ayant droit ou institution peut produire une opinion ou une attestation. Chaque source conserve son identité et son périmètre d'autorité.

12. QR Code dynamique

Un QR Code dynamique peut être associé à l'œuvre, son cadre, son socle ou son dossier. Le scan ouvre le Passeport Art&Culture et son statut courant ; la simple copie visuelle du QR ne doit pas suffire à reproduire l'authenticité.

13. Deep Authenticity©

Deep Authenticity© peut confronter QR, caractéristiques visuelles documentées, dimensions, marques, provenance, certificats, historique de scans et autres preuves disponibles. Il fournit une cohérence de preuve, non une expertise artistique automatique.

14. Vue publique et vue professionnelle

La vue publique peut présenter identité, artiste, provenance publiable, expositions et certificats autorisés. Conservateurs, experts, assureurs ou propriétaires peuvent disposer de vues plus détaillées selon leurs droits.

15. Œuvres numériques

Une œuvre numérique peut être reliée à son fichier de référence, à une empreinte cryptographique, au créateur, à l'édition et aux droits documentés. La possession d'un fichier ou d'un jeton numérique ne doit pas être confondue automatiquement avec la propriété des droits d'auteur.

16. Droits d’auteur

Auteur, propriétaire de l’objet matériel et titulaire des droits d’exploitation peuvent être différents. Le Passeport doit conserver cette séparation et ne pas déduire une licence à partir d’un simple transfert de propriété.

17. Collections et institutions

Musées, fondations, archives, galeries et collections peuvent relier leurs numéros d’inventaire et dossiers aux passeports des œuvres. Les informations sensibles de sécurité ou de localisation ne doivent pas être exposées publiquement.

18. Corrections et nouvelles recherches

Découverte documentaire, expertise nouvelle, restauration ou correction d’inventaire peut enrichir le passeport. Les nouvelles informations sont versionnées avec leur source sans réécrire silencieusement l’historique.

19. AP Ledger et confidentialité

Empreintes minimales d’identité, certificats, transferts documentés, expertises ou restaurations peuvent être ancrées dans AP Ledger. Identité privée des propriétaires, valeurs assurées, localisations précises, dispositifs de sécurité et documents confidentiels restent protégés.

20. Critères d’acceptation et conclusion

Le modèle est acceptable si œuvre, artiste, propriétaire et droits d’auteur restent distincts ; si l’ attribution conserve son niveau de preuve ; si les lacunes de provenance restent visibles ; si le QR copié ne reproduit pas l’authenticité ; si les opinions d’experts restent attribuées ; et si les données sensibles des collections sont protégées. Le Passeport Numérique Art&Culture devient ainsi une mémoire vérifiable de l’œuvre sans prétendre remplacer l’expertise humaine.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 17 — ART ET CULTURE

CHAPITRE 2 — PROVENANCE HISTORIQUE, VENTES, GALERIES, MAISONS DE VENTE, MUSÉES, PRÊTS, EXPOSITIONS, TRANSPORT, RESTAURATION ET CHAÎNE DE POSSESSION DE L'ŒUVRE

1. Objet du chapitre

Ce chapitre définit la chronologie opérationnelle et documentaire d'une œuvre : provenance historique, transactions documentées, galeries, maisons de vente, musées, prêts, expositions, transport, stockage, restauration et transferts de garde.

2. Principe de provenance

La provenance est une chaîne de faits documentés et de périodes de connaissance variable. Authenticity Plus© / Deep Authenticity© distingue événement confirmé, information déclarée, attribution documentaire et lacune de provenance.

3. Provenance historique

Archives, inventaires, catalogues, correspondances, photographies, factures, publications et autres sources peuvent documenter une étape historique. Chaque source conserve son auteur, sa date, sa référence et son niveau de confiance.

4. Lacunes de provenance

Une période sans documentation suffisante doit rester visible comme lacune. Le système ne complète jamais automatiquement un propriétaire, un lieu ou une transaction manquante.

5. Vente documentée

Une vente peut relier vendeur, acquéreur lorsque publiable, intermédiaire, date, œuvre et documents associés. Le prix et l'identité des parties peuvent rester confidentiels selon les droits applicables.

6. Galerie

Une galerie peut être propriétaire, dépositaire, mandataire ou intermédiaire. Son rôle exact doit être enregistré pour éviter de confondre exposition, représentation commerciale et propriété.

7. Maison de vente

Une maison de vente peut documenter lot de vente, catalogue, description, estimation, adjudication et autres informations autorisées. La description du catalogue reste attribuée à son émetteur et peut évoluer avec les recherches.

8. Invendu, retrait ou annulation

Mise en vente, adjudication, invendu, retrait et annulation sont des événements distincts. Une œuvre présentée aux enchères n'est pas automatiquement considérée comme vendue.

9. Musée et institution

Entrée en collection, dépôt, prêt, exposition temporaire ou étude scientifique sont des statuts distincts. L'institution conserve son numéro d'inventaire et ses propres dossiers.

10. Prêt d'œuvre

Un prêt relie prêteur, emprunteur, période, objet et conditions documentées. Le transfert temporaire de garde ne modifie pas automatiquement la propriété.

11. Exposition

Titre de l'exposition, institution, lieu, dates et référence de catalogue peuvent rejoindre le passeport. Une exposition documentée enrichit la provenance mais ne constitue pas, à elle seule, une certification d'authenticité.

12. Transport

Départ, transporteur spécialisé, emballage, arrivée et réception peuvent être documentés. Les informations de trajet et de localisation précises restent protégées afin de ne pas créer de risque de sécurité.

13. Constat d'état

Avant ou après transport, prêt ou exposition, un constat d'état peut documenter l'état observable de l'œuvre. Il doit rester relié à son auteur, sa date, ses photographies et son contexte.

14. Restauration

Nettoyage, consolidation, retouche, remplacement de cadre ou autre intervention peut être enregistré avec restaurateur, date, méthode et documents disponibles. La restauration fait partie de l'histoire matérielle de l'œuvre.

15. Modification matérielle

Une intervention susceptible de modifier dimensions, support, surface, signature, montage ou composants doit être versionnée avec précision. Le passeport doit permettre de comparer l'état avant et après.

16. Chaîne de possession

Propriétaire, dépositaire, transporteur, musée, galerie et restaurateur peuvent successivement avoir la garde physique de l'œuvre. Chaque transfert de garde doit être distinct du transfert juridique de propriété.

17. QR Code dynamique et vérification

Le QR dynamique permet aux acteurs habilités de consulter l'identité et le statut courant de l'œuvre lors d'un transfert, prêt ou réception. Deep Authenticity© peut comparer le contexte du scan aux preuves et caractéristiques disponibles.

18. Offline sécurisé

Dans un lieu sans réseau, une preuve signée et limitée dans le temps peut permettre une vérification Offline. La date de dernière synchronisation et les limites du statut hors ligne doivent être clairement affichées.

19. AP Ledger et confidentialité

Empreintes minimales de transferts, prêts, constats d'état, restaurations ou événements critiques peuvent être ancrées dans AP Ledger. Prix, propriétaires privés, itinéraires, localisations, valeurs assurées et dispositifs de sécurité restent protégés.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si les lacunes historiques restent visibles ; si galerie, maison de vente et musée conservent leurs rôles réels ; si prêt, garde et propriété ne sont pas confondus ; si les restaurations sont historisées ; si le transport n'expose pas les données de sécurité ; et si le QR dynamique accompagne l'œuvre sans remplacer l'expertise. Le Passeport Art&Culture devient ainsi une continuité documentaire et matérielle de l'œuvre dans le temps.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 17 — ART ET CULTURE

CHAPITRE 3 — EXPERTISE, ANALYSES SCIENTIFIQUES, IMAGERIE, SIGNATURE, MATÉRIAUX, DATATION, ÉTAT DE CONSERVATION, RESTAURATION ET NIVEAUX DE PREUVE D'AUTHENTICITÉ

1. Objet du chapitre

Ce chapitre organise les preuves techniques et expertes pouvant contribuer à l'étude d'une œuvre : expertise humaine, analyses scientifiques, imagerie, signature, matériaux, datation, état de conservation et restauration. Deep Authenticity© consolide ces éléments sans produire seul un verdict d'authenticité.

2. Principe de convergence des preuves

L'authenticité d'une œuvre peut dépendre d'un faisceau d'indices historiques, stylistiques, matériels, scientifiques et documentaires. Aucun indicateur isolé ne doit être transformé automatiquement en conclusion définitive.

3. Expertise humaine

L'expert, le conservateur, le comité, la fondation ou l'institution peut formuler une opinion documentée. Le passeport conserve l'auteur, la date, le périmètre, les réserves et la version de cette opinion.

4. Niveaux d'attribution

Œuvre de, attribuée à, atelier de, entourage de, école de, d'après ou auteur inconnu représentent des niveaux différents. Le système doit préserver la formulation exacte de la source experte.

5. Examen visuel

Composition, facture, support, technique, usure, inscriptions, marques et autres caractéristiques observables peuvent être documentées. Une observation visuelle reste distincte d'une analyse instrumentale.

6. Photographie scientifique

Photographie en lumière visible, rasante, ultraviolet, infrarouge ou autre modalité peut produire des images de référence. Chaque image conserve sa date, son opérateur, son dispositif et son contexte lorsqu'ils sont disponibles.

7. Imagerie et couches sous-jacentes

Certaines techniques peuvent révéler repentirs, dessins préparatoires, restaurations ou structures non visibles à l'œil nu. Ces observations doivent être interprétées par des spécialistes et ne constituent pas seules une preuve d'auteur.

8. Signature et inscriptions

Signature, monogramme, date, cachet, inscription ou étiquette peuvent être photographiés et comparés à des références documentées. La présence d'une signature n'établit pas automatiquement l'authenticité de l'œuvre.

9. Supports et matériaux

Toile, bois, papier, pigments, liants, métaux, céramique, pierre ou autres matériaux peuvent être caractérisés. Les résultats restent reliés à l'échantillon, à la méthode et au laboratoire ou spécialiste.

10. Datation

Une méthode scientifique peut fournir une estimation, une plage ou une limite compatible avec une période. Le Passeport Art&Culture doit restituer la nature et l'incertitude du résultat sans transformer une estimation en date exacte.

11. Prélèvements

Tout prélèvement physique doit être documenté avec emplacement, date, quantité, opérateur et autorisation lorsque cela est applicable. Le lien entre l'échantillon et l'œuvre doit rester traçable.

12. Rapport de laboratoire

Un rapport scientifique peut être associé à l'œuvre avec empreinte d'intégrité, méthode, résultats, limites et version. Une modification du rapport de référence doit être détectable.

13. Compatibilité et incompatibilité

Un matériau compatible avec une période ne prouve pas nécessairement l'auteur. À l'inverse, une incompatibilité solidement établie peut devenir un élément important d'investigation, sous réserve du contexte et des limites de la méthode.

14. État de conservation

Altérations, lacunes, craquelures, déformations, corrosion, décoloration ou autres observations peuvent être enregistrées dans un constat d'état. Ces données décrivent l'état observé à une date donnée.

15. Historique des restaurations

Nettoyages, consolidations, retouches, doublages, remplacements ou autres interventions doivent être historisés. Une restauration ancienne peut modifier l'apparence et influencer certaines analyses.

16. Avant et après intervention

Photographies et constats avant, pendant et après restauration permettent de documenter les changements. Deep Authenticity© peut relier ces versions afin d'éviter qu'une modification légitime soit interprétée comme une substitution.

17. Contradictions entre expertises

Deux experts ou laboratoires peuvent aboutir à des interprétations différentes. Le passeport conserve les avis contradictoires avec leurs sources au lieu de supprimer celui qui ne correspond pas au dernier avis.

18. Score et niveaux de preuve

Si une interface synthétise la cohérence des preuves, elle doit montrer les catégories et sources sous-jacentes. Un score numérique ne doit jamais masquer les incertitudes ni devenir une certification automatique d'authenticité.

19. AP Ledger et confidentialité

Empreintes minimales de rapports, expertises, images de référence ou restaurations peuvent être ancrées dans AP Ledger. Données confidentielles, résultats non publiés, localisation, valeur, identité privée du propriétaire et détails de sécurité restent protégés.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si expertise humaine et analyse scientifique restent distinctes ; si chaque résultat conserve méthode et limites ; si une signature n'est pas une preuve suffisante ; si la datation conserve son incertitude ; si les restaurations sont historisées ; si les avis contradictoires restent visibles ; et si aucun score ne remplace le jugement expert. Deep Authenticity© devient ainsi une couche de convergence et de provenance des preuves d'authenticité.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 17 — ART ET CULTURE

CHAPITRE 4 — FAUX, CONTREFAÇONS, ŒUVRES VOLÉES OU DISPARUES, QR CODES CLONÉS, CERTIFICATS FALSIFIÉS, PROVENANCE FRAUDULEUSE, RESTITUTION, LITIGES ET INVESTIGATION

1. Objet du chapitre

Ce chapitre organise la gestion des anomalies et litiges affectant une œuvre ou un objet culturel : faux présumé, contrefaçon, disparition, vol déclaré, QR Code cloné, certificat falsifié, provenance incohérente, revendication de propriété, restitution et investigation.

2. Principe de non-accusation automatique

Une incohérence visuelle, documentaire, scientifique ou numérique constitue un signal à examiner. Authenticity Plus© / Deep Authenticity© conserve les faits, leurs sources et les contradictions ; la qualification juridique de faux, vol, fraude ou propriété relève des acteurs et autorités compétents.

3. Faux ou contrefaçon présumée

Une œuvre peut être signalée lorsque ses caractéristiques, matériaux, documents ou provenance ne concordent pas avec les références disponibles. Le statut doit distinguer suspicion, expertise en cours et conclusion provenant d'une source habilitée.

4. Copie, reproduction et œuvre dérivée

Copie licite, reproduction autorisée, fac-similé, œuvre d'après et contrefaçon ne doivent pas être confondus. Le Passeport conserve la catégorie déclarée et les droits documentés.

5. Œuvre volée ou disparue

Lorsqu'un propriétaire, une institution ou une autorité compétente documente un vol ou une disparition, le passeport peut afficher un statut d'alerte adapté. AP ne crée pas lui-même une déclaration de vol.

6. Blocage du passeport

Un statut de vol ou de disparition documenté peut restreindre certains transferts numériques ou changements de propriétaire dans AP. Le blocage protège la continuité de preuve sans constituer à lui seul une décision juridique de propriété.

7. QR Code cloné

La copie du QR Code d'une œuvre légitime sur un autre objet ne doit pas reproduire son authenticité. Deep Authenticity© peut confronter QR, caractéristiques visuelles, dimensions, marques, contexte de scan et statut courant.

8. Certificat falsifié

Un certificat modifié, reproduit ou attribué à un émetteur qui ne le reconnaît pas peut être signalé comme incohérent. Empreinte du document, référence, émetteur, date et statut contribuent à la vérification.

9. Provenance frauduleuse présumée

Une provenance peut contenir documents fabriqués, dates incompatibles ou propriétaires fictifs. Chaque maillon doit conserver sa source ; une incohérence sur un maillon ne doit pas conduire automatiquement à inventer une histoire alternative.

10. Documents historiques contestés

Facture, lettre, catalogue, photographie ou inventaire peut être contesté ou réinterprété. Le passeport conserve le document, son statut et les analyses successives au lieu de supprimer la trace du débat.

11. Signalement

Propriétaire, musée, galerie, expert ou autre acteur autorisé peut signaler une anomalie. Un signalement est identifié comme tel et reste distinct d'une conclusion officielle.

12. Mise sous vérification

Pendant une expertise ou investigation, l'œuvre peut recevoir un statut temporaire limitant certaines opérations numériques. Auteur, motif, date et durée ou condition de réexamen doivent être traçables.

13. Dossier d'investigation

Le dossier peut réunir photographies, provenance, certificats, rapports scientifiques, constats d'état, restaurations, scans, transactions documentées et déclarations. Chaque élément conserve sa source et son niveau de preuve.

14. Chaîne de preuve

Toute preuve numérique ou documentaire doit rester attribuable et, lorsque possible, protégée par empreinte d'intégrité. Une copie ou capture reste distinguée du document source.

15. Revendications concurrentes

Plusieurs personnes ou institutions peuvent revendiquer une œuvre. Le système doit pouvoir conserver plusieurs revendications contradictoires sans désigner automatiquement un propriétaire légitime.

16. Restitution

Une restitution peut résulter d’un accord, d’une décision institutionnelle, administrative ou judiciaire, ou d’un autre mécanisme compétent. Le passeport enregistre la décision et sa source sans se substituer à l’autorité qui la prononce.

17. Correction et réhabilitation

Lorsqu’une suspicion est levée, le statut actif doit être corrigé. L’historique d’audit peut conserver l’existence de l’investigation avec accès approprié, sans maintenir publiquement une accusation devenue infondée.

18. Alerte lors du scan

Si une œuvre possède un statut documenté de vol, disparition ou restriction, le QR dynamique peut afficher une alerte adaptée aux droits du lecteur. Les données de localisation ou de sécurité sensibles restent protégées.

19. AP Ledger et confidentialité

Empreintes minimales de signalements critiques, restrictions, rapports, décisions ou restitutions peuvent être ancrées dans AP Ledger. Dossiers d’enquête complets, identités privées, valeurs, localisations et informations de sécurité restent hors des couches publiques.

20. Critères d’acceptation et conclusion

Le modèle est acceptable si suspicion et conclusion restent distinctes ; si copie licite et contrefaçon ne sont pas confondues ; si un statut de vol provient d’une source compétente ; si un QR cloné ne reproduit pas l’identité légitime ; si les revendications concurrentes restent visibles ; si la restitution conserve sa décision source ; et si une suspicion levée peut être réhabilitée. Deep Authenticity© transforme ainsi les litiges et anomalies en dossiers de preuve auditables sans devenir juge de l’authenticité ou de la propriété.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 17 — ART ET CULTURE

CHAPITRE 5 — MUSÉES, GALERIES, ARTISTES, EXPERTS, COLLECTIONNEURS, ASSUREURS, GOUVERNANCE, CONFIDENTIALITÉ, CYBERSÉCURITÉ, INTEROPÉRABILITÉ ET AP LEDGER

1. Objet du chapitre

Ce chapitre définit la gouvernance institutionnelle et technique du Passeport Numérique Art&Culture. Il organise les rôles des artistes, ayants droit, musées, galeries, experts, maisons de vente, collectionneurs, restaurateurs, assureurs et autorités compétentes.

2. Identité des acteurs

Chaque acteur dispose d'une identité et d'un rôle distincts. Une même personne ou organisation peut cumuler plusieurs rôles, mais chaque action doit rester attribuée au rôle dans lequel elle a été effectuée.

3. Artiste et créateur

L'artiste peut documenter une œuvre, une édition ou un certificat lorsqu'il est habilité à le faire. Son identité créative, son identité de compte et ses éventuels ayants droit doivent rester correctement reliés.

4. Ayants droit et successions

Après le décès ou selon les droits applicables, fondation, succession, héritier, société de gestion ou autre ayant droit peut intervenir. Le passeport conserve la source et le périmètre de cette qualité sans l'inventer.

5. Musée

Le musée peut gérer inventaire, acquisitions, prêts, expositions, constats d'état et recherches. Ses données internes sensibles restent distinctes de la fiche publique de l'œuvre.

6. Galerie

La galerie peut documenter représentation, dépôt, exposition, vente ou provenance selon son rôle réel. Une galerie ne doit pas pouvoir modifier silencieusement une expertise ou un certificat émis par un tiers.

7. Maison de vente

La maison de vente peut publier ou relier catalogue, lot, description, résultat et statut de vente. Ses descriptions restent attribuées et versionnées, notamment lorsqu'une attribution évolue.

8. Expert et comité

L'expert, le comité ou la fondation peut produire une opinion d'authenticité ou d'attribution. Cette opinion conserve son auteur, sa date, ses réserves et son statut ; AP ne la transforme pas en vérité universelle.

9. Collectionneur et propriétaire

Le propriétaire contrôle les informations privées liées à sa possession, sous réserve des obligations applicables. Son identité n'a pas à être rendue publique pour que l'œuvre reste vérifiable.

10. Restaurateur

Le restaurateur peut documenter constat, intervention, matériaux ajoutés, photographies et recommandations. Il ne doit pas pouvoir modifier rétroactivement la provenance ou la propriété de l'œuvre.

11. Assureur

L'assureur peut accéder, selon autorisation, à l'identité de l'œuvre, aux constats, à certaines expertises, aux événements de transport ou de sinistre. Valeur assurée et conditions contractuelles restent confidentielles.

12. Autorités et patrimoine

Les autorités compétentes peuvent être sources de statuts relatifs au patrimoine, à l'exportation, à la saisie, au vol, à la restitution ou à d'autres décisions officielles. AP restitue ces statuts sans les créer.

13. Séparation des rôles et habilitations

Créer une œuvre, certifier, expertiser, restaurer, transférer, déclarer un incident ou administrer le système sont des opérations distinctes. Les droits numériques appliquent le moindre privilège et la traçabilité.

14. Confidentialité

Propriétaires privés, valeurs, localisations, itinéraires, dispositifs de sécurité, contrats, expertises non publiées et documents d'assurance restent protégés. La transparence de provenance doit être conciliée avec la sécurité des personnes et des œuvres.

15. Cybersécurité des comptes

Comptes d'artistes, institutions, experts et administrateurs doivent être protégés par authentification renforcée, gestion des sessions, révocation et journalisation adaptée aux opérations sensibles.

16. Sécurité du QR et des identifiants

QR Codes, étiquettes, puces ou autres identifiants physiques peuvent être copiés ou déplacés. Leur vérification doit donc s'appuyer sur le statut dynamique et, lorsque disponible, sur les caractéristiques de l'œuvre et le contexte.

17. Interopérabilité

Systèmes de musées, bases d'inventaire, archives, galeries, maisons de vente, laboratoires, assureurs et registres autorisés peuvent échanger des données. Chaque import conserve provenance, date, version et niveau d'autorité.

18. Continuité et pérennité

Le passeport doit rester vérifiable malgré changement de propriétaire, fermeture d'une galerie, transformation d'une institution ou succession d'un artiste. Les mécanismes de gouvernance prévoient autant que possible la continuité des autorités et des preuves.

19. Audit et AP Ledger

Émissions de certificats, changements de statut, transferts documentés, expertises, restaurations, alertes et décisions critiques peuvent produire des traces d'audit et des empreintes minimales dans AP Ledger. Les contenus sensibles complets restent hors des couches publiques.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si les rôles restent séparés ; si l'identité privée du propriétaire n'est pas nécessaire à la vérification publique ; si experts et autorités conservent leur propre autorité ; si QR et identifiants copiés ne suffisent pas ; si les systèmes externes conservent leur provenance ; et si la continuité survit aux changements d'acteurs. Cette gouvernance fournit le socle nécessaire à la clôture fonctionnelle de l'application Art et Culture.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 17 — ART ET CULTURE

CHAPITRE 6 — SYNTHÈSE FONCTIONNELLE, CRITÈRES D'ACCEPTATION ET CLÔTURE DE L'APPLICATION ART ET CULTURE

1. Objet du chapitre

Ce chapitre clôt le Point 17 — Art et Culture. Il consolide l'identité de l'œuvre, l'artiste et l'attribution, la provenance, les certificats, les ventes, prêts et expositions, l'expertise scientifique, la restauration, les incidents, la gouvernance, la confidentialité, la cybersécurité, l'interopérabilité et AP Ledger.

2. Mission consolidée

Le Passeport Numérique Art&Culture constitue une mémoire vérifiable de l'œuvre physique ou numérique. Il relie les preuves disponibles au fil du temps sans se substituer à l'artiste, à l'expert, au musée, au laboratoire, au propriétaire ou aux autorités compétentes.

3. Identité de l'œuvre

Titre, technique, dimensions, date ou période, signature, édition, inventaire et caractéristiques documentées composent l'identité de référence. Les informations inconnues ou incertaines restent explicitement qualifiées.

4. Artiste et attribution

Auteur certain, attribution, atelier, entourage, école ou auteur inconnu restent des statuts distincts. Chaque opinion conserve sa source, sa date, ses réserves et son historique.

5. Provenance

Ventes, collections, successions, galeries, musées, prêts et autres événements documentés forment la provenance. Les lacunes historiques restent visibles et ne sont jamais complétées artificiellement.

6. Propriété, garde et droits

Propriété juridique, garde physique, dépôt, prêt et droits d'auteur ou d'exploitation sont des relations différentes. Le transfert de l'objet ne transfère pas automatiquement les droits intellectuels.

7. Certificats et experts

Certificats, expertises et attestations restent attribués à leurs émetteurs. Authenticity Plus© vérifie leur provenance et leur intégrité sans transformer une opinion contestée en vérité absolue.

8. QR Code dynamique

Le QR dynamique ouvre le statut courant de l'œuvre et son Passeport Art&Culture. Une copie du QR sur un autre objet ne doit pas reproduire l'authenticité de l'œuvre de référence.

9. Deep Authenticity©

Deep Authenticity© confronte les éléments disponibles : identité, photographies, dimensions, marques, provenance, certificats, expertises, analyses, restaurations et contexte de scan. Il mesure une cohérence de preuve sans remplacer le jugement expert.

10. Ventes, prêts et expositions

Galeries, maisons de vente, musées et autres institutions peuvent documenter leurs événements selon leur rôle réel. Mise en vente, adjudication, invendu, prêt, exposition et transfert de propriété restent distincts.

11. Transport et constats d'état

Départ, garde, réception et constats d'état peuvent être documentés sans exposer publiquement itinéraires ou localisations sensibles. Les constats permettent de comparer l'état matériel dans le temps.

12. Analyses scientifiques

Imagerie, analyses de matériaux, datation et autres méthodes conservent leur protocole, laboratoire, échantillon, limites et incertitudes. Un résultat scientifique isolé ne constitue pas automatiquement une preuve d'auteur.

13. Restauration

Les interventions sont historisées avec leur auteur, leur date et les changements observés. Une modification légitime résultant d'une restauration ne doit pas être confondue avec une substitution frauduleuse.

14. Faux, contrefaçons et QR clonés

Une incohérence déclenche une vérification, jamais une accusation automatique. Copie licite, reproduction, œuvre dérivée, faux présumé et contrefaçon doivent rester des catégories distinctes.

15. Vol, disparition et restitution

Un statut documenté de vol ou disparition peut déclencher alerte et restriction de certaines opérations. Revendications concurrentes et restitutions conservent leurs sources et décisions compétentes ; AP ne devient pas juge de propriété.

16. Gouvernance des acteurs

Artistes, ayants droit, musées, galeries, maisons de vente, experts, collectionneurs, restaurateurs, assureurs et autorités disposent de rôles et habilitations distincts, appliquant le principe du moindre privilège.

17. Confidentialité

Identité des propriétaires privés, valeurs, contrats, localisations, itinéraires, dispositifs de sécurité, expertises confidentielles et informations d'assurance restent protégés. La vérifiabilité publique ne nécessite pas leur divulgation.

18. Cybersécurité, continuité et interopérabilité

Comptes, QR, identifiants physiques, API et systèmes partenaires doivent préserver provenance, version, révocabilité et audit. Le passeport doit rester exploitable malgré changements de propriétaire, succession, fermeture d'une galerie ou transformation d'une institution.

19. AP Ledger et critères d'acceptation

AP Ledger peut ancrer des empreintes minimales d'identité, certificats, expertises, restaurations, transferts, alertes et décisions critiques. Le modèle est acceptable si les incertitudes restent visibles, si aucun score ne remplace l'expert, si un QR cloné ne reproduit pas l'authenticité et si les données sensibles restent hors des couches publiques ou irréversibles.

20. Clôture du Point 17 — Art et Culture

Le Point 17 — Art et Culture est désormais fonctionnellement défini : identité de l'œuvre, artiste, attribution, provenance, certificats, QR Codes dynamiques, Deep Authenticity©, ventes, galeries, maisons de vente, musées, prêts, expositions, transport, constats, restauration, analyses scientifiques, niveaux de preuve, faux présumés, œuvres volées ou disparues, restitution, gouvernance, confidentialité, cybersécurité, interopérabilité, audit et AP Ledger. Le Volume IV peut désormais poursuivre avec le Point 18 — Luxury.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 18 — LUXURY

CHAPITRE 1 — IDENTITÉ DU PRODUIT DE LUXE, MARQUE, MODÈLE, NUMÉRO DE SÉRIE, PROVENANCE, PROPRIÉTÉ, QR CODE DYNAMIQUE ET PASSEPORT NUMÉRIQUE LUXURY

1. Objet du chapitre

Le Point 18 — Luxury transpose Authenticity Plus© / Deep Authenticity© aux produits de luxe : montres, bijoux, maroquinerie, mode, accessoires, objets de collection et autres biens à forte valeur. Il crée un Passeport Numérique Luxury reliant l'objet physique à son identité, sa provenance, son historique et ses preuves.

2. Mission sectorielle

La mission est de permettre au propriétaire, à la marque, au professionnel ou à l'acheteur autorisé de vérifier ce qui est documenté sur l'objet : marque, modèle, références, numéro de série, origine, propriété, entretien, réparations, ventes et statut. AP ne se substitue pas à l'expertise de la marque ou du spécialiste.

3. Identité de l'objet

Chaque objet reçoit une identité distincte : catégorie, marque, modèle, variante, dimensions, matériaux, références et caractéristiques disponibles. Deux objets identiques commercialement restent deux unités physiques différentes.

4. Marque et fabricant

La marque, la manufacture ou l'atelier peut être relié à l'objet selon la preuve disponible. Une information déclarée par le propriétaire reste distincte d'une confirmation directe par la marque.

5. Numéro de série

Numéro de série, référence de modèle, numéro de mouvement, poinçon ou autre identifiant peut contribuer à l'identité. Ces données sensibles peuvent être partiellement masquées dans la vue publique afin de limiter leur réutilisation frauduleuse.

6. Objet ancien sans documents

Un propriétaire qui possède, par exemple, une montre héritée sans facture ni certificat peut créer un passeport initial à partir de photographies et d'informations déclarées. Le système doit clairement indiquer que l'enregistrement documente la possession et l'objet présenté, sans inventer une certification d'origine.

7. Photographies de référence

Photographies générales et détails distinctifs — cadran, boîtier, fermoir, poinçons, coutures, gravures, usure ou autres caractéristiques — peuvent former une empreinte visuelle de référence datée.

8. Provenance

Achat, héritage, donation, vente, dépôt, réparation ou autre événement documenté peut enrichir la provenance. Les périodes sans document restent des lacunes et ne sont pas complétées artificiellement.

9. Propriété et possession

Propriété, possession physique, dépôt chez un réparateur, prêt et consignation sont des relations distinctes. Le passeport doit permettre de savoir qui est autorisé à administrer l'objet sans rendre nécessairement l'identité du propriétaire publique.

10. Preuve d'achat et documents

Facture, certificat, carte de garantie, archive de marque, rapport d'expertise ou document de succession peut être associé au passeport avec sa source et son niveau de preuve. Un document téléchargé par l'utilisateur n'est pas automatiquement validé par son émetteur.

11. QR Code dynamique

Un QR Code dynamique peut être associé à l'objet ou à son support sécurisé. Le scan ouvre une fiche de vérification dont le contenu dépend des droits du lecteur et du statut courant de l'objet.

12. Deep Authenticity©

Deep Authenticity© peut confronter QR, photographies, caractéristiques, références, numéro de série masqué ou vérifiable, documents, historique de maintenance, scans et autres preuves disponibles. Il mesure une cohérence documentaire et physique sans remplacer l'expertise professionnelle.

13. QR cloné

La copie visuelle du QR Code d'un objet légitime sur une contrefaçon ne doit pas suffire. Le contexte du scan et les caractéristiques de l'objet doivent pouvoir révéler une incohérence avec le passeport de référence.

14. Vue propriétaire

Le propriétaire peut accéder à l'historique détaillé, aux documents privés, aux opérations de transfert et aux fonctions de déclaration de perte ou de vol. Ces informations ne sont pas automatiquement accessibles à un simple scanner.

15. Vue publique ou acheteur

Une vue minimisée peut confirmer que le passeport existe, présenter les caractéristiques publiables et le statut autorisé. Lors d'une revente, le propriétaire peut accorder temporairement un accès plus riche à l'acheteur potentiel.

16. Héritage et transmission

Un objet transmis dans une famille peut conserver son histoire même lorsque les documents d'origine ont disparu. Les déclarations familiales, photographies anciennes et documents retrouvés peuvent être ajoutés avec leur provenance et leur niveau de preuve.

17. Corrections

Une erreur de référence, date, photographie ou description peut être corrigée par un acteur habilité. La correction est versionnée afin de préserver l'intégrité historique du passeport.

18. Online et Offline

Online permet de consulter le statut courant. Offline sécurisé peut afficher une preuve signée mise en cache avec sa date de dernière synchronisation ; il ne doit jamais présenter un ancien statut comme garantie actuelle.

19. AP Ledger et confidentialité

Empreintes minimales d'identité, création de passeport, transferts, déclarations critiques ou interventions peuvent être ancrées dans AP Ledger. Identité privée du propriétaire, adresse, valeur, localisation, documents complets et identifiants sensibles restent protégés.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si un objet ancien peut être enregistré sans faux certificat ; si les preuves déclarées et confirmées restent distinctes ; si numéro de série et données privées sont protégés ; si un QR cloné ne suffit pas à reproduire l'authenticité ; si propriété et possession ne sont pas confondues ; et si l'histoire familiale peut être conservée avec son niveau de preuve. Le Passeport Numérique Luxury devient ainsi la mémoire vérifiable et évolutive d'un objet de valeur.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 18 — LUXURY

CHAPITRE 2 — ACHAT, BOUTIQUE, CERTIFICAT, GARANTIE, ENTRETIEN, RÉPARATION, PIÈCES REMPLACÉES, EXPERTISE, REVENTE ET TRANSFERT SÉCURISÉ DU PASSEPORT LUXURY

1. Objet du chapitre

Ce chapitre définit le cycle de vie opérationnel d'un produit de luxe après sa création ou son enregistrement : achat, activation du Passeport Luxury, garantie, entretien, réparation, remplacement de composants, expertise, revente et transfert sécurisé au nouveau propriétaire.

2. Achat en boutique

Lors d'un achat auprès d'une boutique ou d'un revendeur habilité, le produit peut être relié à la transaction, à la date, au point de vente et aux documents applicables. Les informations commerciales privées ne sont pas nécessairement visibles dans la fiche publique.

3. Activation du passeport

Le Passeport Luxury peut être activé au moment de la vente ou ultérieurement selon le modèle de la marque. L'activation relie l'objet physique à son identité numérique sans rendre l'identité de l'acheteur publique.

4. Certificat et garantie

Certificat d'authenticité, carte de garantie ou garantie numérique restent des preuves distinctes. Leur émetteur, période, conditions et statut doivent être conservés ; AP ne crée pas lui-même la garantie du fabricant.

5. Facture et preuve d'achat

La facture peut être conservée comme document privé et utilisée comme preuve de transaction. Un extrait minimal peut suffire pour certaines vérifications sans exposer prix, adresse ou autres informations sensibles.

6. Entretien

Révision, nettoyage, polissage, contrôle, réglage ou autre entretien peut devenir un événement du passeport avec atelier, date et travaux documentés. L'historique d'entretien enrichit la provenance technique de l'objet.

7. Réparation

Une réparation doit pouvoir identifier l'acteur, la date, le motif déclaré, les opérations et les pièces concernées. Une intervention indépendante reste distinguée d'une intervention effectuée ou confirmée par la marque.

8. Pièces remplacées

Mouvement, cadran, verre, bracelet, fermoir, pierre, composant électronique, doublure ou autre pièce remplacée peut modifier l'état de référence. Le passeport conserve autant que possible la pièce retirée, la pièce installée et la source de l'intervention.

9. Pièce d'origine et pièce de service

Une pièce installée ultérieurement par la marque ou un atelier peut être authentique sans être la pièce d'origine de fabrication. Deep Authenticity© doit préserver cette distinction importante pour l' historique et l'expertise.

10. Photographies avant et après

Des photographies datées avant et après intervention permettent de documenter l'évolution physique. Elles contribuent à distinguer réparation légitime, usure, modification et substitution.

11. Atelier et habilitation

Atelier de marque, centre agréé et réparateur indépendant sont des statuts différents. Chaque intervention conserve l'identité et le niveau d'habilitation documenté de son auteur.

12. Expertise

Avant assurance, revente, succession ou litige, une expertise peut être ajoutée avec son auteur, sa date, ses réserves et ses conclusions. L'expertise reste une preuve attribuée et ne devient pas automatiquement une certification AP.

13. Estimation de valeur

Une estimation financière est datée et attribuée à sa source. Elle peut évoluer avec le marché, l'état et la rareté ; elle ne doit donc pas être présentée comme une valeur permanente ou garantie.

14. Préparation à la revente

Le propriétaire peut créer un accès temporaire pour un acheteur, une plateforme ou un professionnel afin de consulter les informations autorisées : identité, provenance publiable, entretien, expertises et statut.

15. Vérification avant achat

L’acheteur peut scanner le QR dynamique et comparer l’objet au passeport. Deep Authenticity© peut signaler des incohérences de référence, photographie, composants, historique ou statut sans rendre seul un verdict définitif.

16. Vente et preuve de transaction

Une revente peut produire un événement documenté reliant l’objet au transfert. Prix, identité complète des parties et modalités de paiement restent privés sauf nécessité ou consentement.

17. Transfert sécurisé du passeport

Le changement de propriétaire doit nécessiter une procédure contrôlée : initiation par le propriétaire autorisé, acceptation par le nouveau propriétaire et journalisation du transfert. La simple possession du QR Code ne permet pas de prendre le contrôle du passeport.

18. Annulation et litige de transfert

Une transaction annulée, contestée ou frauduleuse présumée peut suspendre le transfert. Les revendications restent distinctes jusqu’à résolution par les parties ou l’autorité compétente.

19. AP Ledger et confidentialité

Empreintes minimales d’activation, entretien, réparation, expertise et transfert peuvent être ancrées dans AP Ledger. Factures complètes, prix, identité privée, adresse, valeur assurée et détails contractuels restent protégés.

20. Critères d’acceptation et conclusion

Le modèle est acceptable si certificat et garantie restent distincts ; si les interventions conservent leur auteur ; si pièce d’origine et pièce de service ne sont pas confondues ; si l’estimation reste datée ; si un acheteur peut vérifier sans accéder aux données privées ; et si le transfert du passeport exige une autorisation bilatérale. Le Passeport Luxury accompagne ainsi l’objet durant toute sa vie commerciale et technique.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 18 — LUXURY

CHAPITRE 3 — PERTE, VOL, BLOCAGE AP LEDGER/BLOCKCHAIN, DÉCLARATION, RÉCUPÉRATION, RESTITUTION, ASSURANCE, QR CODE CLONÉ ET MARCHÉ DE SECONDE MAIN

1. Objet du chapitre

Ce chapitre définit le dispositif de protection d'un objet Luxury en cas de perte, vol, disparition, tentative de revente ou clonage de son identifiant. Le Passeport Luxury devient alors un mécanisme de statut dynamique, de preuve chronologique et d'alerte.

2. Principe fondamental

Un propriétaire autorisé peut déclarer un objet perdu ou volé dans Authenticity Plus©. Le système modifie le statut du passeport et conserve la chronologie de la déclaration sans se substituer à une déclaration officielle auprès des autorités ou à une décision juridique.

3. Déclaration de perte

En cas de perte, le propriétaire peut placer l'objet dans un statut « perdu » ou équivalent. La date, le compte déclarant et les informations nécessaires sont journalisés. Les données de localisation sensibles ne sont pas rendues publiques.

4. Déclaration de vol

En cas de vol, un statut spécifique peut être appliqué. Lorsque des références officielles existent, elles peuvent être ajoutées au dossier avec accès contrôlé. AP ne prétend pas déterminer l'auteur du vol.

5. Blocage numérique

Le statut perdu ou volé peut bloquer les transferts ordinaires du Passeport Luxury et certaines opérations sensibles. L'objectif est d'empêcher qu'une personne en possession physique de l'objet puisse légitimer facilement une nouvelle propriété numérique.

6. AP Ledger / Blockchain

Une empreinte minimale de la déclaration et du changement de statut peut être ancrée dans AP Ledger ou la couche Blockchain prévue par l'architecture. L'ancrage prouve l'existence et la chronologie du statut sans publier les données personnelles ou le dossier complet.

7. QR Code dynamique après blocage

Le QR Code reste dynamique. Lors d'un scan autorisé, la fiche peut indiquer que l'objet fait l'objet d'un statut de perte, vol ou restriction, selon les droits du lecteur et les règles de confidentialité.

8. Alerte à l'acheteur

Sur le marché de seconde main, un acheteur qui vérifie l'objet avant acquisition peut être averti qu'un transfert est bloqué ou qu'un statut critique est actif. L'alerte doit rester factuelle et ne pas accuser le vendeur.

9. QR Code cloné

Un contrefacteur peut copier l'image d'un QR légitime. Deep Authenticity© confronte alors le code au passeport, au statut, aux photographies, caractéristiques, références et contexte disponibles. Le QR seul n'est jamais la preuve complète.

10. Scans incompatibles

Des scans incompatibles dans le temps ou dans des contextes manifestement contradictoires peuvent produire un signal de vérification. La géolocalisation, lorsqu'elle est utilisée et autorisée, constitue un indice contextuel et non une preuve automatique de fraude.

11. Marché de seconde main

Plateformes, boutiques, maisons de vente ou professionnels peuvent vérifier le statut d'un objet avant mise en vente ou acquisition. Les informations privées du propriétaire précédent ne doivent pas être nécessaires à cette vérification.

12. Tentative de transfert d'un objet bloqué

Une tentative de transfert alors que le passeport est bloqué doit échouer ou être placée sous vérification. L'événement peut être journalisé afin d'alimenter le dossier d'investigation.

13. Assurance

Le propriétaire peut partager avec son assureur, selon autorisation, l'identité du produit, les preuves d' achat, expertises, entretien et statut de perte ou vol. AP ne décide ni de la couvertureni de l' indemnisation.

14. Signalement et dossier de preuve

Photographies, numéro de série, facture, certificat, expertise, historique d'entretien et événements du passeport peuvent constituer un dossier de preuve exportable ou partageable selon les droits.

15. Objet retrouvé

Lorsque l'objet perdu est retrouvé, le propriétaire peut demander la levée du statut après vérification appropriée. La chronologie conserve l'existence de la perte et la date de récupération.

16. Objet récupéré après vol

La récupération d’un objet déclaré volé peut nécessiter des éléments supplémentaires selon le contexte. Le statut ne doit pas être levé par un simple scan ou par la personne qui détient physiquement l’objet.

17. Restitution

Lorsqu’un objet est restitué à son propriétaire légitime selon un processus documenté, le passeport enregistre la restitution et son origine. AP conserve la preuve de l’événement sans devenir arbitre juridique de propriété.

18. Offline

En mode Offline, un terminal peut consulter le dernier statut signé disponible avec sa date de synchronisation. Un statut ancien ne doit pas être présenté comme actuel ; la reconnexion doit vérifier en priorité les alertes de perte ou de vol.

19. Confidentialité et audit

Identité du propriétaire, adresse, références de police, localisation et documents d’assurance restent protégés. Les changements de statut, tentatives de transfert et événements critiques sont auditables, avec empreintes minimales possibles dans AP Ledger.

20. Critères d’acceptation et conclusion

Le modèle est acceptable si le propriétaire peut bloquer rapidement le passeport ; si la possession physique ou le QR ne permet pas un transfert ; si le statut critique est vérifiable sans révéler les données privées ; si le marché de seconde main peut détecter un objet bloqué ; si la récupération exige une vérification ; et si la Blockchain/AP Ledger conserve une preuve minimale et non le dossier personnel. Le Passeport Luxury devient ainsi un mécanisme actif de protection de l’objet tout au long de sa circulation.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 18 — LUXURY

CHAPITRE 4 — CONTREFAÇON, FAUX NUMÉROS DE SÉRIE, FAUX CERTIFICATS, PIÈCES NON CONFORMES, CLONES, DEEP AUTHENTICITY©, EXPERTISE ET INVESTIGATION

1. Objet du chapitre

Ce chapitre définit la détection et le traitement des incohérences pouvant affecter un produit Luxury : contrefaçon présumée, numéro de série falsifié ou dupliqué, faux certificat, composants non conformes, QR Code cloné, passeport détourné et historique documentaire incohérent.

2. Principe de non-accusation automatique

Une anomalie déclenche une vérification, jamais une accusation automatique. Authenticity Plus© / Deep Authenticity© rassemble les indices et leurs sources ; la qualification définitive d'une contrefaçon relève de la marque, de l'expert ou de l'autorité compétente selon le contexte.

3. Identité physique et identité numérique

L'objet présenté doit être confronté au Passeport Luxury : catégorie, modèle, matériaux, dimensions, photographies, marques, gravures, composants et identifiants disponibles. Le QR Code ne constitue qu'un élément de cette identité.

4. Faux numéro de série

Un numéro peut être inventé, modifié ou copié depuis un objet légitime. La présence d'un numéro au bon format ne suffit donc pas ; son association au modèle, aux caractéristiques et aux sources disponibles doit être vérifiée.

5. Numéro de série dupliqué

Deux objets apparaissant avec le même identifiant unitaire peuvent produire un signal critique. Le système conserve les scans et éléments de contexte afin de permettre une investigation sans décider automatiquement lequel est authentique.

6. Faux certificat

Certificat papier ou numérique peut être reproduit, modifié ou attribué à tort à une marque ou un expert. Émetteur, référence, date, empreinte du document et statut de confirmation sont vérifiés lorsque ces données sont disponibles.

7. Fausse facture ou preuve d'achat

Une facture téléchargée ne devient pas automatiquement une preuve confirmée. Le passeport distingue document fourni par l'utilisateur, document vérifié par son émetteur et information provenant directement d'un système de confiance.

8. Pièces non conformes

Un objet peut associer des composants d'origines différentes. Le système documente les incohérences observées et distingue pièce d'origine, pièce de service authentique, pièce indépendante documentée et composant non déterminé.

9. Objet composite

Dans l'horlogerie, la joaillerie ou d'autres secteurs, un objet peut avoir été modifié au cours de sa vie. Une modification documentée n'est pas automatiquement une contrefaçon ; elle doit être intégrée à l' historique technique.

10. QR Code cloné

La copie d'un QR légitime sur un faux produit ne doit pas reproduire le statut de l'objet original. Deep Authenticity© confronte le code aux caractéristiques physiques, à l'historique et au contexte disponible.

11. Clone du Passeport

Une tentative de créer plusieurs passeports pour le même objet ou d'associer un passeport existant à un autre objet doit produire une alerte de duplication ou une demande de vérification renforcée.

12. Analyse photographique

Les photographies de référence peuvent être comparées aux nouvelles images : géométrie, détails, marques, usure et composants visibles. Une différence photographique constitue un indice et doit tenir compte de l'éclairage, de l'angle, de l'entretien et des réparations.

13. Deep Authenticity©

Deep Authenticity© combine les preuves disponibles : identité numérique, QR, documents, photos, numéros, composants, entretien, transferts, scans et statuts. Il doit expliquer les incohérences détectées plutôt que produire un verdict opaque.

14. Expertise de la marque

Lorsque la marque dispose d'un service d'authentification ou d'archives, sa confirmation peut enrichir le passeport avec un niveau de preuve supérieur à une simple déclaration. L'absence de réponse de la marque ne vaut pas automatiquement rejet.

15. Expertise indépendante

Un expert indépendant peut produire un rapport attribué et daté. Son opinion conserve son périmètre et ses réserves et peut coexister avec d'autres avis.

16. Contradiction entre expertises

Des avis différents peuvent être conservés simultanément. Le Passeport Luxury versionne les expertises et leurs sources au lieu de supprimer l'avis antérieur.

17. Mise sous vérification

Lorsqu'une incohérence importante apparaît, certaines opérations — notamment transfert ou publication comme objet vérifié — peuvent être temporairement restreintes. Le motif, l'auteur et la date du statut restent auditables.

18. Dossier d'investigation

Photographies, scans, numéros, documents, expertises, réparations, historique de propriété et événements peuvent être réunis dans un dossier contrôlé. Chaque élément conserve sa provenance et son niveau de preuve.

19. AP Ledger et confidentialité

Empreintes minimales des preuves, changements de statut, expertises ou décisions critiques peuvent être ancrées dans AP Ledger. Documents complets, identité privée, valeur, localisation et données d' enquête sensibles restent protégés.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si le QR seul ne suffit jamais ; si un numéro de série dupliqué déclenche une investigation ; si faux certificat et document non vérifié restent distingués ; si pièce de service et contrefaçon ne sont pas confondues ; si les avis contradictoires sont conservés ; et si Deep Authenticity© explique ses signaux. L'application Luxury transforme ainsi la lutte contre la contrefaçon en une convergence de preuves vérifiables plutôt qu'en un verdict automatique.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 18 — LUXURY

CHAPITRE 5 — MARQUES, BOUTIQUES, ATELIERS, EXPERTS, ASSUREURS, MARKETPLACES, GOUVERNANCE, CONFIDENTIALITÉ, CYBERSÉCURITÉ, INTEROPÉRABILITÉ ET AP LEDGER

1. Objet du chapitre

Ce chapitre définit la gouvernance institutionnelle et technique du Passeport Numérique Luxury. Il organise les rôles des marques, manufactures, boutiques, revendeurs, ateliers, experts, assureurs, marketplaces, propriétaires et autorités compétentes.

2. Identité des acteurs

Chaque acteur professionnel dispose d'une identité, d'un rôle et d'un périmètre d'action. Une marque, une boutique, un atelier et un expert ne disposent pas automatiquement des mêmes droits sur le passeport.

3. Marque et manufacture

La marque ou manufacture peut être source d'identité produit, références, numéros, archives, garanties, interventions et confirmations lorsqu'elle fournit ces données. AP conserve cette provenance sans parler au nom de la marque.

4. Boutique officielle

Une boutique officielle peut activer un passeport, relier une vente ou confirmer certaines informations selon son habilitation. L'identité de l'acheteur et les données commerciales restent privées.

5. Revendeur agréé

Un revendeur agréé peut disposer de droits définis par la marque ou l'écosystème. Son statut doit être vérifiable et daté ; une ancienne habilitation ne doit pas être présentée comme actuelle.

6. Marchand indépendant

Un professionnel indépendant peut documenter acquisition, expertise, vente ou entretien selon son rôle. Ses déclarations restent distinctes des confirmations émises directement par la marque.

7. Atelier et centre de service

Atelier officiel, centre agréé et réparateur indépendant sont distingués. Chaque intervention conserve l' identité de l'acteur, la date, les pièces remplacées et le niveau d'habilitation documenté.

8. Expert

L’expert peut produire une opinion sur authenticité, état, provenance ou valeur. Son rapport reste attribué, daté et versionné ; AP ne transforme pas automatiquement son avis en certification universelle.

9. Assureur

L’assureur peut recevoir, avec autorisation, certaines preuves du passeport : identité de l’objet, facture, expertise, entretien, déclaration de perte ou vol et récupération. Les décisions de couverture ou d’ indemnisation restent propres à l’assureur.

10. Marketplace et seconde main

Une marketplace peut vérifier l’existence et le statut du Passeport Luxury avant publication ou transaction. Elle peut recevoir un résultat de vérification minimisé sans accéder à l’identité privée du propriétaire.

11. Vérification avant mise en vente

Objet bloqué, passeport sous investigation, QR incohérent ou transfert non autorisé peut empêcher ou suspendre une opération selon les règles du service concerné. L’alerte reste factuelle et attribuée.

12. Propriétaire

Le propriétaire contrôle les opérations sensibles : accès privé, partage temporaire, déclaration de perte ou vol et initiation du transfert. La possession physique de l’objet ou du QR ne donne pas automatiquement ces droits.

13. Séparation des rôles

Créer un passeport, confirmer une référence, réparer, expertiser, assurer, vendre, bloquer ou transférer sont des actions distinctes. Les habilitations appliquent le principe du moindre privilège et sont révocables.

14. Confidentialité

Identité du propriétaire, adresse, localisation, valeur, prix d’achat, contrat d’assurance, documents privés et identifiants sensibles sont protégés. La vérification d’authenticité doit utiliser le minimum de données nécessaire.

15. Cybersécurité des comptes

Comptes de marques, boutiques, experts, ateliers et administrateurs doivent bénéficier de protections adaptées : authentification renforcée, contrôle des sessions, révocation, séparation des privilèges et journalisation.

16. Sécurité des QR et terminaux

QR Codes, étiquettes, puces, terminaux de boutique et outils d'atelier peuvent être copiés ou compromis. Leur identité et leur statut doivent être gérés afin qu'un identifiant physique seul ne puisse établir l'authenticité.

17. Interopérabilité

Systèmes de marque, ERP, CRM, ateliers, assureurs, marketplaces et autres partenaires peuvent échanger avec AP par interfaces contrôlées. Chaque donnée importée conserve sa source, son horodatage, sa version et son niveau d'autorité.

18. Continuité et succession

Le passeport doit survivre autant que possible à une fermeture de boutique, un changement de distributeur, une succession, une revente internationale ou une évolution des systèmes de la marque. Les preuves historiques restent conservées.

19. Audit et AP Ledger

Activations, confirmations, réparations, expertises, blocages, transferts et décisions critiques peuvent produire des traces d'audit et des empreintes minimales dans AP Ledger. Les documents et données personnelles complets restent hors des couches publiques ou irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si chaque acteur reste limité à son rôle ; si la marketplace peut vérifier sans connaître le propriétaire ; si l'habilitation d'un revendeur est datée ; si un atelier indépendant reste distingué d'un atelier officiel ; si les droits sont révocables ; et si l'interopérabilité conserve la provenance. Cette gouvernance fournit le socle nécessaire à la clôture fonctionnelle de l'application Luxury.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 18 — LUXURY

CHAPITRE 6 — SYNTHÈSE FONCTIONNELLE, CRITÈRES D'ACCEPTATION ET CLÔTURE DE L'APPLICATION LUXURY

1. Objet du chapitre

Ce chapitre clôt le Point 18 — Luxury. Il consolide l'identité de l'objet, la marque, le modèle, les numéros, la provenance, la propriété, l'héritage, les QR Codes dynamiques, l'entretien, les réparations, la revente, le vol, la contrefaçon, la gouvernance, la cybersécurité, l'interopérabilité et AP Ledger.

2. Mission consolidée

Le Passeport Numérique Luxury constitue la mémoire vérifiable et évolutive d'un objet de valeur. Il accompagne l'objet depuis sa création ou son premier enregistrement jusqu'aux transmissions successives, sans transformer une donnée déclarée en certification automatique.

3. Objet ancien sans documents

Un objet hérité ou ancien peut recevoir un passeport à partir de photographies, caractéristiques et déclarations du propriétaire. L'enregistrement établit une identité numérique et une chronologie à partir de ce moment, sans inventer facture, certificat ou origine antérieure.

4. Identité et numéro de série

Marque, modèle, variante, matériaux, dimensions, photographies, numéros de série, références, poinçons ou autres caractéristiques forment une identité composite. Aucun identifiant isolé ne doit suffire à établir l'authenticité.

5. Provenance et propriété

Achat, héritage, donation, vente, dépôt, prêt, réparation et autres événements documentés enrichissent la provenance. Propriété juridique, possession physique et garde temporaire restent des relations distinctes.

6. QR Code dynamique

Le QR dynamique donne accès au statut courant du passeport selon les droits du lecteur. Sa copie visuelle sur un autre objet ne doit jamais suffire à reproduire l'identité ou l'authenticité de l'original.

7. Deep Authenticity©

Deep Authenticity© confronte QR, photographies, caractéristiques physiques, numéros, documents, composants, interventions, transferts, scans et statuts. Les incohérences sont explicables et investigables plutôt que transformées en verdict opaque.

8. Achat, garantie et documents

Facture, certificat, garantie et archives de marque restent des preuves distinctes avec leur émetteur et leur statut. Les documents privés peuvent contribuer à la vérification sans être exposés publiquement.

9. Entretien et réparation

Chaque intervention peut enrichir l'historique technique. Atelier officiel, centre agréé et réparateur indépendant restent distingués, de même que pièce d'origine, pièce de service authentique et composant d'origine indéterminée.

10. Expertise et valeur

Expertises d'authenticité, d'état ou de valeur sont datées et attribuées. Une estimation financière reste temporelle et ne devient pas une valeur permanente garantie par AP.

11. Revente et marché secondaire

Avant une transaction, un acheteur ou une marketplace peut vérifier le statut et les informations autorisées du passeport. L'identité privée du propriétaire précédent n'est pas nécessaire à cette vérification.

12. Transfert sécurisé

Le changement de contrôle du Passeport Luxury nécessite une procédure autorisée et journalisée. La possession physique de l'objet, du téléphone, d'une photographie ou du QR Code ne suffit pas à transférer la propriété numérique.

13. Perte et vol

Le propriétaire autorisé peut déclarer l'objet perdu ou volé, ce qui déclenche un statut critique et peut bloquer les transferts ordinaires. AP conserve la chronologie sans se substituer aux autorités compétentes.

14. AP Ledger / Blockchain

Une empreinte minimale de déclaration, blocage, transfert ou autre événement critique peut être ancrée dans AP Ledger ou la couche Blockchain prévue. Les données personnelles, documents complets et localisations sensibles n'y sont pas publiés.

15. Objet retrouvé et restitution

La levée d'un statut de perte ou vol exige une vérification adaptée et ne résulte pas d'un simple scan. Récupération et restitution sont historisées avec leur source et leur date.

16. Contrefaçon et clones

Faux numéros, certificats falsifiés, composants incohérents, QR clonés ou passeports dupliqués déclenchent une vérification. Une anomalie ne devient jamais automatiquement une accusation de contrefaçon.

17. Gouvernance des acteurs

Marques, boutiques, revendeurs, ateliers, experts, assureurs, marketplaces et propriétaires disposent de rôles distincts, datés et révocables. Le principe du moindre privilège s'applique aux opérations sensibles.

18. Confidentialité, cybersécurité et interopérabilité

Identité privée, adresse, localisation, valeur, prix, assurance et documents sensibles restent protégés. Comptes, terminaux, QR, API et systèmes partenaires doivent préserver provenance, version, authentification, révocation et audit.

19. Critères d'acceptation

Le modèle est acceptable si un objet sans documents peut être enregistré sans faux certificat ; si le QR et le numéro de série ne suffisent jamais seuls ; si le propriétaire peut bloquer rapidement un objet perdu ou volé ; si la revente peut être vérifiée sans exposer les données privées ; si les réparations restent historisées ; et si AP Ledger ne reçoit que les empreintes minimales nécessaires.

20. Clôture du Point 18 — Luxury

Le Point 18 — Luxury est désormais fonctionnellement défini : identité du produit, marque, modèle, numéros, objet hérité, provenance, propriété, QR dynamique, Deep Authenticity©, achat, garantie, entretien, réparation, pièces remplacées, expertise, revente, transfert sécurisé, perte, vol, blocage AP Ledger/Blockchain, récupération, assurance, marché secondaire, contrefaçon, clones, gouvernance, confidentialité, cybersécurité, interopérabilité et audit. Le Volume IV peut désormais poursuivre avec le Point 19 — Construction.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 19 — CONSTRUCTION

CHAPITRE 1 — IDENTITÉ DU PROJET, TERRAIN, MAÎTRE D'OUVRAGE, ENTREPRISES, PLANS, AUTORISATIONS, MATÉRIAUX, LOTS ET PASSEPORT NUMÉRIQUE CONSTRUCTION

1. Objet du chapitre

Le Point 19 — Construction transpose Authenticity Plus© / Deep Authenticity© aux projets de bâtiment et d'infrastructure. Il crée un Passeport Numérique Construction reliant projet, terrain, acteurs, plans, autorisations, matériaux, lots, travaux, contrôles et preuves documentaires.

2. Mission sectorielle

La mission est de rendre vérifiable la continuité documentaire d'un ouvrage depuis sa conception jusqu'à sa livraison et son exploitation. AP organise les preuves sans se substituer aux architectes, ingénieurs, bureaux de contrôle, laboratoires, entreprises ou autorités compétentes.

3. Identité du projet

Chaque projet dispose d'une identité distincte : nom, type d'ouvrage, localisation, référence, maître d' ouvrage, phase, dates et autres caractéristiques documentées. Les versions successives du projet restent historisées.

4. Terrain et parcelle

Parcelle, emprise, références cadastrales ou foncières et données de localisation peuvent être reliées au projet lorsque disponibles. Une donnée déclarée reste distincte d'un titre ou document officiel.

5. Maître d'ouvrage

Le maître d'ouvrage ou donneur d'ordre est identifié avec son rôle et son périmètre. Propriété du terrain, financement et maîtrise d'ouvrage ne doivent pas être automatiquement confondus.

6. Maîtrise d'œuvre

Architectes, ingénieurs, bureaux d'études et autres concepteurs peuvent être reliés aux documents qu' ils produisent. Chaque plan, note ou modèle conserve son auteur, sa date et sa version.

7. Entreprises et sous-traitants

Entreprise générale, lots techniques, sous-traitants et fournisseurs disposent d'identités et de responsabilités distinctes. Les interventions sont attribuées aux acteurs réellement documentés.

8. Plans et versions

Plans architecturaux, structurels, réseaux, détails et modèles numériques doivent être versionnés. Un plan remplacé ne disparaît pas de l'historique ; le système indique quelle version est applicable.

9. Autorisations

Permis, autorisations administratives, visas ou autres documents officiels peuvent être reliés au projet avec leur émetteur, leur date et leur statut. AP ne crée ni n'accorde lui-même une autorisation.

10. Matériaux

Béton, acier, bois, verre, isolants, câbles, équipements et autres matériaux peuvent être identifiés par produit, fabricant, référence, certification ou lot lorsque ces données existent.

11. Lots de matériaux

Le lot permet de relier une livraison ou une mise en œuvre à une origine et à des documents déterminés. Cette granularité facilite la traçabilité en cas de défaut, rappel ou investigation.

12. Certificats et fiches techniques

Certificats, déclarations de performance, fiches techniques, rapports d'essais ou autres documents restent attribués à leur émetteur. Un fichier fourni par un acteur n'est pas automatiquement validé par son auteur présumé.

13. Réception des matériaux

À la livraison, quantité, lot, fournisseur, date, site et documents peuvent être enregistrés. Une réception physique ne signifie pas automatiquement conformité technique.

14. QR Code dynamique

Matériau, équipement, zone, local technique ou élément critique peut être relié à un QR Code dynamique. Le scan ouvre les informations autorisées et le statut courant sans exposer les documents confidentiels.

15. Deep Authenticity©

Deep Authenticity© peut confronter identifiants, plans applicables, lots, certificats, photographies, livraisons, contrôles et contexte de chantier. Une incohérence déclenche une vérification, non une conclusion automatique de non-conformité.

16. Photographies de chantier

Photographies datées des travaux, matériaux, ouvrages cachés et étapes clés peuvent enrichir la preuve de réalisation. Elles restent liées à leur contexte et ne remplacent pas les contrôles techniques requis.

17. BIM et maquette numérique

Lorsque le projet utilise une maquette BIM, objets, équipements et zones peuvent être reliés aux passeports et documents correspondants. La version du modèle doit rester identifiable.

18. Confidentialité et droits d’accès

Plans sensibles, données de sécurité, contrats, prix, informations personnelles et documents internes ne sont accessibles qu’aux acteurs habilités. La vue publique ou propriétaire applique la minimisation.

19. AP Ledger

Empreintes minimales des versions de plans, autorisations, certificats, livraisons, contrôles et événements critiques peuvent être ancrées dans AP Ledger. Les fichiers techniques complets restent hors des couches publiques ou irréversibles.

20. Critères d’acceptation et conclusion

Le modèle est acceptable si projet, terrain et acteurs restent distincts ; si les plans sont versionnés ; si les autorisations conservent leur émetteur ; si matériaux et lots restent traçables ; si une réception ne vaut pas automatiquement conformité ; si BIM et QR conservent leur version ; et si les données sensibles sont protégées. Le Passeport Numérique Construction devient ainsi la mémoire vérifiable de l’ouvrage dès sa conception.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 19 — CONSTRUCTION

CHAPITRE 2 — CHANTIER, JOURNAL DES TRAVAUX, GÉOLOCALISATION, OUVRAGES CACHÉS, CONTRÔLES, ESSAIS, INSPECTIONS, NON-CONFORMITÉS, CORRECTIONS ET RÉCEPTION

1. Objet du chapitre

Ce chapitre définit la continuité de preuve pendant l'exécution du chantier : journal des travaux, localisation des événements, ouvrages cachés, contrôles, essais, inspections, non-conformités, corrections, réserves et réception.

2. Ouverture du chantier

L'ouverture opérationnelle peut être reliée au projet, au site, aux acteurs autorisés, aux plans applicables et aux documents disponibles. AP conserve les références sans se substituer aux formalités réglementaires.

3. Journal numérique des travaux

Les événements importants peuvent être enregistrés chronologiquement : travaux réalisés, zones concernées, équipes ou entreprises, documents, observations, photos et contrôles. Chaque entrée conserve son auteur et son horodatage.

4. Géolocalisation

Lorsqu'elle est pertinente et autorisée, la géolocalisation peut confirmer qu'un scan, une photographie ou une opération a été enregistré à proximité du chantier ou de la zone attendue. Elle constitue un indice contextuel, non une preuve absolue de conformité.

5. Zones et ouvrages

Bâtiment, niveau, local, axe, ouvrage ou équipement peut disposer d'une référence permettant de rattacher précisément les événements et documents au bon emplacement.

6. Ouvrages cachés

Ferraillage, réseaux, étanchéité, réservations, gaines et autres éléments destinés à être recouverts peuvent être photographiés et documentés avant fermeture. Le passeport conserve ainsi une mémoire de ce qui ne sera plus visible.

7. Plans applicables

Une opération doit pouvoir être reliée à la version de plan ou de modèle applicable au moment de l'exécution. Une mise à jour ultérieure ne doit pas réécrire silencieusement le contexte historique.

8. Contrôles internes

Les entreprises peuvent réaliser leurs propres contrôles et autocontrôles. Ces résultats restent clairement identifiés comme contrôles internes et ne sont pas confondus avec ceux d'un organisme indépendant.

9. Bureau de contrôle et inspection

Un bureau de contrôle, ingénieur, maître d'œuvre ou autre acteur habilité peut produire une observation ou un visa selon son rôle. Chaque avis conserve son auteur, sa date, son périmètre et ses réserves.

10. Essais de laboratoire

Essais sur béton, sols, acier, étanchéité ou autres matériaux et ouvrages peuvent être reliés aux échantillons, lots, zones, méthodes et laboratoires concernés. Un résultat n'est pas généralisé au-delà de son périmètre documenté.

11. Échantillons

Tout prélèvement ou éprouvette doit conserver autant que possible son lien avec le lot, la zone, la date et l'opérateur. Cette chaîne réduit le risque d'associer un rapport au mauvais ouvrage.

12. Non-conformité

Une divergence par rapport à un plan, une spécification, une règle ou un résultat attendu peut être enregistrée comme non-conformité ou observation selon la source compétente. AP ne détermine pas seul sa gravité technique.

13. Correction

Réparation, reprise, remplacement ou autre action corrective est reliée à la non-conformité correspondante. Le système conserve l'état initial, l'action, les preuves et la vérification de clôture.

14. Modification en cours de chantier

Une modification approuvée de conception ou d'exécution doit être versionnée avec son origine et sa date. Une modification légitime ne doit pas apparaître ultérieurement comme une divergence inexpliquée.

15. QR Code de zone

Un QR dynamique peut être associé à une zone, un local, un équipement ou un ouvrage critique. Le scan permet aux acteurs habilités d'accéder aux plans, contrôles, photos et statuts applicables.

16. Deep Authenticity© chantier

Deep Authenticity© peut confronter lieu, QR, plan applicable, lot de matériau, photos, rapports et séquence des événements. Une incohérence déclenche une vérification et reste explicable.

17. Pré-réception et réserves

Avant réception, les réserves ou travaux restant à réaliser peuvent être enregistrés avec leur zone, auteur, date et statut. La correction d'une réserve doit produire une preuve de clôture.

18. Réception

La réception de l'ouvrage ou d'une partie de l'ouvrage est reliée au document et aux acteurs compétents. AP enregistre l'événement mais ne prononce pas lui-même la réception juridique ou technique.

19. AP Ledger et confidentialité

Empreintes minimales des plans applicables, ouvrages cachés, contrôles, non-conformités, corrections et réception peuvent être ancrées dans AP Ledger. Plans sensibles, contrats, prix et informations de sécurité restent protégés.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si chaque événement est attribuable ; si la géolocalisation reste un indice ; si les ouvrages cachés sont documentables avant fermeture ; si contrôles internes et indépendants restent distincts ; si les essais restent liés aux échantillons ; si les corrections conservent l'état antérieur ; et si la réception provient des acteurs compétents. Le Passeport Construction devient ainsi le journal vérifiable de l'exécution réelle de l'ouvrage.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 19 — CONSTRUCTION

CHAPITRE 3 — LIVRAISON DE L'OUVRAGE, DOE NUMÉRIQUE, ÉQUIPEMENTS, GARANTIES, MAINTENANCE, INTERVENTIONS, SINISTRES, RÉNOVATION ET PASSEPORT CONSTRUCTION SUR LE CYCLE DE VIE

1. Objet du chapitre

Ce chapitre prolonge le Passeport Numérique Construction après l'exécution du chantier. Il organise la livraison de l'ouvrage, le dossier des ouvrages exécutés, les équipements, garanties, opérations de maintenance, interventions, incidents, sinistres, rénovations et modifications pendant toute la vie du bâtiment.

2. Passage du chantier à l'exploitation

La réception et la livraison ouvrent une nouvelle phase du passeport. Les données utiles de conception et d'exécution sont transmises aux acteurs habilités de l'exploitation sans supprimer l' historique du chantier.

3. DOE numérique

Le dossier des ouvrages exécutés peut réunir plans conformes à l'exécution, notices, fiches techniques, rapports, essais, certificats, schémas, références d'équipements et autres documents remis. Chaque document conserve sa version et sa source.

4. Plans conformes à l'exécution

Les plans finaux doivent rester distincts des plans initiaux et des versions intermédiaires. Une modification ultérieure du bâtiment produit une nouvelle version sans effacer l'état livré.

5. Identité des équipements

Ascenseur, chaudière, pompe, groupe électrogène, tableau électrique, système de sécurité, climatisation ou autre équipement peut recevoir une identité reliée au bâtiment, à sa zone, au fabricant, au modèle et au numéro disponible.

6. QR Code équipement

Un QR dynamique placé sur un équipement ou dans un local technique peut ouvrir la fiche autorisée : identité, documentation, historique de maintenance, statut et dernières interventions.

7. Garantie

Garantie fabricant, garantie contractuelle ou autre engagement documenté conserve son émetteur, sa période, son périmètre et ses conditions. AP ne prolonge ni ne crée automatiquement une garantie.

8. Maintenance préventive

Inspection, entretien périodique, remplacement programmé ou contrôle peut être enregistré avec l'acteur, la date, l'équipement et les documents associés. Le système permet de distinguer opération prévue et opération effectivement réalisée.

9. Maintenance corrective

Une panne ou anomalie peut déclencher une intervention corrective. Diagnostic, pièces remplacées, travaux, date de remise en service et preuves disponibles enrichissent l'historique.

10. Pièces remplacées

Un composant remplacé ne doit pas disparaître de l'histoire de l'équipement. Référence de la pièce retirée, nouvelle pièce, intervenant et date peuvent être conservés lorsque disponibles.

11. Intervenants

Exploitant, mainteneur, entreprise spécialisée, fabricant, bureau de contrôle ou autre acteur dispose d'un rôle défini. Une intervention reste attribuée à celui qui l'a réellement documentée.

12. Contrôles périodiques

Les contrôles réglementaires ou techniques périodiques peuvent être reliés à l'équipement ou à l'ouvrage avec leur organisme, date, rapport et statut. AP ne remplace pas l'organisme de contrôle.

13. Incident

Fuite, panne, fissure, défaillance, dysfonctionnement ou autre incident peut être enregistré avec sa zone, sa date, ses observations et les mesures prises. L'enregistrement n'établit pas automatiquement la cause.

14. Sinistre

Incendie, dégât des eaux, événement climatique ou autre sinistre documenté peut ouvrir un dossier reliant constats, expertises, réparations et décisions. Les responsabilités restent déterminées par les acteurs compétents.

15. Investigation et cause

Rapports d'experts, données de capteurs, historique de maintenance, matériaux et photographies peuvent contribuer à rechercher une cause. Deep Authenticity© organise la provenance des éléments sans produire seul une conclusion technique ou juridique.

16. Rénovation

Une rénovation crée une nouvelle phase du passeport. Les zones modifiées, nouveaux matériaux, équipements, plans et entreprises sont reliés à l'état antérieur afin de préserver la généalogie du bâtiment.

17. Extension et transformation

Extension, changement d'usage, restructuration ou modification importante doit être documenté comme évolution de l'ouvrage et non comme remplacement silencieux de son identité historique.

18. BIM exploitation et Offline

La maquette BIM peut servir de point d'accès aux équipements et historiques. En zone technique sans réseau, un mode Offline peut fournir les dernières données signées disponibles avec leur date de synchronisation.

19. AP Ledger et confidentialité

Empreintes minimales du DOE, remplacements critiques, contrôles, sinistres et rénovations peuvent être ancrées dans AP Ledger. Plans de sécurité, accès techniques, données personnelles, contrats, prix et dossiers sensibles restent protégés.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si l'état livré reste conservé ; si le DOE est versionné ; si chaque équipement possède son historique ; si garantie et maintenance ne sont pas confondues ; si les pièces remplacées restent traçables ; si un incident ne devient pas automatiquement une cause ; et si les rénovations préservent la généalogie de l'ouvrage. Le Passeport Construction devient ainsi la mémoire technique vérifiable du bâtiment pendant toute sa durée de vie.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 19 — CONSTRUCTION

CHAPITRE 4 — FRAUDE DOCUMENTAIRE, FAUX MATÉRIAUX, FAUX CERTIFICATS, SUBSTITUTION SUR CHANTIER, QR CODES CLONÉS, ANOMALIES BIM, RESPONSABILITÉS, LITIGES ET INVESTIGATION

1. Objet du chapitre

Ce chapitre définit la gestion des incohérences, fraudes présumées et litiges dans le secteur Construction : documents falsifiés, matériaux ou équipements substitués, certificats non authentifiés, QR Codes clonés, incohérences BIM, travaux non documentés et divergences entre l'ouvrage réel et son dossier numérique.

2. Principe de non-accusation automatique

Une anomalie détectée par Authenticity Plus© / Deep Authenticity© déclenche une vérification. Elle ne constitue pas, à elle seule, une preuve de fraude, de faute professionnelle ou de responsabilité juridique.

3. Fraude documentaire présumée

Plan modifié, rapport altéré, faux visa, faux procès-verbal ou document attribué à tort à un acteur peut être signalé. Empreinte, version, auteur présumé, date et source contribuent à l'investigation.

4. Faux certificat

Un certificat de matériau, équipement ou essai peut être copié, modifié ou associé au mauvais lot. Le système confronte document, émetteur, référence, lot et autres preuves disponibles.

5. Faux matériau ou produit

Un produit livré peut ne pas correspondre à la marque, référence, performance ou origine déclarée. Cette divergence est documentée et transmise aux acteurs compétents pour vérification.

6. Substitution sur chantier

Un matériau ou équipement prévu peut être remplacé par un autre. Une substitution approuvée doit être documentée et versionnée ; une substitution non expliquée produit un signal d'investigation.

7. Lots et traçabilité

Le lien entre fournisseur, livraison, lot, zone de mise en œuvre et documents permet de rechercher l'étendue d'une anomalie sans supposer que tout le chantier est affecté.

8. QR Code cloné

La copie d’un QR associé à un matériau ou équipement légitime sur un autre produit ne doit pas reproduire son statut. Deep Authenticity© confronte QR, lot, caractéristiques, localisation et historique disponibles.

9. Photographies et preuves terrain

Les photographies datées peuvent contribuer à comparer ce qui était prévu, livré et réellement mis en œuvre. Elles restent des éléments de preuve contextualisés et non une expertise technique autonome.

10. Anomalie BIM

Une divergence entre maquette BIM, plan applicable, équipement installé et données de terrain peut être signalée. Le système doit identifier la version de chaque source avant de conclure à une incohérence.

11. Données falsifiées ou supprimées

Une tentative de modification rétroactive, suppression ou remplacement silencieux d’un événement critique doit être détectable par la gestion des versions, les journaux d’audit et les empreintes d’ intégrité.

12. Non-conformité et fraude

Une non-conformité technique peut résulter d’une erreur, d’une modification, d’un défaut ou d’autres causes. Elle ne doit pas être automatiquement qualifiée de fraude.

13. Mise sous vérification

Un lot, équipement, document ou zone peut recevoir un statut temporaire de vérification. Le motif, l’ auteur, la date et les conditions de levée doivent rester traçables.

14. Dossier d’investigation

Le dossier peut réunir plans, BIM, commandes, livraisons, certificats, photos, essais, contrôles, échanges et interventions. Chaque élément conserve sa provenance et son niveau de preuve.

15. Responsabilités

Maître d’ouvrage, concepteur, entreprise, fournisseur, sous-traitant, laboratoire et contrôleur ont des rôles différents. AP documente les actions et sources mais n’attribue pas automatiquement une responsabilité juridique.

16. Litiges

En cas de désaccord, les parties peuvent disposer de vues contrôlées d’un même historique de preuves. Les positions contradictoires restent attribuées à leurs auteurs.

17. Expertise contradictoire

Plusieurs expertises peuvent coexister. Chaque rapport conserve auteur, date, périmètre, hypothèses et conclusions, sans suppression automatique de l’avis précédent.

18. Correction et clôture

Lorsqu’une anomalie est corrigée ou une suspicion levée, le statut actif est mis à jour. L’historique d’ audit conserve la séquence de vérification avec les droits d’accès appropriés.

19. AP Ledger et confidentialité

Empreintes minimales de documents critiques, alertes, changements de statut, expertises et décisions peuvent être ancrées dans AP Ledger. Dossiers de litige, contrats, prix, identités privées et données de sécurité restent protégés.

20. Critères d’acceptation et conclusion

Le modèle est acceptable si anomalie et fraude restent distinctes ; si une substitution approuvée est historisée ; si un QR cloné ne reproduit pas la preuve ; si les versions BIM sont identifiées ; si les responsabilités ne sont pas attribuées automatiquement ; si les expertises contradictoires restent visibles ; et si toute correction conserve sa trace. Deep Authenticity© devient ainsi une infrastructure de convergence des preuves pour l’investigation Construction.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 19 — CONSTRUCTION

CHAPITRE 5 — GOUVERNANCE DES ACTEURS, MAÎTRE D'OUVRAGE, ARCHITECTES, INGÉNIEURS, ENTREPRISES, FOURNISSEURS, LABORATOIRES, AUTORITÉS, ASSUREURS, CYBERSÉCURITÉ, INTEROPÉRABILITÉ ET AP LEDGER

1. Objet du chapitre

Ce chapitre définit la gouvernance du Passeport Numérique Construction et la séparation des responsabilités entre les acteurs participant à la conception, l'exécution, le contrôle, la livraison et l' exploitation de l'ouvrage.

2. Identité des acteurs

Chaque personne ou organisation intervient sous une identité et un rôle déterminés. Une même organisation peut cumuler plusieurs fonctions, mais chaque action reste attribuée au rôle exercé au moment de l'événement.

3. Maître d'ouvrage

Le maître d'ouvrage peut administrer le projet, habiliter certains acteurs et accéder aux informations correspondant à ses droits. AP ne lui attribue pas automatiquement la propriété du terrain ni les responsabilités d'autres intervenants.

4. Architectes et maîtrise d'œuvre

Architectes et maîtres d'œuvre peuvent produire, valider ou commenter des documents selon leurs missions. Chaque plan, instruction, visa ou observation conserve son auteur, sa date et sa version.

5. Ingénieurs et bureaux d'études

Les ingénieurs et bureaux d'études restent responsables de leurs propres documents et calculs selon leur mission. Une modification par un tiers ne doit pas pouvoir être présentée comme leur version originale.

6. Entreprises et sous-traitants

Entreprise générale, entreprises de lots et sous-traitants disposent de périmètres distincts. Travaux, autocontrôles, livraisons et corrections sont rattachés à l'acteur réellement documenté.

7. Fournisseurs et fabricants

Fournisseurs et fabricants peuvent être sources de références produits, lots, fiches techniques et certificats. La provenance de chaque donnée permet de distinguer information fabricant, fournisseur et déclaration de chantier.

8. Laboratoires

Les laboratoires produisent des résultats associés à des échantillons, méthodes et rapports. Leurs comptes ne doivent pas permettre de modifier les données de chantier hors de leur périmètre.

9. Bureaux de contrôle et inspecteurs

Les acteurs de contrôle disposent de droits leur permettant de consulter les éléments nécessaires et d'émettre leurs propres observations. Ils ne doivent pas pouvoir réécrire les preuves produites par les entreprises.

10. Autorités compétentes

Permis, autorisations, décisions et autres statuts officiels restent attribués à leur autorité émettrice. AP peut les relier au projet mais ne les crée ni ne les révoque de sa propre initiative.

11. Assureurs et experts

Assureurs et experts peuvent recevoir, avec habilitation, des éléments liés à l'ouvrage, aux sinistres, contrôles ou interventions. Les conditions contractuelles, responsabilités et indemnisations restent hors de la décision d'AP.

12. Exploitant et mainteneur

Après livraison, exploitants et mainteneurs disposent d'accès adaptés aux équipements, DOE, historiques et interventions. Ils ne peuvent pas modifier silencieusement les preuves de la phase chantier.

13. Séparation des rôles

Concevoir, construire, fournir, tester, contrôler, réceptionner, assurer et maintenir sont des fonctions distinctes. Le système applique le moindre privilège, la séparation des habilitations et la révocation des droits.

14. Validation à plusieurs niveaux

Certaines opérations critiques peuvent exiger plusieurs validations : auteur du document, responsable habilité, contrôle ou réception. Cette gouvernance réduit le risque qu'un compte unique puisse modifier seul une preuve critique.

15. Confidentialité

Plans sensibles, accès techniques, contrats, prix, données personnelles, informations de sécurité et dossiers de litige sont protégés. Chaque acteur n'accède qu'aux informations nécessaires à sa mission.

16. Cybersécurité

Authentification renforcée, contrôle des sessions, gestion des terminaux, journalisation, révocation et protection des interfaces sont appliqués aux opérations sensibles. Les comptes institutionnels doivent être séparés des identités personnelles lorsque nécessaire.

17. Interopérabilité

BIM, GED, ERP, logiciels de chantier, laboratoires, fabricants, maintenance et systèmes publics autorisés peuvent échanger avec AP. Toute donnée importée conserve source, version, horodatage et niveau d'autorité.

18. Continuité numérique

Le Passeport Construction doit rester exploitable malgré changement d'entreprise, de mainteneur, de propriétaire ou de logiciel. Les preuves historiques ne doivent pas dépendre de la survie d'un fournisseur unique.

19. Audit et AP Ledger

Création et validation de documents, modifications critiques, contrôles, non-conformités, corrections, réceptions et événements majeurs peuvent produire des traces d'audit et des empreintes minimales dans AP Ledger. Les données techniques sensibles restent hors des couches publiques.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si chaque acteur reste limité à son rôle ; si aucune partie ne peut réécrire seule les preuves d'une autre ; si les habilitations sont révocables ; si les données importées conservent leur provenance ; si la confidentialité est appliquée par mission ; et si la continuité numérique survit aux changements d'acteurs et de systèmes. Cette gouvernance fournit le socle nécessaire à la clôture fonctionnelle de l'application Construction.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 19 — CONSTRUCTION

CHAPITRE 6 — SYNTHÈSE FONCTIONNELLE, CRITÈRES D'ACCEPTATION ET CLÔTURE DE L'APPLICATION CONSTRUCTION

1. Objet du chapitre

Ce chapitre clôt le Point 19 — Construction. Il consolide l'identité du projet, les acteurs, plans, autorisations, matériaux, lots, chantier, contrôles, ouvrages cachés, DOE, équipements, maintenance, incidents, rénovations, investigations, gouvernance, cybersécurité, interopérabilité et AP Ledger.

2. Mission consolidée

Le Passeport Numérique Construction constitue la mémoire vérifiable de l'ouvrage depuis sa conception jusqu'à son exploitation et ses transformations. Authenticity Plus© organise la continuité des preuves sans se substituer aux professionnels ni aux autorités compétentes.

3. Identité du projet et du terrain

Projet, terrain, parcelle, maître d'ouvrage, propriétaire et localisation restent des objets ou rôles distincts. Les références officielles conservent leur source et les données déclarées ne sont jamais transformées automatiquement en titres officiels.

4. Acteurs et responsabilités

Architectes, ingénieurs, entreprises, sous-traitants, fournisseurs, fabricants, laboratoires, bureaux de contrôle, assureurs, exploitants et mainteneurs disposent de rôles séparés. Chaque action reste attribuée à son auteur et à son périmètre.

5. Plans, BIM et versions

Plans, modèles BIM, notes et documents techniques sont versionnés. La version applicable à un événement de chantier doit pouvoir être retrouvée, tandis que les versions remplacées restent dans l'historique.

6. Autorisations et documents officiels

Permis, autorisations, visas et décisions peuvent être reliés au projet avec leur émetteur, date et statut. AP les restitue et les protège contre les altérations sans les créer lui-même.

7. Matériaux et lots

Matériaux, équipements, fabricants, références, lots, certificats, livraisons et zones de mise en œuvre peuvent être reliés. La réception physique d'un produit reste distincte de sa conformité technique.

8. Journal numérique du chantier

Travaux, observations, photographies, livraisons, contrôles et événements importants forment une chronologie attribuable et horodatée. Les modifications ultérieures ne doivent pas réécrire silencieusement cette chronologie.

9. Ouvrages cachés

Ferraillages, réseaux, étanchéité, gaines et autres éléments recouverts peuvent être documentés avant fermeture. Leur localisation et leur contexte permettent de conserver une mémoire technique durable de l'invisible.

10. Contrôles, essais et échantillons

Autocontrôles, inspections indépendantes et essais de laboratoire restent distingués. Les résultats sont reliés à leur échantillon, lot, zone, méthode et auteur et ne sont pas généralisés au-delà de leur périmètre.

11. Non-conformités et corrections

Une non-conformité, réserve ou observation peut être reliée à une correction et à sa preuve de clôture. L'état initial reste conservé afin que la correction ne supprime pas l'historique.

12. Réception, livraison et DOE

La réception et la livraison ouvrent la phase d'exploitation. Le DOE numérique, les plans conformes à l'exécution, notices, certificats et références d'équipements conservent leurs versions et sources.

13. Équipements et maintenance

Chaque équipement critique peut disposer d'une identité, d'un QR dynamique et d'un historique d'entretien, de panne, de réparation et de pièces remplacées. Garantie et maintenance restent des notions distinctes.

14. Cycle de vie et rénovation

Incident, sinistre, transformation, extension ou rénovation produit une nouvelle phase du passeport. L'état antérieur reste accessible afin de préserver la généalogie technique complète du bâtiment.

15. Deep Authenticity©

Deep Authenticity© confronte QR, localisation autorisée, plans, BIM, lots, certificats, photographies, essais, contrôles et séquences d'événements. Il détecte des incohérences explicables sans produire seul un verdict de conformité ou de responsabilité.

16. Fraude, substitution et litiges

Document falsifié, certificat incohérent, substitution non documentée, QR cloné ou divergence BIM déclenche une vérification. Non-conformité et fraude restent distinctes, et les responsabilités juridiques ne sont jamais attribuées automatiquement par AP.

17. Gouvernance et validation

Les droits suivent le principe du moindre privilège. Les opérations critiques peuvent exiger plusieurs validations et aucun acteur ne doit pouvoir réécrire seul les preuves produites par un autre acteur.

18. Confidentialité, cybersécurité et interopérabilité

Plans sensibles, accès techniques, contrats, prix, données personnelles et dossiers de sécurité restent protégés. Les échanges avec BIM, GED, ERP, laboratoires, fabricants et maintenance conservent source, version, horodatage et niveau d'autorité.

19. AP Ledger et critères d'acceptation

AP Ledger peut ancrer des empreintes minimales de versions, autorisations, certificats, contrôles, non-conformités, corrections, réceptions et événements critiques. Le modèle est acceptable si les preuves restent attribuables, versionnées, auditables et protégées, sans publier les données techniques ou personnelles sensibles.

20. Clôture du Point 19 — Construction

Le Point 19 — Construction est désormais fonctionnellement défini : projet, terrain, acteurs, plans, BIM, autorisations, matériaux, lots, chantier, géolocalisation contextuelle, ouvrages cachés, contrôles, essais, non-conformités, réception, DOE, équipements, maintenance, sinistres, rénovation, fraude documentaire, QR clonés, investigation, gouvernance, confidentialité, cybersécurité, interopérabilité, audit et AP Ledger. Le Volume IV peut désormais poursuivre avec le Point 20 — Smart City.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 20 — SMART CITY

CHAPITRE 1 — IDENTITÉ NUMÉRIQUE DE LA VILLE, INFRASTRUCTURES, ÉQUIPEMENTS URBAINS, CAPTEURS, SERVICES, QR CODES DYNAMIQUES ET PASSEPORT NUMÉRIQUE SMART CITY

1. Objet du chapitre

Le Point 20 — Smart City transpose Authenticity Plus© / Deep Authenticity© à l'espace urbain. Il crée un Passeport Numérique Smart City reliant infrastructures, équipements, capteurs, services, opérateurs, interventions et preuves techniques.

2. Mission sectorielle

La mission est de rendre vérifiable l'identité et le statut des actifs urbains tout au long de leur cycle de vie, sans transformer la Smart City en dispositif de surveillance généralisée des habitants.

3. Identité numérique de la ville

La ville ou collectivité peut disposer d'une identité institutionnelle reliée à ses zones, quartiers, réseaux, équipements et services. Les compétences de chaque organisme restent distinctes.

4. Identité des actifs urbains

Lampadaire, feu de circulation, borne, station, caméra autorisée, pompe, capteur, mobilier urbain ou autre équipement peut recevoir une identité unitaire avec type, fabricant, modèle, zone et statut.

5. Infrastructures

Voirie, ponts, tunnels, réseaux, stations, bâtiments publics et autres infrastructures peuvent disposer de passeports reliés aux plans, inspections, interventions et responsables habilités.

6. Géolocalisation

La position d'un actif peut contribuer à son identité et à sa vérification. Les coordonnées sensibles ou les informations susceptibles de créer un risque de sécurité peuvent être restreintes.

7. QR Code dynamique

Un QR dynamique peut être placé sur un équipement ou un point de service. Le scan fournit une vue adaptée : identification, service public, signalement, maintenance ou informations techniques selon les droits du lecteur.

8. Deep Authenticity©

Deep Authenticity© peut confronter QR, identité de l'actif, localisation, fabricant, historique d' intervention, capteurs et statut. Une incohérence déclenche une vérification plutôt qu'un verdict automatique.

9. Capteurs IoT

Les capteurs urbains peuvent produire des mesures reliées à leur identité, calibration, emplacement, horodatage et opérateur. Une donnée de capteur sans provenance technique suffisante ne doit pas être traitée comme une vérité absolue.

10. Identité du capteur

Numéro, type, fabricant, firmware, certificat numérique et historique de maintenance peuvent contribuer à identifier un capteur et à détecter une substitution ou une source inconnue.

11. Données et qualité

Les données urbaines doivent conserver leur source, période, unité, qualité et éventuelles corrections. Une valeur corrigée ne supprime pas nécessairement la trace de la mesure initiale.

12. Services urbains

Éclairage, mobilité, stationnement, déchets, eau, énergie, sécurité opérationnelle et autres services peuvent utiliser le passeport pour relier actifs, interventions et niveaux de service.

13. Signalement citoyen

Un habitant peut scanner un QR pour signaler un équipement défectueux ou une anomalie. Le signalement reste distinct d'un diagnostic technique et peut être transmis au service compétent.

14. Intervention

Maintenance, réparation, remplacement, inspection ou mise à jour logicielle peut être enregistrée avec acteur, date, actif et preuve disponible. L'état avant et après intervention reste traçable.

15. Jumeau numérique

Un jumeau numérique ou modèle urbain peut relier les passeports des infrastructures et équipements. Chaque donnée ou modèle conserve sa version afin d'éviter de confondre état simulé et état réellement observé.

16. Online et Offline

Online fournit le statut courant. En zone sans réseau, une preuve signée mise en cache peut permettre une consultation Offline avec indication explicite de la date de dernière synchronisation.

17. Vie privée

Le système privilégie l'identité des actifs et des services plutôt que le suivi individuel des citoyens. Les données personnelles, déplacements et identifiants individuels ne doivent pas être collectés sans nécessité, base légitime et protections appropriées.

18. Cybersécurité

Comptes, capteurs, passerelles, QR, API et plateformes urbaines doivent être authentifiés, segmentés, journalisés et révocables. Un équipement compromis doit pouvoir être isolé sans perdre son historique.

19. AP Ledger

Empreintes minimales d'identité d'actif, configuration, maintenance, calibration, remplacement et événements critiques peuvent être ancrées dans AP Ledger. Les flux de données massifs et informations sensibles restent hors des couches irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si chaque actif possède une identité vérifiable ; si le QR cloné ne suffit pas ; si capteurs et mesures conservent leur provenance ; si un signalement citoyen reste distinct d'un diagnostic ; si le jumeau numérique est versionné ; si la vie privée est protégée ; et si AP Ledger ne reçoit que les empreintes nécessaires. Le Passeport Smart City devient ainsi une mémoire opérationnelle vérifiable de la ville et de ses infrastructures.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 20 — SMART CITY

CHAPITRE 2 — MOBILITÉ URBAINE, TRANSPORTS PUBLICS, ROUTES, STATIONNEMENT, FEUX INTELLIGENTS, BORNES, VÉHICULES DE SERVICE, GÉOLOCALISATION ET CONTINUITÉ ONLINE/OFFLINE

1. Objet du chapitre

Ce chapitre applique le Passeport Numérique Smart City aux systèmes de mobilité : transports publics, routes, stationnement, feux, bornes, stations et véhicules de service. L'objectif est de vérifier l'identité des actifs et la provenance des opérations sans suivre inutilement les déplacements individuels.

2. Identité des réseaux de mobilité

Lignes, stations, arrêts, axes routiers, parkings et zones de mobilité peuvent disposer d'identités reliées à l'autorité, à l'opérateur et aux actifs techniques correspondants.

3. Transport public

Bus, tramway, métro, navette ou autre véhicule public peut recevoir un passeport reliant identifiant de flotte, opérateur, modèle, maintenance, inspections et statut de service.

4. Véhicules de service

Véhicules municipaux, maintenance, collecte, intervention ou autres flottes publiques peuvent être vérifiés par leur identité et leur statut. L'identité professionnelle de l'équipage n'est exposée que lorsque nécessaire et autorisée.

5. QR Code dynamique

Un QR dynamique sur un véhicule, arrêt, station ou équipement peut donner accès aux informations publiques et techniques autorisées : identité, opérateur, statut, service ou signalement.

6. Géolocalisation de cohérence

Lorsqu'elle est nécessaire, la position du smartphone ou du terminal peut être comparée à celle de l' actif scanné afin de confirmer une cohérence de proximité. Cette donnée doit être minimisée et ne devient pas un historique permanent du déplacement de l'utilisateur.

7. Routes et ouvrages

Chaussées, ponts, tunnels, signalisation et équipements routiers peuvent être reliés aux inspections, travaux, restrictions et historiques d'intervention.

8. Feux intelligents

Un contrôleur ou feu de circulation dispose d'une identité, d'une localisation, d'une configuration et d' un historique technique. Les paramètres opérationnels sensibles restent réservés aux acteurs habilités.

9. Bornes et stations

Borne de recharge, station de vélos, stationnement, information voyageurs ou autre point de service peut être identifié et relié à son opérateur, à sa maintenance et à son état.

10. Stationnement

Parking, zone, horodateur, capteur ou borne peut disposer d'un passeport. Une information d' occupation ou de disponibilité est horodatée et ne doit pas être présentée comme permanente.

11. Capteurs de mobilité

Boucles, radars de comptage, caméras autorisées ou autres capteurs peuvent produire des données de trafic. Leur identité, calibration, configuration et statut contribuent à la confiance dans les mesures.

12. Données agrégées

Les données de mobilité destinées à l'analyse urbaine doivent privilégier l'agrégation et la minimisation. Le besoin de connaître un flux de circulation ne justifie pas automatiquement l' identification des personnes.

13. Maintenance et intervention

Panne, inspection, réparation, remplacement ou mise à jour d'un actif de mobilité est enregistré avec l' acteur, la date et le statut avant/après lorsque disponibles.

14. Deep Authenticity©

Deep Authenticity© confronte QR, actif, localisation autorisée, opérateur, historique, capteurs et statut. Un actif déplacé, substitué ou incohérent peut déclencher une vérification.

15. Continuité Online

En ligne, le scan consulte le statut courant : actif en service, maintenance,restriction, retrait ou autre état publié. Les changements critiques sont synchronisés avec les systèmes autorisés.

16. Continuité Offline

Sans réseau, le terminal peut vérifier une preuve signée et mise en cache, avec date de dernière synchronisation. Les informations susceptibles d'évoluer rapidement sont clairement signalées comme potentiellement non actuelles.

17. Signalement citoyen

Un usager peut signaler une borne hors service, un feu défectueux, une signalisation endommagée ou un autre problème. Le signalement est transmis au service compétent sans devenir automatiquement un diagnostic.

18. Cybersécurité des systèmes de mobilité

Contrôleurs, passerelles, terminaux, véhicules connectés, QR et API doivent être authentifiés, segmentés et révocables. Les fonctions de commande critiques ne doivent pas être accessibles depuis une simple interface publique de scan.

19. AP Ledger et confidentialité

Empreintes minimales d'identité, maintenance, calibration, remplacement et changements de statut critiques peuvent être ancrées dans AP Ledger. Trajets individuels, identités d'usagers et données opérationnelles sensibles restent hors des couches publiques ou irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si actifs et opérateurs sont vérifiables ; si la géolocalisation sert à la cohérence sans créer un suivi permanent ; si les données de mobilité privilégient l'agrégation ; si Offline indique sa fraîcheur ; si les commandes critiques sont isolées du QR public ; et si les interventions restent auditables. Le Passeport Smart City apporte ainsi une continuité de confiance aux systèmes de mobilité urbaine.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 20 — SMART CITY

CHAPITRE 3 — ÉNERGIE, ÉCLAIRAGE PUBLIC, EAU URBAINE, DÉCHETS, ENVIRONNEMENT, QUALITÉ DE L'AIR, CAPTEURS, ALERTES ET MAINTENANCE PRÉDICTIVE

1. Objet du chapitre

Ce chapitre applique le Passeport Numérique Smart City aux services urbains essentiels et environnementaux : énergie, éclairage public, eau, déchets, qualité de l'air, capteurs, alertes, interventions et maintenance prédictive.

2. Principe de continuité opérationnelle

Chaque actif critique peut conserver une identité, un emplacement, un opérateur, un historique technique et un statut. L'objectif est de relier la donnée à l'équipement qui l'a produite et aux interventions qui l'ont modifié.

3. Énergie urbaine

Postes, armoires, compteurs techniques, installations renouvelables, batteries ou autres actifs énergétiques peuvent être reliés à leurs références, inspections, maintenances et statuts, avec protection des informations sensibles.

4. Éclairage public

Lampadaires, armoires et contrôleurs peuvent disposer d'un passeport avec localisation, type, puissance, fabricant, interventions et état. Un QR dynamique peut faciliter l'identification et le signalement d'une panne.

5. Eau urbaine

Réservoirs, pompes, vannes, conduites, compteurs techniques et autres actifs du réseau peuvent être reliés à leur identité, zone, maintenance, inspections et données autorisées.

6. Qualité de l'eau et mesures

Les mesures provenant de capteurs ou laboratoires conservent source, date, unité, méthode et périmètre. Une mesure isolée ne doit pas être généralisée à l'ensemble du réseau sans justification.

7. Déchets

Conteneurs, points de collecte, véhicules, centres ou équipements peuvent recevoir une identité permettant de documenter entretien, collecte, incidents et remplacement.

8. Environnement urbain

Bruit, température, humidité, qualité de l'air ou autres paramètres peuvent être mesurés par des capteurs identifiés. Le passeport permet de connaître l'origine technique d'une donnée environnementale.

9. Qualité de l'air

Station ou capteur de qualité de l'air conserve modèle, localisation, calibration, maintenance et statut. Une valeur publiée doit être accompagnée du contexte nécessaire à son interprétation.

10. Calibration

La calibration d'un capteur est un événement critique : organisme ou opérateur, date, méthode, résultat et prochaine échéance peuvent être enregistrés. Un capteur hors calibration peut recevoir un statut adapté.

11. Provenance des données

Chaque mesure importante doit pouvoir être reliée à un capteur, une configuration, un horodatage et une chaîne de traitement. Les données dérivées ou corrigées restent distinguées des données brutes.

12. Alertes

Seuil dépassé, panne, fuite, anomalie ou perte de communication peut générer une alerte. L'alerte constitue un signal opérationnel et non une conclusion automatique sur la cause.

13. Vérification de l'alerte

Une alerte peut être confirmée, requalifiée ou clôturée après contrôle. L'historique conserve l'alerte initiale, les vérifications et la décision de clôture.

14. Maintenance préventive

Les opérations planifiées peuvent être reliées aux actifs, calendriers et intervenants. Le système distingue maintenance prévue, commencée, réalisée, reportée ou annulée.

15. Maintenance prédictive

Les tendances de capteurs et historiques peuvent contribuer à anticiper une défaillance. Une prédiction reste un indicateur probabiliste et ne doit pas être présentée comme une panne certaine.

16. Deep Authenticity©

Deep Authenticity© confronte identité de l'actif, QR, localisation, calibration, données, alertes et interventions. Il peut détecter une source incohérente, un capteur substitué ou une chronologie anormale.

17. Signalement citoyen

Un citoyen peut signaler fuite visible, lampadaire défectueux, conteneur endommagé ou autre problème via un QR ou service associé. Le signalement reste séparé du diagnostic technique.

18. Résilience et Offline

En cas de panne réseau, les équipes peuvent utiliser des données signées mises en cache selon les besoins opérationnels. La date de dernière synchronisation est visible et les fonctions critiques suivent des procédures de continuité spécifiques.

19. AP Ledger et confidentialité

Empreintes minimales d'identité, calibration, maintenance, remplacement et alertes critiques peuvent être ancrées dans AP Ledger. Flux massifs de capteurs, plans sensibles, données personnelles et configurations de sécurité restent hors des couches irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si toute mesure conserve sa provenance ; si la calibration est traçable ; si une alerte ne devient pas automatiquement une cause ; si la maintenance prédictive reste probabiliste ; si le signalement citoyen ne devient pas un diagnostic ; si Offline affiche sa fraîcheur ; et si les données sensibles sont protégées. Le Passeport Smart City apporte ainsi une continuité de confiance aux services urbains essentiels.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 20 — SMART CITY

CHAPITRE 4 — SÉCURITÉ OPÉRATIONNELLE, INCIDENTS URBAINS, FAUX CAPTEURS, DONNÉES FALSIFIÉES, QR CODES CLONÉS, CYBERATTAQUES, RÉSILIENCE, CENTRE DE SUPERVISION ET INVESTIGATION

1. Objet du chapitre

Ce chapitre définit la protection du Passeport Numérique Smart City face aux incidents opérationnels et aux tentatives d'altération de l'identité ou des données des actifs urbains.

2. Principe de non-accusation automatique

Une anomalie, une donnée incohérente ou un équipement non reconnu déclenche une vérification. Authenticity Plus© / Deep Authenticity© ne qualifie pas automatiquement l'événement de fraude ou de cyberattaque.

3. Incident urbain

Panne, rupture de service, dysfonctionnement, dégradation ou événement affectant un actif peut ouvrir un dossier horodaté reliant équipement, zone, alertes, observations et interventions.

4. Identité de l'actif compromis

Lorsqu'un équipement est suspecté d'être compromis, son identité numérique, ses certificats, son firmware, ses dernières opérations et son historique peuvent être confrontés aux références connues.

5. Faux capteur ou substitution

Un capteur substitué, inconnu ou utilisant une identité copiée peut produire des mesures trompeuses. L'identité matérielle et numérique doit donc être confrontée à l'emplacement, à la configuration et à l' historique.

6. Données falsifiées

Une mesure modifiée, injectée ou réattribuée à une mauvaise source doit pouvoir être détectée par la provenance, les signatures, les horodatages, les contrôles de cohérence et les journaux d'audit.

7. QR Code cloné

Un QR copié sur un faux équipement ne doit pas reproduire son identité. Deep Authenticity© confronte le code à l'actif, à la localisation autorisée, au certificat numérique et au statut courant.

8. Configuration non autorisée

Une modification de configuration, de firmware ou de paramètres critiques doit être attribuable à un acteur habilité. Une divergence non expliquée déclenche une vérification.

9. Centre de supervision

Le centre de supervision peut agréger statuts, alertes et événements provenant des systèmes autorisés. Il doit distinguer données observées, alertes automatiques, diagnostics et décisions humaines.

10. Corrélation des événements

Plusieurs alertes provenant d'actifs différents peuvent être corrélées afin d'identifier un incident plus large. Une corrélation algorithmique reste une hypothèse opérationnelle tant qu'elle n'est pas confirmée.

11. Isolation d'un actif

Un actif compromis ou suspect peut être placé sous restriction ou isolé par les systèmes compétents. Le Passeport Smart City documente le statut et l'autorité de l'action sans exposer publiquement les mécanismes de commande.

12. Cyberattaque présumée

Une perturbation numérique peut provenir de causes multiples. Le système conserve les indices et les sources sans attribuer automatiquement l'incident à un auteur.

13. Continuité des services

Les servicesessentiels doivent prévoir des modes dégradés, procédures manuelles ou architectures redondantes adaptées. Le Passeport fournit les dernières informations vérifiables nécessaires aux équipes habilitées.

14. Offline sécurisé

En cas de perte de connectivité, les terminaux autorisés peuvent utiliser des données signées mises en cache. Leur ancienneté est explicitement indiquée et les opérations critiques suivent des règles spécifiques.

15. Récupération

Après incident, restauration, remplacement, reconfiguration ou remise en service est documenté. L' état antérieur et les étapes de récupération restent dans l'historique.

16. Deep Authenticity© investigation

Deep Authenticity© peut confronter identité, certificats, configuration, localisation, données, alertes, maintenance et journaux afin d'expliquer les incohérences et d'orienter l'investigation.

17. Dossier d’investigation

Le dossier peut réunir événements, journaux, versions, rapports, interventions et preuves techniques. L’ accès est strictement limité selon les rôles et les exigences de confidentialité.

18. Vie privée et proportionnalité

Une investigation sur un actif urbain ne justifie pas automatiquement l’accès aux données personnelles des citoyens. Les analyses privilégient les données techniques et minimisées nécessaires à l’incident.

19. AP Ledger

Empreintes minimales de changements de configuration, alertes critiques, mises sous restriction, remplacements et clôtures d’incident peuvent être ancrées dans AP Ledger. Les secrets techniques, journaux détaillés et données personnelles restent hors des couches irréversibles.

20. Critères d’acceptation et conclusion

Le modèle est acceptable si un faux capteur peut être détecté par convergence de preuves ; si une donnée conserve sa provenance ; si un QR cloné ne suffit pas ; si le centre de supervision distingue alerte et diagnostic ; si l’isolation est réservée aux systèmes habilités ; si Offline indique sa fraîcheur ; et si l’investigation respecte la vie privée. Le Passeport Smart City devient ainsi un socle de résilience et de confiance opérationnelle.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 20 — SMART CITY

CHAPITRE 5 — GOUVERNANCE MUNICIPALE, OPÉRATEURS, CITOYENS, DÉLÉGATAIRES, AUTORITÉS, DROITS D'ACCÈS, INTEROPÉRABILITÉ, CYBERSÉCURITÉ ET SOUVERAINETÉ DES DONNÉES URBAINES

1. Objet du chapitre

Ce chapitre définit la gouvernance institutionnelle du Passeport Numérique Smart City. Il organise les responsabilités de la collectivité, des opérateurs, délégataires, prestataires, autorités, citoyens et administrateurs techniques autour des actifs et données urbaines.

2. Gouvernance municipale

La ville ou collectivité définit les politiques d'habilitation, les périmètres de service, les règles de publication et les exigences de continuité. Authenticity Plus© fournit l'infrastructure de preuve sans se substituer aux compétences légales de la collectivité.

3. Identité des organismes

Municipalité, établissement public, opérateur, régie, délégataire, fournisseur ou prestataire dispose d' une identité institutionnelle vérifiable. Les droits sont associés à la fonction exercée et non au seul nom de l'organisation.

4. Opérateurs de services

Les opérateurs d'eau, énergie, mobilité, éclairage, déchets ou autres services peuvent administrer les actifs correspondant à leur mission. Ils ne disposent pas automatiquement d'un accès transversal aux autres services urbains.

5. Délégataires et prestataires

Un délégataire ou prestataire reçoit des droits limités dans le temps et au périmètre contractuel nécessaire. La fin de mission entraîne la révocation ou la révision des habilitations sans effacer l' historique de ses actions.

6. Citoyens et usagers

Les citoyens peuvent consulter les informations publiques, vérifier certains actifs et transmettre des signalements. Cette participation ne leur donne pas accès aux fonctions de commande, aux données sensibles ni aux identités privées.

7. Autorités et organismes compétents

Les autorités peuvent accéder aux éléments correspondant à leurs compétences selon les règles applicables. Une décision officielle reste attribuée à son émetteur et ne peut être créée par AP.

8. Séparation des rôles

Administrer une identité, maintenir un équipement, contrôler un service, publier une donnée, traiter un incident et auditer sont des fonctions distinctes. Le principe du moindre privilège limite chaque compte au strict nécessaire.

9. Droits d'accès dynamiques

Les autorisations peuvent dépendre du rôle, du service, de la zone, de l'actif, de la durée et du contexte. Elles sont révocables et les opérations sensibles peuvent exiger une authentification renforcée.

10. Validation multiniveau

Modification de configuration, changement d'identité d'un actif, publication critique ou clôture d'un incident peut nécessiter plusieurs validations. Cette séparation réduit le risque qu'un compte unique puisse altérer seul une preuve importante.

11. Vue publique et transparence

La ville peut publier des informations vérifiables sur certains actifs, interventions ou niveaux de service. La transparence est organisée sans exposer plans sensibles, secrets techniques ou données personnelles.

12. Interopérabilité

Systèmes municipaux, plateformes IoT, SIG, BIM, mobilité, énergie, eau, maintenance et autres solutions peuvent échanger avec AP par interfaces contrôlées. Toute donnée importée conserve sa source, sa version et son horodatage.

13. Portabilité

Le Passeport Smart City doit permettre le changement de fournisseur ou de plateforme sans perte de l'historique vérifiable. Les données essentielles ne doivent pas devenir prisonnières d'un prestataire unique.

14. Souveraineté des données urbaines

La collectivité doit pouvoir définir où sont conservées les données, qui peut y accéder, selon quelles finalités et pendant combien de temps. Les contraintes juridiques et territoriales applicables sont intégrées à la gouvernance.

15. Minimisation des données

Le système collecte et partage uniquement les données nécessaires à la finalité concernée. Une fonction de maintenance d'un lampadaire, par exemple, ne justifie pas la collecte de l'identité ou des déplacements des passants.

16. Cybersécurité institutionnelle

Comptes privilégiés, clés, certificats, API, passerelles et consoles sont protégés par authentification renforcée, segmentation, journalisation, rotation et révocation. Les privilèges permanents sont limités.

17. Gestion des fournisseurs

L'ajout d'un fournisseur, d'un intégrateur ou d'un prestataire technique doit être documenté. Ses accès sont contrôlés, datés et supprimables afin qu'une relation contractuelle terminée ne laisse pas d'accès résiduel.

18. Audit indépendant

Des acteurs habilités peuvent vérifier l'intégrité des processus, habilitations et journaux. L'audit accède aux preuves nécessaires sans disposer automatiquement du pouvoir de modifier les actifs ou leurs historiques.

19. AP Ledger et conservation

Empreintes minimales des habilitations critiques, changements d'identité, validations, révocations et événements majeurs peuvent être ancrées dans AP Ledger. Les données urbaines massives, personnelles ou sensibles restent dans les systèmes protégés adaptés.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si chaque organisme reste limité à son périmètre ; si les droits des prestataires sont révocables ; si la participation citoyenne n'ouvre aucune commande critique ; si la portabilité évite l'enfermement fournisseur ; si la souveraineté et la minimisation sont intégrées ; et si l'audit reste indépendant des fonctions opérationnelles. Cette gouvernance fournit le socle nécessaire à la clôture fonctionnelle de l'application Smart City.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 20 — SMART CITY

CHAPITRE 6 — SYNTHÈSE FONCTIONNELLE, CRITÈRES D'ACCEPTATION ET CLÔTURE DE L'APPLICATION SMART CITY

1. Objet du chapitre

Ce chapitre clôt le Point 20 — Smart City. Il consolide l'identité numérique des actifs urbains, infrastructures, mobilité, énergie, eau, déchets, environnement, capteurs, maintenance, incidents, gouvernance, vie privée, cybersécurité, souveraineté des données et AP Ledger.

2. Mission consolidée

Le Passeport Numérique Smart City constitue une mémoire opérationnelle vérifiable des infrastructures et services urbains. Sa finalité première est d'authentifier les actifs, les données et les interventions, et non d'organiser une surveillance généralisée des citoyens.

3. Identité des actifs urbains

Chaque équipement ou infrastructure peut disposer d'une identité unitaire reliée à sa zone, son opérateur, son fabricant, sa configuration, son statut et son historique.

4. QR Codes dynamiques

Les QR dynamiques donnent accès à une vue adaptée au contexte : information publique, signalement, maintenance ou vérification technique. La copie visuelle d'un QR ne doit jamais suffire à reproduire l'identité de l'actif.

5. Géolocalisation de cohérence

Lorsque nécessaire et autorisée, la proximité entre smartphone, terminal et actif peut contribuer à la vérification. Cette opération ponctuelle doit être minimisée et ne devient pas un historique permanent des déplacements de l'usager.

6. Capteurs et provenance

Toute mesure importante doit pouvoir être reliée à l'identité du capteur, sa localisation, sa configuration, sa calibration, son horodatage et sa chaîne de traitement.

7. Mobilité urbaine

Transports publics, routes, stationnement, feux, bornes et véhicules de service peuvent être intégrés au passeport avec leurs identités, statuts, inspections et interventions.

8. Services essentiels

Énergie, éclairage, eau, déchets et autres services urbains utilisent le même principe : identité de l'actif, provenance de la donnée, maintenance, alerte et preuve de l'intervention.

9. Environnement

Qualité de l'air, bruit, température ou autres paramètres conservent source, unité, période, méthode et contexte. Une mesure isolée n'est pas automatiquement généralisée à toute la ville.

10. Alertes et diagnostics

Une alerte automatique reste distincte d'un diagnostic technique et d'une décision humaine. Les corrélations algorithmiques sont des hypothèses opérationnelles tant qu'elles ne sont pas confirmées.

11. Maintenance et prédiction

Maintenance préventive, corrective et prédictive sont distinguées. Une prédiction de panne reste probabiliste ; sa réalisation ou non-réalisation enrichit l'historique d'apprentissage et d'exploitation.

12. Online et Offline

Online fournit le statut courant. Offline sécurisé utilise des preuves signées mises en cache avec indication explicite de la date de dernière synchronisation et des limites liées à la fraîcheur.

13. Incidents et résilience

Panne, actif compromis, faux capteur, donnée falsifiée, QR cloné ou configuration inconnue peut déclencher une investigation. Les services critiques prévoient continuité, isolation et récupération selon les systèmes habilités.

14. Deep Authenticity©

Deep Authenticity© confronte identité, QR, localisation autorisée, certificats, configuration, données, calibration, maintenance, alertes et événements. Les incohérences doivent être explicables et auditables.

15. Participation citoyenne

Le citoyen peut vérifier certaines informations publiques et signaler un problème. Le signalement reste distinct du diagnostic et n'accorde jamais l'accès aux commandes techniques critiques.

16. Vie privée

Le système applique minimisation, finalité et séparation des données. L'identité ou le déplacement d' un citoyen n'est pas collecté simplement parce qu'un service urbain peut fonctionner avec des données techniques ou agrégées.

17. Gouvernance et souveraineté

Collectivités, opérateurs, délégataires, prestataires et autorités disposent de droits limités à leur mission. La ville conserve la capacité de définir conservation, accès, localisation, portabilité et changement de fournisseur.

18. Cybersécurité et interopérabilité

Comptes, certificats, API, passerelles, plateformes IoT et consoles sont protégés et révocables. Les échanges avec SIG, BIM, maintenance et systèmes sectoriels conservent source, version, horodatage et niveau d'autorité.

19. AP Ledger et critères d'acceptation

AP Ledger reçoit seulement des empreintes minimales d'identité, calibration, maintenance, changement critique, habilitation ou incident. Le modèle est acceptable si le QR seul ne suffit pas ; si les mesures sont traçables ; si la géolocalisation ne devient pas surveillance ; si Offline indique sa fraîcheur ; si les droits sont révocables ; et si les données sensibles restent protégées.

20. Clôture du Point 20 — Smart City

Le Point 20 — Smart City est désormais fonctionnellement défini : identité urbaine, infrastructures, équipements, QR dynamiques, mobilité, géolocalisation de cohérence, énergie, eau, déchets, environnement, capteurs, calibration, maintenance, alertes, Offline, incidents, résilience, Deep Authenticity©, participation citoyenne, gouvernance, souveraineté, confidentialité, cybersécurité, interopérabilité, audit et AP Ledger. Le Volume IV peut désormais poursuivre avec le Point 21 — Environnement.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 21 — ENVIRONNEMENT

CHAPITRE 1 — IDENTITÉ ENVIRONNEMENTALE, SITES, ÉCOSYSTÈMES, CAPTEURS, ÉCHANTILLONS, MESURES, PROVENANCE DES DONNÉES, QR CODES DYNAMIQUES ET PASSEPORT NUMÉRIQUE ENVIRONNEMENT

1. Objet du chapitre

Le Point 21 — Environnement transpose Authenticity Plus© / Deep Authenticity© au suivi vérifiable des sites, écosystèmes, mesures, échantillons, équipements et actions environnementales. Il crée un Passeport Numérique Environnement reliant chaque information à sa source et à son contexte.

2. Mission sectorielle

La mission est de renforcer la confiance dans les données environnementales en préservant leur provenance, leur chronologie et leur niveau de preuve. AP organise les éléments disponibles sans se substituer aux laboratoires, experts, organismes de contrôle ou autorités compétentes.

3. Identité du site

Zone naturelle, site industriel, forêt, littoral, bassin, aire protégée ou autre périmètre peut disposer d’ une identité avec localisation, limites, gestionnaire, statut et références documentées.

4. Écosystèmes et habitats

Les habitats, zones humides, espaces forestiers, milieux côtiers ou autres unités écologiques peuvent être reliés au site. Leur état évolue dans le temps et doit être daté plutôt que présenté comme permanent.

5. Identité des actifs environnementaux

Station de mesure, capteur, sonde, balise, équipement de prélèvement ou autre actif technique peut recevoir une identité reliée au fabricant, modèle, configuration, localisation et historique.

6. QR Code dynamique

Un QR dynamique peut être associé à une station, un équipement, un point de prélèvement ou une zone autorisée. Le scan ouvre une vue adaptée aux droits : identité, statut, mesures publiables, maintenance ou documents techniques.

7. Capteurs

Les capteurs de qualité de l'air, bruit, température, humidité, sols, eau ou autres paramètres conservent leur identité, calibration, configuration et état de fonctionnement.

8. Mesures

Toute mesure importante doit conserver au minimum sa source, son horodatage, son unité, sa localisation ou zone, ainsi que le contexte nécessaire à son interprétation.

9. Calibration et maintenance

Calibration, vérification, entretien, remplacement ou reconfiguration d'un équipement est enregistré comme événement. Une mesure provenant d'un capteur hors calibration peut recevoir un niveau de confiance ou un statut adapté.

10. Échantillons

Eau, sol, air, sédiment, matière biologique ou autre échantillon peut recevoir une identité de prélèvement reliant lieu, date, opérateur, méthode, conditionnement et laboratoire destinataire lorsque ces données existent.

11. Chaîne de traçabilité

Le parcours de l'échantillon depuis le prélèvement jusqu'à l'analyse peut être documenté. Toute rupture ou étape inconnue reste visible et n'est pas artificiellement complétée.

12. Laboratoires et analyses

Les résultats d'analyse conservent laboratoire, méthode, date, échantillon et rapport associés. AP ne transforme pas un fichier téléchargé en résultat officiellement confirmé par le laboratoire.

13. Provenance des données

Données brutes, données corrigées, données agrégées, résultats de laboratoire et indicateurs calculés restent distingués. Toute transformation importante doit pouvoir être reliée à sa méthode et à sa source.

14. Photographies et observations terrain

Photographies, observations humaines et constats peuvent enrichir le passeport avec date, zone et auteur. Ils constituent des preuves contextualisées et ne remplacent pas automatiquement une mesure instrumentale ou une expertise.

15. Deep Authenticity©

Deep Authenticity© confronte identité du site, capteurs, calibration, échantillons, résultats, photographies, chronologie et sources. Une incohérence déclenche une vérification explicable, jamais une conclusion automatique de pollution ou de fraude.

16. Online et Offline

Online permet d’accéder au statut courant et aux données autorisées. Offline sécurisé peut fournir les dernières preuves signées disponibles avec indication explicite de la date de synchronisation.

17. Alertes environnementales

Dépassement de seuil, anomalie de mesure, perte de communication ou observation critique peut produire une alerte. L’alerte reste distincte de la confirmation scientifique, du diagnostic et de la décision réglementaire.

18. Confidentialité et données sensibles

Localisation d’espèces vulnérables, données industrielles sensibles, informations personnelles, infrastructures critiques et dossiers d’enquête peuvent nécessiter un accès restreint. La transparence environnementale s’applique avec proportionnalité.

19. AP Ledger

Empreintes minimales d’identité de site, calibration, prélèvement, rapport, changement de statut ou événement critique peuvent être ancrées dans AP Ledger. Les flux massifs, rapports complets et données sensibles restent hors des couches irréversibles.

20. Critères d’acceptation et conclusion

Le modèle est acceptable si chaque mesure conserve sa provenance ; si les capteurs et calibrations sont traçables ; si les échantillons conservent leur chaîne de traçabilité ; si données brutes et dérivées restent distinctes ; si une alerte ne devient pas automatiquement un diagnostic ; si Offline indique sa fraîcheur ; et si les données écologiquement sensibles sont protégées. Le Passeport Numérique Environnement devient ainsi une infrastructure de confiance pour la preuve environnementale.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 21 — ENVIRONNEMENT

CHAPITRE 2 — QUALITÉ DE L'AIR, POLLUTION, ÉMISSIONS, SOLS, BIODIVERSITÉ, PRÉLÈVEMENTS, LABORATOIRES, CARTOGRAPHIE ET SURVEILLANCE ENVIRONNEMENTALE

1. Objet du chapitre

Ce chapitre applique le Passeport Numérique Environnement à la surveillance de l'air, des émissions, des sols et de la biodiversité. Il relie sites, capteurs, prélèvements, laboratoires, cartes, observations et résultats à une chaîne de provenance vérifiable.

2. Qualité de l'air

Stations et capteurs peuvent mesurer particules, gaz ou autres paramètres selon leur capacité documentée. Chaque mesure conserve appareil, localisation, date, unité, configuration et statut de calibration.

3. Station de mesure

Une station dispose d'une identité propre reliée à son opérateur, ses instruments, maintenances, calibrations et périodes de fonctionnement. Une station déplacée ou reconfigurée conserve l' historique de ces changements.

4. Pollution atmosphérique

Un dépassement ou une anomalie de mesure peut déclencher une alerte et une investigation. Une valeur élevée ne permet pas, à elle seule, d'identifier automatiquement la source responsable.

5. Émissions

Une source industrielle, installation, équipement ou point de mesure peut être relié aux données et documents autorisés. Déclaration de l'exploitant, mesure instrumentale et contrôle indépendant restent distingués.

6. Inventaires d'émissions

Les inventaires calculés doivent conserver méthodologie, période, facteurs utilisés, version et organisme producteur. Une estimation calculée reste distincte d'une mesure directe.

7. Sols

Une zone de sol peut être décrite par localisation, profondeur, historique disponible, prélèvements et analyses. Un résultat ponctuel reste rattaché au point et aux conditions de prélèvement.

8. Prélèvements

Chaque échantillon reçoit une identité reliant site, point, date, profondeur ou contexte, opérateur, contenant et laboratoire destinataire lorsque ces informations existent.

9. Chaîne de traçabilité

Collecte, transport, réception au laboratoire, préparation et analyse peuvent être historisés. Une rupture de chaîne ou une information manquante est signalée comme limite de preuve.

10. Laboratoires

Les laboratoires conservent leur identité, méthode, date, résultat, unité et éventuelles réserves. AP ne transforme pas automatiquement un laboratoire déclaré en organisme accrédité.

11. Biodiversité

Espèces, habitats, zones écologiques et observations peuvent être reliés à leur lieu, date, observateur, méthode et niveau de certitude. Une observation unique ne prouve pas automatiquement une population stable.

12. Données sensibles de biodiversité

La localisation précise d’espèces menacées, nids, habitats vulnérables ou autres informations pouvant faciliter une atteinte peut être masquée ou généralisée dans les vues non autorisées.

13. Photographies et observations

Photographies, relevés terrain et observations peuvent documenter l’état environnemental. Leur auteur, date et contexte sont conservés et ils restent distincts d’une analyse de laboratoire.

14. Cartographie

Les mesures et observations peuvent alimenter une carte environnementale. Chaque couche conserve sa source, sa période et sa résolution afin de ne pas présenter une interpolation comme une mesure exacte en tout point.

15. Séries temporelles

La comparaison dans le temps permet d’identifier tendances, épisodes ou changements. Les changements d’instrument, méthode ou emplacement doivent être visibles pour éviter des comparaisons trompeuses.

16. Deep Authenticity©

Deep Authenticity© confronte identité des capteurs, calibration, localisation, prélèvements, laboratoire, méthodes, séries et documents. Les incohérences sont signalées avec leur contexte et restent investigables.

17. Alertes environnementales

Un seuil dépassé, une donnée atypique ou une divergence peut générer une alerte. L'alerte reste distincte d'un diagnostic scientifique, d'une attribution de responsabilité ou d'une décision réglementaire.

18. Online, Offline et terrain

Les équipes terrain peuvent consulter les dernières données signées disponibles. En Offline, la date de synchronisation est affichée et les nouvelles observations sont synchronisées dès le retour du réseau selon les règles prévues.

19. AP Ledger et confidentialité

Empreintes minimales de calibration, prélèvement, réception laboratoire, rapport, correction et événement critique peuvent être ancrées dans AP Ledger. Données sensibles, localisations protégées, rapports complets et flux massifs restent hors des couches irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si mesure directe et estimation restent distinctes ; si chaque prélèvement conserve sa chaîne de traçabilité ; si l'accréditation d'un laboratoire n'est pas supposée ; si les localisations écologiquement sensibles sont protégées ; si les cartes conservent leur résolution et leur source ; et si une alerte n'attribue pas automatiquement une pollution. Le Passeport Environnement fournit ainsi une chaîne de confiance vérifiable pour la surveillance environnementale.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 21 — ENVIRONNEMENT

CHAPITRE 3 — DÉCHETS, RECYCLAGE, ÉCONOMIE CIRCULAIRE, MATIÈRES À RISQUE, TRAÇABILITÉ DES FLUX, COLLECTE, TRANSPORT, TRAITEMENT, VALORISATION ET PREUVE ENVIRONNEMENTALE

1. Objet du chapitre

Ce chapitre applique le Passeport Numérique Environnement aux déchets et aux flux de matières : production, identification, collecte, transport, réception, tri, traitement, recyclage, valorisation et destination finale documentée.

2. Identité du flux

Un flux ou lot de déchets peut recevoir une identité reliant producteur déclaré, catégorie, quantité, date, lieu, conditionnement et statut. Les classifications réglementaires restent attribuées aux acteurs compétents.

3. Producteur et détenteur

Producteur initial, détenteur, collecteur, transporteur et installation de destination sont des rôles distincts. Chaque transfert conserve l’acteur et le moment correspondant.

4. Caractérisation

Nature, composition, propriétés et résultats d’analyse peuvent être associés au lot. Une caractérisation déclarative reste distincte d’une analyse ou classification confirmée.

5. Matières à risque

Les matières présentant des risques particuliers exigent des droits d’accès et procédures renforcés. Le passeport documente identité, statut et chaîne de responsabilité sans exposer publiquement des informations opérationnelles sensibles.

6. Conditionnement

Conteneur, emballage, scellé ou autre unité logistique peut être relié au flux correspondant. Une rupture ou modification documentée du conditionnement devient un événement de traçabilité.

7. QR Code dynamique

Un QR dynamique peut identifier un conteneur, lot ou unité autorisée. Le scan donne accès au statut approprié selon le rôle, mais le QR seul ne suffit jamais à prouver le contenu réel.

8. Collecte

Date, point de collecte, opérateur, quantité et documents associés peuvent être enregistrés. La collecte constitue un événement de chaîne de garde.

9. Transport

Le transfert vers une installation peut conserver transporteur, origine, destination, horaires et preuves autorisées. Les données sensibles sont minimisées et les règles sectorielles applicables restent prioritaires.

10. Réception

L'installation de destination peut enregistrer la réception, la quantité constatée et les éventuelles réserves. La réception physique ne signifie pas automatiquement acceptation de la classification déclarée.

11. Pesée

Une pesée peut être reliée à l'équipement, sa calibration, la date et l'opérateur. Les différences entre poids déclaré, collecté et reçu peuvent être signalées pour vérification.

12. Tri et transformation

Un lot initial peut être séparé en plusieurs flux ou combiné selon le procédé documenté. Le système conserve la généalogie matière afin d'éviter la disparition de l'origine lors des transformations.

13. Recyclage

Une opération de recyclage est documentée avec installation, procédé, quantité entrante, sorties et preuves disponibles. AP ne transforme pas automatiquement une déclaration de recyclage en preuve de performance environnementale.

14. Valorisation et destination

Réemploi, recyclage, valorisation ou autre destination reste attribuée à la source qui la documente. La destination finale déclarée doit être distinguée d'une destination confirmée par réception ou traitement.

15. Économie circulaire

Lorsqu'une matière secondaire devient une ressource pour un nouveau cycle, son passeport peut conserver l'origine, les transformations et les preuves utiles, créant une continuité entre déchet, matière recyclée et nouveau produit.

16. Deep Authenticity©

Deep Authenticity© confronte identité du lot, QR, poids, documents, acteurs, transferts, réceptions et transformations. Des incohérences de quantité, de destination ou de chronologie déclenchent une vérification.

17. Fraude et déclarations environnementales

Faux document, double comptage, destination incohérente ou déclaration de recyclage non étayée peut produire un signal. Une anomalie ne constitue pas automatiquement une fraude et doit être investiguée.

18. Online et Offline

Les équipes peuvent vérifier le dernier statut disponible sur le terrain. En Offline, les preuves signées mises en cache affichent leur date de synchronisation et les nouveaux événements sont synchronisés dès que possible.

19. AP Ledger et confidentialité

Empreintes minimales des transferts, pesées, réceptions, transformations et preuves critiques peuvent être ancrées dans AP Ledger. Itinéraires sensibles, données commerciales, documents complets et informations à risque restent protégés.

20. Critères d’acceptation et conclusion

Le modèle est acceptable si chaque transfert conserve sa chaîne de garde ; si le QR ne prouve pas seul le contenu ; si la pesée est reliée à sa calibration ; si la transformation conserve la généalogie matière ; si déclaration et preuve de recyclage restent distinctes ; et si les anomalies déclenchent une investigation sans accusation automatique. Le Passeport Environnement apporte ainsi une traçabilité vérifiable à l’économie circulaire.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 21 — ENVIRONNEMENT

CHAPITRE 4 — ÉMISSIONS CARBONE, EMPREINTE ENVIRONNEMENTALE, CRÉDITS ET CERTIFICATS, GREEN CLAIMS, DOUBLE COMPTAGE, PREUVES ESG, AUDIT ET LUTTE CONTRE LE GREENWASHING

1. Objet du chapitre

Ce chapitre définit la chaîne de preuve applicable aux déclarations environnementales, inventaires d'émissions, empreintes carbone, certificats, crédits, indicateurs ESG et autres allégations environnementales.

2. Principe de preuve

Une affirmation environnementale doit pouvoir être reliée à sa source, son périmètre, sa période, sa méthodologie, ses données et son auteur. Authenticity Plus© ne transforme pas une déclaration non étayée en fait vérifié.

3. Inventaire des émissions

Un inventaire peut relier organisation, site, activité, période, sources, données d'activité, facteurs d'émission et méthode de calcul. Les versions successives restent historisées.

4. Mesure et calcul

Une mesure instrumentale, une donnée d'activité, un facteur d'émission et une estimation calculée sont des objets distincts. Leur combinaison doit rester explicable et reproductible selon les informations disponibles.

5. Périmètre

Toute empreinte doit préciser son périmètre organisationnel, opérationnel, géographique et temporel. Deux résultats calculés sur des périmètres différents ne doivent pas être présentés comme directement équivalents.

6. Facteurs d'émission

Les facteurs utilisés conservent leur source, version, unité et date d'application. Une modification de facteur peut changer un résultat sans que l'activité réelle ait changé.

7. Données primaires et secondaires

Les données mesurées ou fournies directement et les données estimées ou issues de bases externes restent distinguées. Leur niveau de provenance contribue à l'évaluation de la qualité de la preuve.

8. Empreinte produit ou service

Une empreinte associée à un produit, service ou projet peut être reliée à son identité, sa période, ses hypothèses et ses étapes de cycle de vie documentées. AP n'impose pas à lui seul une méthode réglementaire.

9. Réduction des émissions

Une réduction annoncée doit préciser l'année ou situation de référence, le périmètre, la méthode et la période comparée. Une baisse calculée n'est pas automatiquement attribuable à une action particulière.

10. Compensation

Réduction interne et compensation externe restent séparées. Une organisation ne doit pas présenter une compensation comme si elle constituait nécessairement une réduction physique de ses propres émissions.

11. Crédits et certificats

Un crédit ou certificat peut disposer d'une identité, d'un émetteur, d'une quantité, d'une période, d'un projet ou registre de référence et d'un statut documenté. AP vérifie la cohérence des preuves disponibles sans garantir seul la qualité environnementale du mécanisme.

12. Double comptage

Un même crédit, certificat, bénéfice ou quantité ne doit pas être revendiqué plusieurs fois lorsque les règles applicables l'interdisent. Identité unitaire, transferts, statut et retrait documenté contribuent à détecter les revendications concurrentes.

13. Green Claims

Une allégation telle que « recyclé », « bas carbone », « renouvelable » ou autre déclaration environnementale doit être reliée aux preuves et au périmètre exact qui la soutiennent. Les formulations plus larges que les preuves disponibles sont signalées comme insuffisamment étayées.

14. Greenwashing

Le système peut détecter des incohérences entre affirmation, périmètre, données, certificats et historique. Un signal de greenwashing reste une indication à examiner et non une accusation juridique automatique.

15. ESG

Les indicateurs environnementaux utilisés dans un reporting ESG peuvent être reliés à leurs données sources, méthodes, responsables et versions. Le passeport distingue donnée source, indicateur calculé, commentaire de gestion et assurance externe.

16. Audit et assurance

Auditeur, organisme de vérification ou autre tiers peut produire une conclusion dans son propre périmètre. AP conserve auteur, date, référentiel déclaré, niveau de vérification et réserves sans élargir la portée de l'avis.

17. Deep Authenticity©

Deep Authenticity© confronte données sources, facteurs, calculs, certificats, périodes, transferts, retraits, rapports et déclarations publiques. Une incohérence est explicable et peut ouvrir une vérification.

18. Corrections et retraitement

Une erreur corrigée ou un calcul retraité produit une nouvelle version. La version antérieure et la raison de la correction restent auditables afin d'éviter une réécriture silencieuse de l'historique.

19. AP Ledger et confidentialité

Empreintes minimales des méthodologies, inventaires validés, certificats, transferts, retraits, audits et corrections critiques peuvent être ancrées dans AP Ledger. Données commerciales, calculs détaillés, contrats et informations sensibles restent protégés.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si mesure et estimation restent distinctes ; si tout résultat conserve son périmètre ; si les facteurs sont versionnés ; si réduction et compensation ne sont pas confondues ; si le double comptage peut être détecté ; si les Green Claims restent proportionnés aux preuves ; et si l' audit conserve sa portée réelle. Deep Authenticity© fournit ainsi une infrastructure de preuve contre les déclarations environnementales trompeuses.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 21 — ENVIRONNEMENT

CHAPITRE 5 — GOUVERNANCE ENVIRONNEMENTALE, AUTORITÉS, ENTREPRISES, LABORATOIRES, AUDITEURS, ONG, CITOYENS, DROITS D'ACCÈS, CONFIDENTIALITÉ, INTEROPÉRABILITÉ ET SOUVERAINETÉ DES DONNÉES

1. Objet du chapitre

Ce chapitre définit la gouvernance du Passeport Numérique Environnement et la séparation des rôles entre autorités, entreprises, opérateurs, laboratoires, auditeurs, organismes scientifiques, ONG, citoyens et administrateurs techniques.

2. Principe de gouvernance

Authenticity Plus© organise la provenance, l'accès et l'audit des preuves environnementales. Il ne remplace ni l'autorité réglementaire, ni le laboratoire, ni l'expert, ni l'auditeur dans leurs compétences propres.

3. Autorités compétentes

Une autorité peut publier ou confirmer des décisions, autorisations, seuils ou statuts dans son périmètre. Chaque information officielle reste attribuée à son émetteur et à sa date.

4. Entreprises et exploitants

Une entreprise peut déclarer ses sites, équipements, mesures, inventaires, déchets, émissions et actions selon ses obligations et droits. Ses déclarations restent identifiées comme provenant de l' entreprise lorsqu'elles ne sont pas vérifiées par un tiers.

5. Laboratoires

Les laboratoires accèdent aux échantillons, méthodes et dossiers nécessaires à leurs analyses. Ils produisent leurs propres résultats sans pouvoir modifier silencieusement les données de prélèvement établies par un autre acteur.

6. Auditeurs et vérificateurs

Un auditeur ou organisme de vérification reçoit les preuves nécessaires à sa mission et publie une conclusion limitée à son périmètre. Il ne dispose pas automatiquement de droits d'administration opérationnelle.

7. Organismes scientifiques

Universités, instituts ou experts peuvent contribuer à l'analyse selon des habilitations adaptées. Donnée scientifique, avis d'expert et décision réglementaire restent des catégories distinctes.

8. ONG et société civile

Une ONG peut consulter des informations publiques ou recevoir des données selon un cadre autorisé. Son interprétation ou son rapport reste attribué à l'organisation qui le produit.

9. Citoyens

Le citoyen peut consulter certaines données environnementales, vérifier des informations publiées et transmettre des observations ou signalements. Une observation citoyenne reste distincte d'une mesure instrumentale ou d'un résultat de laboratoire.

10. Séparation des rôles

Déclarer, mesurer, analyser, auditer, contrôler, décider et publier sont des fonctions distinctes. Le système applique le principe du moindre privilège afin d'éviter qu'un même compte puisse accomplir toutes les étapes critiques sans contrôle.

11. Droits d'accès

Les accès peuvent dépendre de l'organisation, du rôle, du site, du projet, du type de donnée, de la durée et du niveau de sensibilité. Ils sont révocables et journalisés.

12. Validation multiniveau

Une correction importante, un retrait de certificat, une modification méthodologique ou une publication critique peut exiger plusieurs validations. Les étapes et auteurs de validation restent auditables.

13. Confidentialité

Secrets industriels, données commerciales, localisations écologiquement sensibles, informations personnelles, rapports d'investigation et configurations techniques sont protégés par des vues et droits adaptés.

14. Données publiques

La publication environnementale doit conserver source, période, méthode, unité et éventuelles limites. Une donnée publique simplifiée ne doit pas perdre les informations nécessaires pour éviter une interprétation trompeuse.

15. Interopérabilité

Capteurs, laboratoires, SIG, systèmes industriels, plateformes ESG, registres autorisés et autres solutions peuvent échanger avec AP. Les données importées conservent source, version, horodatage et niveau d'autorité.

16. Portabilité

Le changement de fournisseur, laboratoire, auditeur ou plateforme ne doit pas effacer l'historique des preuves. Les formats et mécanismes d'export doivent permettre la continuité de la traçabilité.

17. Souveraineté des données

L'organisation compétente doit pouvoir définir localisation, conservation, accès, finalités et règles de transfert des données selon les exigences juridiques applicables. Les données sensibles ne sont pas rendues publiques par défaut.

18. Cybersécurité et audit

Comptes privilégiés, certificats, API et systèmes de collecte sont protégés, journalisés et révocables. Les journaux d'audit doivent permettre de reconstituer les actions critiques sans donner à l'auditeur le pouvoir de les réécrire.

19. AP Ledger

Empreintes minimales des validations, changements méthodologiques, rapports, certificats, révocations et événements critiques peuvent être ancrées dans AP Ledger. Les données brutes massives, secrets industriels et informations sensibles restent dans les systèmes protégés.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si déclarant, mesureur, laboratoire, auditeur et autorité restent distingués ; si les droits sont révocables ; si les publications conservent leur contexte ; si les localisations sensibles sont protégées ; si la portabilité préserve l'historique ; et si la souveraineté des données est gouvernable. Cette architecture fournit le socle nécessaire à la clôture fonctionnelle de l'application Environnement.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 21 — ENVIRONNEMENT

CHAPITRE 6 — SYNTHÈSE FONCTIONNELLE, CRITÈRES D'ACCEPTATION ET CLÔTURE DE L'APPLICATION ENVIRONNEMENT

1. Objet du chapitre

Ce chapitre clôt le Point 21 — Environnement et consolide sites, écosystèmes, capteurs, prélèvements, laboratoires, air, sols, biodiversité, déchets, économie circulaire, carbone, déclarations environnementales, gouvernance et AP Ledger.

2. Mission consolidée

Le Passeport Numérique Environnement organise une chaîne de preuve vérifiable depuis la donnée terrain jusqu'à la déclaration publiée. Authenticity Plus© protège provenance et historique sans remplacer expertise scientifique, laboratoire, audit ou autorité.

3. Identité environnementale

Sites, zones, actifs, stations, capteurs, échantillons, lots et documents peuvent disposer d'identités reliées à leurs opérateurs, emplacements, périodes et statuts.

4. Mesures et provenance

Toute mesure importante conserve appareil, calibration, localisation, date, unité, méthode et chaîne de traitement. Donnée brute, donnée corrigée, estimation et indicateur calculé restent distingués.

5. Prélèvements et laboratoires

Chaque prélèvement peut conserver site, point, date, contexte, opérateur, transport, réception et analyse. Le résultat reste rattaché à l'échantillon et au périmètre réellement analysé.

6. Air, sols et pollution

Mesures atmosphériques et analyses de sols sont contextualisées. Un dépassement ou résultat ponctuel peut déclencher une vérification mais n'attribue pas automatiquement une source ou une responsabilité.

7. Biodiversité

Observations d'espèces et habitats conservent lieu, date, méthode, observateur et niveau de certitude. Les localisations susceptibles de mettre en danger une espèce ou un habitat peuvent être protégées.

8. Cartographie et séries temporelles

Les cartes conservent source, résolution, période et méthode. Les séries temporelles signalent les changements d'instrument, de méthode ou d'emplacement afin de préserver la comparabilité.

9. Déchets et chaîne de garde

Production, collecte, transport, réception, pesée, traitement et destination peuvent être reliés chronologiquement. Producteur, détenteur, transporteur et installation restent des rôles distincts.

10. Économie circulaire

La transformation d'un déchet en matière secondaire puis en nouveau produit peut conserver une généalogie matière. Déclaration de recyclage et preuve documentée de traitement restent distinctes.

11. Carbone et empreinte

Inventaires et empreintes conservent périmètre, période, données d'activité, facteurs, hypothèses et méthode. Mesure directe et estimation calculée ne sont pas confondues.

12. Réduction et compensation

Une réduction physique d'émissions reste distincte d'une compensation. Toute comparaison conserve sa référence, son périmètre et sa période.

13. Crédits, certificats et double comptage

Identité, quantité, transfert, statut et retrait documenté permettent de vérifier la cohérence d'un crédit ou certificat et de détecter des revendications concurrentes lorsque les règles applicables l' interdisent.

14. Green Claims et ESG

Toute allégation environnementale doit rester proportionnée aux preuves disponibles. Les indicateurs ESG conservent leurs sources, calculs, versions et éventuelle assurance externe.

15. Deep Authenticity©

Deep Authenticity© confronte capteurs, calibration, échantillons, laboratoires, lots, pesées, transferts, facteurs, calculs, certificats, audits et déclarations. Les incohérences restent explicables et investigables.

16. Alertes, anomalies et corrections

Une alerte ou anomalie ne constitue ni diagnostic scientifique ni accusation automatique. Une correction produit une nouvelle version et conserve la raison ainsi que l'état antérieur.

17. Gouvernance

Autorités, entreprises, laboratoires, auditeurs, scientifiques, ONG et citoyens disposent de rôles distincts. Déclarer, mesurer, analyser, auditer, contrôler et décider ne sont pas fusionnés.

18. Confidentialité, souveraineté et interopérabilité

Secrets industriels, données personnelles et localisations écologiquement sensibles restent protégés. Les échanges avec capteurs, SIG, laboratoires, plateformes ESG et registres autorisés conservent provenance, version et niveau d'autorité.

19. AP Ledger et critères d'acceptation

AP Ledger reçoit des empreintes minimales de calibrations, prélèvements, rapports, transferts, certificats, audits, validations et corrections critiques. Le modèle est acceptable si provenance et séparation des rôles sont conservées, si les données sensibles sont protégées et si aucune déclaration ne dépasse la portée de ses preuves.

20. Clôture du Point 21 — Environnement

Le Point 21 — Environnement est désormais fonctionnellement défini : identité environnementale, capteurs, mesures, calibration, prélèvements, laboratoires, air, sols, biodiversité, cartographie, déchets, économie circulaire, carbone, crédits, certificats, Green Claims, ESG, Deep Authenticity©, alertes, gouvernance, confidentialité, souveraineté, interopérabilité, audit et AP Ledger. Le Volume IV peut désormais poursuivre avec le Point 22 — Water.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 22 — WATER

CHAPITRE 1 — IDENTITÉ NUMÉRIQUE DE L'EAU, RESSOURCES, CAPTAGE, TRAITEMENT, RÉSEAUX, QUALITÉ, CAPTEURS, QR CODES DYNAMIQUES ET PASSEPORT NUMÉRIQUE WATER

1. Objet du chapitre

Le Point 22 — Water transpose Authenticity Plus© / Deep Authenticity© à la ressource en eau et à ses infrastructures. Il crée un Passeport Numérique Water reliant origine, captage, traitement, stockage, distribution, qualité, équipements, mesures, interventions et preuves.

2. Mission sectorielle

La mission est de rendre vérifiables l'identité des actifs, la provenance des données et la continuité de la chaîne de l'eau, sans transformer le passeport en autorité sanitaire ou réglementaire autonome.

3. Identité de la ressource

Source, forage, barrage, prise d'eau, nappe, bassin ou autre ressource peut disposer d'une identité reliée à sa localisation, son opérateur, ses autorisations et ses données documentées.

4. Captage

Les installations de captage peuvent être reliées à leurs équipements, débits, inspections, maintenances et événements. Une mesure conserve son appareil, sa date, son unité et son contexte.

5. Traitement

Une usine ou unité de traitement peut disposer d'un passeport reliant étapes de procédé, équipements, contrôles, maintenances et données autorisées. Les paramètres opérationnels sensibles restent protégés.

6. Stockage

Réservoirs, châteaux d'eau, bassins et autres ouvrages peuvent être identifiés avec capacité déclarée, zone desservie, inspections et interventions.

7. Réseau de distribution

Conduites, vannes, pompes, branchements techniques et secteurs peuvent être reliés à leur identité, emplacement, matériau, date disponible, maintenance et historique.

8. QR Code dynamique

Un QR dynamique sur un actif autorisé peut ouvrir une fiche adaptée au rôle : identité, maintenance, inspection, signalement ou documentation. Le QR seul ne constitue jamais une preuve suffisante de l'état réel de l'équipement.

9. Capteurs

Débitmètres, pressions, niveaux, turbidité ou autres instruments peuvent être reliés à leur identité, configuration, calibration, localisation et historique.

10. Qualité de l'eau

Les résultats de qualité conservent point de prélèvement, date, méthode, laboratoire ou capteur, unité et périmètre. Un résultat ponctuel n'est pas automatiquement généralisé à tout un réseau.

11. Prélèvements

Chaque échantillon peut recevoir une identité reliant lieu, heure, opérateur, contenant, transport, réception et analyse. Toute rupture de chaîne est conservée comme limite de preuve.

12. Laboratoires

Les laboratoires produisent leurs résultats dans leur propre périmètre. AP conserve la provenance des rapports et ne suppose ni accréditation ni conformité réglementaire au-delà des preuves disponibles.

13. Calibration

La calibration d'un instrument est un événement critique. Date, méthode, intervenant, résultat et statut peuvent être enregistrés afin d'évaluer la confiance dans les mesures.

14. Fuites et anomalies

Une variation de débit, pression ou autre signal peut déclencher une alerte de fuite ou d'anomalie. Cette alerte reste une hypothèse opérationnelle jusqu'à vérification.

15. Deep Authenticity©

Deep Authenticity© confronte actif, QR, localisation autorisée, capteur, calibration, prélèvement, laboratoire, historique et chronologie. Une incohérence déclenche une vérification explicable.

16. Online et Offline

Online fournit les données et statuts courants autorisés. En Offline, les équipes peuvent utiliser des preuves signées mises en cache avec indication de leur date de dernière synchronisation.

17. Signalement

Un usager peut signaler fuite visible, équipement endommagé ou autre problème via un canal autorisé. Le signalement reste distinct d'un diagnostic technique ou d'une conclusion sur la qualité de l'eau.

18. Confidentialité et sécurité

Plans détaillés de réseau, accès aux installations, configurations, données personnelles et informations pouvant compromettre la sécurité des infrastructures sont réservés aux acteurs habilités.

19. AP Ledger

Empreintes minimales d'identité d'actif, calibration, prélèvement, rapport, maintenance et événement critique peuvent être ancrées dans AP Ledger. Les données sensibles et flux massifs restent dans les systèmes protégés.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si ressource, actif, capteur, prélèvement et résultat restent reliés ; si un QR seul ne suffit pas ; si la calibration est traçable ; si un résultat ponctuel n'est pas généralisé ; si une alerte de fuite reste une hypothèse ; et si les informations sensibles du réseau sont protégées. Le Passeport Water devient ainsi une chaîne de confiance vérifiable de la ressource jusqu'au réseau.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 22 — WATER

CHAPITRE 2 — EAU POTABLE, QUALITÉ SANITAIRE, PRÉLÈVEMENTS, LABORATOIRES, CHAÎNE DE GARDE, CONTAMINATION, ALERTES, TRAÇABILITÉ ET GESTION DES INCIDENTS

1. Objet du chapitre

Ce chapitre développe la chaîne de preuve applicable à l'eau destinée à la consommation : points de contrôle, prélèvements, analyses, laboratoires, résultats, alertes, incidents et actions correctives.

2. Principe de prudence

Authenticity Plus© organise l'authenticité et la provenance des données. Il ne déclare pas seul qu'une eau est potable, impropre ou dangereuse : ces qualifications relèvent des autorités et professionnels compétents selon les règles applicables.

3. Points de contrôle

Ressource, sortie de traitement, réservoir, secteur de réseau ou autre point autorisé peut disposer d' une identité afin de rattacher correctement les mesures et prélèvements.

4. Plan de prélèvement

Une campagne peut préciser points, dates, paramètres, fréquence et acteurs prévus. Le plan reste distinct de la preuve qu'un prélèvement a effectivement été réalisé.

5. Prélèvement

L'échantillon peut recevoir une identité reliant point, date, heure, opérateur, méthode, contenant et conditions documentées.

6. Chaîne de garde

Remise, transport, réception, stockage et préparation peuvent être enregistrés. Une rupture, un retard ou une condition inconnue reste visible comme limite potentielle de la preuve.

7. Laboratoire

Le laboratoire rattache le résultat à l'échantillon reçu, à la méthode et à la date. Son statut ou son accréditation ne sont pas supposés au-delà des justificatifs disponibles.

8. Résultat d'analyse

Paramètre, valeur, unité, méthode, limite éventuelle et réserves restent associés au rapport. Une correction produit une nouvelle version sans effacer silencieusement l'ancienne.

9. Mesure en ligne

Un capteur en continu peut compléter les prélèvements. Son identité, calibration, maintenance et qualité de données sont nécessaires pour interpréter correctement ses mesures.

10. Cohérence multi-source

Deep Authenticity© peut confronter capteurs, prélèvements, laboratoire, historique de traitement et localisation afin de repérer des divergences nécessitant une vérification.

11. Contamination suspectée

Une mesure atypique, un résultat analytique ou un événement de réseau peut déclencher une suspicion de contamination. Le système conserve l'origine du signal et ne généralise pas automatiquement l'incident.

12. Confirmation

La confirmation peut nécessiter nouveaux prélèvements, analyses ou contrôles selon les procédures compétentes. Signal initial et confirmation restent deux étapes distinctes.

13. Alerte

Une alerte conserve auteur ou système source, date, périmètre, motif et statut. Elle peut être confirmée, requalifiée ou clôturée sans suppression de l'historique.

14. Incident

Lorsqu'un incident est déclaré par l'acteur compétent, le dossier peut relier zones, actifs, résultats, décisions, interventions et communications autorisées.

15. Action corrective

Purge, intervention technique, réparation, modification de traitement ou autre action décidée par les acteurs compétents peut être documentée avec date, périmètre et preuves.

16. Retour à la normale

La clôture d'un incident doit être reliée aux éléments qui la justifient et à l'autorité ou au responsable habilité. AP ne décide pas seul du retour à la normale.

17. Information du public

Les informations destinées aux usagers doivent provenir des canaux et autorités compétents, avec zone et période clairement indiquées. Les données techniques sensibles restent protégées.

18. Online et Offline

En ligne, les équipes accèdent aux statuts courants. En Offline, elles consultent les dernières preuves signées disponibles avec date de synchronisation clairement affichée.

19. AP Ledger et confidentialité

Empreintes minimales de prélèvement, réception, rapport, alerte, changement de statut, action corrective et clôture peuvent être ancrées dans AP Ledger. Rapports complets, plans sensibles et données personnelles restent protégés.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si plan et prélèvement réel restent distincts ; si la chaîne de garde est vérifiable ; si capteurs et laboratoires conservent leur provenance ; si suspicion et confirmation ne sont pas confondues ; si AP ne prononce pas seul la potabilité ; et si toute clôture d'incident est attribuable. Le Passeport Water devient ainsi une chaîne de confiance pour la qualité et la gestion documentée des incidents.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 22 — WATER

CHAPITRE 3 — DISTRIBUTION, COMPTEURS, CONSOMMATION, PERTES, FUITES, MAINTENANCE, INTERVENTIONS, FRAUDE, BRANCHEMENTS ET CONTINUITÉ DU SERVICE

1. Objet du chapitre

Ce chapitre applique le Passeport Numérique Water à l'exploitation du réseau de distribution : secteurs, branchements, compteurs, volumes, pertes, fuites, interventions, maintenance, anomalies et continuité du service.

2. Identité du secteur

Une zone de distribution peut disposer d'une identité reliant réservoirs, conduites, vannes, pompes, compteurs techniques et autres actifs nécessaires à son exploitation.

3. Branchements

Un branchement peut être relié à son point réseau, à ses équipements et à son statut administratif ou technique lorsque les données sont autorisées. Les informations personnelles de l'abonné restent protégées.

4. Compteurs

Un compteur peut disposer d'une identité associant fabricant, modèle, numéro, date disponible, emplacement, statut, historique de remplacement et contrôles.

5. Relevés

Chaque relevé conserve compteur, date, unité, mode de collecte et source. Une valeur manuelle, télérelevée, estimée ou corrigée doit rester identifiable comme telle.

6. Consommation

Les consommations peuvent être calculées à partir de relevés documentés. Une variation inhabituelle constitue un signal à examiner et non une preuve automatique de fuite ou de fraude.

7. Sectorisation et bilans

Les volumes entrants, distribués ou mesurés peuvent être rapprochés par secteur et période. Les différences peuvent contribuer à estimer des pertes, sous réserve de la qualité et du périmètre des données.

8. Pertes d’eau

Une perte calculée reste distincte d’une fuite physiquement localisée. Les incertitudes de mesure, consommations non mesurées et autres facteurs doivent être considérés dans l’interprétation.

9. Détection de fuite

Pression, débit, acoustique ou autres données peuvent contribuer à détecter une fuite potentielle. L’ alerte est confirmée par les méthodes et équipes compétentes avant toute conclusion définitive.

10. Localisation de l’intervention

Lorsqu’elle est nécessaire, la géolocalisation du terminal d’intervention peut confirmer une cohérence de proximité avec l’actif concerné. Elle reste ponctuelle, proportionnée et limitée à la finalité opérationnelle.

11. Maintenance préventive

Inspection, manœuvre, entretien, calibration ou remplacement planifié peut être documenté avec l’ actif, l’intervenant, la date et le statut.

12. Maintenance corrective

Une panne, casse, fuite ou anomalie peut ouvrir une intervention reliant diagnostic, travaux, pièces ou équipements remplacés et remise en service.

13. QR Code dynamique

Un QR dynamique sur un actif autorisé peut permettre aux équipes habilitées de vérifier son identité et son historique. Le QR seul ne permet ni commande critique ni validation automatique de l’état physique.

14. Anomalie de compteur

Blocage, incohérence, rupture de communication, inversion ou autre anomalie peut être signalée. Le système conserve les indices sans attribuer automatiquement une manipulation intentionnelle.

15. Fraude présumée

Un branchement non autorisé, une altération présumée ou une incohérence de consommation peut déclencher une vérification. AP ne qualifie pas seul l’événement de fraude et n’attribue pas automatiquement une responsabilité.

16. Deep Authenticity©

Deep Authenticity© confronte compteur, QR, localisation autorisée, relevés, historique, interventions et données de secteur afin de détecter substitutions, chronologies anormales ou incohérences nécessitant investigation.

17. Continuité du service

Coupure, baisse de pression, travaux ou incident peuvent être reliés à une zone, une période, un motif et un statut. Les communications aux usagers proviennent des canaux habilités.

18. Online et Offline

En ligne, les équipes consultent les statuts courants. En Offline, les dernières données signées disponibles sont accessibles avec date de synchronisation et limites de fraîcheur clairement indiquées.

19. AP Ledger et confidentialité

Empreintes minimales de remplacement de compteur, intervention, changement de statut, anomalie et événement critique peuvent être ancrées dans AP Ledger. Consommations individuelles, identités d' abonnés, plans détaillés et données commerciales restent protégés.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si chaque compteur et relevé conserve sa provenance ; si estimation et mesure réelle restent distinctes ; si perte calculée et fuite localisée ne sont pas confondues ; si une anomalie ne devient pas automatiquement une fraude ; si la géolocalisation reste proportionnée ; et si la continuité du service est traçable. LePasseport Water devient ainsi la mémoire vérifiable de l' exploitation du réseau.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 22 — WATER

CHAPITRE 4 — EAUX USÉES, ASSAINISSEMENT, STATIONS D'ÉPURATION, REJETS, RÉUTILISATION, BOUES, QUALITÉ, TRAÇABILITÉ ET ÉCONOMIE CIRCULAIRE DE L'EAU

1. Objet du chapitre

Ce chapitre applique le Passeport Numérique Water à l'assainissement : collecte des eaux usées, réseaux, stations d'épuration, traitement, contrôles, rejets, réutilisation, boues, sous-produits et preuves associées.

2. Réseau d'assainissement

Collecteurs, regards, postes de relevage, déversoirs et autres actifs peuvent disposer d'identités reliées à leur zone, opérateur, inspection, maintenance et historique.

3. Entrée en station

Les volumes et caractéristiques disponibles à l'entrée d'une station peuvent être reliés aux instruments, prélèvements et périodes correspondantes. Mesure, estimation et déclaration restent distinguées.

4. Station d'épuration

Une station peut disposer d'un passeport reliant ouvrages, équipements, procédés, opérateur, maintenances, contrôles et événements. Les paramètres opérationnels sensibles restent réservés aux acteurs habilités.

5. Étapes de traitement

Prétraitement, traitement biologique, clarification, désinfection ou autres étapes peuvent être documentés selon le procédé réel. Une modification de procédé est versionnée et historisée.

6. Capteurs et instrumentation

Débit, niveau, paramètres physico-chimiques ou autres mesures peuvent provenir de capteurs identifiés et calibrés. Toute mesure conserve sa provenance et son contexte.

7. Prélèvements et analyses

Échantillons d'entrée, de procédé ou de sortie peuvent conserver point, date, heure, opérateur, chaîne de garde, laboratoire, méthode et résultat.

8. Qualité de sortie

Les résultats de sortie sont rattachés au point et à la période analysés. AP ne prononce pas seul la conformité d'un rejet et ne généralise pas un résultat ponctuel.

9. Rejets

Un rejet documenté peut être relié au point, à la période, au volume disponible, aux résultats et aux autorisations correspondantes. La décision réglementaire reste attribuée à l'autorité compétente.

10. Déversements et incidents

Débordement, panne, by-pass ou autre événement peut ouvrir un dossier reliant actifs, durée, observations, mesures, interventions et décisions. Une alerte automatique reste distincte d'un incident confirmé.

11. Réutilisation de l'eau

Une eau traitée destinée à un nouvel usage peut disposer d'un statut et d'une chaîne de preuve adaptés. La destination déclarée, la qualité mesurée et l'autorisation d'usage restent trois éléments distincts.

12. Traçabilité de la réutilisation

Origine, traitement, stockage, transfert et destination peuvent être reliés lorsque nécessaire. Le passeport conserve les changements de statut sans présenter une eau réutilisée comme équivalente à toute autre catégorie d'eau.

13. Boues

Les boues produites peuvent recevoir une identité de lot reliant origine, période, analyses, quantité, traitement, transport et destination documentée.

14. Traitement des boues

Épaississement, déshydratation, digestion ou autre traitement peut être enregistré avec procédé, installation et résultats disponibles. Les transformations conservent la généalogie du lot.

15. Valorisation et destination

Valorisation, traitement complémentaire ou autre destination reste attribuée à la source qui la documente. Une destination déclarée reste distincte d'une réception ou d'un traitement confirmé.

16. Deep Authenticity©

Deep Authenticity© confronte actifs, capteurs, calibrations, prélèvements, laboratoires, volumes, rejets, lots de boues, transferts et destinations afin de détecter les incohérences nécessitant vérification.

17. Économie circulaire de l'eau

Réutilisation d’eau, récupération de ressources ou valorisation de sous-produits peuvent être documentées comme nouveaux cycles. Les bénéfices environnementaux allégués restent proportionnés aux preuves disponibles.

18. Online et Offline

Les équipes peuvent consulter les statuts et historiques autorisés. En Offline, les dernières preuves signées disponibles affichent leur date de synchronisation et sont mises à jour au retour du réseau.

19. AP Ledger et confidentialité

Empreintes minimales de prélèvements, rapports, incidents, rejets, changements de statut, lots de boues et transferts critiques peuvent être ancrées dans AP Ledger. Plans sensibles, données industrielles et rapports complets restent protégés.

20. Critères d’acceptation et conclusion

Le modèle est acceptable si mesure et estimation restent distinctes ; si chaque rejet conserve son contexte ; si AP ne prononce pas seul la conformité ; si destination, qualité et autorisation de réutilisation restent séparées ; si les boues conservent leur généalogie ; et si les incidents restent auditables. Le Passeport Water étend ainsi la chaîne de confiance de l’eau potable à l’assainissement et à l’économie circulaire.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 22 — WATER

CHAPITRE 5 — GOUVERNANCE DE L'EAU, AUTORITÉS, OPÉRATEURS, LABORATOIRES, COLLECTIVITÉS, USAGERS, DROITS D'ACCÈS, CYBERSÉCURITÉ, INTEROPÉRABILITÉ ET SOUVERAINETÉ DES DONNÉES HYDRIQUES

1. Objet du chapitre

Ce chapitre définit la gouvernance institutionnelle et numérique du Passeport Water : responsabilités, droits, séparation des rôles, confidentialité, cybersécurité, interopérabilité, portabilité et souveraineté des données liées à l'eau.

2. Principe de gouvernance

Authenticity Plus© organise l'identité, la provenance et l'audit des preuves. Il ne remplace ni l'autorité publique, ni l'opérateur, ni le laboratoire, ni l'expert dans leurs compétences respectives.

3. Autorités compétentes

Les autorités peuvent publier décisions, autorisations, restrictions, seuils ou statuts dans leur périmètre. Toute décision officielle reste attribuée à son émetteur, sa date et son champ d'application.

4. Collectivités

Les collectivités peuvent définir politiques de service, niveaux d'accès, information publique et exigences de continuité selon leurs responsabilités. Elles conservent la maîtrise des règles applicables à leurs données.

5. Opérateurs

Les opérateurs de captage, traitement, distribution ou assainissement accèdent aux actifs et données nécessaires à leur mission. Un opérateur ne reçoit pas automatiquement des droits sur l'ensemble de l'écosystème Water.

6. Laboratoires

Les laboratoires accèdent aux échantillons et informations nécessaires à l'analyse. Ils produisent leurs résultats sans pouvoir modifier silencieusement l'identité, le lieu ou l'historique du prélèvement.

7. Prestataires et sous-traitants

Maintenance, travaux, transport d'échantillons ou autres prestations peuvent être confiés à des tiers avec des droits limités dans le temps, au service et aux actifs concernés.

8. Usagers

Les usagers peuvent consulter les informations publiques, recevoir les communications autorisées et transmettre des signalements. Leur accès ne comprend pas les commandes critiques ni les plans techniques sensibles.

9. Séparation des rôles

Exploiter, prélever, analyser, maintenir, contrôler, décider et auditer sont des fonctions distinctes. Le principe du moindre privilège limite chaque acteur aux opérations nécessaires.

10. Droits d'accès dynamiques

Les autorisations peuvent dépendre du rôle, de l'organisation, du site, de l'actif, du type de donnée, de la durée et du contexte. Elles sont journalisées, révisables et révocables.

11. Validation multiniveau

Changement d'identité d'un actif, correction critique, publication sanitaire, modification de configuration ou clôture d'incident peut nécessiter plusieurs validations selon les règles de gouvernance.

12. Confidentialité

Identités d'abonnés, consommations individuelles, plans détaillés, accès aux installations, configurations, rapports sensibles et secrets industriels restent protégés par des vues et droits adaptés.

13. Information publique

Une information destinée aux usagers doit conserver sa source, sa zone, sa période et son statut. Les données simplifiées ne doivent pas supprimer les éléments indispensables à une interprétation correcte.

14. Cybersécurité

Comptes privilégiés, certificats, capteurs, automates, passerelles, API et consoles sont protégés, segmentés, journalisés et révocables. Le scan d'un QR public ne donne jamais accès à une commande opérationnelle critique.

15. Interopérabilité

SIG, systèmes de supervision, laboratoires, facturation, maintenance, IoT et autres plateformes autorisées peuvent échanger avec AP. Toute donnée importée conserve source, version, horodatage et niveau d'autorité.

16. Portabilité

Un changement d'opérateur, fournisseur, laboratoire ou plateforme ne doit pas effacer l'historique vérifiable. Les données essentielles doivent pouvoir être exportées selon des formats et règles gouvernés.

17. Souveraineté des données hydriques

L'entité compétente doit pouvoir définir où les données sont conservées, qui peut y accéder, pour quelles finalités, pendant combien de temps et selon quelles règles de transfert.

18. Audit et responsabilité

Les journaux permettent de reconstituer les actions critiques : création, modification, validation, révocation, intervention ou publication. L'auditeur peut vérifier les preuves sans disposer automatiquement du pouvoir de les modifier.

19. AP Ledger

Empreintes minimales des habilitations critiques, changements d'identité, validations, rapports, incidents, révocations et événementsmajeurs peuvent être ancrées dans AP Ledger. Données personnelles, plans détaillés et secrets techniques restent hors des couches irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si les compétences des autorités, opérateurs, laboratoires et collectivités restent distinctes ; si les prestataires ont des droits temporaires et révocables ; si les données d' usagers sont protégées ; si un QR public n'ouvre aucune commande critique ; si la portabilité préserve l'historique ; et si la souveraineté des données hydriques reste gouvernable. Cette architecture fournit le socle nécessaire à la clôture fonctionnelle de l'application Water.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 22 — WATER

CHAPITRE 6 — SYNTHÈSE FONCTIONNELLE, CRITÈRES D'ACCEPTATION ET CLÔTURE DE L'APPLICATION WATER

1. Objet du chapitre

Ce chapitre clôt le Point 22 — Water. Il consolide la ressource, le captage, le traitement, le stockage, la distribution, la qualité, les prélèvements, les laboratoires, les compteurs, les fuites, l'assainissement, la réutilisation, la gouvernance, la cybersécurité et AP Ledger.

2. Mission consolidée

Le Passeport Numérique Water constitue une mémoire vérifiable de la chaîne de l'eau. Authenticity Plus© / Deep Authenticity© authentifie actifs, données, mesures, documents et interventions sans se substituer aux autorités sanitaires, réglementaires ou aux professionnels compétents.

3. Ressource et captage

Source, forage, barrage, prise d'eau ou autre ressource peut être relié à ses installations, opérateurs, mesures, inspections et événements documentés.

4. Traitement et stockage

Usines, unités de traitement, réservoirs et ouvrages disposent d'identités et d'historiques permettant de relier équipements, contrôles, maintenances et statuts.

5. Réseau de distribution

Conduites, vannes, pompes, secteurs et branchements peuvent être reliés à leur identité, localisation autorisée, maintenance et historique.

6. QR Codes dynamiques

Le QR dynamique permet une vérification adaptée au rôle, mais sa copie visuelle ne suffit jamais à reproduire l'identité ou à prouver l'état réel d'un actif.

7. Capteurs et calibration

Débit, pression, niveau et paramètres de qualité peuvent provenir de capteurs identifiés. Leur calibration, configuration, localisation et maintenance contribuent à la confiance dans les données.

8. Qualité et prélèvements

Chaque résultat conserve point, date, méthode, unité, prélèvement, chaîne de garde et laboratoire ou capteur. Un résultat ponctuel n'est pas automatiquement généralisé à tout un réseau.

9. Qualification sanitaire

AP ne déclare pas seul qu'une eau est potable, impropre ou dangereuse. Les décisions et qualifications restent attribuées aux autorités et professionnels habilités.

10. Alertes et contamination

Une valeur atypique ou un signal de contamination déclenche une vérification. Suspicion, confirmation, décision et communication restent des étapes distinctes.

11. Compteurs et consommation

Compteurs et relevés conservent leur provenance. Mesure réelle, télérelevé, estimation et correction restent identifiables ; une consommation inhabituelle ne constitue pas automatiquement une fraude.

12. Pertes et fuites

Une perte calculée par bilan hydraulique reste distincte d'une fuite physiquement localisée. Les alertes de fuite restent des hypothèses opérationnelles jusqu'à vérification.

13. Maintenance et continuité

Maintenance préventive, corrective, interventions, coupures et remises en service peuvent être historisées. Online fournit le statut courant ; Offline indique clairement la fraîcheur des données signées disponibles.

14. Assainissement

Réseaux d'eaux usées, stations d'épuration, procédés, capteurs, analyses, rejets et incidents peuvent être reliés dans une chaîne de preuve continue.

15. Réutilisation et économie circulaire

Pour l'eau réutilisée, destination déclarée, qualité mesurée et autorisation d'usage restent distinctes. Boues et sous-produits peuvent conserver une généalogie lors de leurs transformations et valorisations.

16. Deep Authenticity©

Deep Authenticity© confronte identité, QR, localisation autorisée, capteurs, calibration, prélèvements, laboratoires, relevés, maintenance, incidents, rejets et chronologie afin de signaler les incohérences explicables.

17. Gouvernance

Autorités, collectivités, opérateurs, laboratoires, prestataires, auditeurs et usagers disposent de rôles séparés. Exploiter, prélever, analyser, maintenir, contrôler, décider et auditer ne sont pas fusionnés.

18. Confidentialité, cybersécurité et souveraineté

Identités d’abonnés, consommations, plans détaillés, configurations et informations sensibles sont protégés. Les accès sont limités, révocables et auditables ; l’entité compétente gouverne localisation, conservation et transfert des données.

19. AP Ledger et critères d’acceptation

AP Ledger reçoit uniquement des empreintes minimales d’identité, calibration, prélèvement, rapport, intervention, validation, incident ou changement critique. Le modèle est acceptable si provenance, séparation des rôles, protection des données, traçabilité Offline et attribution des décisions sont préservées.

20. Clôture du Point 22 — Water

Le Point 22 — Water est désormais fonctionnellement défini : ressource, captage, traitement, stockage, distribution, QR dynamiques, capteurs, calibration, qualité, prélèvements, laboratoires, compteurs, consommation, pertes, fuites, maintenance, assainissement, rejets, réutilisation, économie circulaire, Deep Authenticity©, gouvernance, confidentialité, cybersécurité, souveraineté, interopérabilité, audit et AP Ledger. Le Volume IV peut désormais poursuivre avec le Point 23 — Telecom.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 23 — TELECOM

CHAPITRE 1 — IDENTITÉ NUMÉRIQUE DES INFRASTRUCTURES TÉLÉCOM, RÉSEAUX, ÉQUIPEMENTS, SITES, QR CODES DYNAMIQUES, MAINTENANCE, PROVENANCE ET PASSEPORT NUMÉRIQUE TELECOM

1. Objet du chapitre

Le Point 23 — Telecom transpose Authenticity Plus© / Deep Authenticity© aux infrastructures et services de télécommunications. Le Passeport Numérique Telecom relie sites, équipements, réseaux, opérateurs, configurations, maintenances, incidents et preuves techniques.

2. Mission sectorielle

La mission est d'authentifier l'identité et l'historique des actifs télécoms ainsi que la provenance des opérations documentées, sans exposer publiquement les configurations ou informations pouvant compromettre la sécurité des réseaux.

3. Identité du site

Station radio, central, nœud, datacenter, armoire, chambre technique ou autre site peut disposer d'une identité reliée à l'opérateur, à la localisation autorisée, aux actifs installés et à son statut.

4. Identité des équipements

Antenne, radio, routeur, commutateur, équipement optique, alimentation, batterie ou autre actif peut disposer d'un passeport unitaire avec fabricant, modèle, identifiant, installation, statut et historique.

5. Réseaux physiques

Fibre, câble, liaison, conduit ou autre infrastructure peut être relié à son segment, ses extrémités, son opérateur et ses interventions. Les tracés détaillés restent protégés selon leur sensibilité.

6. QR Code dynamique

Un QR dynamique apposé sur un actif autorisé peut ouvrir une fiche adaptée au rôle : identité, maintenance, inspection ou documentation. Le QR seul ne donne jamais accès à une commande réseau critique.

7. Installation et mise en service

Installation, remplacement ou mise en service d'un équipement peut être documenté avec date, intervenant, site, références et validation habilitée.

8. Configuration

Les changements importants de configuration peuvent être versionnés avec auteur, date, motif et approbation lorsque nécessaire. Les paramètres secrets ou exploitables ne sont pas publiés dans le passeport public.

9. Maintenance

Inspection, entretien, remplacement, mise à jour ou réparation peut être relié à l'actif, au technicien habilité, à la date et au résultat de l'intervention.

10. Pièces et composants

Les composants critiques remplacés peuvent conserver leur provenance et leur relation avec l' équipement parent, permettant d'identifier substitution, incompatibilité ou historique de remplacement.

11. Provenance des données

Alarmes, mesures de performance et événements techniques doivent conserver leur système source, leur horodatage et leur contexte. Une donnée dérivée reste distinguée de l'événement brut.

12. Géolocalisation de cohérence

Pour une intervention autorisée, la proximité entre terminal et site peut contribuer à vérifier la cohérence de l'opération. Cette géolocalisation reste ponctuelle, proportionnée et ne devient pas un suivi permanent du technicien.

13. Deep Authenticity©

Deep Authenticity© confronte identité de l'actif, QR, site, localisation autorisée, configuration, composants, maintenance et chronologie afin de détecter substitutions ou incohérences nécessitant vérification.

14. Actif inconnu ou substitué

Un équipement non reconnu, déplacé ou utilisant une identité incohérente déclenche une vérification. Le système conserve les indices sans qualifier automatiquement l'événement de fraude ou d'intrusion.

15. Online

En ligne, les acteurs habilités consultent le statut courant, les dernières interventions et les preuves autorisées selon leurs droits.

16. Offline

En absence de réseau, un terminal habilité peut vérifier les dernières preuves signées mises en cache. La date de dernière synchronisation et les limites de fraîcheur sont explicitement indiquées.

17. Signalement et incident

Une anomalie, panne ou dommage peut ouvrir un dossier reliant actif, site, alerte, observation et intervention.Le signal initial reste distinct du diagnostic technique confirmé.

18. Cybersécurité

Comptes, certificats, clés, interfaces, API, passerelles et consoles sont protégés par segmentation, authentification, journalisation et révocation. Le Passeport Telecom ne doit pas devenir une nouvelle surface publique de commande du réseau.

19. AP Ledger et confidentialité

Empreintes minimales d'identité, installation, remplacement, changement critique, maintenance et incident peuvent être ancrées dans AP Ledger. Configurations détaillées, secrets, topologies sensibles et données d'abonnés restent hors des couches publiques ou irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si chaque actif conserve une identité et un historique ; si un QR ne donne aucune commande critique ; si les configurations sensibles restent protégées ; si la géolocalisation est proportionnée ; si les événements conservent leur provenance ; et si une anomalie déclenche une vérification sans accusation automatique. Le Passeport Telecom fournit ainsi une chaîne de confiance pour les infrastructures de télécommunications.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 23 — TELECOM

CHAPITRE 2 — ABONNÉS, SIM/eSIM, TERMINAUX, IDENTITÉ DES ÉQUIPEMENTS, ACTIVATION, PORTABILITÉ, FRAUDE D'IDENTITÉ ET AUTHENTIFICATION DES OPÉRATIONS

1. Objet du chapitre

Ce chapitre applique le Passeport Numérique Telecom aux identités et opérations associées aux abonnements, SIM/eSIM et terminaux. Il vise à renforcer la provenance des opérations sans exposer inutilement les données personnelles des abonnés.

2. Principe de séparation

L'identité de l'abonné, l'identité de la ligne, l'identité de la SIM/eSIM et l'identité du terminal sont des objets distincts. Leur association peut évoluer et doit conserver un historique autorisé.

3. Identité de l'abonné

Les données d'identité nécessaires à une relation d'abonnement sont protégées selon les règles applicables. AP peut conserver une preuve de vérification sans rendre les documents d'identité publiquement accessibles.

4. Identité de la ligne

Une ligne ou un abonnement peut disposer d'un identifiant de passeport reliant opérateur, statut, période et événements autorisés, sans exposer publiquement le numéro ou les données personnelles.

5. SIM physique

Une SIM peut être reliée à son identité technique, son opérateur, son statut d'activation, ses remplacements et ses associations autorisées.

6. eSIM

Un profil eSIM peut disposer d'une identité et d'un cycle de vie documenté : émission, téléchargement autorisé, activation, suspension, transfert ou révocation selon les mécanismes de l'opérateur.

7. Terminaux

Un terminal peut être associé à des références techniques nécessaires à la vérification. Le Passeport Telecom ne doit pas devenir un outil public permettant de suivre l'usage ou la localisation personnelle d'un appareil.

8. Activation

Une activation relie demande, canal, contrôles, ligne, SIM/eSIM, date et résultat. L'acteur ou le système ayant autorisé l'opération reste identifiable.

9. Remplacement de SIM

Une demande de remplacement doit être distinguée d'une activation initiale. Les contrôles et validations appliqués sont documentés afin de renforcer la traçabilité d'une opération sensible.

10. SIM Swap présumé

Un changement inhabituel de SIM ou une incohérence peut déclencher une vérification renforcée. Une anomalie ne constitue pas automatiquement une fraude et AP n'attribue pas seul une intention malveillante.

11. Portabilité du numéro

Une portabilité peut conserver opérateur d'origine, opérateur destinataire, demande, validations, date d'exécution et statut, tout en protégeant les informations personnelles et commerciales.

12. Changement de terminal

L'association d'une ligne à un nouveau terminal peut être historisée lorsqu'elle est nécessaire à la sécurité ou au service. Elle ne doit pas créer par défaut un historique public des appareils utilisés.

13. Authentification renforcée

Les opérations sensibles peuvent exiger plusieurs facteurs ou contrôles selon le risque et les règles de l'opérateur. AP documente la preuve de validation sans exposer les secrets d'authentification.

14. Deep Authenticity©

Deep Authenticity© confronte identité de l'opération, historique de ligne, SIM/eSIM, terminal, canal, horodatage et validations autorisées afin de détecter des incohérences nécessitant vérification.

15. Fraude d'identité présumée

Documents incohérents, demandes concurrentes ou séquences anormales peuvent générer un signal. Le système conserve les indices et leur provenance sans prononcer automatiquement une fraude ou une culpabilité.

16. Révocation et récupération

En cas d'incident, un profil, certificat ou accès peut être suspendu ou révoqué par les acteurs habilités. Les étapes de récupération et de réactivation restent auditables.

17. Online et Offline

Les opérations critiques d’abonnement nécessitant un statut courant privilégient le mode Online. Lorsque des preuves Offline sont admises, leur fraîcheur et leur périmètre doivent être explicitement limités.

18. Vie privée

Les données d’identité, numéros, historiques d’appareils, informations de localisation et autres données d’abonnés sont minimisées, compartimentées et accessibles uniquement selon les finalités autorisées.

19. AP Ledger

Empreintes minimales d’activation, remplacement, portabilité, révocation et validation critique peuvent être ancrées dans AP Ledger. Documents d’identité, numéros, secrets, historiques détaillés et données personnelles restent hors des couches publiques ou irréversibles.

20. Critères d’acceptation et conclusion

Le modèle est acceptable si abonné, ligne, SIM/eSIM et terminal restent distingués ; si les opérations sensibles sont attribuables ; si un remplacement de SIM peut déclencher une vérification renforcée ; si aucune anomalie n’est automatiquement qualifiée de fraude ; si les secrets d’authentification restent protégés ; et si la vie privée est préservée. Le Passeport Telecom renforce ainsi la confiance dans le cycle de vie des abonnements et des identités techniques.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 23 — TELECOM

CHAPITRE 3 — SERVICES RÉSEAU, QUALITÉ DE SERVICE, COUVERTURE, INCIDENTS, PANNES, MAINTENANCE, SLA, ITINÉRANCE ET CONTINUITÉ OPÉRATIONNELLE

1. Objet du chapitre

Ce chapitre applique le Passeport Numérique Telecom à l'exploitation des services réseau : disponibilité, qualité de service, couverture, incidents, maintenance, engagements de service, itinérance et continuité opérationnelle.

2. Identité du service

Un service réseau peut être relié à l'opérateur, au périmètre, à la technologie, à la période et aux infrastructures qui le supportent. Le passeport distingue l'identité du service de celle des équipements sous-jacents.

3. Qualité de service

Débit, latence, disponibilité, perte de paquets ou autres indicateurs peuvent être associés à une méthode, un point de mesure, une période et une source. Un résultat ponctuel ne représente pas automatiquement la performance globale du réseau.

4. Mesures réseau

Les mesures issues de sondes, équipements ou plateformes conservent leur provenance, leur horodatage et leur contexte. Mesure brute, agrégation et indicateur calculé restent distingués.

5. Couverture

Une carte de couverture doit conserver technologie, période, méthode, résolution et origine des données. Une couverture modélisée reste distincte d'une mesure réellement effectuée sur le terrain.

6. Expérience utilisateur

Les observations ou tests réalisés depuis des terminaux peuvent contribuer à l'évaluation du service, sous réserve de minimisation des données personnelles et de contextualisation des conditions de mesure.

7. Incident réseau

Une panne, dégradation ou interruption peut ouvrir un dossier reliant zone, services, actifs, alertes, chronologie, interventions et statut.

8. Alerte et diagnostic

Une alerte automatique reste distincte d'un diagnostic technique. Plusieurs alarmes peuvent être corrélées, mais la corrélation demeure une hypothèse tant qu'elle n'est pas confirmée.

9. Cause racine

La cause racine d'un incident est attribuée uniquement après investigation par les acteurs habilités. Deep Authenticity© peut fournir des preuves de cohérence sans inventer une causalité.

10. Maintenance

Maintenance préventive, corrective, remplacement ou mise à jour peut être relié à l'équipement, au site, à l'intervenant et au résultat.

11. SLA

Un engagement de niveau de service peut être relié au contrat ou référentiel applicable, aux indicateurs, à la période et aux preuves de mesure. AP ne décide pas seul qu'un SLA est respecté ou violé.

12. Calcul de disponibilité

Les calculs de disponibilité conservent formule, période, exclusions déclarées, événements pris en compte et version. Deux taux calculés selon des règles différentes ne sont pas présentés comme directement équivalents.

13. Itinérance

Les événements d'itinérance peuvent impliquer plusieurs opérateurs. Les responsabilités, données et preuves sont séparées selon le rôle de chaque acteur et les accords applicables.

14. Interconnexion

Les incidents aux frontières entre réseaux peuvent conserver les observations de chaque opérateur. Une divergence entre sources déclenche une investigation plutôt qu'une attribution automatique.

15. Continuité opérationnelle

Redondance, bascule, restauration ou mode dégradé peuvent être documentés comme événements de continuité. Les mécanismes techniques sensibles ne sont pas exposés dans les vues publiques.

16. Deep Authenticity©

Deep Authenticity© confronte services, actifs, alarmes, mesures, configurations autorisées, maintenance et chronologie afin de détecter les incohérences et de soutenir l'investigation.

17. Online et Offline

Le statut réseau courant exige généralement le mode Online. Les preuves Offline sont limitées aux informations signées mises en cache et affichent clairement leur date de synchronisation.

18. Information client

Les communications de panne, maintenance ou rétablissement destinées aux clients restent attribuées à l'opérateur ou à l'autorité compétente. AP peut en authentifier la provenance sans se substituer à l'émetteur.

19. AP Ledger et confidentialité

Empreintes minimales d'incidents, maintenances, changements critiques, calculs de SLA et restaurations peuvent être ancrées dans AP Ledger. Topologies détaillées, données d'abonnés, journaux sensibles et secrets d'exploitation restent protégés.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si mesure ponctuelle et performance globale restent distinctes ; si couverture modélisée et mesure terrain ne sont pas confondues ; si alerte, diagnostic et cause racine sont séparés ; si les calculs SLA restent reproductibles ; et si les incidents inter-opérateurs ne conduisent pas à une attribution automatique. Le Passeport Telecom fournit ainsi une mémoire vérifiable de la qualité et de la continuité du service.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 23 — TELECOM

CHAPITRE 4 — CYBERSÉCURITÉ TÉLÉCOM, ATTAQUES, USURPATION, ÉQUIPEMENTS COMPROMIS, FRAUDE RÉSEAU, RÉSILIENCE, INVESTIGATION ET RÉCUPÉRATION

1. Objet du chapitre

Ce chapitre définit l'usage du Passeport Numérique Telecom dans la détection, la qualification, l' investigation et la récupération des incidents de cybersécurité affectant les infrastructures et services télécoms.

2. Principe de non-attribution automatique

Une alerte, une anomalie ou un équipement incohérent peut déclencher une investigation. Authenticity Plus© / Deep Authenticity© ne désigne pas automatiquement un attaquant et ne transforme pas un indice technique en accusation.

3. Identité de sécurité des actifs

Équipements, sites, logiciels, certificats et composants peuvent être reliés à des identités et versions autorisées. Une divergence avec la référence connue constitue un signal à vérifier.

4. Équipement compromis présumé

Un actif présentant un comportement, une configuration ou une identité inhabituelle peut être placé sous investigation par les acteurs habilités. Le statut présumé reste distinct d'une compromission confirmée.

5. Usurpation d'identité technique

L'utilisation incohérente d'un identifiant, certificat ou identité d'équipement peut être détectée par confrontation avec l'historique, le site, les associations autorisées et les preuves disponibles.

6. Certificats et clés

Le cycle de vie des certificats peut être documenté : émission, activation, rotation, expiration et révocation. Les clés secrètes elles-mêmes ne sont jamais inscrites dans le passeport ou AP Ledger.

7. Logiciels et firmware

Versions autorisées, mises à jour et changements critiques peuvent être historisés. Les détails exploitables et secrets de sécurité restent protégés dans les systèmes spécialisés.

8. Changement non autorisé

Une configuration, version ou composant non attendu peut générer une alerte. L'écart est conservé avec sa provenance et son contexte avant toute conclusion.

9. Fraude réseau présumée

Une séquence anormale, une identité dupliquée ou un usage incohérent peut produire un signal de fraude présumée. La qualification définitive reste du ressort des acteurs compétents.

10. Corrélation d'incidents

Plusieurs événements peuvent être corrélés entre sites, équipements ou services. Une corrélation algorithmique est une hypothèse d'investigation et non une preuve autonome de causalité.

11. Centre de supervision

Les équipes de supervision peuvent visualiser alertes, statuts, incidents et chronologies autorisées. Le système distingue événement brut, alerte, diagnostic, décision et action.

12. Isolation et restriction

Un équipement ou accès suspect peut être isolé, suspendu ou restreint par les systèmes habilités. Le Passeport documente l'action et son autorité sans exposer les mécanismes de commande.

13. Résilience

Redondance, bascule, segmentation, mode dégradé et restauration peuvent être documentés afin de conserver la chronologie de continuité du service.

14. Investigation

Le dossier d'investigation peut réunir identités, versions, journaux, changements, interventions et preuves techniques. L'accès est strictement limité selon les rôles.

15. Deep Authenticity©

Deep Authenticity© confronte identités, certificats, versions, configurations autorisées, sites, maintenances et chronologie afin de repérer substitutions, divergences ou séquences anormales.

16. Récupération

Réinstallation, remplacement, rotation de certificats, reconfiguration ou remise en service peut être documenté. L'état antérieur reste conservé dans l'historique d'audit.

17. Clôture de l'incident

La clôture est attribuée à l'acteur habilité et reliée aux éléments qui la justifient. AP ne décide pas seul qu'un système est redevenu sûr.

18. Confidentialité et minimisation

Les investigations privilégient les données techniques nécessaires. Données d'abonnés, contenus de communication, secrets, topologies détaillées et informations personnelles restent protégés.

19. AP Ledger

Empreintes minimales de versions, révocations, changements critiques, mises sous restriction, récupérations et clôtures peuvent être ancrées dans AP Ledger. Secrets, journaux détaillés et données sensibles restent hors des couches irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si suspicion et compromission confirmée restent distinctes ; si les clés secrètes ne sont jamais inscrites ; si corrélation et causalité ne sont pas confondues ; si l'isolation reste réservée aux systèmes habilités ; si la récupération conserve l'historique ; et si AP n'attribue ni attaquant ni sécurité restaurée de manière autonome. Le Passeport Telecom devient ainsi un socle de confiance pour la résilience cyber des télécommunications.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 23 — TELECOM

CHAPITRE 5 — GOUVERNANCE TÉLÉCOM, OPÉRATEURS, RÉGULATEURS, ÉQUIPEMENTIERS, PRESTATAIRES, ABONNÉS, INTEROPÉRABILITÉ, CONFIDENTIALITÉ, SOUVERAINETÉ ET AUDIT

1. Objet du chapitre

Ce chapitre définit la gouvernance du Passeport Numérique Telecom : responsabilités, habilitations, séparation des rôles, confidentialité, interopérabilité, portabilité, souveraineté, cybersécurité et audit.

2. Principe de gouvernance

Authenticity Plus© organise l'identité, la provenance et l'historique des preuves sans se substituer aux compétences des opérateurs, régulateurs, autorités ou autres acteurs habilités.

3. Opérateurs

Chaque opérateur administre les actifs, services et données relevant de son périmètre. L'accès à un domaine ne donne pas automatiquement accès aux infrastructures ou données d'un autre opérateur.

4. Régulateurs et autorités

Les décisions, autorisations, obligations ou constats officiels restent attribués à l'autorité qui les émet, avec date et périmètre. AP authentifie leur provenance sans créer lui-même une décision réglementaire.

5. Équipementiers

Fabricants et équipementiers peuvent fournir identité produit, versions, certificats, informations de maintenance ou avis techniques. Ils ne disposent pas automatiquement de droits d'exploitation sur les réseaux installés.

6. Prestataires

Intégrateurs, mainteneurs et sous-traitants reçoivent des habilitations limitées à leur mission, aux sites concernés et à une durée déterminée. La fin de mission entraîne révocation ou révision des accès.

7. Abonnés

Les abonnés disposent d'un accès aux informations et opérations autorisées concernant leurs services. Leurs données personnelles, historiques et identités techniques restent protégés.

8. Séparation des rôles

Exploiter, configurer, maintenir, superviser, auditer, réguler et décider sont des fonctions distinctes. Le principe du moindre privilège limite les droits de chaque acteur.

9. Droits d'accès dynamiques

Les autorisations peuvent dépendre de l'organisation, du rôle, du site, de l'actif, du service, de la durée et du niveau de sensibilité. Elles sont journalisées et révocables.

10. Validation multiniveau

Les opérations critiques telles qu'un changement majeur de configuration, une révocation, une mise en service ou une clôture d'incident peuvent nécessiter plusieurs validations.

11. Interopérabilité

OSS/BSS, supervision, inventaires, systèmes IoT, plateformes d'identité, maintenance et autres solutions autorisées peuvent échanger avec AP. Les données importées conservent source, version, horodatage et niveau d'autorité.

12. Interopérabilité inter-opérateurs

Portabilité, itinérance et interconnexion nécessitent des preuves échangées entre organisations. Chaque acteur conserve la responsabilité de ses propres données et décisions.

13. Portabilité technologique

Le changement de fournisseur ou de plateforme ne doit pas effacer l'historique vérifiable. Les actifs et événements essentiels doivent rester exportables selon des formats gouvernés.

14. Confidentialité

Données d'abonnés, contenus de communication, topologies détaillées, configurations, clés, journaux sensibles et secrets commerciaux sont compartimentés et accessibles uniquement selon les finalités autorisées.

15. Souveraineté des données

L'entité compétente doit pouvoir définir localisation, conservation, accès, transfert et durée de vie des données selon les exigences applicables. Les données sensibles ne sont pas rendues publiques par défaut.

16. Cybersécurité institutionnelle

Comptes privilégiés, certificats, API, consoles et accès fournisseurs sont protégés par authentification renforcée, segmentation, journalisation, rotation et révocation.

17. Audit indépendant

Les auditeurs habilités peuvent vérifier identités, changements, habilitations et journaux nécessaires à leur mission sans recevoir automatiquement le pouvoir de modifier les actifs ou les preuves.

18. Responsabilité et traçabilité

Toute action critique doit pouvoir être reliée à un acteur ou système autorisé, une date, un périmètre et un résultat. Les comptes partagés ou non attribuables sont limités dans les fonctions sensibles.

19. AP Ledger

Empreintes minimales d'habilitations, validations, changements critiques, révocations, mises en service et clôtures d'incident peuvent être ancrées dans AP Ledger. Les secrets, données d'abonnés et journaux détaillés restent hors des couches irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si opérateurs, régulateurs, équipementiers et prestataires restent dans leurs compétences ; si les accès fournisseurs sont temporaires et révocables ; si l'interopérabilité conserve la provenance ; si la portabilité préserve l'historique ; si les données sensibles restent souveraines et protégées ; et si l'audit reste indépendant. Cette gouvernance fournit le socle nécessaire à la clôture fonctionnelle de l'application Telecom.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 23 — TELECOM

CHAPITRE 6 — SYNTHÈSE FONCTIONNELLE, CRITÈRES D'ACCEPTATION ET CLÔTURE DE L'APPLICATION TELECOM

1. Objet du chapitre

Ce chapitre clôt le Point 23 — Telecom. Il consolide infrastructures, équipements, réseaux, abonnements, SIM/eSIM, terminaux, qualité de service, incidents, cybersécurité, gouvernance, interopérabilité, souveraineté et AP Ledger.

2. Mission consolidée

Le Passeport Numérique Telecom constitue une mémoire vérifiable des actifs, identités techniques, opérations et preuves autorisées. Authenticity Plus© / Deep Authenticity© renforce la confiance sans devenir un système autonome de commande réseau, de surveillance des abonnés ou d'attribution d'attaque.

3. Sites et infrastructures

Stations radio, centraux, nœuds, datacenters, armoires, fibres, câbles et autres infrastructures peuvent conserver identité, opérateur, localisation autorisée, statut, installation, maintenance et historique.

4. Équipements et composants

Antennes, radios, routeurs, commutateurs, équipements optiques, alimentations et composants critiques disposent d'identités reliées à leur équipement parent, leur version et leurs remplacements documentés.

5. QR Codes dynamiques

Un QR dynamique permet une vérification adaptée au rôle. Sa copie visuelle ne suffit pas à reproduire l'identité d'un actif et il n'ouvre jamais, à lui seul, une commande réseau critique.

6. Configurations et versions

Les changements critiques de configuration, logiciel ou firmware sont versionnés avec auteur, date, motif et validation lorsque nécessaire. Secrets et paramètres exploitables restent hors des vues publiques.

7. Abonné, ligne, SIM/eSIM et terminal

L’identité de l’abonné, celle de la ligne, celle de la SIM/eSIM et celle du terminal restent quatre objets distincts. Leurs associations peuvent évoluer tout en conservant un historique autorisé et respectueux de la vie privée.

8. Activation, remplacement et portabilité

Activation, remplacement de SIM, changement de terminal et portabilité peuvent être reliés à la demande, au canal, aux contrôles, aux validations et au résultat. Les opérations sensibles restent attribuables.

9. Fraude et SIM Swap présumés

Une incohérence, un changement inhabituel ou une identité dupliquée peut déclencher une vérification renforcée. Une anomalie ne constitue pas automatiquement une fraude, un SIM Swap malveillant ou une culpabilité.

10. Qualité de service et couverture

Débit, latence, disponibilité, perte de paquets et couverture conservent méthode, source, période et contexte. Mesure ponctuelle, agrégation, couverture modélisée et mesure terrain restent distinguées.

11. Incidents, alertes et cause racine

Événement brut, alerte, diagnostic, cause racine, décision et action sont des étapes distinctes. Une corrélation technique soutient l’investigation mais ne crée pas automatiquement une causalité.

12. SLA et continuité

Les calculs de SLA conservent formule, période, exclusions et version. Redondance, bascule, restauration et mode dégradé peuvent être historisés sans exposer les mécanismes sensibles de continuité.

13. Itinérance et interconnexion

Les opérations impliquant plusieurs opérateurs conservent la provenance des preuves et la responsabilité de chaque acteur. Une divergence entre opérateurs ouvre une investigation plutôt qu’ une attribution automatique.

14. Cybersécurité

Identités techniques, certificats, versions et configurations autorisées peuvent être confrontés afin de détecter des écarts. Suspicion et compromission confirmée restent distinctes ; les clés secrètes ne sont jamais inscrites dans le passeport ou AP Ledger.

15. Deep Authenticity©

Deep Authenticity© confronte actifs, QR, sites, identités techniques, versions, opérations, mesures, maintenances, incidents et chronologies afin de signaler des incohérences explicables et investigables.

16. Résilience et récupération

Isolation, restriction, remplacement, réinstallation, rotation de certificats et remise en service restent réservés aux systèmes et acteurs habilités. La récupération conserve l'état antérieur et la chronologie d'audit.

17. Gouvernance

Opérateurs, régulateurs, équipementiers, prestataires, auditeurs et abonnés disposent de rôles séparés. Exploiter, configurer, maintenir, superviser, auditer, réguler et décider ne sont pas fusionnés.

18. Confidentialité, interopérabilité et souveraineté

Données d'abonnés, contenus de communication, topologies, configurations, journaux sensibles et secrets restent protégés. Les échanges inter-systèmes conservent source et version ; la localisation, la conservation et le transfert des données restent gouvernables.

19. AP Ledger et critères d'acceptation

AP Ledger reçoit uniquement des empreintes minimales d'identité, mise en service, changement critique, validation, révocation, maintenance, incident ou clôture. Le modèle est acceptable si les secrets restent hors chaîne, si les droits sont révocables, si la provenance est conservée, si les rôles sont séparés et si aucune anomalie ne devient automatiquement une accusation.

20. Clôture du Point 23 — Telecom

Le Point 23 — Telecom est désormais fonctionnellement défini : infrastructures, équipements, QR dynamiques, configurations, maintenance, abonnés, lignes, SIM/eSIM, terminaux, activation, portabilité, qualité de service, couverture, SLA, itinérance, interconnexion, incidents, cybersécurité, Deep Authenticity©, résilience, gouvernance, confidentialité, interopérabilité, souveraineté, audit et AP Ledger. Le Volume IV peut désormais poursuivre avec l'application sectorielle suivante.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 24 — TOURISME

CHAPITRE 1 — IDENTITÉ NUMÉRIQUE TOURISTIQUE, ÉTABLISSEMENTS, HÉBERGEMENTS, PRESTATAIRES, RÉSERVATIONS, BILLETS, QR CODES DYNAMIQUES, AVIS ET PASSEPORT NUMÉRIQUE TOURISME

1. Objet du chapitre

Le Point 24 — Tourisme transpose Authenticity Plus© / Deep Authenticity© à l'écosystème touristique. Le Passeport Numérique Tourisme relie établissements, hébergements, prestataires, offres, réservations, billets, visites, certifications, avis et preuves de service.

2. Mission sectorielle

La mission est de rendre vérifiables l'identité des acteurs et la provenance des informations touristiques, sans transformer AP en agence de voyage, autorité de classement ou plateforme autonome de décision.

3. Identité de l'établissement

Hôtel, résidence, auberge, camping, agence, site touristique, musée ou autre établissement peut disposer d'une identité reliée à son exploitant, sa localisation, son statut et ses informations documentées.

4. Identité du prestataire

Guide, transporteur, agence, organisateur ou autre prestataire peut disposer d'un profil vérifiable reliant organisation, rôle, habilitations déclarées et historique autorisé.

5. Hébergements et unités

Un établissement peut relier chambres, logements ou autres unités à leur catégorie, caractéristiques documentées, disponibilité publiée et historique de maintenance lorsque pertinent.

6. Offre touristique

Une offre conserve prestataire, description, période, conditions, inclusions et version. Une modification tarifaire ou contractuelle importante doit pouvoir être distinguée de l'offre précédemment publiée.

7. Réservation

Une réservation peut être reliée à l'offre, au canal, à la date, au statut et aux conditions applicables. Les données personnelles du voyageur restent protégées et ne sont jamais rendues publiques par défaut.

8. Billet et titre d'accès

Billet, voucher ou titre d'accès peut disposer d'une identité vérifiable associée à l'émetteur, au service, à la période de validité et au statut d'utilisation.

9. QR Code dynamique

Un QR dynamique peut permettre de vérifier établissement, billet, réservation ou service selon le rôle. Une copie visuelle du QR ne suffit pas à reproduire un droit d'accès valide.

10. Check-in et validation

Une arrivée, une entrée ou une prestation consommée peut produire un événement de validation attribuable. La vérification doit limiter les données affichées au strict nécessaire.

11. Classement et certification

Étoiles, labels, licences ou certifications restent attribués à l'organisme qui les émet. AP conserve source, date,portée et statut sans inventer ni prolonger une certification expirée.

12. Photos et descriptions

Les contenus descriptifs peuvent conserver leur source et leur date. Une photographie promotionnelle ou une description commerciale reste distincte d'une certification indépendante.

13. Avis et évaluations

Un avis peut être relié à son auteur ou à une preuve de transaction selon les règles de la plateforme, tout en protégeant l'identité lorsque nécessaire. Un avis authentifié reste une opinion et non un fait universel.

14. Faux avis et manipulation présumée

Des séquences anormales, duplications ou incohérences peuvent déclencher une vérification. Deep Authenticity© ne qualifie pas automatiquement un avis de faux ni son auteur de fraudeur.

15. Deep Authenticity©

Deep Authenticity© confronte identité de l'établissement, offre, réservation, billet, QR, certification, historique et événements de service afin de détecter substitutions, expirations ou incohérences nécessitant vérification.

16. Online et Offline

Online fournit les statuts courants de réservation, billet ou certification. En Offline, seules les preuves signées admises sont consultables avec date de synchronisation et limites de fraîcheur clairement affichées.

17. Signalement et litige

Un voyageur ou prestataire peut signaler une divergence entre offre, réservation et service fourni. Le dossier conserve preuves, versions et réponses sans décider automatiquement de la responsabilité juridique.

18. Vie privée et sécurité

Identité des voyageurs, documents, itinéraires, données de paiement, localisation et informations de séjour sont minimisés et compartimentés. Les vues publiques ne doivent pas permettre le suivi d'une personne.

19. AP Ledger

Empreintes minimales d'identité d'établissement, certification, réservation, émission ou validation de billet, changement critique et litige peuvent être ancrées dans AP Ledger. Données personnelles, paiements et itinéraires détaillés restent hors des couches irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si établissement, prestataire, offre, réservation et billet restent distingués ; si les certifications restent attribuées à leur émetteur ; si un QR copié ne reproduit pas un droit valide ; si avis et faits ne sont pas confondus ; si les données voyageurs restent privées ; et si les litiges conservent une chaîne de preuve sans jugement automatique. Le Passeport Tourisme fournit ainsi un socle de confiance pour l'expérience touristique.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 24 — TOURISME

CHAPITRE 2 — PARCOURS VOYAGEUR, RÉSERVATION, PAIEMENT, CHECK-IN/CHECK-OUT, TRANSPORT TOURISTIQUE, ACTIVITÉS, BILLETS ET CONTINUITÉ DE L'EXPÉRIENCE

1. Objet du chapitre

Ce chapitre applique le Passeport Numérique Tourisme au parcours du voyageur, depuis la recherche et la réservation jusqu'à l'arrivée, la consommation des prestations, les activités, les déplacements et la clôture du séjour.

2. Parcours voyageur

Le parcours peut relier plusieurs prestations sans fusionner leurs responsabilités : hébergement, transport, activité, visite, restauration ou autre service conserve son propre prestataire, ses conditions et ses preuves.

3. Offre et réservation

Une réservation conserve l'offre et la version des conditions acceptées, le canal, la date, le statut et les prestations incluses. Une modification ultérieure ne doit pas réécrire silencieusement l'offre initiale.

4. Confirmation

La confirmation de réservation peut disposer d'une preuve vérifiable reliant émetteur, référence, prestation, période et statut. Elle ne rend publiques ni l'identité du voyageur ni les informations sensibles du séjour.

5. Paiement

Le passeport peut conserver une preuve minimale du statut de paiement ou de garantie sans stocker les données sensibles de carte ou les secrets de paiement. L'opération financière reste attribuée au prestataire de paiement compétent.

6. Modification et annulation

Modification, report, annulation ou remboursement sont des événements distincts avec date, auteur, conditions applicables et statut. L'historique permet de déterminer quelle version était valide à chaque étape.

7. Check-in

Le check-in peut relier réservation, établissement, date et validation autorisée. Les contrôles d'identité éventuellement requis restent soumis aux règles applicables et à la minimisation des données.

8. Accès à l'hébergement

Clé numérique, badge, QR ou autre titre d'accès peut être relié à une réservation et à une période limitée. La preuve d'accès ne doit pas devenir un mécanisme public de suivi du voyageur.

9. Check-out

Le check-out peut clôturer l'occupation et relier les prestations ou événements nécessaires. Il reste distinct du règlement financier final et de la résolution d'un éventuel litige.

10. Transport touristique

Navette, excursion, transfert, véhicule touristique ou autre transport peut disposer d'une identité de prestation reliant opérateur, trajet ou zone, période, billet et statut, selon les données autorisées.

11. Activités et excursions

Une activité peut relier organisateur, lieu, horaire, capacité, conditions et billet. Une modification ou annulation est historisée afin d'éviter la substitution silencieuse de la prestation réservée.

12. Billets et contrôle d'accès

Un billet ou voucher dynamique peut être validé selon son statut courant. Une copie, capture d'écran ou duplication visuelle ne doit pas suffire à créer plusieurs droits d'accès valides.

13. Prestations combinées

Lorsqu'un voyage associe plusieurs prestataires, le système conserve la provenance de chaque composant. Une défaillance d'un service n'est pas automatiquement attribuée aux autres acteurs du parcours.

14. Continuité de l'expérience

Retard, indisponibilité, changement ou interruption peut déclencher une proposition ou action par les acteurs habilités. AP conserve les versions et décisions sans imposer seul une solution commerciale.

15. Deep Authenticity©

Deep Authenticity© confronte offre, réservation, paiement attesté, billet, check-in, prestataire, horaire et événements afin de détecter duplications, substitutions, incohérences de statut ou chronologies anormales.

16. Online et Offline

Le statut courant des billets, annulations et droits d'accès privilégie Online. En Offline, les preuves signées admises indiquent leur dernière synchronisation et les limites associées à leur fraîcheur.

17. Réclamations et preuves

Une réclamation peut relier offre initiale, confirmation, paiements attestés, modifications, prestation constatée et réponses des acteurs. Le système organise la preuve sans déterminer automatiquement la responsabilité juridique.

18. Vie privée

Identité, documents, moyens de paiement, localisation, chambre, itinéraire et historique de voyage sont minimisés et compartimentés. Les partenaires n'accèdent qu'aux données nécessaires à leur propre prestation.

19. AP Ledger

Empreintes minimales de confirmation, modification, annulation, validation de billet, check-in/check-out et événement critique peuvent être ancrées dans AP Ledger. Données de paiement, documents d'identité et itinéraires détaillés restent hors des couches irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si chaque prestation conserve son prestataire et ses conditions ; si les versions de réservation restent auditables ; si les secrets de paiement ne sont pas stockés ; si les titres d'accès résistent à la simple copie ; si les partenaires ne voient que les données nécessaires ; et si une réclamation conserve ses preuves sans jugement automatique. Le Passeport Tourisme fournit ainsi une continuité vérifiable du parcours voyageur.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 24 — TOURISME

CHAPITRE 3 — HÔTELS, HÉBERGEMENTS, CHAMBRES, ÉQUIPEMENTS, HOUSEKEEPING, MAINTENANCE, SÉCURITÉ, CLASSEMENT ET QUALITÉ DE SERVICE

1. Objet du chapitre

Ce chapitre applique le Passeport Numérique Tourisme à l'exploitation des hôtels et autres hébergements : établissement, unités d'hébergement, équipements, préparation des chambres, maintenance, sécurité, classement, incidents et qualité de service.

2. Identité de l'établissement

Chaque hôtel, résidence, auberge, camping ou autre hébergement peut disposer d'une identité reliant exploitant, localisation, statut, certifications et informations opérationnelles autorisées.

3. Identité de l'unité d'hébergement

Une chambre, suite, logement ou emplacement peut disposer d'un identifiant interne relié à sa catégorie, capacité, caractéristiques documentées, statut d'exploitation et historique technique, sans exposer publiquement l'occupation en temps réel.

4. Catégories et caractéristiques

Type de chambre, capacité, équipements, accessibilité ou autres caractéristiques restent rattachés à leur source et à leur version. Une description commerciale ne vaut pas certification indépendante.

5. Disponibilité et statut

Disponible, occupée, en préparation, hors service ou en maintenance sont des statuts opérationnels distincts. Les vues publiques ne doivent pas permettre de déduire la présence ou l'absence d'un voyageur déterminé.

6. Housekeeping

Une opération de préparation ou de nettoyage peut être reliée à l'unité, à la date, au statut et à l'équipe ou au système autorisé. Le passeport conserve la preuve opérationnelle nécessaire sans créer un suivi personnel permanent du personnel.

7. Contrôle de préparation

Une chambre déclarée prête peut faire l'objet d'une validation selon les procédures de l'établissement. La validation confirme une étape opérationnelle documentée et non une garantie absolue de satisfaction du client.

8. Équipements de chambre

Climatisation, coffre, minibar, serrure, détecteur ou autre équipement peut être relié à son identité, son statut,ses maintenances et ses remplacements lorsque cette traçabilité est pertinente.

9. Équipements communs

Ascenseurs, installations techniques, piscines, équipements de sécurité ou autres actifs communs peuvent disposer d'un historique de contrôle, maintenance et intervention adapté à leur criticité.

10. Maintenance préventive

Les inspections et entretiens planifiés peuvent conserver actif, date, intervenant, action, résultat et prochaine échéance lorsque applicable.

11. Maintenance corrective

Une panne ou anomalie peut ouvrir une intervention reliant signalement, diagnostic, actif, travaux, pièces remplacées et remise en service. Signal initial et diagnostic confirmé restent distincts.

12. QR Codes dynamiques

Un QR dynamique réservé aux usages appropriés peut permettre au personnel habilité de vérifier un actif ou d'ouvrir une intervention. Un QR accessible au public ne donne jamais accès à une commande technique critique.

13. Sécurité de l'établissement

Les contrôles, équipements et incidents de sécurité peuvent être documentés selon les habilitations. Plans sensibles, systèmes d'accès, configurations et informations susceptibles de compromettre la sécurité restent protégés.

14. Classement et labels

Étoiles, labels et certifications restent attribués à l'organisme émetteur avec date, portée et statut. Authenticity Plus© ne crée pas, ne prolonge pas et ne modifie pas seul un classement officiel.

15. Qualité de service

Des indicateurs de service peuvent être reliés à leur période, méthode et source. Un avis client, un indicateur interne et un audit indépendant restent trois catégories de preuve distinctes.

16. Deep Authenticity©

Deep Authenticity© confronte identité de l'établissement, unité, équipements, statuts, maintenance, classement, événements et preuves de service afin de détecter incohérences, substitutions ou informations expirées.

17. Incidents et réclamations

Dommage, indisponibilité, dysfonctionnement ou réclamation peut être relié à l'unité ou au service concerné, aux observations, aux interventions et aux réponses. AP organise la preuve sans attribuer automatiquement une responsabilité.

18. Vie privée et accès

Numéro de chambre associé à une personne, horaires de présence, identité, demandes particulières et autres données de séjour sont compartimentés. Chaque rôle n'accède qu'aux informations nécessaires à sa mission.

19. AP Ledger

Empreintes minimales de classement, contrôle critique, maintenance, remplacement, changement de statut majeur et clôture d'incident peuvent être ancrées dans AP Ledger. Données voyageurs, clés d' accès, plans sensibles et journaux détaillés restent hors des couches irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si établissement, unité et équipement restent distingués ; si l'occupation n' est pas publiquement traçable ; si housekeeping et maintenance sont attribuables sans surveillance excessive ; si classement et qualité de service ne sont pas confondus ; si les commandes critiques restent protégées ; et si les incidents conservent leur chaîne de preuve. Le Passeport Tourisme devient ainsi une mémoire vérifiable de l'exploitation et de la qualité des hébergements.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 24 — TOURISME

CHAPITRE 4 — DESTINATIONS, SITES TOURISTIQUES, PATRIMOINE, MUSÉES, ATTRACTIONS, GUIDES, ÉVÉNEMENTS, BILLETTERIE, CAPACITÉ ET GESTION DES FLUX VISITEURS

1. Objet du chapitre

Ce chapitre applique le Passeport Numérique Tourisme aux destinations, sites patrimoniaux, musées, attractions, guides, événements et flux de visiteurs. Il relie identité du lieu, opérateur, capacité, programmation, billetterie, accès, incidents et preuves de service.

2. Identité de la destination

Une destination, zone touristique ou territoire peut disposer d'une identité documentaire reliant organismes compétents, périmètre, informations officielles et services autorisés, sans confondre promotion touristique et décision publique.

3. Sites touristiques et patrimoine

Monument, site historique, parc, espace naturel ou autre lieu d'intérêt peut disposer d'un passeport reliant gestionnaire, localisation, statut, périodes d'ouverture, interventions et informations patrimoniales documentées.

4. Musées et collections

Un musée peut relier établissement, espaces, expositions et informations publiques. Les objets de collection conservent leurs propres règles de provenance, de sécurité et d'accès lorsque leur traçabilité est intégrée.

5. Attractions

Une attraction peut disposer d'une identité reliant exploitant, caractéristiques, horaires, capacité déclarée, maintenance et statut. Les contrôles techniques réglementaires restent attribués aux organismes compétents.

6. Guides et médiateurs

Un guide ou médiateur peut disposer d'un profil vérifiable reliant rôle, organisation, langues, habilitations ou qualifications documentées. AP ne crée pas une qualification officielle qui n'aurait pas été émise par l'autorité compétente.

7. Événements touristiques

Festival, visite spéciale, exposition temporaire ou autre événement peut conserver organisateur, lieu, dates, programme, capacité et versions successives. Toute modification importante reste historisée.

8. Billetterie

Un billet relie émetteur, événement ou site, catégorie, période de validité et statut. Les données du visiteur sont minimisées et ne sont associées que lorsque la prestation l'exige.

9. QR Codes dynamiques

Le QR dynamique peut vérifier billet, créneau ou droit d'accès. Une capture d'écran ou duplication visuelle ne doit pas permettre plusieurs validations valides lorsque le titre est à usage unique.

10. Créneaux horaires

Une réservation à créneau peut conserver horaire, capacité, statut et règles applicables. Le système distingue la réservation d'un créneau de l'entrée réellement validée.

11. Capacité

La capacité d'un site ou événement peut provenir de règles, décisions ou paramètres d'exploitation documentés. AP conserve la source et ne détermine pas seul la capacité réglementaire autorisée.

12. Gestion des flux visiteurs

Les entrées, sorties ou niveaux d'occupation agrégés peuvent contribuer à la gestion des flux. Les mécanismes doivent éviter le suivi individuel permanent des visiteurs lorsque celui-ci n'est pas nécessaire.

13. Files d'attente et affluence

Temps d'attente ou niveau d'affluence peut être mesuré, estimé ou déclaré. Ces trois origines restent distinguées afin de ne pas présenter une estimation comme une mesure directe.

14. Accessibilité

Les informations relatives à l'accessibilité d'un site peuvent être reliées à leur source, date et périmètre. Une déclaration de service reste distincte d'une certification ou d'un audit indépendant.

15. Deep Authenticity©

Deep Authenticity© confronte identité du site, événement, billet, QR, créneau, capacité, horaires, validations et certifications afin de détecter duplications, incohérences, expirations ou substitutions nécessitant vérification.

16. Incidents et évacuation

Un incident peut relier lieu, période, alerte, décision, intervention et statut. Les procédures, plans détaillés et informations de sécurité sensibles restent réservés aux acteurs habilités.

17. Online et Offline

Online fournit les statuts courants des billets, créneaux et capacités. En Offline, seules les preuves signées admises sont utilisées, avec date de synchronisation et limites de fraîcheur clairement indiquées.

18. Données visiteurs et vie privée

Identité, déplacement, billet nominatif, besoins particuliers et autres données personnelles sont minimisés. Les statistiques de fréquentation destinées à l'analyse privilégient des données agrégées ou protégées.

19. AP Ledger

Empreintes minimales d'identité de site, certification, événement, émission ou validation de billet, changement critique et incident peuvent être ancrées dans AP Ledger. Données visiteurs, plans de sécurité et journaux détaillés restent hors des couches irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si destination, site, événement, billet et visiteur restent distingués ; si la capacité conserve sa source ; si réservation et entrée réelle ne sont pas confondues ; si mesure et estimation d'affluence restent séparées ; si les flux sont gérés sans surveillance individuelle excessive ; et si les informations de sécurité sensibles restent protégées. Le Passeport Tourisme fournit ainsi une chaîne de confiance pour les destinations et les expériences de visite.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 24 — TOURISME

CHAPITRE 5 — GOUVERNANCE TOURISTIQUE, AUTORITÉS, OFFICES DE TOURISME, ÉTABLISSEMENTS, PLATEFORMES, AGENCES, PRESTATAIRES, VOYAGEURS, INTEROPÉRABILITÉ, CONFIDENTIALITÉ, SOUVERAINETÉ ET AUDIT

1. Objet du chapitre

Ce chapitre définit la gouvernance du Passeport Numérique Tourisme : responsabilités, droits d'accès, séparation des rôles, échanges entre acteurs, confidentialité, portabilité, souveraineté des données et audit.

2. Principe de gouvernance

Authenticity Plus© organise l'identité, la provenance et l'historique des preuves touristiques. Il ne se substitue ni aux autorités publiques, ni aux organismes de classement, ni aux opérateurs commerciaux dans leurs compétences respectives.

3. Autorités compétentes

Les autorités peuvent publier licences, décisions, obligations, restrictions ou autres statuts dans leur périmètre. Toute information officielle conserve son émetteur, sa date, sa portée et son statut.

4. Offices de tourisme

Les offices de tourisme peuvent publier des informations institutionnelles, référencer des acteurs ou promouvoir une destination selon leur mandat. Une information promotionnelle reste distincte d'une certification réglementaire.

5. Établissements

Hôtels, hébergements, musées, attractions etautres établissements administrent les informations et opérations relevant de leur périmètre. Ils ne peuvent modifier silencieusement les preuves émises par un autre acteur.

6. Agences et organisateurs

Agences, tour-opérateurs et organisateurs peuvent composer plusieurs prestations. Chaque composant conserve son prestataire, ses conditions, son statut et sa chaîne de preuve.

7. Plateformes numériques

Une plateforme de réservation ou de distribution peut transmettre offres, disponibilités, réservations, paiements attestés ou avis selon ses droits. Elle reste identifiée comme intermédiaire lorsque l' information provient d'un tiers.

8. Prestataires

Guides, transporteurs, activités et autres prestataires disposent de droits limités à leurs propres services et données. La participation à un parcours touristique ne donne pas accès à l'ensemble du dossier du voyageur.

9. Voyageurs

Le voyageur peut consulter ses réservations, titres et preuves autorisées, exercer les actions prévues et transmettre une réclamation. Ses informations personnelles restent privées par défaut.

10. Séparation des rôles

Promouvoir, vendre, fournir, certifier, contrôler, auditer et décider sont des fonctions distinctes. Le système conserve l'auteur et la nature de chaque information afin d'éviter leur confusion.

11. Droits d'accès dynamiques

Les accès peuvent dépendre du rôle, de l'organisation, de la prestation, du voyage, de la durée et du niveau de sensibilité. Ils sont limités, journalisés, révisables et révocables.

12. Validation multiniveau

Modification critique d'identité, certification, statut de billet, résolution de litige ou publication sensible peut nécessiter plusieurs validations selon les règles applicables.

13. Interopérabilité

PMS, systèmes de réservation, billetterie, plateformes de distribution, CRM, transport, paiement et autres services autorisés peuvent échanger avec AP. Toute donnée importée conserve sa source, sa version et son horodatage.

14. Portabilité

Un voyageur ou un établissement ne doit pas perdre l'historique vérifiable nécessaire du seul fait d'un changement de plateforme ou de fournisseur. Les données exportables restent soumises aux droits et obligations applicables.

15. Confidentialité

Documents d'identité, paiements, numéros de chambre, itinéraires, préférences, localisation et données de séjour sont compartimentés. Les partenaires n'accèdent qu'aux informations nécessaires à leur mission.

16. Souveraineté des données

L’entité compétente doit pouvoir définir localisation, conservation, finalités, accès et règles de transfert des données. Les informations sensibles ne sont pas rendues publiques ou irréversibles par défaut.

17. Cybersécurité

Comptes privilégiés, API, intégrations, certificats et accès fournisseurs sont authentifiés, journalisés et révocables. Un QR ou lien public ne donne jamais accès à une fonction administrative critique.

18. Audit et responsabilité

L’auditeur habilité peut vérifier les preuves nécessaires à sa mission sans recevoir automatiquement le pouvoir de les modifier. Toute action critique reste attribuable à un acteur ou système autorisé.

19. AP Ledger

Empreintes minimales de licences, certifications, validations, changements critiques, révocations et clôtures de litige peuvent être ancrées dans AP Ledger. Données voyageurs, paiements, itinéraires et secrets commerciaux restent hors des couches irréversibles.

20. Critères d’acceptation et conclusion

Le modèle est acceptable si autorités, offices, établissements, plateformes, agences et prestataires restent dans leurs rôles ; si promotion et certification ne sont pas confondues ; si les intermédiaires restent identifiables ; si les accès sont révocables ; si l’interopérabilité conserve la provenance ; si la souveraineté et la vie privée sont préservées ; et si l’audit reste indépendant. Cette gouvernance fournit le socle nécessaire à la clôture fonctionnelle de l’application Tourisme.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 24 — TOURISME

CHAPITRE 6 — SYNTHÈSE FONCTIONNELLE, CRITÈRES D'ACCEPTATION ET CLÔTURE DE L'APPLICATION TOURISME

1. Objet du chapitre

Ce chapitre clôt le Point 24 — Tourisme. Il consolide établissements, hébergements, voyageurs, offres, réservations, paiements attestés, billets, destinations, patrimoine, activités, avis, qualité de service, gouvernance, confidentialité et AP Ledger.

2. Mission consolidée

Le Passeport Numérique Tourisme constitue une chaîne de confiance vérifiable entre acteurs, offres, transactions et prestations. Authenticity Plus© / Deep Authenticity© authentifie provenance et historique sans devenir agence de voyage, organisme de classement ou juge automatique d'un litige.

3. Établissements et prestataires

Hôtels, agences, sites touristiques, musées, attractions, guides, transporteurs et autres prestataires peuvent disposer d'identités reliées à leur exploitant, statut, certifications et historique autorisé.

4. Offres et versions

Toute offre conserve son prestataire, sa description, sa période, ses conditions et sa version. Une modification ne réécrit pas silencieusement les conditions antérieurement proposées ou acceptées.

5. Réservations et confirmations

Réservation, confirmation, modification, annulation et remboursement sont des événements distincts et attribuables. Les données personnelles du voyageur restent protégées.

6. Paiements

Le passeport peut conserver une preuve minimale du statut d'un paiement ou d'une garantie sans inscrire les secrets ou données sensibles de paiement dans les couches de preuve irréversibles.

7. Billets et QR dynamiques

Billets, vouchers et titres d'accès peuvent disposer d'un statut vérifiable. Une copie visuelle d'un QR ne doit pas suffire à reproduire un droit d'accès valide ou à multiplier un titre à usage unique.

8. Parcours voyageur

Hébergement, transport, activité, visite et autres prestations peuvent être reliés dans un parcours sans fusionner les responsabilités. Chaque composant conserve son prestataire et sa chaîne de preuve.

9. Hébergements

Établissement, chambre ou unité et équipement restent des objets distincts. Housekeeping, maintenance, incidents et changements de statut sont historisés sans rendre publiquement traçable l'occupation d'un voyageur.

10. Destinations et patrimoine

Destinations, sites, musées, attractions et événements conservent identité, opérateur, horaires, capacité et informations documentées. Promotion touristique et décision ou certification officielle restent distinctes.

11. Capacité et flux visiteurs

Réservation de créneau et entrée réellement validée ne sont pas confondues. Mesure, estimation et déclaration d'affluence restent identifiables, tandis que la gestion des flux privilégie les données agrégées ou protégées.

12. Classements, labels et certifications

Toute étoile, licence, qualification ou certification reste attribuée à son organisme émetteur, avec date, portée et statut. AP ne crée ni ne prolonge une certification officielle.

13. Avis et qualité de service

Avis client, indicateur interne, description commerciale et audit indépendant restent des catégories distinctes. Un avis authentifié demeure une opinion et non un fait universel.

14. Deep Authenticity©

Deep Authenticity© confronte établissements, offres, réservations, billets, QR, certifications, statuts, événements et chronologies afin de signaler duplications, substitutions, expirations et incohérences nécessitant vérification.

15. Litiges et réclamations

Une réclamation peut réunir offre initiale, confirmation, paiement attesté, modifications, prestation et réponses des acteurs. AP organise la chaîne de preuve sans déterminer automatiquement la responsabilité juridique.

16. Online et Offline

Online fournit les statuts courants des réservations, billets et certifications. Offline se limite aux preuves signées admises, avec date de dernière synchronisation et limites de fraîcheur explicitement visibles.

17. Gouvernance

Autorités, offices de tourisme, établissements, agences, plateformes, prestataires, auditeurs et voyageurs disposent de rôles distincts. Promouvoir, vendre, fournir, certifier, contrôler, auditer et décider ne sont pas fusionnés.

18. Vie privée, cybersécurité et souveraineté

Identité, documents, paiements, chambre, itinéraires, localisation et données de séjour sont minimisés et compartimentés. Les accès sont révocables et l'entité compétente gouverne conservation, localisation et transfert des données.

19. AP Ledger et critères d'acceptation

AP Ledger reçoit uniquement des empreintes minimales d'identité, certification, réservation, validation de billet, changement critique, révocation ou clôture de litige. Le modèle est acceptable si la provenance est conservée, les rôles séparés, les droits révocables, les données voyageurs protégées et les affirmations limitées à la portée réelle des preuves.

20. Clôture du Point 24 — Tourisme

Le Point 24 — Tourisme est désormais fonctionnellement défini : établissements, prestataires, hébergements, offres, réservations, paiements attestés, billets, QR dynamiques, parcours voyageur, destinations, patrimoine, attractions, événements, capacité, flux visiteurs, classements, avis, Deep Authenticity©, litiges, gouvernance, confidentialité, cybersécurité, souveraineté, interopérabilité, audit et AP Ledger. Le Volume IV peut désormais poursuivre avec le Point 25 — Insurance.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 25 — INSURANCE

CHAPITRE 1 — IDENTITÉ NUMÉRIQUE DE L'ASSURANCE, ASSURÉS, CONTRATS, BIENS ASSURÉS, GARANTIES, ATTESTATIONS, QR CODES DYNAMIQUES, PROVENANCE ET PASSEPORT NUMÉRIQUE INSURANCE

1. Objet du chapitre

Le Point 25 — Insurance transpose Authenticity Plus© / Deep Authenticity© au secteur de l'assurance. Le Passeport Numérique Insurance relie assureurs, assurés, contrats, biens ou intérêts assurés, garanties, attestations, événements et preuves autorisées.

2. Mission sectorielle

La mission est d'authentifier l'identité, la provenance et l'historique des informations d'assurance sans se substituer à l'assureur, au régulateur, à l'expert, au professionnel de santé ou à l'autorité compétente dans leurs décisions.

3. Identité de l'assureur

Une compagnie, mutuelle ou autre organisme autorisé peut disposer d'une identité vérifiable reliant dénomination, statut, habilitations documentées, produits et informations institutionnelles.

4. Identité de l'assuré

L'identité d'un assuré ou bénéficiaire est protégée et compartimentée. AP peut conserver la preuve qu' une vérification a été réalisée sans rendre publiquement accessibles les documents d'identité.

5. Identité du contrat

Une police ou un contrat peut disposer d'un identifiant reliant assureur, souscripteur autorisé, produit, période, statut, versions et documents applicables.

6. Objet ou intérêt assuré

Véhicule, bien immobilier, équipement, voyage, activité ou autre intérêt assurable peut être relié au contrat selon le périmètre nécessaire. Son identité reste distincte de celle du titulaire du contrat.

7. Garanties

Chaque garantie conserve sa définition contractuelle, sa période, ses limites, exclusions et version applicables. Une synthèse numérique ne remplace pas les documents contractuels faisant foi.

8. Attestation d’assurance

Une attestation peut disposer d’une preuve vérifiable reliant émetteur, contrat, période et statut. La vérification publique éventuelle doit révéler uniquement les informations strictement nécessaires.

9. QR Code dynamique

Un QR dynamique peut permettre de vérifier l’authenticité et le statut d’une attestation selon les droits disponibles. Une copie visuelle du QR ne doit pas permettre de fabriquer une nouvelle attestation valide.

10. Souscription

La souscription peut relier demande, informations fournies, contrôles, version des conditions, date et décision de l’assureur. AP conserve la provenance des éléments sans prendre lui-même la décision d’ accepter ou de refuser le risque.

11. Modification du contrat

Avenant, ajout ou retrait de garantie, changement d’objet assuré ou autre modification est versionné avec date d’effet et auteur. L’ancienne version reste identifiable dans l’historique.

12. Renouvellement

Le renouvellement est distingué de la souscription initiale. Nouvelle période, conditions, garanties et statut sont rattachés à leur version correspondante.

13. Suspension et résiliation

Suspension, expiration ou résiliation sont des statuts distincts, attribués à l’acteur habilité et associés à leur date d’effet. AP ne déduit pas seul qu’une couverture est juridiquement inexistante.

14. Documents et provenance

Contrat, avenant, attestation, expertise, facture ou autre document conserve émetteur, date, version et relation avec le dossier concerné.

15. Deep Authenticity©

Deep Authenticity© confronte assureur, assuré, contrat, objet assuré, garanties, attestations, documents, versions et chronologie afin de détecter duplications, substitutions, expirations ou incohérences nécessitant vérification.

16. Anomalie ou fraude présumée

Un document incohérent, une identité dupliquée ou une séquence inhabituelle peut déclencher une vérification. Une anomalie ne constitue pas automatiquement une fraude et AP n’attribue pas seul une intention malveillante.

17. Online et Offline

Online fournit les statuts courants des contrats et attestations. Lorsque l'Offline est admis, seules les preuves signées disponibles sont utilisées, avec date de synchronisation et limites de fraîcheur clairement visibles.

18. Vie privée et données sensibles

Identité, situation financière, données de santé lorsqu'elles existent, coordonnées, sinistres et autres informations sensibles sont minimisés et protégés. Les vues publiques ne doivent pas permettre de reconstituer le profil assurantiel d'une personne.

19. AP Ledger

Empreintes minimales d'identité d'organisme, émission de contrat, avenant, attestation, changement critique, suspension ou résiliation peuvent être ancrées dans AP Ledger. Documents d'identité, données médicales, financières et dossiers détaillés restent hors des couches publiques ou irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si assuré, contrat et objet assuré restent distincts ; si chaque garantie conserve sa version ; si une attestation est vérifiable sans surexposer les données ; si les décisions restent attribuées à l'assureur ou à l'autorité compétente ; si anomalie et fraude ne sont pas confondues ; et si les données sensibles restent protégées. Le Passeport Insurance fournit ainsi le socle d'une chaîne de confiance pour le cycle de vie des contrats d'assurance.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 25 — INSURANCE

CHAPITRE 2 — SINISTRES, DÉCLARATION, PREUVES, DOMMAGES, EXPERTISE, RÉPARATIONS, INDEMNISATION, FRAUDE PRÉSUMÉE ET CHAÎNE DE DÉCISION

1. Objet du chapitre

Ce chapitre applique le Passeport Numérique Insurance au cycle de vie d'un sinistre : déclaration, réception, preuves, dommages allégués, expertise, décisions, réparations, indemnisation, recours et clôture.

2. Identité du sinistre

Chaque dossier peut disposer d'un identifiant reliant contrat, objet assuré, date déclarée, événement, parties autorisées, statut et historique, sans exposer publiquement les données personnelles du dossier.

3. Déclaration

La déclaration conserve auteur ou canal, date, circonstances déclarées, pièces transmises et version. Elle constitue le récit initial du déclarant et non une constatation indépendante des faits.

4. Date et chronologie

Date de l'événement, date de découverte, date de déclaration et date de réception peuvent être différentes. Le système les conserve séparément afin d'éviter toute reconstruction artificielle de la chronologie.

5. Preuves initiales

Photographies, vidéos, factures, constats, rapports, attestations ou autres pièces peuvent être reliés au dossier avec source, date, version et empreinte. Leur présence n'établit pas automatiquement leur exactitude matérielle.

6. Dommage allégué

Le dommage déclaré reste distinct du dommage observé, expertisé ou accepté par l'assureur. Cette séparation est conservée tout au long du traitement.

7. Expertise

L’expert habilité peut produire observations, méthodologie, réserves, estimation et rapport. Authenticity Plus© authentifie la provenance du rapport sans se substituer à l’expertise professionnelle.

8. Visite et inspection

Une visite peut être reliée au lieu ou à l’objet assuré, à la date, à l’expert et aux éléments collectés. Toute géolocalisation utilisée reste ponctuelle et proportionnée à la mission.

9. Estimation

Coût estimé, valeur de remplacement, valeur de réparation ou autre estimation conserve méthode, hypothèses, date et auteur. Une estimation n’est pas automatiquement le montant indemnisable.

10. Réparation

Devis, ordre de réparation, pièces, travaux et facture peuvent être reliés au dossier. Le système distingue réparation proposée, autorisée, exécutée et facturée.

11. Chaîne de décision

Réception, instruction, expertise, demande de complément, proposition, acceptation, refus, paiement et clôture sont des événements distincts. Chaque décision reste attribuée à l’acteur habilité.

12. Couverture applicable

Le rapprochement entre sinistre et garanties peut soutenir l’instruction, mais AP ne décide pas seul de l’application juridique d’une garantie, d’une exclusion ou d’une franchise.

13. Indemnisation

Une indemnisation peut être reliée à la décision, au bénéficiaire autorisé, au montant, à la date et au statut de paiement. Les coordonnées bancaires et secrets de paiement restent hors des preuves publiques ou irréversibles.

14. Fraude présumée

Duplications, incohérences documentaires, chronologies inhabituelles ou divergences peuvent déclencher une vérification renforcée. Un signal algorithmique ne constitue ni une preuve autonome de fraude ni une attribution de culpabilité.

15. Deep Authenticity©

Deep Authenticity© confronte contrat, objet assuré, déclaration, documents, métadonnées autorisées, expertise, réparations, décisions et chronologie afin de détecter substitutions, duplications ou incohérences explicables.

16. Contestation et recours

L’assuré, l’assureur ou un autre acteur habilité peut contester une étape selon les procédures applicables. Les versions, arguments, pièces et décisions successives restent historisés.

17. Clôture du sinistre

La clôture conserve motif, date et autorité de décision. Un dossier peut être rouvert selon les règles applicables sans effacer l’historique de la clôture précédente.

18. Vie privée et données sensibles

Données d’identité, santé, situation financière, localisation, images privées, coordonnées bancaires et autres éléments sensibles sont minimisés et accessibles uniquement aux rôles autorisés.

19. AP Ledger

Empreintes minimales de déclaration, dépôt de pièce, expertise, décision, indemnisation, recours et clôture peuvent être ancrées dans AP Ledger. Documents complets, données médicales, bancaires et autres données personnelles restent hors des couches irréversibles.

20. Critères d’acceptation et conclusion

Le modèle est acceptable si déclaration et constatation indépendante restent distinctes ; si dommage allégué, observé et accepté ne sont pas confondus ; si estimation et indemnisation restent séparées ; si toute décision est attribuable ; si un signal de fraude n’est jamais traité comme une culpabilité automatique ; et si la confidentialité du dossier est préservée. Le Passeport Insurance fournit ainsi une chaîne de preuve vérifiable du sinistre jusqu’à sa clôture.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 25 — INSURANCE

CHAPITRE 3 — ASSURANCE AUTOMOBILE, HABITATION, BIENS, ENTREPRISES, SANTÉ/VIE, RISQUES SPÉCIALISÉS, PREUVES SECTORIELLES ET PRÉVENTION

1. Objet du chapitre

Ce chapitre décline le Passeport Numérique Insurance selon plusieurs familles d'assurance. Il conserve un socle commun d'identité, contrat, garanties, preuves, décisions et confidentialité tout en adaptant la chaîne de preuve à la nature du risque.

2. Principe transversal

Chaque branche conserve ses propres règles, documents, professionnels compétents et données nécessaires. Authenticity Plus© authentifie la provenance et la chronologie sans uniformiser artificiellement des risques de nature différente.

3. Assurance automobile

Le dossier peut relier véhicule, contrat, conducteur autorisé lorsque nécessaire, attestations, sinistres, expertises, réparations et pièces justificatives. L'identité du véhicule reste distincte de celle de l' assuré.

4. Preuves automobiles

Photographies, constats, rapports d'expertise, devis, factures et historique de réparation peuvent être reliés au sinistre. Une donnée télématique éventuelle conserve sa source et son contexte et ne constitue pas, isolément, une preuve universelle de responsabilité.

5. Assurance habitation

Le passeport peut relier bien assuré, adresse protégée, caractéristiques contractuelles, garanties, inventaires documentés, sinistres, expertises et réparations.

6. Biens mobiliers et objets

Un objet assuré peut disposer d'une identité, de documents de provenance, d'évaluations ou de preuves d'acquisition selon les besoins. Une valeur déclarée reste distincte d'une valeur expertisée ou acceptée par l'assureur.

7. Assurance des entreprises

Sites, équipements, stocks, activités et garanties peuvent être reliés au contrat de l'entreprise. Les informations commerciales, financières et de sécurité restent compartimentées selon leur sensibilité.

8. Interruption d'activité

Un événement affectant l'activité peut relier période, site, cause déclarée, données financières autorisées et expertise. AP ne calcule ni ne décide seul du préjudice indemnisable.

9. Responsabilité

Une réclamation mettant en cause une responsabilité conserve déclaration, parties, faits allégués, pièces, expertises et décisions. Une mise en cause ne constitue pas automatiquement une responsabilité établie.

10. Assurance santé

Lorsque le cadre applicable le permet, le passeport peut authentifier des documents administratifs ou des preuves d'éligibilité. Les données médicales restent hautement sensibles, minimisées et accessibles uniquement aux acteurs autorisés.

11. Décisions médicales

Authenticity Plus© / Deep Authenticity© ne pose pas de diagnostic, ne remplace pas un professionnel de santé et ne transforme pas une donnée médicale en décision automatique de couverture.

12. Assurance vie

Contrat, souscripteur, assuré et bénéficiaire sont des rôles pouvant être distincts. Les désignations, modifications et événements sont protégés, versionnés et accessibles uniquement selon les droits applicables.

13. Risques spécialisés

Transport, agriculture, industrie, cyber, événementiel ou autres risques spécialisés peuvent utiliser des passeports adaptés aux actifs, événements et preuves propres à leur secteur.

14. Prévention

Inspection, maintenance, contrôle ou autre action préventive peut être documenté avec date, source et résultat. Une action de prévention ne garantit pas l'absence future de sinistre.

15. Capteurs et données connectées

Des capteurs autorisés peuvent contribuer à documenter un événement ou un risque. Leur identité, calibration, période, qualité de données et finalité doivent être connues avant toute interprétation.

16. Deep Authenticity©

Deep Authenticity© confronte contrat, objet assuré, documents, capteurs autorisés, expertises, réparations et chronologie afin de détecter incohérences, duplications ou substitutions nécessitant vérification.

17. Segmentation et équité

Les traitements automatisés doivent rester gouvernés, explicables et contrôlables selon les règles applicables. Un indicateur ou score ne doit pas être présenté comme une vérité absolue sur une personne.

18. Vie privée et minimisation

Les données collectées varient selon la branche et doivent rester proportionnées à la finalité. Santé, finances, localisation, habitudes et informations familiales bénéficient d'une protection renforcée.

19. AP Ledger

Empreintes minimales de contrats, attestations, expertises, changements critiques et décisions peuvent être ancrées dans AP Ledger. Données médicales, financières, télématiques détaillées et autres informations sensibles restent hors des couches irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si chaque branche conserve ses spécificités ; si valeur déclarée, expertisée et acceptée restent distinctes ; si mise en cause et responsabilité établie ne sont pas confondues ; si les données médicales et financières restent protégées ; si les capteurs conservent leur contexte ; et si les décisions restent attribuées aux acteurs compétents. Le Passeport Insurance peut ainsi couvrir plusieurs familles de risques sans perdre la provenance ni la proportionnalité des preuves.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 25 — INSURANCE

CHAPITRE 4 — RÉASSURANCE, COASSURANCE, COURTIERS, EXPERTS, RÉPARATEURS, PARTENAIRES, ÉCHANGES INTER-ASSUREURS, RECOURS, SUBROGATION ET INTEROPÉRABILITÉ

1. Objet du chapitre

Ce chapitre étend le Passeport Numérique Insurance aux relations entre assureurs, réassureurs, coassureurs, courtiers, experts, réparateurs et autres partenaires. Il organise la provenance des échanges, décisions et preuves sans fusionner les responsabilités.

2. Principe multi-acteurs

Chaque organisation conserve son identité, son rôle, son périmètre et la responsabilité de ses propres données. Le partage d'un dossier ne confère pas automatiquement un droit d'accès à l'ensemble des informations.

3. Réassurance

Un traité ou une opération de réassurance peut être relié aux parties, au périmètre, à la période, aux versions et aux événements autorisés. Les conditions commerciales sensibles restent protégées.

4. Cession et exposition

Les informations nécessaires à une cession peuvent conserver source, période et méthode. Une donnée agrégée, estimée ou déclarée reste identifiée comme telle.

5. Coassurance

Lorsqu'un risque est partagé entre plusieurs assureurs, le passeport conserve rôle, quote-part ou périmètre documenté de chaque participant ainsi que les décisions qui lui sont attribuées.

6. Apériteur et participants

La coordination par un assureur chef de file ne supprime pas l'identité ni les responsabilités des autres participants. Les actes de coordination et les décisions propres restent distingués.

7. Courtiers et intermédiaires

Un courtier ou intermédiaire peut transmettre demandes, documents et informations selon son mandat. Il reste identifiable comme source ou transmetteur et ne devient pas automatiquement l' émetteur du document transmis.

8. Experts

L’expert conserve identité professionnelle, mission, date, méthodologie, observations et rapport. Les versions ou compléments ultérieurs ne remplacent pas silencieusement le rapport initial.

9. Réparateurs et prestataires

Devis, pièces, travaux, factures et validations peuvent être reliés au réparateur ou prestataire. Réparation proposée, autorisée, réalisée et facturée restent des états distincts.

10. Échanges inter-assureurs

Les échanges nécessaires à un sinistre commun ou à un recours peuvent conserver émetteur, destinataire, objet, date et statut. Les données sont limitées au besoin opérationnel et juridique.

11. Recours

Un recours peut être relié au dossier, à la partie concernée, au fondement déclaré, aux pièces, montants réclamés, réponses et décisions. Une demande de recours n’établit pas automatiquement une responsabilité.

12. Subrogation

Lorsqu’une subrogation est applicable, le passeport peut documenter l’événement, sa portée, les droits invoqués et les actes associés. AP ne détermine pas seul la validité juridique ou l’étendue de la subrogation.

13. Règlements entre acteurs

Paiements, remboursements ou répartitions entre organisations peuvent conserver référence, montant, date et statut. Coordonnées bancaires et secrets de paiement restent hors des couches publiques ou irréversibles.

14. Interopérabilité

Systèmes de gestion de sinistres, courtiers, experts, réparateurs, réassureurs et plateformes autorisées peuvent échanger avec AP. Toute donnée importée conserve sa source, sa version, son horodatage et son niveau d’autorité.

15. Normalisation des preuves

Des formats communs peuvent faciliter l’échange de pièces et statuts, mais la normalisation ne doit pas effacer les différences de méthode, de juridiction, de contrat ou de responsabilité.

16. Deep Authenticity©

Deep Authenticity© confronte acteurs, mandats, documents, versions, expertises, réparations, paiements attestés, recours et chronologies afin de détecter duplications, substitutions ou incohérences nécessitant vérification.

17. Litiges multi-acteurs

Une divergence entre assureur, réassureur, courtier, expert ou prestataire ouvre une chaîne de contestation documentée. AP conserve les positions et preuves sans trancher automatiquement le litige.

18. Confidentialité et cloisonnement

Données d'assurés, conditions de réassurance, secrets commerciaux, rapports sensibles et informations financières sont compartimentés. Chaque acteur n'accède qu'aux éléments nécessaires à son rôle.

19. AP Ledger

Empreintes minimales de mandats, échanges critiques, expertises, validations, recours, règlements et changements de statut peuvent être ancrées dans AP Ledger. Contrats complets, données personnelles et conditions commerciales sensibles restent hors des couches irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si les responsabilités des acteurs restent distinctes ; si le transmetteur d'un document n'est pas confondu avec son émetteur ; si proposition, autorisation, exécution et facturation d'une réparation restent séparées ; si recours et responsabilité établie ne sont pas confondus ; si l' interopérabilité conserve la provenance ; et si les données sont strictement cloisonnées. Le Passeport Insurance fournit ainsi une chaîne de confiance inter-organisationnelle pour l'écosystème assurantiel.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 25 — INSURANCE

CHAPITRE 5 — GOUVERNANCE DE L'ASSURANCE, ASSUREURS, RÉGULATEURS, INTERMÉDIAIRES, EXPERTS, ASSURÉS, DROITS D'ACCÈS, IA, EXPLICABILITÉ, CONFIDENTIALITÉ, SOUVERAINETÉ ET AUDIT

1. Objet du chapitre

Ce chapitre définit la gouvernance du Passeport Numérique Insurance : responsabilités institutionnelles, séparation des rôles, habilitations, traitements automatisés, explicabilité, confidentialité, souveraineté, interopérabilité et audit.

2. Principe de gouvernance

Authenticity Plus© organise l'identité, la provenance, la version et l'historique des preuves. Il ne se substitue ni à l'assureur dans ses décisions contractuelles, ni au régulateur, ni à l'expert, ni aux autres professionnels compétents.

3. Assureurs

L'assureur administre contrats, garanties, dossiers et décisions relevant de son périmètre. Toute décision importante reste attribuable à une organisation, un rôle, une date et une version des éléments examinés.

4. Régulateurs et autorités

Les autorités et régulateurs conservent leurs compétences de contrôle, décision et supervision. Les décisions officielles intégrées au passeport restent rattachées à leur émetteur, leur date, leur portée et leur statut.

5. Intermédiaires

Courtiers, agents et autres intermédiaires disposent de droits correspondant à leur mandat. La transmission d'une information ne leur confère pas automatiquement la qualité d'émetteur du document d'origine.

6. Experts et professionnels

Experts, réparateurs, professionnels de santé ou autres intervenants habilités n'accèdent qu'aux éléments nécessaires à leur mission. Leurs conclusions restent attribuées à leur rôle professionnel.

7. Assurés et bénéficiaires

Les assurés et bénéficiaires peuvent accéder aux informations et actions qui leur sont autorisées. Leur identité, leurs contrats, leurs sinistres et leurs données sensibles restent privés par défaut.

8. Séparation des rôles

Souscrire, tarifer, expertiser, instruire, décider, payer, contrôler, auditer et réguler sont des fonctions distinctes. Les droits sont construits selon le principe du moindre privilège.

9. Droits d'accès dynamiques

Les habilitations peuvent dépendre de l'organisation, du rôle, du dossier, du type de donnée, de la finalité et de la durée. Elles sont journalisées, révisables et révocables.

10. Validation multiniveau

Décisions ou changements critiques peuvent nécessiter plusieurs validations selon les règles applicables. Le système conserve l'identité des validateurs et l'ordre des étapes sans masquer les désaccords.

11. Intelligence artificielle

L'IA peut assister le tri, la détection d'incohérences, l'analyse documentaire ou la priorisation lorsque cela est autorisé. Un résultat algorithmique reste identifié comme tel et ne devient pas automatiquement une décision contractuelle ou juridique.

12. Explicabilité et contestabilité

Lorsqu'un traitement automatisé contribue à une décision importante, les éléments nécessaires à son interprétation et à sa contestation doivent être conservés selon le cadre applicable. Un score ne doit pas être présenté comme une vérité absolue.

13. Deep Authenticity©

Deep Authenticity© confronte identités, contrats, documents, versions, expertises, décisions et chronologies afin de produire des signaux de cohérence ou d'anomalie. Il ne prononce ni fraude, ni responsabilité, ni droit à indemnisation de manière autonome.

14. Interopérabilité

Systèmes de souscription, sinistres, CRM, paiement, experts, courtiers, réassurance et autres plateformes autorisées peuvent échanger avec AP. Toute donnée importée conserve sa source, son horodatage, sa version et son niveau d'autorité.

15. Confidentialité

Données d'identité, santé, finances, localisation, contrats, sinistres, bénéficiaires et autres informations sensibles sont compartimentées. Les accès sont limités à la finalité autorisée et au besoin réel.

16. Souveraineté des données

L’entité compétente doit pouvoir définir localisation, conservation, accès, transfert, durée de vie et règles de suppression des données selon les exigences applicables.

17. Cybersécurité

Comptes privilégiés, API, certificats, intégrations, accès partenaires et consoles sont protégés par authentification, segmentation, journalisation et révocation. Aucun QR public ne donne accès à une fonction administrative critique.

18. Audit indépendant

L’auditeur habilité peut vérifier preuves, décisions, accès et journaux nécessaires à sa mission sans disposer automatiquement du pouvoir de modifier le dossier ou les systèmes opérationnels.

19. AP Ledger

Empreintes minimales d’habilitations, validations, décisions, révocations, changements critiques et clôtures peuvent être ancrées dans AP Ledger. Données médicales, financières, personnelles, modèles propriétaires et dossiers complets restent hors des couches irréversibles.

20. Critères d’acceptation et conclusion

Le modèle est acceptable si les rôles institutionnels restent distincts ; si les accès sont limités et révocables ; si toute décision critique est attribuable ; si l’IA reste identifiable, explicable et contestable selon le cadre applicable ; si un score n’est jamais assimilé à une vérité absolue ; si les données sensibles restent souveraines et protégées ; et si l’audit demeure indépendant. Cette gouvernance fournit le socle nécessaire à la clôture fonctionnelle de l’application Insurance.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 25 — INSURANCE

CHAPITRE 6 — SYNTHÈSE FONCTIONNELLE, CRITÈRES D'ACCEPTATION ET CLÔTURE DE L'APPLICATION INSURANCE

1. Objet du chapitre

Ce chapitre clôt le Point 25 — Insurance. Il consolide assureurs, assurés, contrats, garanties, attestations, sinistres, expertises, indemnisations, branches de risques, partenaires, intelligence artificielle, gouvernance, confidentialité, souveraineté et AP Ledger.

2. Mission consolidée

Le Passeport Numérique Insurance constitue une mémoire vérifiable du cycle de vie assurantiel. Authenticity Plus© / Deep Authenticity© authentifie identités, documents, versions, opérations et décisions attribuées sans se substituer à l'assureur, au régulateur, à l'expert ou à l'autorité compétente.

3. Assuré, contrat et objet assuré

L'identité de l'assuré, celle du contrat et celle du bien, intérêt ou risque assuré restent distinctes. Leurs associations évoluent selon des événements versionnés et autorisés.

4. Garanties et versions

Chaque garantie conserve définition, période, limites, exclusions, conditions et version applicables. Une synthèse numérique ne remplace pas les documents contractuels faisant foi.

5. Attestations et QR dynamiques

Une attestation peut être vérifiée avec un minimum de données. Une copie visuelle d'un QR ne doit pas permettre de fabriquer ou prolonger une attestation valide.

6. Souscription et cycle contractuel

Souscription, avenant, renouvellement, suspension, expiration et résiliation restent des événements distincts. Toute décision contractuelle est attribuée à l'acteur habilité.

7. Sinistres et déclarations

La déclaration initiale reste distincte d'une constatation indépendante. Date de l'événement, découverte, déclaration et réception sont conservées séparément.

8. Dommages et expertise

Dommage allégué, dommage observé, estimation et dommage accepté ne sont pas confondus. L’ expertise conserve auteur, méthode, réserves, date et version.

9. Réparations et indemnisation

Réparation proposée, autorisée, exécutée et facturée restent des états distincts. Une estimation n’est pas automatiquement un montant indemnisable, et toute indemnisation reste reliée à sa décision.

10. Fraude présumée

Duplications, incohérences ou chronologies inhabituelles peuvent produire un signal de vérification. Aucun signal, score ou corrélation n’est traité comme une preuve autonome de fraude ou de culpabilité.

11. Branches d’assurance

Automobile, habitation, biens, entreprises, responsabilité, santé, vie et risques spécialisés conservent leurs règles, acteurs, données et preuves propres sans être artificiellement uniformisés.

12. Données sensibles

Santé, finances, localisation, identité, bénéficiaires, données télématiques et informations familiales sont minimisés, compartimentés et accessibles uniquement selon les finalités autorisées.

13. Écosystème multi-acteurs

Réassureurs, coassureurs, courtiers, experts, réparateurs et partenaires conservent identité, mandat, rôle et responsabilité. Le partage d’un dossier ne fusionne ni les compétences ni les responsabilités.

14. Recours et subrogation

Recours, subrogation, règlements inter-organisations et contestations conservent leurs preuves et statuts. Une demande de recours ne constitue pas automatiquement une responsabilité établie.

15. Deep Authenticity©

Deep Authenticity© confronte contrats, objets assurés, attestations, documents, expertises, réparations, décisions, partenaires et chronologies afin de détecter des incohérences explicables et investigables.

16. Intelligence artificielle

L’IA peut assister le tri, l’analyse documentaire ou la détection d’anomalies lorsqu’elle est autorisée. Ses résultats restent identifiables, gouvernés, explicables et contestables selon le cadre applicable.

17. Gouvernance

Assureurs, régulateurs, intermédiaires, experts, professionnels, auditeurs, assurés et bénéficiaires disposent de rôles distincts. Souscrire, tarifer, expertiser, instruire, décider, payer, contrôler, auditer et réguler ne sont pas fusionnés.

18. Interopérabilité, cybersécurité et souveraineté

Les échanges entre systèmes conservent source, version, horodatage et niveau d'autorité. Les accès sont limités et révocables ; l'entité compétente gouverne localisation, conservation, transfert et durée de vie des données.

19. AP Ledger et critères d'acceptation

AP Ledger reçoit uniquement des empreintes minimales de contrats, attestations, déclarations, expertises, validations, décisions, paiements attestés, révocations ou clôtures. Le modèle est acceptable si la provenance est préservée, les rôles séparés, les décisions attribuables, l'IA contestable et les données sensibles hors des couches irréversibles.

20. Clôture du Point 25 — Insurance

Le Point 25 — Insurance est désormais fonctionnellement défini : assureurs, assurés, contrats, garanties, attestations, QR dynamiques, souscription, sinistres, preuves, expertises, réparations, indemnisation, fraude présumée, branches d'assurance, réassurance, coassurance, courtiers, recours, subrogation, Deep Authenticity©, IA, gouvernance, confidentialité, interopérabilité, cybersécurité, souveraineté, audit et AP Ledger. Le Volume IV peut désormais poursuivre avec le Point 26 — Real Estate / Property.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 26 — REAL ESTATE / PROPERTY

CHAPITRE 1 — IDENTITÉ NUMÉRIQUE IMMOBILIÈRE, PARCELLES, BÂTIMENTS, UNITÉS, TITRES, DROITS, DOCUMENTS, QR CODES DYNAMIQUES, PROVENANCE ET PASSEPORT NUMÉRIQUE PROPERTY

1. Objet du chapitre

Le Point 26 — Real Estate / Property transpose Authenticity Plus© / Deep Authenticity© au patrimoine immobilier. Le Passeport Numérique Property relie parcelles, bâtiments, unités, propriétaires ou titulaires autorisés, droits, documents, transactions, travaux et preuves institutionnelles.

2. Mission sectorielle

La mission est d'authentifier identité, provenance, versions et événements relatifs à un bien immobilier sans se substituer au registre foncier, au cadastre, au notaire, au juge, à l'administration ou à tout autre acteur compétent.

3. Identité de la parcelle

Une parcelle peut disposer d'une identité reliant référence cadastrale ou équivalente, périmètre documentaire, localisation, statut et sources officielles disponibles. AP ne redéfinit pas seul les limites juridiques d'un terrain.

4. Identité du bâtiment

Un bâtiment peut disposer d'un passeport reliant parcelle, adresse, caractéristiques documentées, usage déclaré, permis ou références disponibles, équipements et historique autorisé.

5. Identité de l'unité

Appartement, local, bureau, lot, garage ou autre unité peut disposer d'une identité distincte reliée au bâtiment et aux références officielles applicables.

6. Propriétaire et titulaire de droits

L'identité d'un propriétaire, usufruitier, locataire ou autre titulaire est protégée. La relation entre personne et bien reste attribuée à la source juridique ou administrative compétente.

7. Titres et actes

Titre, acte, certificat, contrat ou autre document peut conserver émetteur, date, référence, version et relation au bien. Une copie numérique authentifiée ne crée pas à elle seule un droit réel.

8. Droits et charges

Propriété, usufruit, bail, hypothèque, servitude ou autre droit ou charge peut être représenté avec source, portée, période et statut lorsque les données sont autorisées. AP n'en détermine pas seul la validité juridique.

9. Cadastre et registre foncier

Les informations cadastrales, foncières ou équivalentes conservent leur organisme source et leur date. En cas de divergence, le système signale l'incohérence sans décider quelle prétention juridique doit prévaloir.

10. QR Code dynamique

Un QR dynamique peut permettre de vérifier l'identité d'un bien ou l'authenticité d'un document selon le niveau d'accès. Une copie du QR ne permet ni transfert de propriété ni modification d'un registre officiel.

11. Documents techniques

Plans, diagnostics, certificats, permis, rapports, inspections et autres documents techniques peuvent être reliés au bien avec source, date, version et statut.

12. Historique du bien

Construction, division, fusion, changement d'usage, rénovation, vente ou autre événement peut être historisé. Une nouvelle version ne supprime pas silencieusement l'état antérieur.

13. Travaux et rénovations

Travaux déclarés, autorisés, réalisés et réceptionnés restent des étapes distinctes. Les permis et validations restent attribués aux autorités ou professionnels compétents.

14. Provenance des données

Toute donnée importée depuis cadastre, registre, notaire, promoteur, gestionnaire, expert ou autre source conserve son origine, son horodatage et son niveau d'autorité.

15. Deep Authenticity©

Deep Authenticity© confronte identité du bien, références, documents, droits, versions, signatures, acteurs et chronologie afin de détecter duplications, substitutions, documents expirés ou incohérences nécessitant vérification.

16. Fraude documentaire présumée

Un titre incohérent, une identité dupliquée ou une chronologie anormale peut déclencher une vérification. AP ne qualifie pas automatiquement le document de faux et n'attribue pas seul une fraude à une personne.

17. Online et Offline

Online permet de consulter les statuts courants provenant des sources autorisées. En Offline, seules les dernières preuves signées admises sont accessibles avec date de synchronisation et limites de fraîcheur clairement indiquées.

18. Vie privée et sécurité

Identité des titulaires, prix, coordonnées, plans sensibles, accès au bâtiment et autres données privées sont compartimentés. Les vues publiques se limitent aux informations légalement et opérationnellement nécessaires.

19. AP Ledger

Empreintes minimales d'identité du bien, titre, acte, droit, permis, changement critique ou transaction peuvent être ancrées dans AP Ledger. Actes complets, données personnelles, plans sensibles et secrets financiers restent hors des couches publiques ou irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si parcelle, bâtiment et unité restent distingués ; si les droits conservent leur source juridique ; si une copie numérique ne crée pas un droit réel ; si travaux déclarés, autorisés et réalisés ne sont pas confondus ; si les divergences sont signalées sans arbitrage automatique ; et si les données privées restent protégées. Le Passeport Property fournit ainsi le socle d'une chaîne de confiance immobilière.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 26 — REAL ESTATE / PROPERTY

CHAPITRE 2 — TRANSACTIONS IMMOBILIÈRES, VENTE, ACQUISITION, LOCATION, BAUX, MANDATS, OFFRES, SIGNATURES, PAIEMENTS, REMISE DES CLÉS ET CHAÎNE DE PREUVE TRANSACTIONNELLE

1. Objet du chapitre

Ce chapitre applique le Passeport Numérique Property aux transactions immobilières : mise en vente ou location, mandat, offre, négociation, vérifications, contrat, signatures, paiements attestés, transfert, bail, état des lieux et remise des clés.

2. Identité de la transaction

Chaque transaction peut disposer d'un identifiant reliant bien, parties autorisées, intermédiaires, documents, étapes, dates et statuts. Le dossier transactionnel reste distinct du passeport permanent du bien.

3. Mise en vente ou en location

Une annonce peut conserver émetteur, bien concerné, caractéristiques déclarées, prix ou loyer proposé, date et version. Une annonce commerciale ne constitue pas à elle seule une preuve de propriété ou de droit de louer.

4. Mandat

Le mandat d'un agent ou intermédiaire conserve mandant, mandataire, périmètre, durée et statut selon les données autorisées. L'existence d'un mandat ne transfère pas la propriété du bien.

5. Visites

Une visite peut être reliée à la transaction et au créneau nécessaire sans publier l'identité, la localisation en temps réel ou les habitudes des visiteurs. Les données sont limitées à la finalité opérationnelle.

6. Offre d'achat ou de location

Une offre conserve auteur, bien, montant ou conditions, date, durée éventuelle et statut. Offre, contre-offre, acceptation et contrat définitif restent des événements distincts.

7. Vérifications préalables

Les documents, références foncières, diagnostics, charges, autorisations ou autres éléments peuvent être vérifiés auprès de leurs sources compétentes. AP conserve la provenance et le résultat de la vérification sans garantir seul la validité juridique globale de l'opération.

8. Négociation et versions

Toute modification significative des conditions est versionnée. Le système permet d'identifier la version proposée, acceptée, refusée ou remplacée sans effacer l'historique.

9. Contrat et acte

Promesse, compromis, contrat de vente, bail, acte ou autre instrument conserve émetteur ou rédacteur, parties, date, version et signatures. Une copie numérique authentifiée ne remplace pas les formalités légales exigées.

10. Signatures

Les signatures électroniques ou attestations de signature peuvent être reliées au document, au signataire, à la date et au mécanisme de validation autorisé. AP n'invente pas une signature et ne présume pas sa validité juridique au-delà de la preuve disponible.

11. Paiements attestés

Dépôt, acompte, loyer, prix, frais ou autre paiement peut être relié à une preuve minimale de statut. Les coordonnées bancaires, secrets de paiement et données financières détaillées restent protégés.

12. Financement

Une opération peut référencer une preuve autorisée de financement, accord, condition ou décaissement. AP ne prend pas la décision de crédit et ne remplace pas l'établissement financier.

13. Transfert de propriété

Le transfert de propriété reste attribué aux actes, inscriptions et autorités compétentes. AP peut authentifier la chaîne documentaire et le changement de statut sans créer lui-même le transfert juridique.

14. Location et bail

Un bail relie bien, bailleur, locataire autorisé, période, conditions et versions. Les informations personnelles, montants et modalités sensibles restent accessibles uniquement selon les droits.

15. État des lieux

Un état des lieux peut relier date, parties, observations, photographies autorisées et signatures. État déclaré, dommage allégué et responsabilité restent des notions distinctes.

16. Remise des clés et accès

La remise d’une clé physique, badge ou droit d’accès numérique peut être enregistrée avec date, statut et bénéficiaire autorisé. Un QR public ne donne jamais accès à une serrure ou fonction critique.

17. Deep Authenticity©

Deep Authenticity© confronte identité du bien, mandat, annonces, offres, documents, signatures, paiements attestés, droits, versions et chronologie afin de détecter substitutions, duplications ou incohérences nécessitant vérification.

18. Litiges et annulations

Retrait, annulation, contestation ou litige conserve motif déclaré, documents, positions et décisions attribuées. AP organise la preuve sans déterminer automatiquement la responsabilité ou l’issue juridique.

19. AP Ledger et confidentialité

Empreintes minimales de mandat, offre acceptée, contrat, signature, paiement attesté, remise de clés ou changement de statut peuvent être ancrées dans AP Ledger. Identités complètes, données bancaires, codes d’accès et contrats détaillés restent hors des couches publiques ou irréversibles.

20. Critères d’acceptation et conclusion

Le modèle est acceptable si annonce et preuve de propriété restent distinctes ; si offre, acceptation et contrat ne sont pas confondus ; si les versions sont auditables ; si les paiements restent attestés sans exposer les secrets financiers ; si AP ne crée ni signature ni transfert de propriété ; si les accès physiques restent protégés ; et si les litiges conservent une chaîne de preuve sans jugement automatique. Le Passeport Property fournit ainsi une continuité vérifiable de la transaction immobilière.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 26 — REAL ESTATE / PROPERTY

CHAPITRE 3 — CONSTRUCTION, PROMOTION IMMOBILIÈRE, PERMIS, PLANS, BIM, CHANTIER, MATÉRIAUX, INSPECTIONS, CONFORMITÉ, RÉCEPTION, GARANTIES ET MAINTENANCE DU BÂTIMENT

1. Objet du chapitre

Ce chapitre applique le Passeport Numérique Property au cycle de construction et d'exploitation technique d'un bien : projet, permis, plans, BIM, chantier, entreprises, matériaux, inspections, réception, garanties, équipements et maintenance.

2. Identité du projet immobilier

Un projet peut disposer d'une identité reliant maître d'ouvrage, parcelle, programme, acteurs autorisés, versions, calendrier et documents de référence. Le projet reste distinct du bâtiment achevé et de ses futures unités.

3. Promotion immobilière

Le promoteur peut publier les informations et documents relevant de son rôle. Une communication commerciale, un plan de vente ou une projection reste distinct d'une autorisation administrative ou d' un état effectivement construit.

4. Permis et autorisations

Permis de construire, autorisations, modifications ou décisions conservent organisme émetteur, référence, date, portée et statut. AP ne délivre ni ne prolonge seul une autorisation officielle.

5. Plans et versions

Plans architecturaux, structurels, techniques ou d'exécution sont versionnés. Toute révision conserve auteur, date, motif et relation avec la version précédente afin d'éviter la substitution silencieuse.

6. BIM et maquette numérique

Une maquette BIM peut relier objets, zones, équipements, documents et versions du projet. Elle constitue une représentation numérique gouvernée et ne remplace pas automatiquement les documents contractuels ou réglementaires faisant foi.

7. Chantier

Les phases du chantier peuvent être reliées à leurs dates, entreprises, lots, événements et statuts. Les informations opérationnelles sensibles sont limitées aux acteurs autorisés.

8. Entreprises et sous-traitants

Entreprise générale, bureau d'études, architecte, ingénieur, sous-traitant ou autre intervenant conserve identité, rôle, mission, période et habilitations documentées.

9. Matériaux et produits

Les matériaux ou produits critiques peuvent disposer de références reliant fabricant, lot, documents techniques, certificats et destination sur le chantier lorsque cette traçabilité est nécessaire.

10. Livraison et réception des matériaux

Commande, livraison, contrôle, acceptation ou rejet sont des événements distincts. Une livraison sur site ne constitue pas automatiquement une preuve de conformité ou d'installation.

11. Installation

Un équipement ou composant installé peut être relié à son emplacement, date, intervenant et documents applicables. Produit livré, produit installé et produit mis en service restent distingués.

12. Inspections

Une inspection conserve organisme ou professionnel, périmètre, méthode, date, observations et résultat. AP authentifie la provenance du rapport sans se substituer au professionnel compétent.

13. Non-conformités

Une anomalie ou non-conformité présumée peut ouvrir un dossier reliant observation, référence, action corrective, contrôle et clôture. Un signal automatique ne constitue pas à lui seul une décision réglementaire.

14. Réception des travaux

Pré-réception, réserves, corrections, réception et levée des réserves sont historisées séparément. La réception reste attribuée aux parties ou autorités habilitées selon le cadre applicable.

15. Dossier de l'ouvrage

Plans finaux, notices, certificats, rapports, garanties, références d'équipements et autres documents peuvent être consolidés dans le passeport avec source, version et niveau d'accès.

16. Garanties

Une garantie constructeur, fabricant ou autre garantie conserve émetteur, objet, période, conditions et statut. AP ne crée ni ne prolonge une garantie au-delà de l'engagement documenté.

17. Maintenance du bâtiment

Inspection périodique, entretien, panne, réparation, remplacement ou mise à niveau d'un équipement peut être historisé. Maintenance prévue, réalisée et validée restent des états distincts.

18. Deep Authenticity©

Deep Authenticity© confronte permis, plans, BIM, matériaux, lots, installations, inspections, réception, garanties et maintenance afin de détecter incohérences de version, substitutions ou séquences nécessitant vérification.

19. AP Ledger, confidentialité et sécurité

Empreintes minimales de permis, version critique, livraison, inspection, réception, garantie ou maintenance peuvent être ancrées dans AP Ledger. Plans de sécurité, accès techniques, secrets commerciaux et documents sensibles restent hors des couches publiques ou irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si projet et bâtiment achevé restent distincts ; si promotion commerciale et autorisation officielle ne sont pas confondues ; si les plans et BIM restent versionnés ; si livraison, conformité, installation et mise en service restent séparées ; si les inspections restent attribuées ; si les garanties conservent leur émetteur ; et si la maintenance préserve l'historique technique. Le Passeport Property fournit ainsi une mémoire vérifiable de la construction jusqu'à l'exploitation du bâtiment.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 26 — REAL ESTATE / PROPERTY

CHAPITRE 4 — GESTION IMMOBILIÈRE, COPROPRIÉTÉ, SYNDIC, PROPRIÉTAIRES, LOCATAIRES, CHARGES, LOYERS, MAINTENANCE, INCIDENTS, DIAGNOSTICS, ÉNERGIE ET EXPLOITATION DU PATRIMOINE

1. Objet du chapitre

Ce chapitre applique le Passeport Numérique Property à l'exploitation quotidienne du patrimoine immobilier : gestion, copropriété, occupation, loyers, charges, équipements, maintenance, incidents, diagnostics, énergie et relations entre acteurs.

2. Identité du patrimoine exploité

Un portefeuille, immeuble, bâtiment ou ensemble immobilier peut être relié à son gestionnaire, ses unités, équipements, contrats de service et événements autorisés. La gestion opérationnelle reste distincte de la propriété juridique.

3. Propriétaires et titulaires

Les propriétaires ou autres titulaires de droits conservent une relation au bien fondée sur les sources compétentes. Le gestionnaire ne devient pas propriétaire du seul fait de son mandat d'administration.

4. Copropriété

Lots privatifs, parties communes, quotes-parts ou informations équivalentes peuvent être reliés aux documents et sources applicables. AP ne redéfinit pas seul les droits ou règles juridiques de copropriété.

5. Syndic ou gestionnaire

Le syndic, administrateur ou gestionnaire dispose d'une identité, d'un mandat, d'une période et de droits limités. Ses actions critiques restent attribuables et son accès est révisable ou révocable.

6. Locataires et occupants

L'identité des locataires ou occupants est protégée. Bail, période d'occupation, droits d'usage et événements nécessaires peuvent être reliés au dossier sans créer de suivi permanent de la présence des personnes.

7. Loyers

Échéance, appel, paiement attesté, retard ou régularisation peuvent être historisés. Les coordonnées bancaires et détails financiers sensibles restent hors des couches publiques ou irréversibles.

8. Charges

Les charges peuvent être reliées à leur période, catégorie, source, méthode de répartition et justificatifs. Un calcul ou appel de charges reste distingué du paiement effectivement reçu.

9. Contrats de service

Nettoyage, sécurité, ascenseurs, chauffage, espaces verts ou autres prestations peuvent être reliés au prestataire, au contrat, à la période, aux interventions et aux preuves de service.

10. Maintenance préventive

Inspection, entretien planifié, contrôle réglementaire ou remplacement programmé peut conserver actif, date, intervenant, action, résultat et prochaine échéance lorsque pertinente.

11. Maintenance corrective

Une panne ou anomalie peut ouvrir une intervention reliant signalement, diagnostic, action, pièces remplacées et remise en service. Signalement initial, diagnostic confirmé et résolution restent distincts.

12. Incidents

Dégât, panne, fuite, accès défaillant ou autre incident peut être relié au lieu, à la période, aux observations, interventions et statuts. AP organise la chronologie sans attribuer automatiquement une responsabilité.

13. Diagnostics immobiliers

Un diagnostic conserve professionnel ou organisme, périmètre, méthode, date, résultat et durée de validité éventuelle. AP authentifie sa provenance sans se substituer au diagnostiqueur.

14. Énergie et consommations

Des données de consommation peuvent être reliées au bâtiment, à l’unité ou à un équipement selon les droits applicables. Mesure réelle, estimation et calcul restent identifiables comme des catégories différentes.

15. Performance énergétique

Un indicateur ou certificat de performance conserve méthode, source, date et statut. Une mesure opérationnelle instantanée ne remplace pas automatiquement une certification officielle.

16. Deep Authenticity©

Deep Authenticity© confronte mandats, baux, charges, paiements attestés, contrats, équipements, interventions, diagnostics, consommations et chronologie afin de détecter incohérences, duplications ou substitutions nécessitant vérification.

17. Accès physiques et numériques

Clés, badges, droits numériques et accès techniques sont limités au rôle, au lieu et à la durée nécessaires. Les secrets d'accès ne sont jamais inscrits dans un QR public ou dans AP Ledger.

18. Vie privée et données des occupants

Identité, unité occupée, horaires, consommations individualisées, paiements, demandes et incidents sont compartimentés. Les vues publiques ne doivent pas permettre de profiler les habitudes d'un occupant.

19. AP Ledger

Empreintes minimales de mandat, bail, appel ou paiement attesté, maintenance critique, diagnostic, changement d'équipement et clôture d'incident peuvent être ancrées dans AP Ledger. Données personnelles, codes d'accès, détails bancaires et consommations fines restent hors des couches irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si gestion et propriété restent distinctes ; si les mandats sont limités et révocables ; si appel de charges et paiement ne sont pas confondus ; si signalement, diagnostic et résolution restent séparés ; si mesure, estimation et certification énergétique restent identifiables ; si les accès sont protégés ; et si la vie privée des occupants est préservée. Le Passeport Property fournit ainsi une mémoire vérifiable de l'exploitation du patrimoine immobilier.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 26 — REAL ESTATE / PROPERTY

CHAPITRE 5 — GOUVERNANCE IMMOBILIÈRE, CADASTRE, REGISTRE FONCIER, NOTAIRES, AUTORITÉS, PROPRIÉTAIRES, PROMOTEURS, AGENTS, GESTIONNAIRES, INTEROPÉRABILITÉ, CONFIDENTIALITÉ, SOUVERAINETÉ ET AUDIT

1. Objet du chapitre

Ce chapitre définit la gouvernance du Passeport Numérique Property : autorités, cadastre, registre foncier, notaires et professionnels compétents, propriétaires, promoteurs, agents, gestionnaires, droits d'accès, interopérabilité, confidentialité, souveraineté et audit.

2. Principe de gouvernance

Authenticity Plus© organise identité, provenance, version et historique des preuves immobilières sans se substituer aux institutions et professionnels auxquels le droit attribue l'enregistrement, l' authentification, le contrôle ou la décision.

3. Cadastre

Les données cadastrales conservent leur organisme source, référence, date, périmètre et version. AP peut les relier au passeport du bien mais ne modifie pas seul une référence ou une limite cadastrale officielle.

4. Registre foncier

Les inscriptions relatives à la propriété et aux droits réels restent sous l'autorité du registre ou de l' institution compétente. Le Passeport Property peut authentifier une preuve ou un statut reçu sans créer lui-même une inscription juridique.

5. Notaires et professionnels habilités

Notaires et autres professionnels légalement compétents peuvent produire, authentifier ou transmettre des actes selon leur rôle. Leur identité, qualité, mandat et signature restent attribuables et vérifiables.

6. Autorités publiques

Permis, décisions d'urbanisme, certificats, restrictions et autres actes officiels conservent leur autorité émettrice, leur date, leur portée et leur statut. AP ne transforme pas une information privée en décision publique.

7. Propriétaires et titulaires

Les propriétaires et titulaires de droits accèdent aux informations et opérations autorisées concernant leurs biens. Leur identité et leur patrimoine ne sont pas rendus publics au-delà de ce que permettent les règles applicables.

8. Promoteurs et constructeurs

Promoteurs, constructeurs et maîtres d'ouvrage disposent de droits limités à leurs projets, documents et obligations. Ils ne peuvent modifier une preuve officielle émise par une autorité ou un autre professionnel.

9. Agents et intermédiaires

Agents immobiliers, mandataires et autres intermédiaires opèrent selon un mandat documenté. La publication d'une annonce ou la transmission d'un document ne leur confère ni propriété ni qualité d' émetteur du document d'origine.

10. Gestionnaires et syndics

Gestionnaires et syndics disposent d'habilitations correspondant au mandat, au bien, à la période et aux fonctions nécessaires. La fin du mandat entraîne révision ou révocation des droits sans effacer l' historique des actions passées.

11. Séparation des rôles

Posséder, vendre, représenter, authentifier, enregistrer, construire, gérer, contrôler, auditer et décider sont des fonctions distinctes. Le principe du moindre privilège limite les droits de chaque acteur.

12. Validation multiniveau

Une modification critique d'identité du bien, de droit, de document, de statut ou d'accès peut exiger plusieurs validations selon le cadre applicable. Les validations restent attribuées et chronologiques.

13. Interopérabilité institutionnelle

Cadastre, registre foncier, systèmes notariaux, urbanisme, gestion immobilière, BIM, banques, assurances et autres plateformes autorisées peuvent échanger avec AP. Toute donnée importée conserve sa source, son horodatage, sa version et son niveau d'autorité.

14. Divergences entre sources

Lorsque deux sources autorisées divergent, AP conserve les deux états, leurs dates et leur provenance et déclenche une vérification. Il ne tranche pas automatiquement un conflit de titre, de limite ou de droit.

15. Portabilité et continuité

Le changement de gestionnaire, plateforme ou prestataire ne doit pas effacer l'historique vérifiable du bien. Les données exportables restent soumises aux droits, formats et obligations applicables.

16. Confidentialité

Actes complets, identités, prix, hypothèques, données financières, plans sensibles, codes d'accès et informations d'occupation sont compartimentés. Chaque acteur n'accède qu'aux éléments nécessaires à sa mission.

17. Souveraineté des données

L'entité compétente doit pouvoir gouverner localisation, conservation, accès, transfert, durée de vie et suppression des données immobilières selon les exigences applicables.

18. Cybersécurité et audit

Comptes privilégiés, API, signatures, certificats et accès partenaires sont protégés et révocables. L' auditeur habilité peut vérifier preuves, accès et journaux nécessaires sans disposer automatiquement du pouvoir de modifier le registre ou le dossier.

19. AP Ledger

Empreintes minimales de titres, actes, mandats, validations, permis, inscriptions reçues, changements critiques et révocations peuvent être ancrées dans AP Ledger. Actes complets, données personnelles, secrets financiers et plans sensibles restent hors des couches irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si les compétences institutionnelles restent distinctes ; si AP ne crée ni titre ni inscription foncière ; si les mandats et accès sont limités et révocables ; si les divergences sont conservées sans arbitrage automatique ; si l'interopérabilité préserve la provenance ; si les données privées restent souveraines ; et si l'audit demeure indépendant. Cette gouvernance fournit le socle nécessaire à la clôture fonctionnelle de l'application Real Estate / Property.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 26 — REAL ESTATE / PROPERTY

CHAPITRE 6 — SYNTHÈSE FONCTIONNELLE, CRITÈRES D'ACCEPTATION ET CLÔTURE DE L'APPLICATION REAL ESTATE / PROPERTY

1. Objet du chapitre

Ce chapitre clôt le Point 26 — Real Estate / Property. Il consolide parcelles, bâtiments, unités, titres, droits, transactions, construction, BIM, exploitation, copropriété, maintenance, gouvernance, confidentialité, souveraineté et AP Ledger.

2. Mission consolidée

Le Passeport Numérique Property constitue une mémoire vérifiable du cycle de vie immobilier. Authenticity Plus© / Deep Authenticity© relie identités, sources, documents, versions et événements sans se substituer au cadastre, au registre foncier, au notaire, au juge, à l'administration ou aux autres professionnels compétents.

3. Parcelle, bâtiment et unité

Parcelle, bâtiment et unité immobilière restent trois objets distincts reliés par des références documentées. Une évolution physique ou administrative est historisée sans réécrire silencieusement l'état antérieur.

4. Titres, actes et droits

Titres, actes, propriété, usufruit, bail, hypothèque, servitude et autres droits ou charges conservent leur source, leur portée, leur date et leur statut. Une copie numérique authentifiée ne crée pas à elle seule un droit réel.

5. Cadastre et registre foncier

Les données cadastrales et foncières restent attribuées à leurs institutions compétentes. En cas de divergence, AP conserve provenance, date et versions et déclenche une vérification sans arbitrer automatiquement le conflit juridique.

6. QR Codes dynamiques

Un QR dynamique peut permettre une vérification proportionnée de l'identité du bien ou d'un document. Sa copie ne permet ni transfert de propriété, ni modification d'un registre, ni accès physique critique.

7. Transactions immobilières

Annonce, mandat, visite, offre, contre-offre, acceptation, contrat, acte, paiement attesté et transfert sont des événements distincts. Une annonce ne constitue pas une preuve de propriété et une offre acceptée ne remplace pas les formalités légales applicables.

8. Signatures et paiements

Les signatures et paiements peuvent être attestés avec leur mécanisme, date et statut. AP n'invente pas une signature, ne prend pas une décision de crédit et ne conserve pas les secrets bancaires dans les couches irréversibles.

9. Location et occupation

Bail, état des lieux, remise de clés, occupation et fin d'occupation sont historisés selon les droits. Les informations permettant de suivre les habitudes ou la présence d'un occupant restent protégées.

10. Construction et promotion

Projet, bâtiment achevé et unité livrée restent distincts. Promotion commerciale, autorisation administrative et état effectivement construit ne sont pas confondus.

11. Plans, BIM et versions

Plans et maquettes BIM conservent auteurs, versions, dates et relations avec les documents applicables. La maquette numérique ne remplace pas automatiquement les documents contractuels ou réglementaires faisant foi.

12. Matériaux, installation et conformité

Produit commandé, livré, contrôlé, installé et mis en service restent des états distincts. Les inspections et décisions de conformité restent attribuées aux professionnels ou autorités habilités.

13. Réception, garanties et maintenance

Pré-réception, réserves, corrections, réception et levée des réserves sont séparées. Les garanties conservent leur émetteur et leur période ; la maintenance conserve l'historique des équipements et interventions.

14. Gestion immobilière et copropriété

Propriété juridique, gestion, mandat de syndic, copropriété et occupation restent distincts. Les droits du gestionnaire sont limités à son mandat et révocables à son terme.

15. Charges, loyers, diagnostics et énergie

Appel de charges et paiement reçu restent séparés. Signalement, diagnostic et résolution ne sont pas confondus. Mesure énergétique, estimation et certification officielle conservent chacune leur source et leur nature.

16. Deep Authenticity©

Deep Authenticity© confronte références du bien, droits, documents, signatures, plans, BIM, matériaux, transactions, maintenances, diagnostics et chronologie afin de signaler duplications, substitutions, incohérences ou expirations nécessitant vérification.

17. Gouvernance et interopérabilité

Cadastre, registre foncier, notaires, autorités, propriétaires, promoteurs, agents, gestionnaires, banques, assurances et autres systèmes autorisés conservent leurs rôles. Toute donnée échangée conserve source, version, horodatage et niveau d'autorité.

18. Confidentialité, cybersécurité et souveraineté

Identités, actes complets, prix, données financières, hypothèques, plans sensibles, accès et informations d'occupation sont compartimentés. Les accès sont révocables et l'entité compétente gouverne localisation, conservation, transfert et durée de vie des données.

19. AP Ledger et critères d'acceptation

AP Ledger reçoit uniquement des empreintes minimales de titres, actes, mandats, permis, validations, transactions, inspections, maintenances ou révocations. Le modèle est acceptable si les rôles restent séparés, la provenance préservée, les divergences non arbitrées automatiquement et les données sensibles hors des couches irréversibles.

20. Clôture du Point 26 — Real Estate / Property

Le Point 26 — Real Estate / Property est désormais fonctionnellement défini : parcelles, bâtiments, unités, titres, droits, QR dynamiques, transactions, signatures, paiements attestés, baux, construction, permis, BIM, matériaux, inspections, réception, garanties, maintenance, copropriété, énergie, Deep Authenticity©, gouvernance, interopérabilité, confidentialité, cybersécurité, souveraineté, audit et AP Ledger. Le Volume IV peut désormais poursuivre avec le Point 27 — Public Administration.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 27 — PUBLIC ADMINISTRATION

CHAPITRE 1 — IDENTITÉ NUMÉRIQUE ADMINISTRATIVE, ADMINISTRATIONS, AGENTS, USAGERS, DOSSIERS, DOCUMENTS OFFICIELS, DÉMARCHES, QR CODES DYNAMIQUES, PROVENANCE ET PASSEPORT NUMÉRIQUE ADMINISTRATION

1. Objet du chapitre

Le Point 27 — Public Administration transpose Authenticity Plus© / Deep Authenticity© aux services administratifs. Le Passeport Numérique Administration relie administrations, agents habilités, usagers, dossiers, demandes, documents officiels, décisions, paiements administratifs attestés et preuves institutionnelles.

2. Mission sectorielle

La mission est d'authentifier identité, provenance, version et chronologie des démarches publiques sans se substituer à l'administration, au fonctionnaire compétent, au juge ou à toute autorité disposant légalement du pouvoir de décision.

3. Identité de l'administration

Ministère, direction, collectivité, établissement public, agence ou autre organisme peut disposer d'une identité vérifiable reliant dénomination, compétence déclarée, services, canaux officiels et informations institutionnelles.

4. Identité de l'agent

Un agent habilité peut disposer d'une identité professionnelle reliant organisme, rôle, périmètre et période d'habilitation. Son identité personnelle n'est exposée que dans la mesure nécessaire à l'acte ou au contrôle.

5. Identité de l'usager

L'usager peut être une personne ou une organisation. Son identité administrative est protégée et peut être vérifiée sans rendre publiquement accessibles ses documents, identifiants ou données personnelles.

6. Identité du dossier

Chaque dossier peut disposer d'un identifiant reliant administration, démarche, demandeur autorisé, pièces, événements, statuts et décisions. Le dossier reste cloisonné selon sa sensibilité.

7. Démarches administratives

Une démarche conserve service compétent, conditions publiées, formulaire ou version, pièces requises, date de dépôt et statut. Une modification des règles ne réécrit pas silencieusement les exigences applicables à une étape antérieure.

8. Dépôt de demande

Le dépôt peut produire une preuve vérifiable de réception avec administration, date, référence et liste ou empreinte des pièces reçues. Un accusé de réception ne constitue pas automatiquement une acceptation de la demande.

9. Documents officiels

Certificat, attestation, autorisation, licence, extrait ou autre document officiel conserve émetteur, référence, date, portée, période de validité et statut lorsque applicable.

10. QR Code dynamique

Un QR dynamique peut permettre de vérifier l'authenticité et le statut d'un document administratif en révélant uniquement les informations nécessaires. Sa copie visuelle ne permet pas de créer un nouveau document officiel valide.

11. Instruction du dossier

Demande de complément, contrôle, avis, validation intermédiaire, décision et notification restent des événements distincts. Chaque étape est attribuée au service, rôle ou système habilité.

12. Décision administrative

Une décision conserve autorité, date, fondement ou référence lorsque disponible, portée et statut. Authenticity Plus© n'émet pas seul une décision administrative et n'en modifie pas le sens.

13. Notifications

Une notification peut être reliée à son émetteur, son destinataire autorisé, son contenu ou empreinte, sa date et son statut de remise. Les canaux de communication restent gouvernés par l'administration compétente.

14. Paiements administratifs attestés

Taxe, droit, redevance ou autre paiement peut être relié à une preuve minimale de statut. Les coordonnées bancaires et secrets de paiement restent hors des couches publiques ou irréversibles.

15. Provenance et versioning

Toute pièce ou donnée importée conserve source, date, version et niveau d'autorité. Une copie fournie par l'usager reste distincte d'une donnée obtenue directement depuis une source institutionnelle.

16. Deep Authenticity©

Deep Authenticity© confronte identité de l'administration, habilitation de l'agent, dossier, pièces, documents officiels, versions, signatures, décisions et chronologie afin de détecter incohérences, substitutions ou expirations nécessitant vérification.

17. Anomalie ou fraude présumée

Un document incohérent, une identité dupliquée ou une séquence inhabituelle peut déclencher une vérification renforcée. Une anomalie ne constitue pas automatiquement une fraude ni une culpabilité.

18. Vie privée et minimisation

État civil, adresse, situation familiale, finances, santé, identifiants administratifs et autres données sensibles sont minimisés et compartimentés. Les vues publiques ne permettent pas de reconstituer le dossier administratif d'une personne.

19. AP Ledger

Empreintes minimales de dépôt, document officiel, validation, décision, notification, révocation ou changement critique peuvent être ancrées dans AP Ledger. Dossiers complets, données personnelles, secrets et pièces sensibles restent hors des couches irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si administration, agent, usager et dossier restent distincts ; si accusé de réception et acceptation ne sont pas confondus ; si toute décision reste attribuée à l'autorité compétente ; si les documents sont vérifiables sans surexposer les données ; si anomalie et fraude restent distinctes ; et si la vie privée est préservée. Le Passeport Administration fournit ainsi le socle d' une chaîne de confiance pour les services administratifs.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 27 — PUBLIC ADMINISTRATION

CHAPITRE 2 — IDENTITÉ ADMINISTRATIVE, ÉTAT CIVIL, CERTIFICATS, LICENCES, PERMIS, DEMANDES CITOYENNES, SIGNATURES, DÉLÉGATIONS, PAIEMENTS ET DÉLIVRANCE DES DOCUMENTS PUBLICS

1. Objet du chapitre

Ce chapitre approfondit le Passeport Numérique Administration pour les actes et services publics : identité administrative, état civil, certificats, licences, permis, demandes citoyennes, signatures, délégations, paiements attestés et délivrance de documents.

2. Identité administrative

L'identité administrative d'une personne ou d'une organisation peut être vérifiée à partir de sources autorisées. Le système privilégie la preuve minimale nécessaire et évite la duplication publique de documents d'identité.

3. État civil

Les actes et informations d'état civil restent sous l'autorité des organismes compétents. Naissance, mariage, décès ou autre événement enregistré conserve source, référence, date, version ou rectification applicable.

4. Rectifications

Une correction ou rectification administrative est historisée avec autorité, date, motif ou référence disponible. La nouvelle version ne doit pas effacer silencieusement l'existence de la version antérieure.

5. Certificats et attestations

Un certificat ou une attestation officielle conserve émetteur, bénéficiaire autorisé, objet, date, période de validité et statut. La vérification publique éventuelle révèle uniquement les informations nécessaires.

6. Licences

Une licence peut être reliée à son titulaire, activité, autorité émettrice, période, conditions et statut. Émission, renouvellement, suspension, expiration et révocation sont des événements distincts.

7. Permis et autorisations

Un permis ou une autorisation conserve demande, pièces, instruction, autorité, date, portée et statut. Authenticity Plus© ne délivre ni ne prolonge seul une autorisation publique.

8. Demandes citoyennes

Une demande citoyenne peut concerner un document, une prestation, une autorisation, une correction ou une autre démarche. Le dépôt, l'instruction, la réponse et la décision restent séparés.

9. Pièces justificatives

Les pièces fournies par l'usager conservent source déclarée, date de dépôt, version et statut de vérification. Une copie fournie par le demandeur reste distincte d'une donnée obtenue directement auprès de l'émetteur.

10. Signatures

Une signature électronique ou autre preuve de signature peut être reliée au document, au signataire, au mécanisme utilisé et à la date. AP authentifie la preuve disponible sans inventer une signature ou étendre sa portée juridique.

11. Délégations de pouvoir

Une délégation conserve délégant, délégataire, compétence, périmètre, période et statut. Toute action effectuée sous délégation reste attribuable à l'agent concerné et à la délégation applicable.

12. Révocation des délégations

Expiration, retrait ou révocation d'une délégation entraîne la fin des droits correspondants sans effacer les actes régulièrement enregistrés pendant sa période de validité.

13. Paiements administratifs

Taxe, droit, redevance, amende administrative ou autre paiement peut être relié à une preuve minimale de statut. Paiement demandé, initié, reçu, rapproché et remboursé restent des états distincts.

14. Délivrance des documents

Préparation, validation, émission, remise et retrait éventuel d'un document public sont historisés séparément. La délivrance reste attribuée à l'autorité ou au service habilité.

15. QR Codes dynamiques

Un QR dynamique peut vérifier émetteur, référence, validité et statut d'un document selon le niveau d' accès. Une copie visuelle ne permet ni d'émettre un nouveau document ni de modifier son statut officiel.

16. Deep Authenticity©

Deep Authenticity© confronte identité, sources d'état civil, pièces, signatures, délégations, certificats, licences, permis, paiements attestés et chronologie afin de signaler incohérences, duplications ou substitutions nécessitant vérification.

17. Recours et contestations

Un recours administratif ou une contestation peut conserver demandeur, acte concerné, arguments, pièces, dates et décisions successives. AP organise la chaîne de preuve sans trancher automatiquement le recours.

18. Confidentialité et droits d'accès

Les données d'état civil, identité, finances, situation familiale et dossiers personnels sont compartimentées. Les agents accèdent uniquement aux informations nécessaires à leur compétence et à la démarche traitée.

19. AP Ledger

Empreintes minimales d'actes, certificats, licences, permis, délégations, signatures, paiements attestés, décisions et révocations peuvent être ancrées dans AP Ledger. Les dossiers complets et données personnelles restent hors des couches irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si identité et documents restent protégés ; si dépôt, instruction, décision et délivrance ne sont pas confondus ; si toute délégation est limitée et révocable ; si les signatures restent attribuables ; si les paiements conservent leurs statuts ; si les recours ne sont pas tranchés automatiquement ; et si toute délivrance reste attribuée à l'autorité compétente. Le Passeport Administration fournit ainsi une chaîne vérifiable des actes et services publics.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 27 — PUBLIC ADMINISTRATION

CHAPITRE 3 — SERVICES PUBLICS, GUICHETS PHYSIQUES ET NUMÉRIQUES, DOSSIERS INTER-ADMINISTRATIONS, AIDES, PRESTATIONS, MARCHÉS ADMINISTRATIFS, INSPECTIONS, RÉCLAMATIONS ET CONTINUITÉ DE SERVICE

1. Objet du chapitre

Ce chapitre applique le Passeport Numérique Administration à l'exécution des services publics : guichets, portails numériques, échanges inter-administrations, aides, prestations, marchés administratifs, inspections, réclamations et continuité de service.

2. Identité du service public

Chaque service peut disposer d'une identité reliant administration responsable, compétence, canaux, conditions, versions des procédures et informations officielles. Un prestataire technique n'est pas confondu avec l'autorité publique responsable.

3. Guichet physique

Une interaction au guichet peut produire une preuve de dépôt, de remise ou de rendez-vous lorsque nécessaire. La collecte de données reste limitée à la démarche et l'identité de l'agent n'est exposée qu' au niveau requis.

4. Guichet numérique

Un portail ou service en ligne conserve identité de l'administration, version du formulaire, date de soumission, accusé de réception et statuts. Une interface numérique ne devient pas elle-même l' autorité de décision.

5. Omnicanal

Une démarche commencée en ligne et poursuivie au guichet, par courrier ou autre canal conserve le même dossier ou des liens explicites entre dossiers afin d'éviter doublons et ruptures de preuve.

6. Dossiers inter-administrations

Plusieurs administrations peuvent contribuer à une démarche selon leurs compétences. Chaque donnée partagée conserve source, finalité, date et niveau d'autorité ; l'accès à un dossier ne donne pas automatiquement accès à tous les autres dossiers de l'usager.

7. Principe de minimisation inter-administrations

Une administration ne reçoit que les informations nécessaires à la compétence exercée. La mutualisation technique ne doit pas devenir une centralisation illimitée des données personnelles.

8. Aides et prestations

Une demande d'aide, subvention, allocation ou prestation peut conserver critères publiés, pièces, instruction, décision, période et paiements attestés. AP ne détermine pas seul l'éligibilité juridique d'un usager.

9. Calculs et simulations

Une simulation ou estimation peut aider l'usager à comprendre une prestation. Elle reste identifiée comme simulation et ne constitue pas une décision, un droit acquis ou un montant définitivement dû.

10. Versements

Ordre de paiement, paiement initié, exécuté, reçu, rejeté ou récupéré restent des statuts distincts. Les données bancaires sensibles sont protégées et ne sont pas inscrites dans les couches irréversibles.

11. Marchés administratifs

Appel, dossier de consultation, soumission, évaluation, attribution, contrat, exécution et réception peuvent être historisés selon les règles applicables. AP authentifie la chaîne documentaire sans sélectionner automatiquement l'attributaire.

12. Soumissionnaires et fournisseurs

Une entreprise ou organisation participante conserve identité, rôle, documents transmis et statuts. Les informations confidentielles d'une offre restent cloisonnées selon les droits et procédures applicables.

13. Inspections administratives

Une inspection conserve autorité ou agent habilité, périmètre, date, méthode, observations et résultat. AP authentifie la provenance du rapport sans se substituer à l'autorité de contrôle.

14. Non-conformités et mesures

Observation, non-conformité présumée, demande corrective, décision, correction et clôture restent des étapes distinctes. Un signal automatique ne constitue pas à lui seul une sanction ou une décision administrative.

15. Réclamations

Une réclamation peut relier usager, service, objet, date, pièces, réponses et décisions successives. Le système conserve les versions et délais sans effacer les positions antérieures.

16. Deep Authenticity©

Deep Authenticity© confronte services, agents, dossiers, pièces, aides, paiements attestés, marchés, inspections, décisions et chronologies afin de détecter incohérences, duplications ou substitutions nécessitant vérification.

17. Continuité de service

Les administrations peuvent prévoir des modes dégradés ou Offline pour certaines fonctions autorisées. Toute opération différée conserve auteur, heure, preuve locale, date de synchronisation et contrôle lors du retour Online.

18. Accessibilité et égalité de canal

La transformation numérique doit préserver des voies adaptées lorsque le cadre ou les besoins l’ exigent. Le canal utilisé ne doit pas modifier silencieusement la nature de la décision ou de la preuve administrative.

19. AP Ledger, confidentialité et sécurité

Empreintes minimales de dépôts, décisions, marchés, inspections, paiements attestés, réclamations et événements critiques peuvent être ancrées dans AP Ledger. Dossiers complets, offres confidentielles, données bancaires et données personnelles restent hors des couches irréversibles.

20. Critères d’acceptation et conclusion

Le modèle est acceptable si service et prestataire technique restent distincts ; si les canaux conservent une continuité de dossier ; si les échanges inter-administrations sont minimisés ; si simulation et décision ne sont pas confondues ; siles marchés conservent une chaîne documentaire attribuable ; si une inspection reste distincte d’une sanction ; si l’Offline est resynchronisé et contrôlé ; et si la confidentialité est préservée. Le Passeport Administration fournit ainsi une continuité vérifiable des services publics.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 27 — PUBLIC ADMINISTRATION

CHAPITRE 4 — COLLECTIVITÉS TERRITORIALES, MUNICIPALITÉS, URBANISME, SERVICES LOCAUX, FISCALITÉ ADMINISTRATIVE, REGISTRES, CONSULTATIONS PUBLIQUES, TRANSPARENCE ET PARTICIPATION CITOYENNE

1. Objet du chapitre

Ce chapitre applique le Passeport Numérique Administration à l'échelon territorial : collectivités, municipalités, urbanisme, services locaux, fiscalité administrative, registres, consultations publiques, transparence et participation citoyenne.

2. Identité de la collectivité

Une collectivité ou municipalité peut disposer d'une identité vérifiable reliant territoire, compétences, services, organes habilités, canaux officiels et documents institutionnels.

3. Compétences territoriales

Chaque acte ou service conserve l'autorité compétente et son périmètre territorial. AP ne transfère pas une compétence d'une administration à une autre et ne déduit pas seul une compétence juridique.

4. Services municipaux

État civil local, voirie, propreté, équipements, marchés, autorisations ou autres services peuvent être reliés à leurs procédures, dossiers, interventions et décisions selon les règles applicables.

5. Urbanisme

Demandes, avis, permis, certificats, prescriptions, contrôles et décisions d'urbanisme peuvent être historisés. Une information cartographique ou technique ne constitue pas automatiquement une autorisation.

6. Plans et zonage

Plans d'urbanisme, zonages ou documents équivalents conservent source, version, date d'effet et statut. Les versions antérieures restent identifiables afin de reconstituer le cadre applicable à une date donnée.

7. Demandes locales

Une demande d'autorisation, d'intervention ou de service conserve dépôt, pièces, instruction, échanges, décision et notification. Un signalement citoyen reste distinct d'un constat administratif.

8. Services techniques locaux

Une intervention sur voirie, éclairage, réseau, bâtiment ou équipement public peut conserver signalement, ordre d'intervention, exécution, contrôle et clôture.

9. Fiscalité administrative locale

Avis, taxe, redevance ou autre créance administrative locale peut conserver période, base ou référence autorisée, montant, statut et paiement attesté. AP ne fixe pas seul l'assiette ou le montant légalement dû.

10. Registres administratifs

Un registre local peut conserver entrées, modifications, radiations et références selon sa nature. Les écritures restent attribuées à l'autorité compétente et les données personnelles sont protégées.

11. Délibérations et décisions

Projet, inscription à l'ordre du jour, délibération, vote institutionnel, décision, publication et entrée en vigueur restent des événements distincts lorsqu'ils sont applicables.

12. Consultations publiques

Une consultation peut conserver organisateur, objet, période, documents publiés, contributions reçues et synthèse. Une contribution citoyenne ne constitue pas automatiquement une décision de la collectivité.

13. Participation citoyenne

Pétitions, propositions, budgets participatifs ou autres mécanismes peuvent disposer de preuves de dépôt et de traitement. AP authentifie la procédure sans transformer une participation en mandat politique ou décision juridique.

14. Transparence administrative

Documents, décisions, budgets ou données rendus publics peuvent être vérifiés par leur source, version et date. La transparence ne justifie pas la publication de données personnelles ou confidentielles non nécessaires.

15. Données ouvertes

Les jeux de données ouverts peuvent conserver producteur, date, licence, version, fréquence de mise à jour et transformations documentées. Une donnée ouverte dérivée reste distincte de sa source institutionnelle.

16. Deep Authenticity©

Deep Authenticity© confronte compétences, documents, versions, décisions, registres, interventions, consultations et publications afin de détecter incohérences, substitutions ou altérations nécessitant vérification.

17. Consultation, vote institutionnel et élections

Les mécanismes de consultation ou de vote institutionnel documentés restent distincts des élections publiques régies par des cadres spécifiques. AP ne détermine pas seul la validité d'un scrutin, d'un résultat électoral ou d'un mandat.

18. Vie privée et sécurité

Données des habitants, adresses, fiscalité, demandes individuelles, plans sensibles et informations de sécurité sont compartimentés. Les publications territoriales appliquent minimisation et contrôle d' accès.

19. AP Ledger

Empreintes minimales de décisions, versions de plans, permis, registres, consultations, publications et événements critiques peuvent être ancrées dans AP Ledger. Données personnelles, secrets administratifs et informations de sécurité restent hors des couches irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si chaque compétence reste attribuée ; si signalement et constat ne sont pas confondus ; si information d'urbanisme et autorisation restent distinctes ; si consultation, décision et élection ne sont pas fusionnées ; si la transparence respecte la vie privée ; et si les données ouvertes conservent leur provenance. Le Passeport Administration fournit ainsi une chaîne de confiance vérifiable pour l'action publique territoriale.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 27 — PUBLIC ADMINISTRATION

CHAPITRE 5 — GOUVERNANCE ADMINISTRATIVE, AUTORITÉS, AGENTS, DÉLÉGATIONS, CONTRÔLE INTERNE, INTEROPÉRABILITÉ, IA PUBLIQUE, EXPLICABILITÉ, CYBERSÉCURITÉ, CONFIDENTIALITÉ, SOUVERAINETÉ ET AUDIT

1. Objet du chapitre

Ce chapitre définit la gouvernance du Passeport Numérique Administration : autorités, agents, délégations, séparation des fonctions, contrôle interne, échanges entre administrations, intelligence artificielle, explicabilité, cybersécurité, confidentialité, souveraineté et audit.

2. Principe de gouvernance

Authenticity Plus© organise l'identité, la provenance, la version et la chronologie des actes administratifs. Il ne crée pas une compétence publique et ne se substitue ni à l'autorité décisionnaire, ni au contrôle juridictionnel, ni aux mécanismes légaux de recours.

3. Autorités administratives

Chaque autorité conserve son identité, sa compétence, son périmètre territorial ou fonctionnel et ses actes. Une donnée partagée par plusieurs services conserve toujours l'autorité qui l'a produite.

4. Agents publics

Un agent dispose d'une identité professionnelle, d'un rôle, d'une affectation et d'habilitations limitées. Les actions sensibles sont attribuables sans exposer inutilement les données personnelles de l'agent.

5. Délégations

Une délégation conserve délégant, délégataire, compétence, périmètre, date de début, date de fin et statut. La délégation n'efface jamais l'identité de l'agent ayant effectivement réalisé l'action.

6. Séparation des fonctions

Recevoir, instruire, contrôler, valider, décider, payer, auditer et administrer les droits d'accès sont des fonctions distinctes lorsque le processus l'exige. Les cumuls sensibles peuvent nécessiter des contrôles supplémentaires.

7. Principe du moindre privilège

Chaque utilisateur ou système reçoit uniquement les droits nécessaires à sa mission, pour la durée utile. Les habilitations sont révisables, révocables et journalisées.

8. Validation multiniveau

Un acte critique, une modification de registre, un paiement important ou un changement d'habilitation peut nécessiter plusieurs validations. Les validateurs, dates, séquences et éventuels rejets restent historisés.

9. Contrôle interne

Les contrôles peuvent vérifier séparation des fonctions, habilitations, cohérence des dossiers, respect des procédures et traçabilité. Un contrôle interne reste distinct d'un audit indépendant ou d'une décision juridictionnelle.

10. Interopérabilité administrative

Administrations, collectivités, registres et plateformes autorisées peuvent échanger des données. Chaque échange conserve source, finalité, horodatage, version, base d'autorité disponible et destinataire autorisé.

11. Minimisation des échanges

L'interopérabilité ne signifie pas accès généralisé. Seules les données nécessaires à la démarche et à la compétence exercée sont transmises, avec limitation de durée et de réutilisation.

12. Intelligence artificielle publique

L'IA peut assister classement, recherche, analyse documentaire, détection d'incohérences ou priorisation lorsqu'elle est autorisée. Elle reste identifiée comme outil d'assistance et ne reçoit pas implicitement une compétence administrative.

13. Explicabilité et contestabilité

Lorsqu'un système automatisé contribue de manière significative à une décision, les éléments nécessaires à sa compréhension, à son contrôle et à sa contestation sont conservés selon le cadre applicable.

14. Deep Authenticity©

Deep Authenticity© confronte identités, habilitations, délégations, documents, décisions, signatures, paiements attestés et chronologies afin de signaler incohérences ou substitutions. Un signal ne constitue ni une sanction ni une décision autonome.

15. Cybersécurité

Comptes privilégiés, API, certificats, signatures, consoles et accès inter-administrations sont protégés par authentification, segmentation, journalisation et révocation. Aucun QR public ne donne accès à une fonction administrative critique.

16. Confidentialité

État civil, santé, finances, fiscalité, dossiers sociaux, adresses, identifiants et autres données sensibles sont compartimentés. Les agents et systèmes n'accèdent qu'aux informations nécessaires à la finalité autorisée.

17. Souveraineté des données

L'autorité compétente doit pouvoir gouverner localisation, conservation, transfert, durée de vie, archivage et suppression des données administratives conformément au cadre applicable.

18. Audit indépendant

L'auditeur habilité peut vérifier journaux, habilitations, preuves et décisions nécessaires à sa mission sans disposer automatiquement du pouvoir de modifier les dossiers ou de prendre une décision administrative.

19. AP Ledger

Empreintes minimales de délégations, habilitations, validations, décisions, changements critiques, révocations et clôtures d'audit peuvent être ancrées dans AP Ledger. Dossiers complets, données personnelles, secrets de sécurité et modèles sensibles restent hors des couches irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si les compétences restent attribuées ; si les délégations sont limitées et révocables ; si les fonctions sensibles sont séparées ; si l'interopérabilité respecte la minimisation ; si l'IA reste identifiable, explicable et contestable ; si la cybersécurité protège les fonctions critiques ; si les données restent souveraines ; et si l'audit demeure indépendant. Cette gouvernance fournit le socle nécessaire à la clôture fonctionnelle de l'application Public Administration.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 27 — PUBLIC ADMINISTRATION

CHAPITRE 6 — SYNTHÈSE FONCTIONNELLE, CRITÈRES D'ACCEPTATION ET CLÔTURE DE L'APPLICATION PUBLIC ADMINISTRATION

1. Objet du chapitre

Ce chapitre clôt le Point 27 — Public Administration. Il consolide administrations, agents, usagers, dossiers, démarches, documents officiels, services publics, collectivités, interopérabilité, intelligence artificielle, gouvernance, confidentialité, souveraineté et AP Ledger.

2. Mission consolidée

Le Passeport Numérique Administration constitue une mémoire vérifiable des démarches et actes publics. Authenticity Plus© / Deep Authenticity© authentifie identités, habilitations, documents, versions, décisions et chronologies sans exercer lui-même une compétence administrative.

3. Administration, agent, usager et dossier

Administration, agent habilité, usager et dossier restent des objets distincts. Toute action sensible conserve son acteur, son rôle, sa date, sa source et son niveau d'autorité.

4. Démarches et dépôts

Formulaire, dépôt, accusé de réception, instruction, demande de complément, validation, décision et notification restent des étapes distinctes. Un accusé de réception ne constitue pas une acceptation.

5. Documents officiels et QR dynamiques

Certificats, attestations, licences, permis et autres documents conservent émetteur, référence, portée, validité et statut. Un QR dynamique permet une vérification proportionnée sans créer un nouveau document officiel.

6. État civil et rectifications

Les actes d'état civil restent sous l'autorité des organismes compétents. Toute rectification conserve sa source, sa date et son historique sans effacement silencieux des versions antérieures.

7. Signatures et délégations

Les signatures restent attribuées au signataire et au mécanisme de validation disponible. Les délégations conservent délégant, délégataire, compétence, période et statut et sont limitées et révocables.

8. Paiements administratifs

Paiement demandé, initié, reçu, rapproché, rejeté ou remboursé restent des statuts distincts. Les données bancaires sensibles demeurent hors des couches publiques ou irréversibles.

9. Services publics et omnicanal

Guichet physique, portail numérique, courrier ou autre canal peuvent participer au même dossier. Le canal utilisé ne modifie pas silencieusement la nature de la preuve ou de la décision.

10. Inter-administrations

Les échanges entre administrations conservent source, finalité, version, date et destinataire. L’ interopérabilité ne crée pas un accès généralisé aux dossiers des citoyens.

11. Aides et prestations

Demande, critères publiés, instruction, simulation, décision et versement restent distingués. Une simulation ne constitue ni un droit acquis ni une décision administrative.

12. Marchés, inspections et réclamations

Consultation, soumission, évaluation, attribution, exécution et réception restent attribuables. Inspection et sanction ne sont pas confondues ; les réclamations conservent leurs versions, réponses et décisions.

13. Collectivités et action territoriale

Collectivités, municipalités, urbanisme, fiscalité locale, registres et services techniques conservent leurs compétences et sources. Un signalement citoyen reste distinct d’un constat administratif.

14. Transparence et participation citoyenne

Consultations, contributions, données ouvertes et publications conservent organisateur, source, version et date. Consultation, participation, décision institutionnelle et élection ne sont pas fusionnées.

15. Deep Authenticity©

Deep Authenticity© confronte identités, habilitations, délégations, pièces, signatures, documents, décisions, paiements attestés et chronologies afin de signaler incohérences, duplications ou substitutions nécessitant vérification.

16. Intelligence artificielle publique

L’IA peut assister classement, recherche, analyse documentaire ou détection d’anomalies lorsqu’elle est autorisée. Elle reste identifiable, gouvernée, explicable et contestable et ne reçoit pas implicitement une compétence administrative.

17. Gouvernance et contrôle

Recevoir, instruire, contrôler, valider, décider, payer, administrer les droits et auditer sont des fonctions distinctes lorsque nécessaire. Contrôle interne, audit indépendant et contrôle juridictionnel restent séparés.

18. Confidentialité, cybersécurité et souveraineté

État civil, santé, finances, fiscalité, dossiers sociaux, identifiants et autres données sensibles sont compartimentés. Les accès sont révocables et l'autorité compétente gouverne localisation, conservation, transfert, archivage et suppression.

19. AP Ledger et critères d'acceptation

AP Ledger reçoit uniquement des empreintes minimales de dépôts, documents, délégations, validations, décisions, paiements attestés, révocations et événements critiques. Le modèle est acceptable si les compétences restent attribuées, les rôles séparés, les données minimisées, l'IA contestable et les dossiers sensibles hors des couches irréversibles.

20. Clôture du Point 27 — Public Administration

Le Point 27 — Public Administration est désormais fonctionnellement défini : administrations, agents, usagers, dossiers, état civil, certificats, licences, permis, QR dynamiques, signatures, délégations, paiements, services publics, aides, marchés, inspections, collectivités, urbanisme, participation citoyenne, Deep Authenticity©, IA publique, gouvernance, interopérabilité, cybersécurité, confidentialité, souveraineté, audit et AP Ledger. Le Volume IV peut désormais poursuivre avec le Point 28 — Defense.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 28 — DEFENSE

CHAPITRE 1 — IDENTITÉ NUMÉRIQUE INSTITUTIONNELLE, PERSONNELS HABILITÉS, ÉQUIPEMENTS NON OPÉRATIONNELS, DOCUMENTS, FOURNITURES, MAINTENANCE, CONTRÔLE D'ACCÈS, PROVENANCE ET PASSEPORT NUMÉRIQUE DEFENSE

1. Objet du chapitre

Le Point 28 — Defense transpose Authenticity Plus© / Deep Authenticity© aux fonctions de gouvernance, conformité, administration et logistique non opérationnelle du secteur de la défense. Le Passeport Numérique Defense relie institutions, personnels habilités, équipements non opérationnels, documents, fournitures, maintenance et preuves autorisées.

2. Périmètre de sécurité

Le modèle exclut les plans d'opérations, tactiques, ciblage, capacités offensives détaillées, vulnérabilités, positions sensibles, secrets de défense et toute information dont l'exposition pourrait compromettre la sécurité des personnes ou des missions.

3. Identité institutionnelle

Une institution, direction, base administrative, établissement ou organisme autorisé peut disposer d' une identité vérifiable reliant dénomination, autorité de rattachement, rôle administratif et informations publiables.

4. Identité professionnelle

Un personnel habilité peut disposer d'une identité professionnelle reliant organisme, fonction, périmètre d'accès et période d'habilitation. Les données personnelles et informations sensibles restent compartimentées.

5. Habilitations

Une habilitation conserve autorité émettrice, catégorie ou niveau abstrait, périmètre, date d'effet, expiration et statut. Le passeport ne révèle pas publiquement les droits détaillés donnant accès à des informations classifiées.

6. Séparation des rôles

Demander, approuver, réceptionner, maintenir, contrôler, auditer et administrer les accès sont des fonctions distinctes lorsque nécessaire. Les actions critiques restent attribuables.

7. Équipements non opérationnels

Véhicules administratifs, équipements de bâtiment, matériels informatiques non classifiés, outillage ou autres actifs de soutien peuvent disposer d'un passeport reliant identité, affectation autorisée, maintenance et statut.

8. Documents administratifs

Ordres administratifs, certificats, rapports de conformité, inventaires ou autres documents non opérationnels peuvent conserver émetteur, date, version, classification ou niveau de diffusion applicable.

9. Classification et diffusion

Toute information conserve son niveau de sensibilité et ses règles de diffusion. Authenticity Plus© ne déclassifie pas une information et n'élargit jamais automatiquement son cercle d'accès.

10. Fournitures et chaîne de provenance

Les fournitures non sensibles peuvent être reliées à fournisseur, lot, réception, contrôle, stockage et affectation autorisée. Livraison, acceptation et mise en service restent des événements distincts.

11. Maintenance

Inspection, entretien, panne, réparation, remplacement et remise en service d'un actif de soutien peuvent être historisés. Maintenance planifiée, réalisée et validée restent distinctes.

12. Inventaire

Un inventaire peut relier actif, organisation responsable, statut et contrôles périodiques. Les emplacements précis d'actifs sensibles ne sont pas exposés dans les vues publiques ou non habilitées.

13. Contrôle d'accès

Les accès physiques et numériques reposent sur le moindre privilège, la durée nécessaire et la révocation. Un QR public ne donne jamais accès à une zone sensible, un système critique ou une information classifiée.

14. Prestataires et fournisseurs

Un fournisseur ou prestataire conserve identité, contrat ou mandat, périmètre et période. Son accès est limité aux données et espaces nécessaires à la prestation.

15. Inspections et conformité

Une inspection conserve organisme ou rôle habilité, périmètre, date, méthode et résultat. AP authentifie la provenance du rapport sans se substituer à l'autorité de contrôle.

16. Deep Authenticity©

Deep Authenticity© confronte identités, habilitations, documents, lots, maintenances, validations et chronologies afin de signaler duplications, substitutions ou incohérences nécessitant une vérification humaine autorisée.

17. Online et Offline

Les fonctions Offline éventuellement autorisées se limitent aux preuves nécessaires, chiffrées et contrôlées. Toute resynchronisation conserve date, auteur, origine et vérification sans exposer de données opérationnelles sensibles.

18. Confidentialité et compartimentation

Identités sensibles, habilitations détaillées, plans, localisations, vulnérabilités, configurations, journaux critiques et informations classifiées sont compartimentés selon le besoin d'en connaître.

19. AP Ledger

Seules des empreintes minimales d'événements administratifs ou logistiques autorisés peuvent être ancrées dans AP Ledger. Aucun secret de défense, plan opérationnel, localisation sensible, clé, code d' accès ou donnée classifiée n'est inscrit dans une couche publique ou irréversible.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si le périmètre reste non opérationnel ; si les habilitations sont limitées et révocables ; si classification et diffusion sont respectées ; si livraison, acceptation et mise en service restent distinctes ; si les localisations et accès sensibles sont protégés ; et si AP Ledger exclut toute information classifiée. Le Passeport Defense fournit ainsi un socle de confiance pour la gouvernance et la traçabilité administrative sans exposer les capacités opérationnelles.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 28 — DEFENSE

CHAPITRE 2 — ACHATS ET APPROVISIONNEMENTS NON OPÉRATIONNELS, FOURNISSEURS, CONTRATS, LOTS, RÉCEPTION, CONFORMITÉ, STOCKS, MAINTENANCE, AUDITS ET CHAÎNE DE PROVENANCE SÉCURISÉE

1. Objet du chapitre

Ce chapitre applique le Passeport Numérique Defense aux achats et approvisionnements non opérationnels : fournisseurs, contrats, commandes, lots, réception, contrôles, stocks de soutien, maintenance, audits et provenance. Il exclut les armes, munitions, systèmes offensifs et informations opérationnelles sensibles.

2. Périmètre des approvisionnements

Le modèle vise les fournitures administratives, équipements de soutien, composants non sensibles, services, maintenance d'infrastructures et autres acquisitions dont la traçabilité peut être organisée sans révéler de capacité militaire opérationnelle.

3. Identité du fournisseur

Un fournisseur peut disposer d'une identité vérifiable reliant organisation, statut, contrat ou qualification documentée et période de relation. Les informations commerciales sensibles restent compartimentées.

4. Qualification et habilitation fournisseur

Une qualification, autorisation ou habilitation conserve son émetteur, son périmètre, sa date et son statut. AP ne crée ni ne prolonge seul une habilitation officielle.

5. Contrats

Un contrat conserve parties, objet non sensible, période, versions, validations et statut. Les clauses classifiées, prix sensibles ou informations pouvant révéler une capacité opérationnelle restent hors des vues non habilitées.

6. Commandes

Une commande peut être reliée au contrat, au demandeur autorisé, à l'approbation, au fournisseur, aux références non sensibles et au statut. Demande, approbation et émission restent des événements distincts.

7. Lots et provenance

Un lot de fournitures peut disposer d'une référence reliant fabricant ou fournisseur, documents autorisés, dates, contrôles et destination administrative abstraite. La traçabilité évite d'exposer les lieux ou volumes sensibles.

8. Transport et livraison

Expédition, arrivée et remise peuvent être attestées au niveau nécessaire. Les itinéraires, horaires détaillés et localisations sensibles ne sont pas publiés ni ancrés dans des couches irréversibles.

9. Réception

La réception conserve organisme ou rôle habilité, date, référence et état administratif. Réception physique, contrôle, acceptation et mise en service restent distincts.

10. Contrôle de conformité

Un contrôle peut relier référentiel autorisé, méthode, résultat et contrôleur. AP authentifie la provenance du rapport sans se substituer à l'autorité ou au professionnel chargé de la conformité.

11. Non-conformités

Une non-conformité présumée peut ouvrir un dossier reliant observation, lot, fournisseur, action corrective, recontrôle et clôture. Un signal automatisé ne constitue pas à lui seul une sanction ou une accusation de fraude.

12. Stocks de soutien

Les stocks non sensibles peuvent être suivis par identité d'article, lot, statut et mouvements autorisés. Les quantités, seuils, emplacements ou consommations susceptibles de révéler une capacité opérationnelle restent protégés.

13. Affectation et consommation

Affectation, transfert administratif, consommation et retrait d'un actif de soutien peuvent être historisés à un niveau compatible avec la sécurité. Les destinations sensibles sont abstraites ou compartimentées.

14. Maintenance

Inspection, entretien, panne, réparation, remplacement et remise en service des équipements de soutien peuvent être reliés à leurs preuves. Les détails techniques susceptibles d'exposer une vulnérabilité sont exclus des vues non habilitées.

15. Rappels et retraits

Un rappel fournisseur, retrait de lot ou mise en quarantaine administrative peut conserver source, périmètre, date et statut. La diffusion est limitée aux acteurs ayant besoin d'en connaître.

16. Deep Authenticity©

Deep Authenticity© confronte fournisseurs, contrats, commandes, lots, documents, contrôles, maintenances et chronologies afin de signaler duplications, substitutions ou incohérences nécessitant une vérification humaine autorisée.

17. Audits

Un audit peut vérifier habilitations, contrats, réception, contrôles, stocks de soutien et journaux nécessaires. L'auditeur ne reçoit pas automatiquement accès aux informations opérationnelles ou classifiées sans habilitation correspondante.

18. Cybersécurité et cloisonnement

Portails fournisseurs, API, comptes privilégiés, signatures et systèmes d'approvisionnement sont segmentés et journalisés. Les accès sont limités, temporaires lorsque possible et révocables.

19. AP Ledger

Seules des empreintes minimales de contrats, commandes, réceptions, contrôles, rappels, maintenances ou validations non sensibles peuvent être ancrées dans AP Ledger. Aucun itinéraire sensible, volume opérationnel, emplacement précis, secret technique ou information classifiée n'y est inscrit.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si le périmètre demeure non opérationnel ; si demande, approbation, réception, contrôle et acceptation restent séparés ; si la provenance des lots est vérifiable sans révéler les capacités ; si les stocks sensibles sont compartimentés ; si les audits respectent le besoin d'en connaître ; et si AP Ledger exclut toute donnée classifiée. Le Passeport Defense fournit ainsi une chaîne de provenance sécurisée pour les approvisionnements de soutien.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 28 — DEFENSE

CHAPITRE 3 — INFRASTRUCTURES ET INSTALLATIONS ADMINISTRATIVES, BÂTIMENTS, ÉQUIPEMENTS DE SOUTIEN, INSPECTIONS, MAINTENANCE, ÉNERGIE, SÛRETÉ NON OPÉRATIONNELLE, CONTINUITÉ ET GESTION DOCUMENTAIRE SÉCURISÉE

1. Objet du chapitre

Ce chapitre applique le Passeport Numérique Defense aux infrastructures et installations administratives ou de soutien : bâtiments, équipements techniques non opérationnels, inspections, maintenance, énergie, continuité et gestion documentaire sécurisée.

2. Périmètre de sécurité

Le modèle exclut les implantations sensibles détaillées, plans de défense, dispositifs tactiques, vulnérabilités, capacités opérationnelles, schémas de protection exploitables et toute information classifiée dont la divulgation pourrait compromettre la sécurité.

3. Identité de l’infrastructure

Une infrastructure autorisée peut disposer d’une identité reliant organisme responsable, catégorie abstraite, documents administratifs, équipements de soutien et historique technique. Les coordonnées ou plans sensibles restent compartimentés.

4. Bâtiments administratifs et de soutien

Bureaux, centres de formation non sensibles, ateliers administratifs, entrepôts non sensibles ou autres bâtiments de soutien peuvent disposer d’un passeport limité aux informations nécessaires à leur gestion.

5. Documents techniques

Plans autorisés, notices, certificats, rapports et dossiers techniques peuvent conserver auteur, source, date, version et niveau de diffusion. Les plans révélant une configuration de sécurité sensible restent exclus des vues ordinaires.

6. Équipements de soutien

Ascenseurs, groupes techniques, climatisation, alimentation électrique, équipements de sécurité civile, informatique non classifiée et autres actifs de soutien peuvent être historisés selon leur cycle de vie.

7. Installation et mise en service

Livraison, installation, contrôle, validation et mise en service restent des événements distincts. Chaque étape conserve l'intervenant habilité et les preuves autorisées.

8. Inspections

Une inspection conserve organisme ou rôle habilité, périmètre, date, méthode et résultat. Authenticity Plus©authentifie la provenance du rapport sans se substituer à l'autorité ou au professionnel compétent.

9. Maintenance préventive

Inspection périodique, entretien programmé, remplacement planifié ou contrôle réglementaire peut conserver actif, date, intervenant, résultat et prochaine échéance lorsque cela est autorisé.

10. Maintenance corrective

Signalement, diagnostic, intervention, remplacement et remise en service restent des étapes distinctes. Les détails techniques susceptibles d'exposer une vulnérabilité restent compartimentés.

11. Gestion des incidents techniques

Un incident non opérationnel peut être relié à son signalement, catégorie abstraite, impact administratif, interventions et clôture. Les informations sensibles de sûreté ou de configuration ne sont pas publiées.

12. Énergie et utilités

Consommations d'énergie, eau ou autres utilités peuvent être suivies à un niveau agrégé compatible avec la sécurité. Les profils détaillés susceptibles de révéler l'activité ou la capacité d'une installation restent protégés.

13. Performance et durabilité

Indicateurs de maintenance, disponibilité administrative, consommation agrégée ou performance environnementale peuvent être suivis sans exposer les rythmes, capacités ou contraintes opérationnelles.

14. Sûreté non opérationnelle

Les contrôles liés à la sécurité générale des bâtiments peuvent être documentés à un niveau abstrait. Les dispositifs, emplacements, procédures et configurations exploitables par un tiers ne sont pas exposés.

15. Prestataires

Entreprise de maintenance, inspection, nettoyage ou service technique conserve identité, mandat, périmètre, période et habilitations nécessaires. Son accès est limité aux zones et données strictement utiles.

16. Continuité de service

Les plans de continuité administrative peuvent conserver versions, responsables, exercices et validations à un niveau non sensible. Les scénarios détaillés révélant des vulnérabilités ou réponses opérationnelles restent compartimentés.

17. Deep Authenticity©

Deep Authenticity© confronte documents, versions, équipements, inspections, maintenances, prestataires, validations et chronologies afin de signaler incohérences ou substitutions nécessitant une vérification humaine autorisée.

18. Gestion documentaire sécurisée

Les documents sont classés selon sensibilité, besoin d'en connaître, durée de conservation et droits d'accès. Consultation, copie, export ou partage d'un document sensible sont soumis aux règles de sécurité applicables.

19. AP Ledger

Seules des empreintes minimales de documents autorisés, inspections, maintenances, validations ou changements de statut non sensibles peuvent être ancrées dans AP Ledger. Aucun plan sensible, code d'accès, vulnérabilité, profil énergétique révélateur ou donnée classifiée n'y est inscrit.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si le périmètre demeure administratif et non opérationnel ; si les infrastructures sensibles ne sont pas localisées ou décrites de manière exploitable ; si installation, contrôle et mise en service restent séparés ; si les maintenances conservent leur provenance ; si les profils énergétiques sensibles sont protégés ; si les prestataires respectent le moindre privilège ; et si AP Ledger exclut toute donnée classifiée. Le Passeport Defense fournit ainsi une mémoire technique vérifiable des infrastructures de soutien sans exposer leur sécurité opérationnelle.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 28 — DEFENSE

CHAPITRE 4 — PERSONNELS, QUALIFICATIONS, FORMATIONS, HABILITATIONS, AFFECTATIONS ADMINISTRATIVES, SANTÉ ET SÉCURITÉ AU TRAVAIL, PRESTATAIRES, RÉVOCATIONS ET GOUVERNANCE DES ACCÈS

1. Objet du chapitre

Ce chapitre applique le Passeport Numérique Defense à la gouvernance administrative des personnels : identité professionnelle, qualifications, formations, habilitations, affectations administratives, santé et sécurité au travail, prestataires, révocations et droits d'accès. Il exclut les affectations opérationnelles, missions, capacités, plans et informations classifiées.

2. Identité professionnelle

Chaque personnel autorisé peut disposer d'une identité professionnelle reliant organisme, statut, fonction administrative, qualifications et habilitations nécessaires. L'identité civile complète et les données personnelles restent compartimentées.

3. Qualifications

Diplômes, certifications, qualifications professionnelles ou autorisations peuvent conserver émetteur, domaine, date, période de validité et statut. AP authentifie la preuve disponible sans créer lui-même une qualification.

4. Formations

Une formation peut être reliée à son organisme, programme non sensible, participant autorisé, date, résultat ou attestation. Participation, réussite, certification et habilitation restent des états distincts.

5. Maintien des compétences

Renouvellement, recyclage, contrôle périodique ou expiration d'une compétence peuvent être historisés. Une qualification expirée ne doit pas être présentée comme actuellement valide.

6. Habilitations

Une habilitation conserve autorité émettrice, niveau abstrait, périmètre, période et statut. Les détails permettant de déduire l'accès à des capacités, sites ou informations classifiées ne sont pas exposés.

7. Besoin d'en connaître

Une habilitation générale ne donne pas automatiquement accès à toutes les informations de même sensibilité. Les droits sont également limités par la mission administrative autorisée et le besoin d'en connaître.

8. Affectations administratives

Une affectation administrative peut relier organisme, unité organisationnelle abstraite, rôle, période et statut. Les affectations opérationnelles, déploiements, positions ou mouvements sensibles sont exclus.

9. Mobilité interne

Mutation administrative, changement de fonction ou fin d'affectation entraîne une révision des droits. Les anciennes habilitations opérationnelles ou applicatives ne restent pas actives sans justification.

10. Santé et sécurité au travail

Formations de prévention, aptitudes administratives nécessaires, incidents professionnels non sensibles et mesures de sécurité au travail peuvent être documentés selon les règles applicables. Les données médicales détaillées restent strictement protégées.

11. Données de santé

Le système privilégie des statuts minimaux tels que validation, restriction administrative ou échéance lorsque cela est autorisé, sans exposer diagnostic, dossier médical ou information clinique aux acteurs non compétents.

12. Prestataires et personnels externes

Consultants, techniciens et personnels de fournisseurs conservent identité professionnelle, organisation, mandat, durée et droits nécessaires. Leur accès expire avec la mission sauf renouvellement explicite.

13. Accueil et départ

Création de compte, attribution de droits, remise de moyens administratifs, modification, suspension, restitution et clôture peuvent être historisées. Le départ déclenche la révocation des accès concernés.

14. Révocation

Expiration, suspension ou retrait d'une habilitation ou d'un mandat entraîne la révocation des droits associés. La révocation est propagée aux systèmes autorisés sans effacer l'historique des actions antérieures.

15. Séparation des rôles

Demander un accès, l'approuver, l'administrer, l'utiliser, le contrôler et l'auditer sont des fonctions distinctes lorsque le niveau de risque l'exige.

16. Deep Authenticity©

Deep Authenticity© confronte identité professionnelle, qualifications, formations, habilitations, mandats, accès et chronologies afin de signaler incohérences, expirations ou substitutions nécessitant une vérification humaine autorisée.

17. Journalisation

Les créations, modifications, utilisations sensibles, suspensions et révocations de droits peuvent être journalisées selon le niveau nécessaire. Les journaux eux-mêmes sont protégés contre les accès non autorisés.

18. Confidentialité et compartimentation

Données personnelles, santé, habilitations détaillées, affectations sensibles et journaux critiques sont compartimentés. Les vues de gestion affichent uniquement les informations nécessaires à la fonction exercée.

19. AP Ledger

Seules des empreintes minimales de qualifications, validations, habilitations abstraites, changements de droits, suspensions ou révocations non sensibles peuvent être ancrées dans AP Ledger. Aucune donnée médicale, affectation opérationnelle, localisation, secret d'accès ou information classifiée n'y est inscrit.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si qualifications, formations et habilitations restent distinctes ; si le besoin d'en connaître complète le niveau d'habilitation ; si les changements d'affectation entraînent la révision des droits ; si les données de santé sont minimisées ; si les prestataires disposent d'accès temporaires ; si les révocations sont propagées ; et si aucune affectation opérationnelle ou donnée classifiée n'est exposée. Le Passeport Defense fournit ainsi une gouvernance vérifiable des identités et accès administratifs.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 28 — DEFENSE

CHAPITRE 5 — GOUVERNANCE INSTITUTIONNELLE, CONTRÔLE INTERNE, CONFORMITÉ, INTEROPÉRABILITÉ SÉCURISÉE, INTELLIGENCE ARTIFICIELLE, DEEP AUTHENTICITY©, SOUVERAINETÉ, CYBERSÉCURITÉ ET AUDIT INDÉPENDANT

1. Objet du chapitre

Ce chapitre définit la gouvernance du Passeport Numérique Defense dans son périmètre administratif et non opérationnel : autorités, séparation des responsabilités, contrôle interne, conformité, interopérabilité sécurisée, intelligence artificielle, souveraineté, cybersécurité et audit.

2. Périmètre institutionnel

Authenticity Plus© organise identité, provenance, version, habilitation et chronologie des preuves autorisées. Il n’exerce aucune fonction de commandement et n’héberge pas, dans ses couches publiques ou irréversibles, de plans opérationnels, capacités sensibles, vulnérabilités ou secrets de défense.

3. Autorités et responsabilités

Chaque organisme conserve son autorité, sa compétence, ses responsabilités et ses processus devalidation. Une plateforme technique ne devient jamais l’autorité décisionnaire du seul fait qu’elle transporte ou authentifie une preuve.

4. Séparation des fonctions

Demander, approuver, exécuter, réceptionner, contrôler, administrer les accès et auditer sont séparés lorsque le risque l’exige. Les cumuls exceptionnels doivent rester identifiables et contrôlables.

5. Contrôle interne

Le contrôle interne peut vérifier habilitations, séparation des fonctions, provenance documentaire, conformité des processus et cohérence des journaux. Il reste distinct de l’audit indépendant et de toute autorité externe de contrôle.

6. Conformité

Les exigences applicables peuvent être associées à des contrôles, preuves, responsables, échéances et statuts. Une preuve de conformité reste attribuée à l’organisme ou au professionnel habilité qui l’ émet.

7. Gestion des exceptions

Dérogation, exception, non-conformité ou mesure corrective conserve demandeur, autorité de validation, portée, période, justification documentée et clôture. Une exception temporaire ne modifie pas silencieusement la règle générale.

8. Interopérabilité sécurisée

Les échanges entre systèmes autorisés conservent source, destination, finalité, version, horodatage et niveau de sensibilité. L'interopérabilité ne crée pas un droit d'accès transversal à toutes les données.

9. Compartimentation

Les informations sont segmentées selon rôle, besoin d'en connaître, sensibilité et finalité. Les identités, journaux, documents et métadonnées pouvant révéler une information sensible sont protégés au même titre que le contenu.

10. Intelligence artificielle

L'IA peut assister classification documentaire non sensible, recherche, détection d'incohérences ou priorisation administrative lorsqu'elle est autorisée. Elle ne reçoit ni pouvoir de commandement ni autonomie décisionnelle sur une fonction opérationnelle.

11. Explicabilité et contrôle humain

Tout résultat algorithmique utilisé dans une fonction administrative sensible reste identifiable comme tel et soumis au contrôle humain autorisé. Un score ou signal ne constitue pas à lui seul une sanction, une fraude établie ou une décision institutionnelle.

12. Deep Authenticity©

Deep Authenticity© confronte identités, habilitations, fournisseurs, documents, validations, maintenances, inspections et chronologies autorisées afin de signaler incohérences, expirations, substitutions ou duplications nécessitant vérification.

13. Gestion des modèles et versions

Les modèles automatisés autorisés conservent version, périmètre d'usage, validation, changements et retrait. Une nouvelle version ne doit pas effacer la possibilité d'identifier le modèle ayant contribué à une analyse antérieure.

14. Cybersécurité

Comptes privilégiés, API, certificats, signatures, systèmes d'administration et intégrations sont protégés par authentification, segmentation, journalisation et révocation. Les secrets d'accès ne sont jamais placés dans un QR public ou AP Ledger.

15. Réponse aux incidents numériques

Un incident de sécurité administratif peut conserver détection, qualification, actions autorisées, restauration et clôture à un niveau non sensible. Les détails exploitables concernant des vulnérabilités ou défenses restent compartimentés.

16. Souveraineté des données

L'autorité compétente gouverne localisation, conservation, accès, transfert, archivage et suppression des données. Les informations classifiées ou sensibles restent soumises aux infrastructures et règles de souveraineté applicables.

17. Continuité et résilience

Les mécanismes de continuité administrative conservent responsables, versions, exercices et validations sans publier les scénarios détaillés, architectures sensibles ou procédures exploitables.

18. Audit indépendant

L'auditeur habilité peut examiner les preuves nécessaires à sa mission selon son niveau d'accès. L' audit n'accorde pas automatiquement un accès illimité aux informations classifiées, aux localisations sensibles ou aux systèmes opérationnels.

19. AP Ledger

Seules des empreintes minimales d'habilitations abstraites, validations, contrôles, exceptions, audits, révocations et changements administratifs non sensibles peuvent être ancrées dans AP Ledger. Aucun secret, vulnérabilité, plan, localisation sensible ou donnée classifiée n'y est inscrit.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si la gouvernance reste non opérationnelle ; si autorités et plateforme technique restent distinctes ; si les fonctions sensibles sont séparées ; si l'interopérabilité respecte compartimentation et besoin d'en connaître ; si l'IA reste assistive et contrôlée ; si la souveraineté est préservée ; si l'audit est indépendant et limité par habilitation ; et si AP Ledger exclut toute information classifiée. Cette gouvernance fournit le socle nécessaire à la clôture fonctionnelle du Point 28 — Defense.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 28 — DEFENSE

CHAPITRE 6 — SYNTHÈSE FONCTIONNELLE, CRITÈRES D'ACCEPTATION ET CLÔTURE DE L'APPLICATION DEFENSE

1. Objet du chapitre

Ce chapitre clôt le Point 28 — Defense. Il consolide identité institutionnelle, personnels habilités, approvisionnements non opérationnels, infrastructures de soutien, maintenance, gouvernance des accès, conformité, intelligence artificielle, cybersécurité, souveraineté, audit et AP Ledger.

2. Périmètre consolidé

Le Passeport Numérique Defense demeure strictement administratif, institutionnel et logistique non opérationnel. Sont exclus les plans d'opérations, tactiques, ciblage, capacités offensives détaillées, vulnérabilités exploitables, positions sensibles, secrets de défense et autres informations classifiées non destinées au dispositif.

3. Identités institutionnelles et professionnelles

Institutions, organismes, personnels et prestataires conservent des identités distinctes, attribuables et gouvernées. Les informations personnelles ou sensibles sont limitées au besoin d'en connaître.

4. Habilitations et besoin d'en connaître

Une habilitation conserve autorité, niveau abstrait, périmètre, période et statut. Elle ne donne jamais automatiquement accès à toutes les informations de même sensibilité : le rôle et le besoin d'en connaître restent déterminants.

5. Qualifications et formations

Diplôme, certification, formation, réussite, qualification et habilitation restent des notions distinctes. Les expirations, renouvellements et contrôles périodiques sont historisés.

6. Affectations administratives

Les affectations administratives peuvent être versionnées avec organisme, rôle et période. Les déploiements, mouvements, positions et affectations opérationnelles sensibles sont exclus.

7. Fournisseurs et contrats

Fournisseurs et prestataires conservent identité, qualification, contrat, mandat et période. Les clauses, prix ou informations susceptibles de révéler une capacité sensible restent compartimentés.

8. Approvisionnements non opérationnels

Demande, approbation, commande, livraison, réception, contrôle, acceptation et mise en service restent des événements distincts. La provenance est vérifiable sans publier itinéraires, volumes ou destinations sensibles.

9. Stocks et actifs de soutien

Les actifs non sensibles peuvent être historisés par référence, lot, statut, maintenance et affectation administrative abstraite. Les emplacements précis et niveaux de stock révélateurs de capacité sont protégés.

10. Infrastructures de soutien

Les bâtiments et équipements administratifs ou de soutien peuvent disposer d'une mémoire technique limitée aux données autorisées. Plans sensibles, configurations de protection et localisations exploitables restent compartimentés.

11. Maintenance et inspections

Maintenance planifiée, intervention réalisée, contrôle, validation et remise en service restent distincts. Les inspections conservent organisme, périmètre, date, méthode et résultat autorisés.

12. Continuité et énergie

La continuité administrative et les données énergétiques peuvent être suivies à un niveau agrégé. Les scénarios détaillés, profils révélateurs d'activité et informations exploitables sur la résilience restent protégés.

13. Gouvernance des accès

Création, modification, utilisation sensible, suspension et révocation des droits sont attribuables. Changement d'affectation, fin de mission ou expiration entraîne la révision des accès concernés.

14. Deep Authenticity©

Deep Authenticity© confronte identités, habilitations, qualifications, fournisseurs, documents, lots, inspections, maintenances, validations et chronologies autorisées afin de signaler incohérences, expirations, duplications ou substitutions nécessitant vérification humaine.

15. Intelligence artificielle

L'IA peut assister certaines fonctions administratives non opérationnelles telles que classement, recherche ou détection d'incohérences. Elle ne reçoit ni pouvoir de commandement ni autonomie décisionnelle opérationnelle.

16. Contrôle humain et conformité

Un score ou signal algorithmique ne constitue pas à lui seul une sanction, une fraude établie ou une décision institutionnelle. Les contrôles et décisions sensibles restent attribués aux personnes ou autorités habilitées.

17. Cybersécurité et compartimentation

Comptes privilégiés, API, certificats, signatures, journaux et systèmes administratifs sont segmentés, protégés et révocables. Les métadonnées susceptibles de révéler une information sensible sont protégées au même titre que le contenu.

18. Souveraineté et audit

L'autorité compétente gouverne localisation, conservation, transfert, archivage et suppression des données. L'audit indépendant respecte les habilitations et ne crée pas un accès illimité aux systèmes ou informations classifiées.

19. AP Ledger et critères d'acceptation

AP Ledger reçoit uniquement des empreintes minimales d'événements administratifs non sensibles : habilitations abstraites, validations, contrôles, maintenances, révocations ou audits. Le modèle est acceptable si le périmètre reste non opérationnel, si le besoin d'en connaître est respecté et si aucune donnée classifiée ou exploitable n'est inscrite dans une couche irréversible.

20. Clôture du Point 28 — Defense

Le Point 28 — Defense est désormais fonctionnellement défini : identité institutionnelle, personnels, qualifications, formations, habilitations, approvisionnements non opérationnels, fournisseurs, contrats, infrastructures de soutien, inspections, maintenance, gouvernance des accès, Deep Authenticity©,IA assistive, conformité, cybersécurité, souveraineté, audit et AP Ledger. Le Volume IV peut désormais poursuivre avec le Point 29 — Media.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 29 — MEDIA

CHAPITRE 1 — IDENTITÉ DES MÉDIAS ET CRÉATEURS, PROVENANCE DES CONTENUS, AUTEURS, SOURCES, PHOTOS, VIDÉOS, AUDIO, DOCUMENTS, SIGNATURES, QR CODES DYNAMIQUES ET LUTTE CONTRE LES FALSIFICATIONS

1. Objet du chapitre

Le Point 29 — Media transpose Authenticity Plus© / Deep Authenticity© à la chaîne de confiance des contenus médiatiques. Le Passeport Numérique Media relie organisations, créateurs, auteurs, sources, contenus, versions, transformations, publications et preuves de provenance.

2. Mission sectorielle

La mission est de permettre de vérifier qui a produit, publié ou transformé un contenu, à quel moment et à partir de quelles sources documentées, sans transformer Authenticity Plus© en arbitre automatique de la vérité éditoriale.

3. Identité du média

Une organisation de presse, chaîne, studio, agence, éditeur ou autre entité médiatique peut disposer d’ une identité vérifiable reliant nom, marque, canaux officiels, rôles et signatures numériques autorisées.

4. Identité du créateur

Journaliste, photographe, vidéaste, réalisateur, auteur, monteur ou autre créateur peut disposer d’une identité professionnelle ou pseudonyme vérifiable selon le contexte. Les données personnelles non nécessaires restent protégées.

5. Identité du contenu

Article, photographie, vidéo, audio, podcast, reportage, document ou autre contenu peut disposer d’un identifiant reliant origine, auteur ou organisation, date, version, empreinte et historique de publication.

6. Sources

Une source peut être publique, institutionnelle, documentaire, humaine ou autre. Son identité peut être révélée, pseudonymisée ou protégée selon les règles éditoriales, juridiques et de sécurité applicables.

7. Protection des sources

Le système ne doit jamais forcer la divulgation publique d'une source confidentielle. Les preuves de provenance peuvent être conservées sous forme compartimentée ou minimale selon les droits d'accès.

8. Photographies

Une photographie peut conserver appareil ou application autorisée, date, auteur, empreinte, transformations déclarées et contexte disponible. L'absence de métadonnées ne prouve pas automatiquement qu'une image est fausse.

9. Vidéos

Une vidéo peut conserver origine, séquences, versions, montage, sous-titres, transformations et publication. Extrait, montage et version intégrale restent identifiables comme des objets distincts.

10. Audio

Un contenu audio peut conserver enregistrement, auteur, montage, version, transcription et transformations déclarées. Une transcription reste distincte de l'enregistrement original.

11. Documents et pièces

Un document utilisé comme source peut conserver émetteur déclaré, référence, date, version et statut de vérification. Une copie transmise à une rédaction reste distincte du document obtenu directement auprès de son émetteur.

12. Signatures et attestations

Une signature numérique ou attestation de provenance peut relier contenu, auteur ou organisation, date et version. Elle authentifie une relation documentée sans garantir à elle seule la véracité de toutes les affirmations du contenu.

13. QR Codes dynamiques

Un QR dynamique peut permettre au public de vérifier l'émetteur, la version, la date, les corrections et certains éléments de provenance. Une copie du QR ne permet pas de signer une nouvelle publication.

14. Transformations éditoriales

Recadrage, montage, correction technique, traduction, doublage, compression ou autre transformation peut être historisé lorsqu'elle est pertinente. Transformation technique et modification du sens restent distinguées.

15. Corrections et mises à jour

Une correction, mise à jour ou rétractation conserve date, auteur ou organisation, version antérieure et nouvelle version. La publication corrigée ne doit pas effacer silencieusement l'existence de l'état précédent.

16. Contenus synthétiques et IA

Un contenu généré ou substantiellement modifié par IA peut être étiqueté selon les règles applicables et conserver les informations de provenance disponibles. L'usage d'IA ne signifie pas automatiquement que le contenu est faux.

17. Deep Authenticity©

Deep Authenticity© confronte identités, empreintes, métadonnées, signatures, versions, transformations et chronologies afin de signaler incohérences, substitutions ou manipulations nécessitant une vérification éditoriale ou humaine.

18. Falsification et manipulation présumées

Une incohérence technique, un média modifié ou une provenance incomplète peut déclencher une vérification renforcée. Un signal algorithmique ne constitue pas à lui seul une preuve de falsification, de désinformation ou d'intention trompeuse.

19. AP Ledger

Des empreintes minimales de contenus, signatures, publications, corrections, rétractations ou changements critiques peuvent être ancrées dans AP Ledger. Sources confidentielles, rushes sensibles, données personnelles et secrets éditoriaux restent hors des couches publiques ou irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si auteur, média, source et contenu restent distincts ; si les sources confidentielles sont protégées ; si original, extrait et montage restent identifiables ; si correction et version antérieure sont historisées ; si l'IA est signalée lorsque nécessaire sans présomption automatique de fausseté ; et si Deep Authenticity© produit des signaux vérifiables plutôt que des verdicts éditoriaux. Le Passeport Media fournit ainsi le socle d'une provenance médiatique vérifiable.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 29 — MEDIA

CHAPITRE 2 — AP INFORMATIONS / AP PRESSE : PRODUCTION, CERTIFICATION, PUBLICATION, DIFFUSION, DROITS, CORRECTIONS ET ARCHIVAGE

1. Positionnement d'AP Informations

AP Informations constitue la couche transversale de certification, traçabilité, sécurisation et validation des informations et contenus publics, institutionnels, numériques ou médiatiques. Dans le Point 29 — Media, AP Presse et AP Media en constituent les sous-modules directement liés à la production et à la diffusion médiatique.

2. Architecture fonctionnelle

L'architecture retenue reprend AP Presse pour la communication officielle et médiatique, AP Media pour les contenus numériques et multimédias, AP Alertes pour les messages urgents, AP Rapports pour les documents institutionnels, AP Données Stratégiques pour les informations autorisées correspondantes et AP Vérification pour le contrôle d'authenticité.

3. AP Presse

AP Presse organise les communiqués officiels, dossiers de presse, articles validés et horodatés, interviews ou déclarations authentifiées, preuves d'antériorité et mécanismes de vérification destinés aux journalistes et au public.

4. AP Media

AP Media couvre articles et publications numériques, vidéos, enregistrements audio, podcasts, contenus web, publications sociales, contenus de créateurs et preuves d'origine de contenus numériques.

5. Identité du projet éditorial

Chaque projet peut relier média responsable, contributeurs autorisés, sources documentées, versions, validations, droits et publications. Projet interne, brouillon, contenu validé et publication publique restent des états distincts.

6. Certification numérique

La certification associe au contenu une identité de publication, une empreinte, une signature ou attestation disponible, une date et une version. Elle établit ce qui a été certifié et par qui, sans transformer automatiquement toute affirmation éditoriale en vérité établie.

7. Horodatage et antériorité

L’horodatage contribue à établir qu’une version ou empreinte existait à un moment donné. La preuve technique d’antériorité reste distincte de l’attribution automatique d’un droit juridique exclusif.

8. QR Code vérifiable

Un QR Code unique ou dynamique peut conduire à une vue de vérification publique affichant l’ émetteur, la version, la date, le statut et les corrections publiables. La copie du QR ne permet pas de créer une nouvelle signature authentique.

9. Signatures multimédias

Texte, photographie, vidéo, audio ou document peut être associé à une signature numérique ou une attestation de provenance. Toute transformation ultérieure pertinente doit pouvoir être distinguée de la version signée.

10. Rédaction et validation

Commande, rédaction, vérification factuelle, relecture, validation juridique éventuelle, validation éditoriale et publication restent séparées. Authenticity Plus© conserve leur provenance sans se substituer à la responsabilité éditoriale.

11. Sources et confidentialité

Les sources peuvent être publiques, documentaires, institutionnelles, humaines ou confidentielles. Une source protégée ne doit pas être révélée par le mécanisme de certification ; seules les preuves minimales autorisées sont exposées.

12. Droits d’auteur et licences

Auteur, titulaire, licence, territoire, durée et usages autorisés peuvent être reliés au contenu lorsque les documents le permettent. AP conserve la provenance documentaire mais ne tranche pas automatiquement un litige de titularité ou de licence.

13. Agences et syndication

Les contenus d’agence ou syndiqués conservent leur source initiale, référence, licence, date et transformations locales. Une republication ne devient pas une création originale du seul fait de son changement de canal.

14. Diffusion multicanale

Site, application, télévision, radio, podcast, newsletter et plateforme sociale peuvent diffuser des variantes reliées au contenu source. Chaque canal conserve sa version et sa date de publication.

15. Détection et traçabilité des modifications

Les différences entre versions, transformations déclarées, corrections ou substitutions peuvent être historisées. Une modification détectée constitue un signal à examiner ; elle ne prouve pas automatiquement une falsification intentionnelle.

16. Corrections, rétractations et retraits

Toute correction significative conserve la version antérieure, la nouvelle version, la date et le responsable. Rétractation ou retrait ne détruit pas la preuve interne de l'existence et de la chronologie du contenu.

17. Archivage sécurisé

Les versions publiées, signatures, empreintes, corrections, rétractations et statuts peuvent être archivés selon les politiques applicables. Une archive authentifiée reste distincte d'un contenu actuellement actif.

18. Deep Authenticity© et AP Vérification

Deep Authenticity© peut confronter empreintes, signatures, métadonnées, versions, sources autorisées et chronologies pour signaler incohérences, deepfakes présumés, substitutions ou ruptures de provenance. AP Vérification fournit le cadre de contrôle ; le résultat technique ne constitue pas à lui seul un verdict éditorial ou juridique.

19. AP Ledger et portée probatoire

AP Ledger peut ancrer des empreintes minimales de publications, signatures, validations, corrections ou rétractations. La formulation probatoire doit rester précise : AP peut renforcer la preuve d'existence, de date, d'intégrité et de provenance selon le dispositif utilisé et le droit applicable ; il ne doit pas promettre abstraitement une opposabilité universelle.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si AP Informations reste la couche transversale ; si AP Presse et AP Media conservent leurs fonctions propres ; si certification, vérité éditoriale et décision juridique restent distinguées ; si les sources confidentielles sont protégées ; si les versions et modifications restent reconstructibles ; si droits et licences conservent leur provenance ; et si la vérification publique permet de contrôler l'authenticité sans exposer les informations protégées.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 29 — MEDIA

CHAPITRE 3 — RÉSEAUX SOCIAUX, PLATEFORMES, COMPTES OFFICIELS, VIRALITÉ, MODÉRATION, CONTENUS SYNTHÉTIQUES, DEEPFAKES, CONTEXTE, SIGNALEMENTS ET CHAÎNE DE PROVENANCE PUBLIQUE

1. Objet du chapitre

Ce chapitre étend AP Informations, AP Media et AP Vérification aux contenus diffusés sur les réseaux sociaux et plateformes numériques : comptes officiels, republications, contenus viraux, modération, contenus synthétiques, deepfakes présumés, contexte, signalements et provenance publique.

2. Identité des comptes officiels

Un média, une institution, un journaliste ou un créateur peut relier ses comptes officiels à une identité vérifiable. La vérification AP reste distincte du badge ou du mécanisme de vérification propre à une plateforme.

3. Identité d’une publication

Une publication peut conserver auteur ou compte, plateforme, date, empreinte, contenu source, version et relation avec une publication certifiée antérieure. Une capture d’écran reste distincte de la publication originale.

4. Republication et partage

Partage, repost, citation, intégration ou republication conservent, lorsque disponible, le lien avec la source initiale. La viralité ne transforme pas une copie en source primaire.

5. Chaîne de provenance publique

AP Vérification peut présenter au public une chaîne simplifiée : source déclarée ou certifiée, première version connue, transformations documentées, publication et corrections. Les éléments confidentiels restent masqués.

6. Vidéos virales

Une vidéo virale peut être comparée à des empreintes ou versions de référence afin d’identifier recadrage, montage, extraction ou réutilisation. Une forte diffusion ne constitue ni une preuve d’ authenticité ni une preuve de falsification.

7. Images et extraits hors contexte

Une image ou un extrait authentique peut être présenté dans un contexte trompeur. Le Passeport Media distingue donc l'intégrité du fichier, sa provenance et le contexte éditorial qui accompagne sa republication.

8. Contenus synthétiques

Les contenus générés ou substantiellement modifiés par IA peuvent conserver les informations de provenance disponibles et un étiquetage approprié. Le caractère synthétique ne signifie pas automatiquement que le contenu est mensonger.

9. Deepfakes présumés

Deep Authenticity© peut signaler des incohérences techniques ou de provenance compatibles avec une manipulation. Le système parle de contenu suspect ou nécessitant vérification tant qu'une conclusion fiable n'est pas établie.

10. Voix et audio synthétiques

Les contenus vocaux ou audio peuvent être reliés à leur origine, version, montage et attestations disponibles. Un signal de synthèse vocale ne doit pas être présenté comme une identification certaine de l'auteur ou de l'intention.

11. Influenceurs et créateurs

Les contenus de créateurs peuvent relier identité publique, publication, provenance, partenariat déclaré et transformations. La certification de provenance ne constitue pas une approbation du message commercial ou éditorial.

12. Contenus sponsorisés

Lorsqu'un contenu est déclaré sponsorisé ou issu d'un partenariat, cette information peut être reliée au passeport du contenu. AP ne déduit pas automatiquement une relation commerciale en l'absence de preuve documentée.

13. Modération

Signalement, examen, restriction, étiquetage, retrait et rétablissement restent des événements distincts. Authenticity Plus© peut conserver leur provenance sans se substituer aux règles de la plateforme ou aux autorités compétentes.

14. Signalements

Un utilisateur, média ou organisme peut signaler une incohérence, une usurpation ou une manipulation présumée. Un signalement constitue une demande de vérification, non une preuve de culpabilité ou de désinformation.

15. Contexte et annotations

Des annotations de contexte peuvent être reliées à une publication avec auteur, source, date et version. L'annotation doit rester distinguée du contenu original afin de préserver la lisibilité de la chaîne de provenance.

16. Corrections sur plateformes

Une correction publiée sur un réseau social peut être reliée à la publication concernée et à la version corrigée. Suppression, édition et republication ne doivent pas effacer silencieusement la chronologie disponible.

17. Deep Authenticity© et AP Vérification

Deep Authenticity© confronte empreintes, métadonnées, signatures, versions et chronologies ; AP Vérification restitue un résultat compréhensible et proportionné. Le dispositif privilégie preuve et contexte plutôt qu'un classement automatique des opinions.

18. Protection des personnes

Les mécanismes de vérification ne doivent pas faciliter le harcèlement, la révélation d'identité d'une source protégée ou la publication de données personnelles. Les vues publiques appliquent minimisation et contrôle d'accès.

19. AP Ledger

Des empreintes minimales de publications certifiées, corrections, attestations, retraits ou changements critiques peuvent être ancrées dans AP Ledger. Données privées, messages directs, identités protégées et contenus confidentiels restent hors des couches irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si compte, publication, capture et source restent distincts ; si partage et viralité n'effacent pas l'origine ; si intégrité et contexte sont évalués séparément ; si contenus synthétiques et deepfakes présumés sont traités sans verdict automatique ; si modération et vérification restent distinctes ; et si la provenance publique protège les personnes et les sources.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 29 — MEDIA

CHAPITRE 4 — AP ALERTES, AP RAPPORTS, AP DONNÉES STRATÉGIQUES, COMMUNICATIONS OFFICIELLES, INFORMATIONS D'URGENCE, PUBLICATIONS INSTITUTIONNELLES, VÉRIFICATION ET DIFFUSION CONTRÔLÉE

1. Objet du chapitre

Ce chapitre développe les sous-modules AP Alertes, AP Rapports et AP Données Stratégiques au sein d'AP Informations. Il organise la certification, la provenance, la diffusion et la vérification des communications officielles, informations urgentes, rapports publics et données stratégiques autorisées.

2. AP Alertes

AP Alertes permet de relier une alerte à son organisme émetteur, son type, sa date, sa version, son périmètre de diffusion et son statut. L'authentification vise à distinguer une alerte officielle d'une copie, d'une imitation ou d'une republication non autorisée.

3. Autorité émettrice

Toute alerte ou communication officielle conserve l'identité de l'autorité ou de l'organisation qui l' émet. Authenticity Plus© ne crée pas lui-même l'autorité ni la compétence de l'émetteur.

4. Cycle de vie d'une alerte

Préparation, validation, émission, mise à jour, prolongation et clôture restent des événements distincts. Une ancienne alerte doit pouvoir être identifiée comme expirée, remplacée ou clôturée.

5. Diffusion multicanale

Une alerte peut être diffusée par site, application, média, réseau social, notification ou autre canal autorisé. Chaque copie publique peut conserver une relation vérifiable avec la version officielle de référence.

6. Urgence et authenticité

Le caractère urgent d'un message ne remplace pas la vérification de son origine. Le dispositif privilégie une validation rapide de l'émetteur, du statut et de la version sans exiger l'exposition de données sensibles.

7. AP Rapports

AP Rapports organise rapports publics, études institutionnelles, bilans, publications techniques et autres documents autorisés en conservant émetteur, auteurs, date, version, validation et statut.

8. Versions des rapports

Projet, version de travail, version validée, publication, correction et archive restent distincts. Une version remplacée demeure identifiable afin de reconstituer la chronologie documentaire.

9. Annexes et données sources

Un rapport peut être relié à des annexes, tableaux, jeux de données ou documents sources autorisés. La provenance d'une donnée reste distincte de l'interprétation qui en est faite dans le rapport.

10. AP Données Stratégiques

AP Données Stratégiques peut authentifier des données autorisées à forte importance institutionnelle ou économique en conservant producteur, période, version, méthode déclarée et statut de diffusion.

11. Périmètre des données stratégiques

Le qualificatif stratégique n'implique pas une publication ouverte. Les informations confidentielles, personnelles, classifiées ou susceptibles de créer un risque de sécurité restent compartimentées selon les droits applicables.

12. Publication statistique

Une statistique publiée peut conserver organisme producteur, période de référence, méthodologie ou référence méthodologique, date et version. Une révision statistique doit rester distinguée de la valeur antérieure.

13. Communications officielles

Communiqué, déclaration, note, rapport ou donnée officielle peut être relié à son canal de référence et à ses republications. Une citation médiatique reste distincte du document ou message officiel d' origine.

14. AP Vérification

AP Vérification fournit une vue permettant de contrôler émetteur, empreinte, date, version, statut et chaîne de provenance disponible. La vérification technique ne constitue pas à elle seule une approbation du contenu ou de son interprétation.

15. QR Codes et vérification publique

Un QR dynamique peut conduire vers la version officielle ou son statut actuel. La vérification doit signaler clairement lorsqu'un document a été remplacé, corrigé, retiré ou archivé.

16. Deep Authenticity©

Deep Authenticity© confronte signatures, empreintes, versions, canaux, documents sources et chronologies afin de signaler imitation, substitution, republication altérée ou incohérence nécessitant vérification.

17. Lutte contre les faux communiqués

Une communication prétendant provenir d'une organisation peut être comparée aux preuves officielles disponibles. L'absence de correspondance déclenche une alerte de vérification mais ne permet pas d'attribuer automatiquement l'auteur de la falsification.

18. Confidentialité et diffusion contrôlée

Embargos, rapports non publics, données restreintes et informations sensibles sont accessibles uniquement aux acteurs autorisés. Les mécanismes de preuve publique ne doivent pas révéler le contenu protégé.

19. AP Ledger

Des empreintes minimales d'alertes, rapports, publications, corrections, retraits ou jeux de données autorisés peuvent être ancrées dans AP Ledger. Documents confidentiels, données personnelles et informations sensibles restent hors des couches publiques ou irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si AP Alertes, AP Rapports et AP Données Stratégiques conservent leurs fonctions propres ; si émetteur, version et statut sont vérifiables ; si urgence et authenticité ne sont pas confondues ; si données sources et interprétation restent distinctes ; si les versions remplacées restent traçables ; et si la diffusion contrôlée protège les informations non publiques.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 29 — MEDIA

CHAPITRE 5 — GOUVERNANCE D'AP INFORMATIONS, MÉDIAS, AGENCES, PLATEFORMES, CRÉATEURS, DROITS D'ACCÈS, STANDARDS DE PROVENANCE, INTEROPÉRABILITÉ, IA, CONFIDENTIALITÉ, SOUVERAINETÉ ET AUDIT

1. Objet du chapitre

Ce chapitre définit la gouvernance d'AP Informations et de ses composantes AP Presse, AP Media, AP Alertes, AP Rapports, AP Données Stratégiques et AP Vérification. Il organise responsabilités, droits, provenance, interopérabilité, intelligence artificielle, confidentialité, souveraineté et audit.

2. Gouvernance d'AP Informations

AP Informations agit comme couche transversale de certification, traçabilité et vérification. Chaque sous-module conserve sa fonction et les organisations utilisatrices conservent leur responsabilité éditoriale, institutionnelle ou juridique.

3. Médias et éditeurs

Un média ou éditeur conserve son identité, ses comptes officiels, ses signatures autorisées, ses rôles et ses politiques internes. Authenticity Plus© ne détermine pas sa ligne éditoriale.

4. Agences de presse

Une agence peut certifier la provenance de dépêches, photographies, vidéos ou autres contenus. Les médias réutilisateurs conservent le lien avec la source et documentent leurs transformations significatives.

5. Créateurs et contributeurs

Journalistes, auteurs, photographes, vidéastes, podcasteurs et autres créateurs conservent identité professionnelle ou pseudonyme autorisé, contributions, droits et attestations disponibles.

6. Plateformes numériques

Les plateformes peuvent consommer ou restituer des preuves de provenance selon les intégrations autorisées. Leur système de modération, recommandation ou vérification reste distinct du statut de provenance AP.

7. Séparation des responsabilités

Créer, vérifier, valider, publier, corriger, modérer, certifier techniquement et auditer sont des fonctions distinctes. Un même acteur peut cumuler certaines fonctions uniquement lorsque la gouvernance applicable le permet et que ce cumul reste identifiable.

8. Droits d’accès

Les droits sont limités par organisation, rôle, contenu, finalité et durée. Sources protégées, contenus sous embargo, contrats, brouillons et données personnelles restent accessibles uniquement aux acteurs autorisés.

9. Standards de provenance

Les preuves de provenance doivent conserver au minimum identité ou émetteur disponible, empreinte, date, version, relation au contenu source et transformations déclarées pertinentes. L’absence d’un champ ne doit pas être interprétée automatiquement comme une fraude.

10. Interopérabilité

AP Informations peut échanger avec systèmes éditoriaux, archives, agences, plateformes, registres de droits et services de vérification. Toute donnée importée conserve source, version et niveau de confiance ou d’autorité disponible.

11. Portabilité

Un contenu certifié doit pouvoir conserver sa chaîne de provenance lors d’une migration ou d’une diffusion vers un autre canal, dans la limite des standards et droits applicables. La portabilité ne transfère pas automatiquement les licences.

12. Intelligence artificielle

L’IA peut assister classification, transcription, traduction, recherche, comparaison de versions et détection d’anomalies. Son utilisation doit rester identifiable lorsque pertinente et ne lui confère pas une autorité éditoriale autonome.

13. Modèles de détection

Les modèles utilisés pour détecter des manipulations ou incohérences conservent version, périmètre, validation et limites documentées. Un score de détection ne constitue pas à lui seul une preuve de deepfake, de désinformation ou d’intention.

14. Deep Authenticity©

Deep Authenticity© confronte signatures, empreintes, métadonnées, versions, droits, sources autorisées et chronologies. Ses résultats sont des signaux de vérification pouvant être expliqués, réexaminés et, lorsque nécessaire, contestés.

15. Transparence et explicabilité

Une vue de vérification publique doit distinguer ce qui est certifié, ce qui est déclaré, ce qui est dérivé et ce qui reste inconnu. Elle évite les formulations donnant une certitude supérieure à la preuve disponible.

16. Confidentialité

Sources confidentielles, données personnelles, contenus sous embargo, contrats, communications internes et informations sensibles sont compartimentés. Les empreintes publiques ne doivent pas permettre de reconstruire les contenus protégés.

17. Souveraineté

Les organisations compétentes gouvernent localisation, conservation, transfert, archivage et suppression des données selon le droit et leurs obligations. Les contenus sensibles peuvent nécessiter des environnements de stockage spécifiques.

18. Audit

Un audit peut vérifier identités, signatures, accès, versions, transformations, corrections, retraits et journaux nécessaires. L'auditeur ne reçoit pas automatiquement un accès illimité aux sources confidentielles ou contenus protégés.

19. AP Ledger

AP Ledger peut recevoir des empreintes minimales de certifications, publications, licences, corrections, rétractations, révocations et événements critiques. Les sources confidentielles, contenus protégés, secrets d'accès et données personnelles restent hors des couches irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si AP Informations conserve une gouvernance transversale sans absorber la responsabilité éditoriale ; si médias, agences, plateformes et créateurs restent distincts ; si les standards de provenance sont interopérables ; si l'IA reste assistive et explicable ; si les signaux Deep Authenticity© ne deviennent pas des verdicts automatiques ; si la confidentialité et la souveraineté sont préservées ; et si l'audit reste indépendant et proportionné.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 29 — MEDIA / AP INFORMATIONS

CHAPITRE 6 — SYNTHÈSE FONCTIONNELLE, CRITÈRES D'ACCEPTATION ET CLÔTURE DE L'APPLICATION MEDIA / AP INFORMATIONS

1. Objet du chapitre

Ce chapitre clôt le Point 29 — Media / AP Informations. Il consolide AP Presse, AP Media, AP Alertes, AP Rapports, AP Données Stratégiques et AP Vérification avec la provenance des contenus, les chaînes éditoriales, les plateformes, les contenus synthétiques, la gouvernance, la confidentialité et AP Ledger.

2. Architecture consolidée

AP Informations constitue la couche transversale de certification, traçabilité et vérification. AP Presse traite les communications et contenus de presse ; AP Media les contenus numériques et multimédias ; AP Alertes les messages urgents ; AP Rapports les publications structurées ; AP Données Stratégiques les données autorisées correspondantes ; AP Vérification restitue les preuves disponibles.

3. Identités

Média, agence, institution, créateur, auteur, source, compte officiel et contenu restent des identités distinctes. Une identité vérifiée n'emporte pas validation automatique de toutes les affirmations publiées.

4. Provenance des contenus

Article, photographie, vidéo, audio, podcast, document ou publication sociale peut conserver origine, auteur ou organisation, date, empreinte, version, transformations et historique de diffusion.

5. Sources et protection

Les sources publiques, institutionnelles, documentaires ou humaines conservent leur statut. Les sources confidentielles restent protégées et ne sont pas révélées par les mécanismes publics de certification.

6. Production éditoriale

Commande, brouillon, contribution, vérification, relecture, validation et publication restent des étapes distinctes. Authenticity Plus© trace leur chronologie sans exercer la responsabilité éditoriale.

7. Droits, licences et syndication

Paternité, droits documentés, licences, agences et republications conservent leur provenance. Une republication ou syndication n’efface pas la source initiale et ne transfère pas automatiquement les droits.

8. Diffusion multicanale

Site, application, télévision, radio, podcast, newsletter et plateforme sociale peuvent diffuser des versions reliées à une source commune. Chaque version conserve son canal, sa date et ses transformations pertinentes.

9. Corrections et archivage

Correction, mise à jour, rétractation, retrait et archivage restent historisés. Une nouvelle version ne doit pas effacer silencieusement l’existence de l’état antérieur.

10. Réseaux sociaux et viralité

Compte, publication originale, capture, partage, extrait et republication restent distingués. La viralité ne constitue ni une preuve d’authenticité ni une preuve de fausseté.

11. Contexte

Intégrité du fichier, provenance et contexte éditorial sont trois dimensions distinctes. Un contenu authentique peut être réutilisé hors contexte sans que son fichier d’origine ait été falsifié.

12. Contenus synthétiques et IA

Un contenu généré ou substantiellement modifié par IA peut être étiqueté et relié aux informations de provenance disponibles. Le caractère synthétique ne constitue pas automatiquement une preuve de désinformation.

13. Deep Authenticity©

Deep Authenticity© confronte empreintes, signatures, métadonnées, versions, transformations, droits et chronologies afin de signaler incohérences, substitutions ou manipulations présumées nécessitant vérification.

14. AP Vérification

AP Vérification présente ce qui est certifié, déclaré, dérivé ou inconnu. Il doit restituer le niveau réel de preuve et éviter toute formulation donnant une certitude supérieure aux éléments disponibles.

15. AP Alertes, Rapports et Données Stratégiques

Alertes, rapports et données autorisées conservent émetteur, date, version et statut. Urgence et authenticité restent distinctes ; donnée source et interprétation restent distinctes ; une version remplacée reste traçable.

16. Gouvernance et interopérabilité

Médias, agences, plateformes, créateurs et institutions conservent leurs responsabilités. Les échanges entre systèmes préservent source, version, droits disponibles et niveau de confiance ou d'autorité.

17. Intelligence artificielle et explicabilité

L'IA peut assister transcription, traduction, classement, comparaison et détection d'anomalies. Un score ou signal reste explicable, réexaminable et ne constitue pas à lui seul un verdict de deepfake, de désinformation ou d'intention.

18. Confidentialité, souveraineté et audit

Sources protégées, brouillons, embargos, contrats, données personnelles et informations sensibles sont compartimentés. Les organisations compétentes gouvernent conservation et transfert ; l'audit reste indépendant et proportionné aux droits.

19. AP Ledger et portée probatoire

AP Ledger reçoit uniquement des empreintes minimales de certifications, publications, signatures, corrections, rétractations, révocations et événements critiques. AP peut renforcer la preuve d'existence, de date, d'intégrité et de provenance selon le dispositif et le droit applicable, sans promettre une opposabilité juridique universelle.

20. Clôture du Point 29 — Media / AP Informations

Le Point 29 est désormais fonctionnellement défini : AP Informations, AP Presse, AP Media, AP Alertes, AP Rapports, AP Données Stratégiques, AP Vérification, identités, sources, contenus multimédias, QR dynamiques, signatures, droits, licences, syndication, réseaux sociaux, contenus synthétiques, Deep Authenticity©, gouvernance, interopérabilité, confidentialité, souveraineté, audit et AP Ledger. Le Volume IV peut désormais poursuivre avec le Point 30 — Government.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 30 — GOVERNMENT

CHAPITRE 1 — IDENTITÉ INSTITUTIONNELLE, AUTORITÉS PUBLIQUES, MANDATS, ACTES OFFICIELS, DOCUMENTS, SIGNATURES, QR DYNAMIQUES, PROVENANCE ET PASSEPORT NUMÉRIQUE GOVERNMENT

1. Objet du chapitre

Le Point 30 — Government transpose Authenticity Plus© / Deep Authenticity© au niveau de la gouvernance institutionnelle de l'État : institutions, autorités publiques, mandats, actes officiels, documents, signatures, publications et preuves de provenance. Il complète le Point 27 — Public Administration sans le confondre avec celui-ci.

2. Distinction Government / Public Administration

Public Administration concerne principalement l'exécution administrative, les services, dossiers, démarches et agents. Government concerne la couche institutionnelle : autorités constituées, mandats, décisions officielles, textes, nominations, publications et continuité de l'État.

3. Identité institutionnelle

Présidence, gouvernement, ministère, assemblée, juridiction ou autre institution compétente peut disposer d'une identité numérique vérifiable reliant dénomination officielle, rôle, période, canaux officiels et signatures autorisées.

4. Autorités publiques

Une autorité conserve son fondement institutionnel, sa fonction, son périmètre et sa période d' exercice. Authenticity Plus© authentifie les preuves disponibles mais ne crée ni compétence constitutionnelle ni pouvoir public.

5. Mandats

Un mandat peut conserver titulaire, fonction, autorité ou procédure d'origine, date de début, date de fin et statut. Mandat politique, fonction administrative et habilitation technique restent distincts.

6. Continuité institutionnelle

Le changement de titulaire d'une fonction ne détruit pas l'identité de l'institution. Les actes antérieurs restent attribués à leur auteur et à la fonction exercée au moment de leur émission.

7. Actes officiels

Décret, décision, arrêté, nomination, proclamation, résolution ou autre acte autorisé peut conserver émetteur, référence, date, version, signature, statut et source officielle.

8. Textes et versions

Projet, texte adopté, texte signé, texte publié, correction et version consolidée restent distingués. Une consolidation documentaire ne doit pas effacer les versions juridiquement ou historiquement pertinentes.

9. Signatures officielles

Une signature numérique ou attestation peut relier l'acte à son signataire autorisé, à sa fonction et à la version signée. La plateforme ne doit jamais permettre qu'une copie de signature soit réutilisée pour produire un nouvel acte authentique.

10. QR Codes dynamiques

Un QR dynamique peut conduire vers une vue officielle permettant de vérifier institution, référence, version, date, statut et éventuelles corrections. Le QR est un mécanisme de vérification et non la source juridique autonome de l'acte.

11. Publications officielles

Journal officiel, portail institutionnel, communiqué ou registre autorisé peut être relié au document publié. Publication, diffusion médiatique et republication par un tiers restent des événements distincts.

12. Nominations et cessations de fonctions

Nomination, prise de fonction, intérim, délégation, suspension et cessation restent historisés avec leur base documentaire. Une mise à jour de statut ne réécrit pas les actes valablement attribués à une période antérieure.

13. Délégations institutionnelles

Une délégation conserve délégant, délégataire, compétence, périmètre, période et statut. Elle ne doit pas être interprétée au-delà de la portée documentée par l'acte qui la fonde.

14. Documents et archives

Documents institutionnels, procès-verbaux, rapports, décisions et archives peuvent conserver provenance, classification, version, droits d'accès et statut d'archivage. Les archives historiques restent distinctes des actes actuellement en vigueur.

15. Communications gouvernementales

Une communication officielle peut être reliée à l'institution, au porte-parole ou à l'autorité compétente, à la date et au canal de référence. La certification de provenance ne signifie pas approbation automatique de son contenu politique.

16. Deep Authenticity©

Deep Authenticity© confronte identités institutionnelles, mandats, signatures, références, versions, publications et chronologies afin de signaler faux actes, substitutions, incohérences ou usurpations nécessitant vérification.

17. Interopérabilité

Les institutions peuvent échanger des preuves et références avec administrations, registres, archives et systèmes autorisés. Chaque échange conserve source, version, finalité et niveau d'autorité disponible.

18. Confidentialité et souveraineté

Documents non publics, délibérations protégées, données personnelles, informations sensibles et secrets légalement protégés restent compartimentés. L'autorité compétente gouverne localisation, conservation, accès, transfert et archivage.

19. AP Ledger

Des empreintes minimales d'actes, nominations, délégations, signatures, publications, corrections ou révocations peuvent être ancrées dans AP Ledger. Les documents confidentiels, secrets, données personnelles et contenus protégés restent hors des couches publiques ou irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si institution, autorité, titulaire et mandat restent distincts ; si Government et Public Administration ne sont pas confondus ; si les actes conservent source, version et signature ; si les changements de titulaire préservent la continuité institutionnelle ; si les QR vérifient sans créer l' autorité ; et si les données sensibles restent souveraines et compartimentées. Le Passeport Government fournit ainsi le socle de provenance vérifiable des institutions et actes de l'État.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 30 — GOVERNMENT

CHAPITRE 2 — CYCLE DE VIE DES DÉCISIONS GOUVERNEMENTALES, PRÉPARATION, VALIDATION, ADOPTION, SIGNATURE, PROMULGATION, PUBLICATION, ENTRÉE EN VIGUEUR, MODIFICATION, ABROGATION ET ARCHIVAGE

1. Objet du chapitre

Ce chapitre applique le Passeport Numérique Government au cycle de viedes décisions gouvernementales et actes institutionnels. Il organise préparation, validation, adoption, signature, promulgation ou formalité équivalente, publication, entrée en vigueur, modification, abrogation et archivage sans se substituer aux procédures constitutionnelles ou légales applicables.

2. Identité de la décision

Chaque décision ou acte peut disposer d'un identifiant reliant institution, autorité, référence, objet, versions, étapes, signatures, publications et statut. L'identité documentaire de l'acte reste distincte de son effet juridique.

3. Préparation

Une décision peut commencer par une note, un projet, une proposition, un dossier technique ou un texte préparatoire. Ces documents conservent auteur ou service, date, version, diffusion et statut de travail.

4. Consultation et avis

Avis techniques, juridiques, financiers, institutionnels ou autres contributions peuvent être reliés au dossier lorsqu'ils sont communicables. Un avis reste distinct de la décision finale et conserve son auteur, sa date et sa portée.

5. Validation interne

Les validations internes peuvent vérifier forme, compétence, cohérence documentaire ou conformité procédurale. Validation interne et adoption politique ou institutionnelle restent des étapes distinctes.

6. Adoption

Lorsqu'une procédure exige une adoption par un organe compétent, le passeport peut conserver organe, date, référence, version adoptée et statut. Authenticity Plus© ne déduit pas seul qu'une adoption est juridiquement valide.

7. Signature officielle

La signature relie l'acte à un signataire habilité, à sa fonction, à la version signée et à la date. Une signature authentifiée prouve la relation documentée avec cette version, sans étendre automatiquement la compétence du signataire.

8. Promulgation ou formalité équivalente

Lorsque le cadre applicable prévoit une promulgation, approbation, visa, sanction ou autre formalité, cette étape reste distincte de l'adoption et de la publication. Son effet dépend du droit applicable.

9. Publication officielle

La publication dans un journal officiel, portail institutionnel ou autre canal autorisé peut être reliée à la version publiée, à la date et à la référence. Une republication médiatique ou sociale reste distincte de la source officielle.

10. Entrée en vigueur

La date d'entrée en vigueur peut être immédiate, différée ou conditionnée selon l'acte. Le passeport conserve la date ou règle publiée sans décider lui-même de l'interprétation juridique de ses effets.

11. Versions consolidées

Une version consolidée peut faciliter la lecture d'un texte modifié. Elle doit rester reliée aux actes successifs qui ont produit cette consolidation et ne doit pas effacer les versions officielles antérieures.

12. Modification

Amendement, décret modificatif, rectification, nouvelle décision ou autre changement conserve auteur, base, date, version touchée et portée. Une modification ne réécrit pas silencieusement l'acte initial.

13. Rectification

Une correction matérielle ou rectification conserve sa nature, son autorité, sa date et la version concernée. Rectification et modification substantielle restent distinguées.

14. Suspension

Lorsqu'une suspension existe, le passeport peut conserver autorité, fondement ou référence, date de début, durée ou condition de fin et statut. AP ne crée pas lui-même la suspension.

15. Abrogation ou retrait

Abrogation, retrait, expiration ou cessation d'effet restent des statuts distincts. L'acte cesse d'être présenté comme actif lorsque la source compétente l'indique, tout en restant conservé dans l' historique.

16. Deep Authenticity©

Deep Authenticity© confronte identité institutionnelle, compétence déclarée, versions, signatures, publications, dates et chronologies afin de signaler substitution, faux acte, version incohérente ou rupture de chaîne nécessitant vérification.

17. QR Code et statut courant

Un QR dynamique peut afficher référence, version officielle, statut courant, date d'entrée en vigueur et éventuelle abrogation ou modification. Il aide à éviter qu'une ancienne copie soit présentée comme texte actuellement applicable.

18. Archivage institutionnel

Les actes, versions, pièces de procédure et preuves de publication peuvent être archivés selon les politiques applicables. Archive historique, texte consolidé et texte actuellement en vigueur restent des objets distincts.

19. AP Ledger

Des empreintes minimales de versions adoptées, signatures, publications, modifications, suspensions, abrogations ou changements critiques peuvent être ancrées dans AP Ledger. Les délibérations protégées, documents confidentiels et secrets institutionnels restent hors des couches publiques ou irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si projet, validation, adoption, signature, promulgation, publication et entrée en vigueur restent distingués ; si les modifications préservent l'historique ; si rectification et changement substantiel ne sont pas confondus ; si le QR restitue le statut courant sans créer l'effet juridique ; et si l'archivage conserve la chaîne institutionnelle complète. Le Passeport Government fournit ainsi une mémoire vérifiable du cycle de vie des décisions de l'État.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 30 — GOVERNMENT

CHAPITRE 3 — INSTITUTIONS EXÉCUTIVES, LÉGISLATIVES ET JUDICIAIRES, COORDINATION INTERINSTITUTIONNELLE, NOMINATIONS, DÉLÉGATIONS, DÉCISIONS, REGISTRES, TRANSPARENCE ET CONTINUITÉ DE L'ÉTAT

1. Objet du chapitre

Ce chapitre structure le Passeport Government autour des institutions de l'État et de leurs relations documentées. Il traite des fonctions exécutives, législatives et judiciaires à un niveau institutionnel, de la coordination interinstitutionnelle, des nominations, délégations, décisions, registres, mécanismes de transparence et continuité de l'État.

2. Principe de séparation institutionnelle

Les institutions exécutives, législatives et judiciaires conservent des identités, compétences, procédures et archives distinctes selon l'ordre juridique applicable. Authenticity Plus© documente les relations et preuves sans fusionner les pouvoirs ni redéfinir leur équilibre.

3. Institutions exécutives

Les institutions exécutives peuvent conserver identité, autorités, mandats, actes, délégations, réunions officielles, décisions et publications autorisées. Gouvernement, ministère, cabinet et administration d' exécution restent distingués selon leur rôle.

4. Institutions législatives

Assemblée, chambre, commission ou autre organe compétent peut conserver identité, composition officielle, mandats, sessions, textes, votes ou décisions publiables et archives. AP ne détermine ni la validité d'un mandat électif ni le résultat juridique d'une procédure parlementaire.

5. Institutions judiciaires

Juridictions et organes judiciaires peuvent conserver identité institutionnelle, compétence publiée, décisions ou documents communicables et provenance officielle. AP ne se substitue ni au juge, ni aux règles de procédure, ni aux systèmes judiciaires officiels.

6. Coordination interinstitutionnelle

Une procédure impliquant plusieurs institutions peut relier demandes, transmissions, avis, validations, décisions et réponses. Chaque institution conserve la responsabilité de l'étape qui lui appartient.

7. Nominations

Une nomination conserve autorité ou procédure d'origine, titulaire, fonction, acte, date de prise d'effet et statut. Nomination, confirmation éventuelle, prise de fonction et exercice effectif restent des événements distincts.

8. Intérim et suppléance

Intérim, suppléance ou remplacement temporaire conserve fondement, titulaire, fonction, période et limites. L'intérim n'efface pas l'identité institutionnelle ni l'historique du titulaire précédent.

9. Délégations

Une délégation conserve délégant, délégataire, compétence, limites, période et acte fondateur. Sous-délégation ou modification éventuelle doit disposer de sa propre base documentée.

10. Révocation et cessation

Révocation, démission, expiration de mandat, remplacement ou autre cessation conserve date, source et statut. Les actes antérieurs restent attribués à la fonction et au titulaire qui les a émis à la date concernée.

11. Décisions collégiales

Lorsqu'un organe décide collectivement, le passeport conserve organe, séance ou procédure, version, résultat officiel et publication autorisée. La plateforme ne transforme pas une donnée technique en interprétation politique du vote.

12. Registres institutionnels

Des registres peuvent organiser mandats, nominations, délégations, actes, décisions et publications officielles. Chaque entrée conserve source, version, date, statut et historique des modifications.

13. Transparence institutionnelle

Les informations légalement publiques peuvent être restituées sous une forme vérifiable : institution, autorité, acte, date, version et statut. Transparence ne signifie pas publication de toutes les délibérations, données personnelles ou informations protégées.

14. Traçabilité des responsabilités

La chaîne documentaire permet d'identifier quelle institution ou autorité a préparé, validé, adopté, signé, publié ou modifié un acte lorsque ces informations sont disponibles. La traçabilité ne crée pas à elle seule une responsabilité juridique.

15. Continuité de l'État

Alternance, remaniement, dissolution, renouvellement, succession de titulaires ou réorganisation ne doivent pas rompre la mémoire institutionnelle. Les identités des institutions et les archives persistent selon le cadre applicable.

16. Réorganisation institutionnelle

Création, fusion, changement de dénomination, transfert de compétence ou suppression d'une institution peut être historisé. Une nouvelle structure conserve les liens documentaires nécessaires avec les institutions antérieures sans réécrire leur histoire.

17. Deep Authenticity©

Deep Authenticity© confronte identités institutionnelles, mandats, nominations, délégations, actes, signatures, registres et chronologies afin de signaler incohérences, usurpations ou substitutions nécessitant vérification.

18. Confidentialité et contrôle d'accès

Délibérations protégées, dossiers judiciaires non publics, données personnelles, informations de sécurité et documents légalement confidentiels restent compartimentés. La transparence publique s' applique uniquement aux éléments autorisés.

19. AP Ledger

Des empreintes minimales de nominations, délégations, décisions, changements institutionnels, publications ou révocations peuvent être ancrées dans AP Ledger. Les contenus confidentiels et données protégées restent hors des couches publiques ou irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si les institutions et pouvoirs restent distincts ; si nomination, prise de fonction, délégation et cessation sont historisées ; si la coordination conserve l'auteur de chaque étape ; si transparence et confidentialité restent compatibles ; si les changements politiques ne détruisent pas la mémoire institutionnelle ; et si Deep Authenticity© vérifie la provenance sans devenir une autorité constitutionnelle. Le Passeport Government renforce ainsi la continuité vérifiable de l'État.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 30 — GOVERNMENT

CHAPITRE 4 — TRANSPARENCE GOUVERNEMENTALE, ENGAGEMENTS PUBLICS, PROGRAMMES, BUDGETS ET DÉPENSES PUBLIABLES, MARCHÉS ET CONTRATS, INDICATEURS DE RÉALISATION, CONTRÔLE INSTITUTIONNEL ET REDEVABILITÉ

1. Objet du chapitre

Ce chapitre définit la couche de transparence et de redevabilité du Passeport Government. Il relie engagements publics, programmes, autorisations budgétaires publiables, dépenses agrégées ou communicables, marchés, contrats, résultats et contrôles institutionnels, sans dupliquer les opérations administratives détaillées du Point 27 — Public Administration.

2. Distinction Government / Public Administration

Government conserve la vision institutionnelle : décision, engagement, programme, autorisation, responsabilité politique ou institutionnelle et résultat public. Public Administration conserve l’ exécution opérationnelle : dossiers, procédures, agents, paiements, traitements et services administratifs.

3. Engagements publics

Un engagement officiellement publié peut conserver institution ou autorité, date, texte de référence, horizon, périmètre, indicateurs déclarés et statut. Une déclaration politique non formalisée reste distinguée d’un engagement institutionnel documenté.

4. Programmes gouvernementaux

Un programme peut relier autorité responsable, objectifs, période, textes fondateurs, enveloppes publiables, indicateurs et rapports. Programme, projet d’exécution et opération administrative restent des niveaux distincts.

5. Objectifs et indicateurs

Chaque objectif peut être associé à des indicateurs définis, une méthode, une période de référence et une source. Authenticity Plus© trace l’indicateur publié sans prétendre que celui-ci mesure à lui seul toute la performance d’une politique publique.

6. Budgets publiables

Les autorisations, enveloppes ou agrégats budgétaires légalement publiables peuvent être reliés au programme et à leur source officielle. AP ne remplace ni le système budgétaire national ni la comptabilité publique.

7. Dépenses publiables

Des données de dépenses agrégées ou communicables peuvent être reliées aux autorisations correspondantes, périodes et programmes. Les écritures comptables détaillées et traitements administratifs restent dans les systèmes compétents.

8. Écart budget / réalisation

Lorsqu'une comparaison est publiée, budget initial, budget révisé, engagement, exécution et résultat restent des notions distinctes. Les écarts conservent période, méthode et source afin d'éviter des comparaisons trompeuses.

9. Marchés publics

À un niveau Government, un marché publiable peut être relié au programme, à l'autorité contractante, à l'objet, au montant ou agrégat communicable, au titulaire et au statut. La procédure détaillée d'achat reste du ressort des systèmes administratifs et de commande publique compétents.

10. Contrats publics

Un contrat publiable peut conserver référence, parties institutionnelles, objet, date, durée, montant communicable, avenants et statut. Les clauses confidentielles, secrets protégés et données personnelles restent compartimentés.

11. Avenants et modifications

Toute modification significative publiable conserve référence au contrat initial, date, autorité, portée et effet financier communicable. Une version mise à jour ne doit pas effacer silencieusement l'état antérieur.

12. Bénéficiaires institutionnels et territoires

Les programmes peuvent être associés aux secteurs, institutions ou territoires concernés lorsque cette information est publiable. Les données nominatives de citoyens ou bénéficiaires individuels ne sont pas exposées par défaut.

13. Indicateurs de réalisation

Livrables, jalons, taux d'avancement et résultats officiellement publiés peuvent être historisés. Une déclaration de réalisation conserve sa source et ne devient pas automatiquement une certification indépendante de performance.

14. Preuves de réalisation

Rapport, procès-verbal, audit, photographie institutionnelle, attestation ou autre preuve autorisée peut être relié à un jalon. Chaque preuve conserve auteur, date, périmètre et statut de validation.

15. Contrôle institutionnel

Inspection, cour des comptes ou organe équivalent, contrôle parlementaire, audit interne ou autre mécanisme compétent peut être relié aux programmes et actes examinés selon les informations publiables. AP ne se substitue pas à ces organes.

16. Redevabilité

Le passeport peut permettre de relier engagement, responsable institutionnel, ressources publiables, calendrier, réalisations et contrôles. Cette traçabilité soutient la redevabilité sans produire automatiquement un jugement politique, administratif ou pénal.

17. Deep Authenticity©

Deep Authenticity© confronte engagements, budgets publiés, marchés, contrats, avenants, indicateurs, preuves et chronologies afin de signaler incohérences, substitutions ou ruptures de provenance nécessitant vérification.

18. Transparence et limites

La transparence est limitée par le droit applicable, la sécurité, la confidentialité contractuelle légitime, les données personnelles et les secrets protégés. Une absence de publication n’est pas automatiquement une preuve d’irrégularité.

19. AP Ledger

Des empreintes minimales d’engagements, programmes, autorisations publiables, contrats, avenants, rapports, contrôles ou changements critiques peuvent être ancrées dans AP Ledger. Les données confidentielles et documents protégés restent hors des couches publiques ou irréversibles.

20. Critères d’acceptation et conclusion

Le modèle est acceptable si Government conserve la couche institutionnelle et Public Administration l’ exécution détaillée ; si engagements, budgets, dépenses, marchés, contrats et réalisations restent sourcés et versionnés ; si indicateur et jugement de performance restent distincts ; si les organes de contrôle conservent leur autorité ; et si transparence et protection des informations légitimes restent compatibles. Le Passeport Government fournit ainsi une chaîne vérifiable de l’engagement public à la réalisation documentée.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 30 — GOVERNMENT

CHAPITRE 5 — GOUVERNANCE NUMÉRIQUE DE L'ÉTAT, INTEROPÉRABILITÉ, IDENTITÉS ET ACCÈS INSTITUTIONNELS, SOUVERAINETÉ, CYBERSÉCURITÉ, IA GOUVERNEMENTALE, CONTRÔLE HUMAIN, CONTINUITÉ, AUDIT ET AP LEDGER

1. Objet du chapitre

Ce chapitre définit la gouvernance numérique du Passeport Government. Il organise identités institutionnelles, droits d'accès, interopérabilité, souveraineté des données, cybersécurité, intelligence artificielle, contrôle humain, continuité, audit et AP Ledger au niveau de l'État.

2. Gouvernance numérique de l'État

Authenticity Plus© agit comme infrastructure de provenance, certification et traçabilité. Il ne devient ni autorité politique, ni pouvoir constitutionnel, ni système unique imposant ses décisions aux institutions.

3. Identités institutionnelles

Institutions, autorités, organes, titulaires, services et systèmes disposent d'identités distinctes. Toute identité conserve son statut, son rôle, sa période et les preuves autorisées qui la fondent.

4. Identités techniques

Compte de service, API, certificat, application et système automatisé possèdent une identité technique séparée de l'identité humaine ou institutionnelle. Une identité technique ne reçoit pas automatiquement une compétence publique.

5. Droits d'accès

Les accès sont attribués selon institution, rôle, fonction, finalité, périmètre et durée. Un mandat institutionnel ne donne pas automatiquement accès à toutes les données détenues par l'État.

6. Séparation des fonctions

Préparer, valider, signer, publier, administrer les accès, auditer et révoquer sont des fonctions distinctes. Les cumuls éventuels restent documentés et soumis aux règles institutionnelles applicables.

7. Interopérabilité gouvernementale

Les institutions peuvent échanger actes, références, preuves et statuts avec les systèmes autorisés. Chaque échange conserve source, version, finalité, niveau d'autorité et responsabilité de l'émetteur.

8. Fédération et autonomie institutionnelle

L'interopérabilité ne signifie pas centralisation absolue. Chaque institution peut conserver ses systèmes, responsabilités et règles tout en participant à une couche commune de vérification et de provenance.

9. Souveraineté des données

L'État et les institutions compétentes gouvernent localisation, conservation, transfert, archivage, réplication et suppression des données selon le droit applicable et leur niveau de sensibilité.

10. Classification et compartimentation

Informations publiques, internes, confidentielles, sensibles ou légalement protégées sont traitées selon leur niveau. Une preuve d'existence ou d'intégrité peut être exposée sans publier le contenu protégé.

11. Cybersécurité

Identités, clés, certificats, API, journaux, systèmes de signature et infrastructures de vérification sont protégés par authentification, segmentation, chiffrement, supervision, révocation et procédures de réponse aux incidents.

12. Révocation et compromission

Un compte, certificat, mandat technique ou droit compromis peut être suspendu ou révoqué. Les signatures ou actes antérieurs conservent leur contexte historique tandis que les usages futurs sont bloqués selon le statut.

13. Intelligence artificielle gouvernementale

L'IA peut assister recherche documentaire, classement, traduction, comparaison de versions, détection d'incohérences, analyse de données publiables ou autres fonctions autorisées. Elle ne reçoit pas, du seul fait de son intégration, une compétence institutionnelle autonome.

14. Modèles, données et traçabilité IA

Les modèles utilisés dans des fonctions sensibles conservent version, finalité, périmètre, données ou références pertinentes, validations et limites documentées. Les résultats importants doivent pouvoir être rattachés au système et au contexte qui les ont produits.

15. Contrôle humain

Toute décision nécessitant une autorité humaine ou institutionnelle reste sous contrôle des acteurs habilités. Une recommandation, un score ou un signal algorithmique ne constitue pas automatiquement un acte gouvernemental.

16. Deep Authenticity©

Deep Authenticity© confronte identités, mandats, actes, signatures, accès, versions, publications et chronologies afin de signaler incohérences, usurpations, substitutions ou anomalies nécessitant vérification.

17. Continuité et résilience

Les fonctions critiques de vérification et de provenance disposent de mécanismes de sauvegarde, restauration, redondance et continuité adaptés. Une interruption technique ne doit pas effacer la mémoire institutionnelle ni permettre la réécriture de l'historique.

18. Audit indépendant et contrôle

Les audits peuvent examiner identités, droits, signatures, événements, journaux, modèles et contrôles selon leur mandat. L'auditeur ne reçoit pas automatiquement un accès illimité aux informations classifiées, judiciaires, personnelles ou autrement protégées.

19. AP Ledger

AP Ledger peut recevoir des empreintes minimales d'actes, mandats, signatures, délégations, publications, révocations, contrôles ou événements critiques. Secrets, clés, données personnelles, délibérations protégées et documents sensibles restent hors des couches publiques ou irréversibles.

20. Critères d'acceptation et conclusion

Le modèle est acceptable si plateforme technique et autorité publique restent distinctes ; si identités humaines, institutionnelles et techniques ne sont pas confondues ; si les accès sont limités et révocables ; si l'interopérabilité préserve l'autonomie institutionnelle ; si souveraineté et compartimentation sont garanties ; si l'IA reste assistive et contrôlée ; et si l'audit demeure indépendant et proportionné. Le Passeport Government fournit ainsi une infrastructure numérique de confiance sans transférer le pouvoir de l'État à la plateforme.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

POINT 30 — GOVERNMENT

CHAPITRE 6 — SYNTHÈSE FONCTIONNELLE, CRITÈRES D'ACCEPTATION ET CLÔTURE DU POINT 30 — GOVERNMENT

1. Objet du chapitre

Ce chapitre clôt le Point 30 — Government et consolide l'identité institutionnelle, les autorités et mandats, le cycle de vie des actes, les relations entre institutions, la transparence gouvernementale, la gouvernance numérique, la souveraineté, l'intelligence artificielle, l'audit et AP Ledger.

2. Positionnement de Government

Government constitue la couche institutionnelle du Volume IV : autorités constituées, mandats, décisions, actes, publications, engagements et continuité de l'État. Il reste distinct du Point 27 — Public Administration, centré sur l'exécution administrative, les dossiers, démarches et services.

3. Identité institutionnelle

Institution, autorité, titulaire, mandat, service et identité technique restent des objets distincts. Le changement de titulaire ne détruit pas l'identité de l'institution ni la provenance des actes antérieurs.

4. Autorité et compétence

Authenticity Plus© documente les preuves relatives aux mandats, délégations et fonctions sans créer de compétence constitutionnelle, législative, judiciaire ou administrative. La plateforme technique reste séparée de l'autorité publique.

5. Cycle de vie des actes

Préparation, consultation, validation, adoption, signature, promulgation ou formalité équivalente, publication et entrée en vigueur restent distinguées. Leur portée juridique dépend du droit et des institutions compétentes.

6. Versions et statut

Projet, version adoptée, version signée, version publiée, rectification, modification, suspension, abrogation et archive restent historisés. Une version consolidée facilite la lecture sans effacer les actes qui l'ont produite.

7. Signatures et QR dynamiques

Les signatures relient un acte à un signataire, une fonction, une date et une version. Les QR dynamiques permettent de vérifier référence, version et statut courant sans devenir eux-mêmes la source autonome de l'autorité juridique.

8. Institutions et séparation des pouvoirs

Les institutions exécutives, législatives et judiciaires conservent leurs identités, compétences, procédures et archives selon l'ordre juridique applicable. AP documente les relations interinstitutionnelles sans fusionner les pouvoirs.

9. Nominations, intérims et délégations

Nomination, prise de fonction, intérim, délégation, révocation et cessation restent des événements distincts. Chaque délégation conserve son fondement, son périmètre, sa période et ses limites.

10. Continuité de l'État

Alternance, remaniement, renouvellement, réorganisation ou succession de titulaires ne rompent pas la mémoire institutionnelle. Les actes et archives restent attribués à leur contexte historique.

11. Transparence gouvernementale

Les engagements, programmes, budgets et dépenses publiables, marchés, contrats, avenants, indicateurs et preuves de réalisation peuvent être reliés à leurs sources officielles et versions.

12. Redevabilité

Engagement, autorité responsable, ressources publiables, calendrier, résultats et contrôles peuvent être reliés dans une chaîne vérifiable. Cette traçabilité soutient la redevabilité sans produire automatiquement un jugement politique, administratif, civil ou pénal.

13. Contrôle institutionnel

Audits, inspections, contrôles parlementaires, juridictions financières ou autres organes compétents conservent leur indépendance et leur autorité. Authenticity Plus© fournit la provenance et la traçabilité nécessaires sans se substituer à leurs conclusions.

14. Interopérabilité et autonomie

Les institutions peuvent partager références, preuves et statuts par des interfaces autorisées. L' interopérabilité préserve l'autonomie des institutions et ne suppose pas une centralisation absolue de tous les systèmes de l'État.

15. Souveraineté et compartimentation

Localisation, conservation, transfert, archivage et suppression sont gouvernés selon le droit et la sensibilité des données. Les informations publiques, internes, confidentielles, sensibles ou protégées restent compartimentées.

16. Cybersécurité et continuité numérique

Identités, clés, certificats, API, journaux et systèmes de signature sont protégés, supervisés et révocables. Sauvegarde, restauration et redondance préservent la mémoire institutionnelle en cas d'incident.

17. Intelligence artificielle et contrôle humain

L'IA peut assister recherche, classement, traduction, comparaison, analyse et détection d'incohérences. Elle ne reçoit pas automatiquement une compétence publique ; les décisions nécessitant une autorité humaine ou institutionnelle restent sous contrôle des acteurs habilités.

18. Deep Authenticity©

Deep Authenticity© confronte identités, mandats, signatures, actes, versions, publications, accès et chronologies afin de signaler incohérences, substitutions ou usurpations. Ses résultats restent des signaux explicables et vérifiables, non des décisions institutionnelles automatiques.

19. AP Ledger et critères d'acceptation

AP Ledger reçoit uniquement des empreintes minimales d'actes, mandats, délégations, signatures, publications, modifications, révocations et contrôles autorisés. Le modèle est acceptable si Government et Public Administration restent distincts ; si plateforme et autorité restent séparées ; si les actes sont versionnés ; si l'IA reste assistive ; si les données protégées restent hors des couches publiques ou irréversibles ; et si l'audit demeure indépendant.

20. Clôture du Point 30 — Government et du Volume IV

Le Point 30 est désormais fonctionnellement défini : identité institutionnelle, autorités, mandats, décisions, actes, signatures, QR dynamiques, cycle de vie juridique, institutions exécutives, législatives et judiciaires, nominations, délégations, continuité de l'État, transparence, programmes, budgets publiables, contrats, redevabilité, interopérabilité, souveraineté, cybersécurité, IA, Deep Authenticity©, audit et AP Ledger. Avec cette clôture, la série des 30 applications sectorielles du Volume IV dispose de son dernier point sectoriel.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

SYNTHÈSE GÉNÉRALE DES 30 APPLICATIONS SECTORIELLES

ARCHITECTURE UNIFIÉE, PRINCIPES TRANSVERSAUX, INTEROPÉRABILITÉ ET CONVERGENCE DES PASSEPORTS NUMÉRIQUES

1. Objet de la synthèse générale

Cette synthèse clôt la construction sectorielle du Volume IV et présente la logique commune des trente applications. Chaque secteur conserve ses acteurs, règles, preuves, niveaux de sensibilité et autorités compétentes, tandis qu'Authenticity Plus© fournit une architecture commune d'identité, provenance, traçabilité, vérification et continuité.

2. Principe d'architecture unifiée

Le Volume IV repose sur une idée constante : un objet, une personne, une organisation, un document, un droit, un service ou un événement peut disposer d'un Passeport Numérique reliant identité, preuves, versions, acteurs, statuts et chronologie. Le passeport n'efface jamais les systèmes métiers ou registres officiels qui conservent leur autorité propre.

3. Les Passeports Numériques sectoriels

Les applications sectorielles adaptent le même noyau à des contextes différents : patrimoine, biens, services, infrastructures, organisations, médias, administrations et institutions. Le modèle commun est réutilisable sans imposer que toutes les données ou tous les secteurs soient centralisés dans un registre unique.

4. Identité et attribution

Chaque secteur distingue l'identité de l'objet suivi de l'identité de ses acteurs. Titulaire, propriétaire, détenteur, auteur, émetteur, autorité, professionnel, organisme, système technique ou prestataire restent attribués selon leur rôle et la preuve disponible.

5. Provenance

La provenance décrit d'où vient une information, un document, un contenu, un bien ou un événement. Une déclaration, une preuve documentaire, une certification professionnelle et une inscription dans un registre officiel restent des niveaux de preuve distincts.

6. Chronologie et versioning

Création, acquisition, modification, maintenance, transfert, validation, publication, correction, révocation, retrait et archivage peuvent être historisés. Une nouvelle version enrichit ou modifie l'état courant sans effacer silencieusement l'existence des états antérieurs.

7. Certification numérique

Empreintes, horodatages, signatures et attestations permettent de fixer l'existence, l'intégrité ou l' attribution d'éléments déterminés. La certification précise toujours ce qui est techniquement établi et ne transforme pas automatiquement une déclaration en vérité juridique, scientifique, médicale, éditoriale ou institutionnelle.

8. QR Codes dynamiques

Les QR Codes constituent une porte d'accès à une vue de vérification contrôlée. Ils peuvent restituer identité, statut, version ou preuves publiables, mais ne doivent pas exposer les données privées, confidentielles, classifiées ou commercialement protégées.

9. Deep Authenticity©

Deep Authenticity© constitue la couche d'analyse transversale. Elle confronte identités, signatures, documents, photographies, métadonnées, versions, droits, statuts et chronologies afin de signaler incohérences, substitutions, duplications ou ruptures de provenance nécessitant vérification.

10. Principe de non-verdict automatique

Un signal Deep Authenticity©, un score algorithmique ou une anomalie technique ne constitue pas à lui seul une preuve de fraude, de falsification, de désinformation, d'illégalité ou de responsabilité. Les décisions restent attribuées aux personnes, professionnels, organisations ou autorités compétentes.

11. Intelligence artificielle

L'intelligence artificielle peut assister recherche, classement, traduction, transcription, comparaison, analyse et détection d'incohérences. Les modèles sensibles doivent être versionnés, gouvernés et explicables ; l'IA ne reçoit pas automatiquement l'autorité professionnelle, juridique, médicale, éditoriale, administrative ou gouvernementale du secteur.

12. Contrôle humain

Les décisions à conséquence significative demeurent sous le contrôle des acteurs habilités. Le Volume IV maintient une séparation constante entre assistance algorithmique et autorité décisionnelle humaine ou institutionnelle.

13. Confidentialité par défaut

Les informations personnelles, patrimoniales, médicales, commerciales, contractuelles, judiciaires, administratives, militaires ou institutionnelles sensibles ne deviennent pas publiques du seul fait de leur intégration à Authenticity Plus©. Les vues et échanges appliquent minimisation, finalité et contrôle d'accès.

14. Partage sélectif

Le modèle privilégie le partage de la preuve nécessaire plutôt que l'ouverture du dossier complet. Un acteur peut vérifier un statut, une certification ou un document précis sans obtenir automatiquement l'ensemble des informations liées à la personne, au bien ou à l'organisation.

15. Interopérabilité

Authenticity Plus© est conçu comme une couche interopérable avec registres, systèmes métiers, administrations, entreprises, plateformes, assureurs, professionnels et institutions. Toute donnée importée ou échangée conserve sa source, sa version, sa finalité et son niveau d'autorité disponible.

16. Autonomie des secteurs

L'interopérabilité ne signifie pas absorption. Chaque secteur conserve ses normes, systèmes, autorités, procédures et responsabilités. Authenticity Plus© apporte la continuité de preuve et de provenance sans remplacer les infrastructures spécialisées.

17. Souveraineté numérique

Les conditions de localisation, conservation, transfert, archivage et suppression sont gouvernées selon les droits applicables, les obligations sectorielles et la sensibilité des données. Les architectures peuvent rester distribuées ou souveraines tout en participant à une couche commune de vérification.

18. Cybersécurité

Identités, comptes, certificats, clés, API, signatures, QR, journaux et infrastructures de vérification sont protégés par des mécanismes adaptés d'authentification, chiffrement, segmentation, supervision, sauvegarde et révocation.

19. Continuité et résilience

Les Passeports Numériques préservent la mémoire des objets, droits, documents et institutions au-delà des changements de propriétaires, responsables, prestataires, systèmes ou titulaires. La continuité documentaire constitue l'un des fils directeurs du Volume IV.

20. Audit et traçabilité

Les opérations sensibles peuvent être journalisées et auditées selon les droits applicables. L'audit vérifie la chaîne de preuve et les contrôles sans obtenir automatiquement un accès illimité aux contenus protégés.

21. AP Ledger

AP Ledger constitue la couche d'ancrage minimal des événements critiques. Il peut recevoir des empreintes de certifications, validations, changements de statut, transferts, révocations ou publications, tandis que les documents complets, secrets, données personnelles et contenus sensibles restent hors des couches publiques ou irréversibles.

22. Portée probatoire

Authenticity Plus© peut renforcer la preuve d'existence, de date, d'intégrité, d'attribution et de provenance selon les mécanismes utilisés. La portée juridique, réglementaire ou opposable de cette preuve dépend du droit applicable, des autorités compétentes et du contexte d'utilisation.

23. Séparation des rôles

Créer, déclarer, vérifier, expertiser, certifier, valider, décider, publier, contrôler et auditer sont des fonctions différentes. Le Volume IV évite systématiquement qu'une infrastructure technique absorbe l' autorité des acteurs qui portent légalement ou professionnellement ces fonctions.

24. Protection contre la centralisation excessive

L'architecture commune ne doit pas devenir une base universelle exposant tous les citoyens, entreprises, actifs ou institutions. Les passeports peuvent être fédérés, compartimentés et accessibles selon des droits différents tout en conservant une capacité de vérification commune.

25. Valeur pour le citoyen

Pour le citoyen, l'architecture vise la continuité de ses preuves, documents, biens, droits et interactions. Elle facilite la vérification et le partage sélectif tout en maintenant la maîtrise des informations privées dans les domaines où cette maîtrise lui appartient.

26. Valeur pour les professionnels et entreprises

Pour les professionnels et entreprises, le modèle facilite l'attribution des documents, la provenance des produits et services, la maintenance des actifs, la conformité, les échanges de preuves et la réduction des ruptures documentaires entre organisations.

27. Valeur pour les institutions

Pour les institutions, le Volume IV fournit une architecture de provenance vérifiable des actes, décisions, publications, contrôles et interactions autorisées. La plateforme demeure une infrastructure de confiance et non une autorité institutionnelle parallèle.

28. Convergence des trente applications

Les trente applications ne constituent pas trente plateformes isolées. Elles forment un écosystème de Passeports Numériques sectoriels partageant les mêmes principes de base tout en conservant leurs spécificités. Cette convergence permet qu'un même événement puisse être vérifié entre secteurs sans fusionner leurs données.

29. Critères transversaux d'acceptation

L'architecture du Volume IV est acceptable si chaque donnée conserve sa source ; si les niveaux de preuve ne sont pas confondus ; si l'historique est préservé ; si les accès sont minimisés et révocables ; si les systèmes métiers gardent leur autorité ; si l'IA reste assistive ; si Deep Authenticity© produit des signaux vérifiables ; et si les données sensibles restent protégées.

30. Conclusion générale du Volume IV

Le Volume IV établit Authenticity Plus© comme une architecture transversale de confiance applicable à trente domaines sectoriels. Son unité ne repose pas sur la centralisation de toutes les données, mais sur un langage commun de preuve : identité, provenance, chronologie, certification, vérification, droits d'accès, interopérabilité et continuité. Deep Authenticity© et AP Ledger complètent cette architecture en renforçant la détection d'incohérences et la mémoire minimale des événements critiques, sans retirer aux personnes, professionnels, entreprises ou institutions leurs responsabilités et autorités propres.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

MATRICE TRANSVERSALE DES 30 APPLICATIONS SECTORIELLES

PASSEPORT — PROVENANCE — QR — DEEP AUTHENTICITY© — IA — INTEROPÉRABILITÉ — CONFIDENTIALITÉ / SOUVERAINETÉ — AUDIT — AP LEDGER

Lecture : « Socle » = capacité structurante ; « Ciblé » = usage selon le contexte. La matrice synthétise les chapitres sectoriels et ne les remplace pas.

Pt	Application	Objet principal	Provenance / cycle	QR	Deep Authenticity©	IA	Interopérabilité	Confidentialité / souveraineté	Audit	Ledger
1	Industrie	Produit / lot / unité	Généalogie&cycle de vie	Ciblé	Identité / composants	Assistive	Oui	Industrielle	Oui	Oui
2	Artisanat	Pièce / série	Création&provenance	Ciblé	Provenance	Assistive	Oui	Savoir-faire	Oui	Oui
3	Agriculture	Exploitation / parcelle / lot	Origine agricole&lots	Ciblé	Filière / lots	Assistive	Oui	Exploitation	Oui	Oui
4	Élevage	Animal / troupeau / lot	Généalogie&productions	Ciblé	Identité / lots	Assistive	Oui	Élevage	Oui	Oui
5	Pharmacie	Produit / lot / unité	Fabrication&distribution	Socle	Anti-falsification	Assistive	Oui	Renforcée	Oui	Oui
6	Santé	Personne / épisode / document	Parcours documentaire de soins	Ciblé	Cohérence documentaire	Assistive	Oui	Très renforcée	Oui	Oui
7	Automobile	Véhicule / VIN / composant	Cycle de vie véhicule	Ciblé	VIN / kilométrage	Assistive	Oui	Personnelle	Oui	Oui
8	Propriété intellectuelle	Création / version / droits	Antériorité&chaîne de droits	Ciblé	Versions / droits	Assistive	Oui	Secrets / contenus	Oui	Oui
9	Transport	Expédition / unité	Déplacement&garde	Ciblé	Flux / documents	Assistive	Oui	Opérationnelle	Oui	Oui
10	Billetterie	Billet / droit d'accès	Émission → usage	Socle	Anti-duplication	Assistive	Oui	Client	Oui	Oui
11	Seconde main	Objet / propriété	Revente&circularité	Socle	Clonage / contrefaçon	Assistive	Oui	Partage contrôlé	Oui	Oui
12	AP Self — Patrimoine	Bien / coffre patrimonial	Preuve progressive&transmission	Socle sécurisé	Bien / documents	Assistive	Oui	Privé par défaut	Oui	Oui

13	TAXI	Chauffeur / véhicule / autorisation	Course&concordance	Socle	Anti-faux taxi	Assistive	Oui	Identité / localisation	Oui	Oui
14	Logistique	Marchandise / contenant	Chaîne de possession	Socle	Anti-clonage / trajet	Assistive	Oui	Flux	Oui	Oui
15	Education	Apprenant / diplôme	Parcours académique	Socle	Diplômes / usurpation	Assistive	Oui	Renforcée / mineurs	Oui	Oui
16	Food	Produit / lot / ingrédient	Généalogie alimentaire	Socle	Lots / origine	Assistive	Oui	Recettes / acteurs	Oui	Oui
17	Art et Culture	Œuvre / provenance	Provenance&conservation	Socle	Œuvre / certificats	Assistive	Oui	Propriétaires / valeurs	Oui	Oui
18	Luxury	Objet / marque / propriété	Cycle de vie&propriété	Socle	Contrefaçon / vol	Assistive	Oui	Propriétaire / localisation	Oui	Oui
19	Construction	Projet / ouvrage / équipement	Conception → exploitation	Socle	BIM / documents	Assistive	Oui	Plans / sécurité	Oui	Oui
20	Smart City	Actif urbain / capteur	Infrastructure&intervention	Socle	Capteurs / interventions	Assistive	Oui	Anti-surveillance	Oui	Oui
21	Environnement	Site / mesure / échantillon	Mesure → déclaration	Socle	Mesures / provenance	Assistive	Oui	Sites sensibles	Oui	Oui
22	Water	Ressource / réseau / actif	Captage → assainissement	Socle	Capteurs / prélèvements	Assistive	Oui	Abonnés / plans	Oui	Oui
23	Telecom	Site / réseau / équipement	Actifs&opérations réseau	Socle	Configurations / anomalies	Assistive	Oui	Réseau / abonnés	Oui	Oui
24	Tourisme	Établissement / réservation / billet	Parcours&prestation	Socle	Acteurs / prestations	Assistive	Oui	Voyageur / séjour	Oui	Oui
25	Insurance	Assuré / contrat / sinistre	Contrat&sinistre	Socle	Fraude présumée	Assistive	Oui	Dossiers / finance	Oui	Oui
26	Real Estate / Property	Parcelle / bâtiment / droit	Cycle de vie immobilier	Socle	Titres / BIM / transactions	Assistive	Oui	Droits / occupation	Oui	Oui
27	Public Administration	Administration / agent / dossier	Démarche&acte	Socle	Décisions / habilitations	Assistive	Oui	Dossiers citoyens	Oui	Oui
28	Defense	Institution / personnel / soutien	Administratif non opérationnel	Ciblé	Habilitations / preuves	Assistive	Oui	Besoin d’en connaître	Oui	Oui
29	Media / AP Informations	Média / source / contenu	Production&diffusion	Socle	Contenus / provenance	Assistive	Oui	Sources / embargos	Oui	Oui
30	Government	Institution / mandat / acte	Cycle institutionnel	Socle	Mandats / signatures	Assistive	Oui	Institutionnelle	Oui	Oui

Principes transversaux

• Le Passeport Numérique constitue la mémoire sectorielle ; le QR reste une porte de vérification et non l’identité elle-même.

• Deep Authenticity© produit des signaux explicables : il ne prononce pas automatiquement fraude, conformité, responsabilité ou vérité.

• L’IA demeure assistive et sous contrôle humain ou institutionnel lorsque la décision exige une autorité compétente.

• L’interopérabilité relie les systèmes sans imposer leur centralisation ni transférer leur autorité à Authenticity Plus©.

• AP Ledger conserve des empreintes minimales d’événements critiques ; les dossiers complets, secrets et données sensibles restent hors des couches publiques ou irréversibles.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME IV — APPLICATIONS SECTORIELLES

CONCLUSION GÉNÉRALE ET CLÔTURE OFFICIELLE

DES 30 APPLICATIONS SECTORIELLES À L'ÉCOSYSTÈME UNIFIÉ DE CONFIANCE

1. Objet de la conclusion

Cette conclusion clôt le Volume IV après la définition des trente applications sectorielles, leur synthèse générale et leur matrice transversale. Elle fixe les acquis fonctionnels du volume et prépare leur articulation avec la suite du Livre Blanc 2026.

2. Du socle technologique aux usages sectoriels

Le Volume IV démontre comment les principes d'Authenticity Plus© / Deep Authenticity© peuvent être appliqués à des environnements très différents sans perdre leur cohérence : identité, provenance, chronologie, certification, vérification, contrôle d'accès, interopérabilité, audit et continuité.

3. Trente applications, une architecture commune

Les trente applications ne sont pas conçues comme trente systèmes isolés. Elles partagent un langage commun de preuve et de confiance, tout en conservant leurs objets, acteurs, normes, responsabilités, autorités et niveaux de sensibilité propres.

4. Le Passeport Numérique comme mémoire

Le Passeport Numérique constitue la mémoire structurée d'un objet, d'un document, d'un actif, d'un droit, d'un contenu, d'une organisation ou d'une institution. Il relie l'état courant à son historique sans effacer les versions et événements antérieurs.

5. Identité, rôle et autorité

Le Volume IV maintient une séparation constante entre identité, rôle, mandat, propriété, détention, expertise, validation et autorité. Une infrastructure technique peut vérifier une preuve ou une attribution sans acquérir la compétence juridique ou professionnelle de l'acteur concerné.

6. Provenance comme fil directeur

La provenance relie chaque information à sa source. Déclaration, observation, document, signature, expertise, registre et décision officielle restent distingués afin que le système n'accorde jamais à une donnée un niveau d'autorité supérieur à celui qu'elle possède réellement.

7. Continuité de la preuve

Le système est conçu pour préserver la chaîne documentaire malgré transfert, succession, changement de propriétaire, changement d'opérateur, remplacement d'un responsable, migration de système ou réorganisation institutionnelle.

8. QR Codes et vérification

Les QR Codes dynamiques fournissent une interface de vérification adaptée au contexte. Ils donnent accès aux informations autorisées et au statut pertinent sans constituer eux-mêmes la preuve complète ni exposer automatiquement les dossiers sous-jacents.

9. Deep Authenticity©

Deep Authenticity© constitue la couche transversale de confrontation des preuves. Elle peut détecter des incohérences entre identités, documents, images, signatures, versions, droits, événements et chronologies, puis restituer des signaux explicables nécessitant une vérification appropriée.

10. Refus du verdict algorithmique automatique

Le Volume IV adopte un principe commun aux trente secteurs : un score, une anomalie ou un signal technique ne devient pas automatiquement une décision de fraude, falsification, conformité, propriété, responsabilité, vérité, diagnostic ou légalité.

11. Intelligence artificielle sous gouvernance

L'IA peut assister les acteurs dans la recherche, la comparaison, le classement, la traduction, l'analyse et la détection d'incohérences. Elle demeure soumise à la traçabilité, au versioning, à l'explicabilité appropriée et au contrôle humain ou institutionnel requis.

12. Confidentialité et minimisation

La vérifiabilité n'exige pas la publication universelle des données. Les architectures sectorielles privilégient le partage sélectif, le moindre privilège et la minimisation, notamment pour les données personnelles, médicales, patrimoniales, commerciales, judiciaires, militaires ou institutionnelles.

13. Souveraineté

La souveraineté est compatible avec l'interopérabilité. Une preuve peut demeurer dans son domaine juridique, institutionnel ou opérationnel tandis que des références, attestations, empreintes ou résultats vérifiables permettent les échanges nécessaires.

14. Interopérabilité sans centralisation absolue

Authenticity Plus© fournit une couche commune de confiance sans imposer qu'un registre central possède toutes les données. Les systèmes métiers, registres, institutions et partenaires conservent leurs fonctions et responsabilités propres.

15. Cybersécurité et révocation

Identités, comptes, certificats, clés, API, QR et mécanismes de signature doivent être protégés, supervisés et révocables. La compromission d'un accès futur ne doit pas permettre de réécrire silencieusement l'historique des preuves antérieures.

16. Auditabilité

Les opérations critiques doivent pouvoir être reconstruites selon les droits applicables : qui a créé, déclaré, signé, validé, transféré, modifié, publié, révoqué ou audité. L'audit reste proportionné et n' ouvre pas automatiquement tous les contenus protégés.

17. AP Ledger

AP Ledger fournit une mémoire minimale des événements critiques par l'ancrage d'empreintes et références nécessaires à l'intégrité et à la chronologie. Les documents complets, secrets, clés et données sensibles restent hors des couches publiques ou irréversibles lorsque leur protection l'exige.

18. Portée probatoire et limites

Authenticity Plus© peut renforcer la preuve d'existence, de date, d'intégrité, d'attribution et de provenance. Cette capacité ne constitue pas une promesse universelle d'opposabilité : la portée juridique dépend du contexte, des mécanismes utilisés et du droit applicable.

19. Acquis du Volume IV

Le Volume IV dispose désormais de trente applications sectorielles structurées, d'une synthèse générale et d'une matrice transversale. Il établit la cohérence fonctionnelle de l'écosystème depuis les usages individuels et économiques jusqu'aux infrastructures, médias, administrations et institutions gouvernementales.

20. Clôture officielle du Volume IV

Le Volume IV — Applications Sectorielles est officiellement clôturé dans son architecture fonctionnelle. Il démontre qu'Authenticity Plus© / Deep Authenticity© peut fournir une infrastructure de confiance fédérable et sectoriellement adaptable, fondée non sur la centralisation de toute l' information, mais sur la continuité vérifiable des identités, preuves, droits, versions et événements. La suite du Livre Blanc pourra désormais s'appuyer sur ce corpus consolidé pour traiter les dimensions de déploiement, gouvernance globale, adoption, industrialisation ou autres volumes prévus par l' architecture éditoriale générale.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME V

DONNÉES, IA ET INTELLIGENCE SYSTÉMIQUE

DOCUMENT MAÎTRE CONSOLIDÉ

20 CHAPITRES

Donnée gouvernée → Analyse explicable → Veille continue → Anticipation → Intelligence systémique → Simulation → Décision assistée → Responsabilité humaine → Mémoire vérifiable

SOMMAIRE GÉNÉRAL

CHAPITRE 1 — ARCHITECTURE DES DONNÉES, IA ET INTELLIGENCE SYSTÉMIQUE

CHAPITRE 2 — DONNÉES INTERNES ET EXTERNES

CHAPITRE 3 — ANALYSE STATISTIQUE ET INTELLIGENCE DES TENDANCES

CHAPITRE 4 — DÉTECTION D'ANOMALIES

CHAPITRE 5 — WATCH SYSTEM©

CHAPITRE 6 — SIGNAUX FAIBLES ET DÉTECTION PRÉCOCE

CHAPITRE 7 — TABLEAUX DE BORD ÉCONOMIQUES ET SOCIAUX PRÉVISIONNELS

CHAPITRE 8 — PÉNURIES ET TENSIONS

CHAPITRE 9 — SURPLUS ET CAPACITÉS EXCÉDENTAIRES

CHAPITRE 10 — DISPARITÉS

CHAPITRE 11 — CARTOGRAPHIE DYNAMIQUE©

CHAPITRE 12 — INTELLIGENCE PRÉDICTIVE

CHAPITRE 13 — INTELLIGENCE SYSTÉMIQUE INTERSECTORIELLE

CHAPITRE 14 — SIMULATION, SCÉNARIOS ET STRESS TESTS

CHAPITRE 15 — IA DÉCISIONNELLE ASSISTIVE

CHAPITRE 16 — GOUVERNANCE, SOUVERAINETÉ ET SÉCURITÉ DES DONNÉES ET DES MODÈLES IA

CHAPITRE 17 — DEEP AUTHENTICITY© APPLIQUÉ AUX DONNÉES ET AUX MODÈLES IA

CHAPITRE 18 — AP LEDGER ET MÉMOIRE ANALYTIQUE

CHAPITRE 19 — CENTRE D'INTELLIGENCE SYSTÉMIQUE

MISE À NIVEAU TRANSVERSALE — PASSEPORT NUMÉRIQUE UNIVERSEL

DE L'ÉVÉNEMENT VÉRIFIABLE À L'INTELLIGENCE SYSTÉMIQUE GOUVERNÉE

Le Passeport Numérique Universel constitue une source structurée d'événements vérifiables pour les capacités analytiques de Deep Authenticity©. Activation, transfert, maintenance, rappel, changement de statut ou fin de vie appartiennent d'abord à l'histoire d'un actif déterminé ; leur exploitation analytique exige sélection, minimisation, pseudonymisation ou agrégation selon la finalité et les droits applicables.

Le Volume V distingue strictement : données individuelles ou événementielles ; données agrégées ou statistiques ; données estimées ou prédites ; données simulées. Une information issue d'un Passeport Numérique Universel ne devient pas automatiquement une vérité statistique, et une prédiction ou simulation ne doit jamais être présentée comme un fait observé.

Chaque donnée analytique doit conserver sa provenance, sa temporalité et, lorsque pertinent, son niveau d'assurance. Les événements issus des mécanismes natifs de vérité, des acteurs autorisés, des IoT, ERP ou sources externes ne possèdent pas nécessairement la même force probante.

AP Core orchestre les identités, événements, droits et contextes avant exploitation analytique. Un modèle d'IA peut détecter tendances, anomalies, corrélations et signaux faibles, mais ses résultats restent probabilistes et ne modifient pas directement l'histoire de preuve du Passeport Numérique Universel.

Watch System© peut observer des flux agrégés d'événements : variations anormales de statuts, anomalies de transfert, rappels, tensions logistiques ou comportements atypiques. Une alerte déclenche une vérification appropriée ; elle ne constitue pas, à elle seule, une conclusion de fraude ou de causalité.

Les tableaux de bord et la Cartographie Dynamique© peuvent présenter des indicateurs issus de données gouvernées en distinguant clairement source, période, couverture, granularité et incertitude. Les vues institutionnelles privilégient les agrégats nécessaires et ne doivent pas exposer inutilement l' identité ou la localisation d'un propriétaire individuel.

Les événements vérifiables et agrégés issus des passeports peuvent contribuer aux Jumeaux Numériques et à la Simulation Institutionnelle Profonde. Le Passeport constitue la couche de réalité observée ; les modèles ajoutent représentation, estimation et scénarios. Ces niveaux restent séparés.

Chaîne analytique de référence : Passeport Numérique Universel → événements vérifiables → gouvernance et minimisation → agrégation → indicateurs → Watch System© et signaux faibles → tableaux de bord → prévision → Jumeaux Numériques → simulation → décision assistée et responsabilité humaine.

Invariant : l'IA, les statistiques et la simulation complètent la preuve mais ne remplacent jamais les mécanismes déterministes d'authenticité ni l'autorité compétente.

CHAPITRE 20 — SYNTHÈSE GÉNÉRALE, CRITÈRES D'ACCEPTATION ET CLÔTURE DU VOLUME V

Note de consolidation. Le présent document rassemble les vingt chapitres du Volume V dans leur ordre de production. Les formulations, distinctions conceptuelles, garde-fous de gouvernance et chaînes de traçabilité sont conservés afin de constituer une référence maîtresse unique.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME V — DONNÉES, IA ET INTELLIGENCE SYSTÉMIQUE

CHAPITRE 1 — ARCHITECTURE DES DONNÉES, IA ET INTELLIGENCE SYSTÉMIQUE

DE LA DONNÉE AUTHENTIFIÉE À L'OBSERVATION, L'ANALYSE, L'ANTICIPATION ET L'AIDE À LA DÉCISION

1. Objet du Volume V

Le Volume V transforme les données authentifiées, documentées et gouvernées de l'écosystème Authenticity Plus© en capacités d'observation, d'analyse, de détection, d'anticipation et d'aide à la décision. Il relie données internes et externes, analyse statistique, détection d'anomalies, Watch System©, signaux faibles, tableaux de bord, pénuries, surplus, disparités, Cartographie Dynamique© et intelligence prédictive.

2. De la confiance documentaire à l'intelligence systémique

Les volumes précédents structurent identité, provenance, preuve, sécurité, architecture et applications sectorielles. Le Volume V exploite ces fondations pour comprendre les relations entre événements, secteurs, territoires et périodes, sans confondre la qualité de la preuve avec la certitude d'une interprétation.

3. Chaîne de valeur analytique

L'architecture suit une chaîne explicite : source → acquisition → qualification → provenance → normalisation → enrichissement → analyse → détection → prévision → visualisation → alerte → recommandation → décision humaine ou institutionnelle. Chaque étape doit rester identifiable et auditable selon sa criticité.

4. Donnée brute, donnée qualifiée et indicateur

Une donnée brute est conservée avec son contexte d'origine. Une donnée qualifiée résulte de contrôles documentés. Un indicateur est une construction méthodologique dérivée d'une ou plusieurs données. Ces trois niveaux ne doivent jamais être présentés comme équivalents.

5. Données internes

Les données internes proviennent des composants, applications sectorielles, Passeports Numériques, événements, systèmes autorisés et autres sources propres à l'écosystème. Leur usage analytique reste limité par leur finalité, leur niveau d'accès et les règles de gouvernance applicables.

6. Données externes

Les données externes peuvent provenir de sources publiques, institutionnelles, scientifiques, économiques, sociales, territoriales, environnementales ou partenaires autorisés. Chaque source conserve identité, date, conditions d'usage, méthode disponible, fréquence de mise à jour et niveau de confiance.

7. Provenance analytique

Toute analyse importante doit pouvoir être reliée aux données et versions qui l'ont produite. Deep Authenticity© conserve la distinction entre donnée originale, transformation, enrichissement, estimation, prédiction et interprétation.

8. Qualité et fraîcheur

Complétude, exactitude disponible, cohérence, granularité, représentativité, fréquence, latence et fraîcheur influencent l'analyse. Une donnée ancienne ou incomplète peut rester utile si sa limite est explicitement conservée.

9. Analyse statistique

Le moteur analytique peut produire distributions, tendances, variations, corrélations, comparaisons, séries temporelles et autres mesures pertinentes. Méthode, population, période, unité et incertitude doivent accompagner les résultats lorsqu'elles conditionnent leur interprétation.

10. Détection d'anomalies

Les mécanismes de détection recherchent ruptures, valeurs atypiques, incohérences, changements de régime ou comportements inhabituels. Une anomalie est un signal à examiner ; elle ne constitue automatiquement ni fraude, ni panne, ni crise.

11. Watch System©

Watch System© constitue la couche de veille continue. Il observe des indicateurs et événements autorisés, applique des règles ou modèles versionnés, détecte les changements significatifs et produit des alertes graduées selon criticité, confiance et horizon temporel.

12. Signaux faibles

Un signal faible est une indication précoce, limitée ou dispersée pouvant annoncer une évolution plus importante. Le système conserve sa source, sa fréquence, son niveau de confiance et les éléments qui renforcent ou affaiblissent l'hypothèse au fil du temps.

13. Pénuries et tensions

L'intelligence systémique peut rapprocher stocks, capacités, flux, consommation, saisonnalité, incidents, importations, production et autres facteurs disponibles afin d'identifier des risques de pénurie. Une prévision de tension reste probabiliste et doit afficher son horizon et ses hypothèses.

14. Surplus et capacités disponibles

Le système peut également identifier excédents, surproduction, stocks élevés ou capacités sous-utilisées. Pénurie et surplus peuvent coexister dans des territoires, périodes ou segments différents ; l'analyse doit donc préserver la granularité.

15. Disparités

Les tableaux de bord peuvent mesurer des écarts entre territoires, populations, secteurs, infrastructures ou niveaux d'accès lorsque les données le permettent. Une disparité statistique ne doit pas être transformée automatiquement en explication causale.

16. Cartographie Dynamique©

La Cartographie Dynamique© représente spatialement ressources, flux, événements, indicateurs, anomalies, tensions et projections. Les couches géographiques sont datées, versionnées et filtrées selon les droits afin d'éviter l'exposition de localisations ou populations sensibles.

17. Intelligence prédictive

Les modèles prédictifs estiment des trajectoires possibles à partir des informations disponibles. Chaque prévision conserve modèle, version, horizon, variables principales, date de calcul et niveau d' incertitude approprié. Une prévision n'est jamais présentée comme un futur certain.

18. Intelligence systémique

L'intelligence systémique analyse les interdépendances : un événement dans l'eau, l'énergie, l' agriculture, le transport, la santé, l'emploi ou les prix peut produire des effets dans d'autres secteurs. L'objectif est d'identifier les chaînes possibles d'impact sans réduire les phénomènes complexes à une causalité unique.

19. Contrôle humain, gouvernance et souveraineté

Les alertes, scénarios et recommandations sont soumis à des droits d'accès, à la traçabilité et au contrôle des acteurs compétents. L'architecture ne doit pas devenir un système de surveillance généralisée des citoyens ; elle privilégie données agrégées, minimisation, finalité et protection des informations sensibles.

20. Principes d'acceptation du Chapitre 1

L'architecture est acceptable si donnée, indicateur, anomalie, prévision et décision restent distincts ; si toute analyse importante conserve sa provenance ; si les modèles sont versionnés ; si l'incertitude est visible ; si les données sensibles sont protégées ; et si l'IA reste un instrument d'observation et d' aide à la décision plutôt qu'une autorité autonome.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME V — DONNÉES, IA ET INTELLIGENCE SYSTÉMIQUE

CHAPITRE 2 — DONNÉES INTERNES ET EXTERNES

ACQUISITION, SOURCES, QUALITÉ, PROVENANCE, NORMALISATION, TEMPORALITÉ ET GOUVERNANCE DES DONNÉES

1. Objet du chapitre

Ce chapitre définit la matière première de l'intelligence systémique : les données internes et externes. Il organise leur acquisition, identification, provenance, qualification, normalisation, temporalité, accès et gouvernance afin que les analyses du Volume V reposent sur des sources traçables et interprétables.

2. Principe de pluralité des sources

Aucune source unique ne doit être considérée comme une représentation complète du réel. L' architecture peut croiser plusieurs sources indépendantes ou complémentaires, tout en conservant leurs différences de méthode, de fréquence, de granularité et d'autorité.

3. Données internes Authenticity Plus©

Les Passeports Numériques, événements de cycle de vie, certifications, statuts, journaux autorisés et applications sectorielles peuvent alimenter la couche analytique. Leur réutilisation respecte les finalités, droits d'accès et niveaux de confidentialité associés.

4. Données opérationnelles

Stocks, capacités, flux, production, maintenance, délais, consommation, incidents ou autres mesures opérationnelles peuvent contribuer à l'analyse lorsque leur usage est autorisé. Leur contexte métier reste attaché à la donnée afin d'éviter les interprétations hors contexte.

5. Données institutionnelles

Statistiques officielles, registres, publications, indicateurs économiques ou sociaux et autres données institutionnelles peuvent être intégrés avec leur organisme d'origine, période, méthode, date de publication et éventuelles révisions.

6. Données scientifiques et environnementales

Mesures de laboratoire, capteurs, observations environnementales, données météorologiques, hydrologiques, agricoles ou autres sources scientifiques peuvent être exploitées en conservant unité, méthode, localisation appropriée, incertitude et conditions de mesure.

7. Données économiques et sociales

Prix, emploi, activité, consommation, commerce, mobilité, démographie ou autres indicateurs peuvent être rapprochés lorsque les définitions et périodes sont compatibles. Une comparaison statistique ne doit pas masquer les différences méthodologiques entre sources.

8. Données partenaires et privées

Des partenaires autorisés peuvent fournir des données contractuelles ou opérationnelles. Les droits d'usage, limites de redistribution, confidentialité et durée de conservation doivent être enregistrés avec la source.

9. Acquisition et connecteurs

L'acquisition peut utiliser API, fichiers, flux, bases autorisées, capteurs ou saisies contrôlées. Chaque connecteur dispose d'une identité technique, d'un périmètre, d'une fréquence et de mécanismes de supervision et révocation.

10. Registre des sources

Un registre de sources conserve identité, propriétaire ou émetteur, type, domaine, fréquence, conditions d'usage, schéma, historique des versions et statut de confiance. Une source retirée reste identifiable dans les analyses historiques qui l'ont utilisée.

11. Provenance de bout en bout

La provenance relie chaque donnée à sa source et chaque transformation à son processus. Une valeur dérivée doit pouvoir être distinguée d'une valeur observée ou déclarée.

12. Qualification des données

La qualification peut contrôler format, unité, plage plausible, doublons, valeurs manquantes, cohérence temporelle et concordance avec d'autres sources. Un contrôle réussi n'équivaut pas à une garantie universelle d'exactitude.

13. Normalisation

Unités, nomenclatures, identifiants, catégories, formats temporels et géographiques peuvent être harmonisés pour permettre les analyses croisées. La valeur originale et la règle de transformation restent conservées lorsque cela est nécessaire à l'audit.

14. Résolution d'identité

Lorsque plusieurs systèmes décrivent le même objet, territoire, organisation ou événement, des mécanismes de rapprochement peuvent proposer une correspondance. Les correspondances incertaines restent marquées comme telles et ne sont pas fusionnées silencieusement.

15. Temporalité

Date de mesure, date d’événement, date de réception, date de publication et date de traitement sont distinguées. Cette séparation est essentielle pour analyser retards, révisions et signaux en temps réel ou différé.

16. Fraîcheur et fréquence

Chaque jeu de données possède une fréquence et une fraîcheur attendues. Watch System© peut signaler une source en retard, interrompue ou inhabituellement stable lorsque cela affecte l’analyse.

17. Données manquantes et biais

Les absences, changements de couverture, ruptures de séries et biais connus doivent être visibles. L’IA ne doit pas combler silencieusement une donnée manquante comme si elle avait été réellement observée.

18. Gouvernance et droits d’accès

Les droits distinguent consultation, analyse, export, partage et administration. Les données personnelles ou sensibles sont minimisées, agrégées ou pseudonymisées lorsque l’objectif analytique peut être atteint sans identification directe.

19. Deep Authenticity© et AP Ledger

Deep Authenticity© peut confronter source, schéma, fréquence, historique, transformations et données associées afin de détecter incohérences ou substitutions. AP Ledger peut ancrer des empreintes minimales de versions de jeux de données, règles de transformation et événements critiques sans publier les contenus protégés.

20. Critères d’acceptation et conclusion

Le modèle est acceptable si toute donnée analytique importante possède une source identifiable ; si original, transformation et estimation restent distincts ; si les méthodes de normalisation sont auditables ; si les temporalités sont explicites ; si les données manquantes et biais sont visibles ; et si l’accès reste proportionné à la finalité. Le Volume V dispose ainsi d’une base de données gouvernée avant toute analyse statistique ou prédictive.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME V — DONNÉES, IA ET INTELLIGENCE SYSTÉMIQUE

CHAPITRE 3 — ANALYSE STATISTIQUE ET INTELLIGENCE DES TENDANCES

SÉRIES TEMPORELLES, DISTRIBUTIONS, SAISONNALITÉ, CORRÉLATIONS, INDICATEURS, COMPARAISONS, RUPTURES ET INCERTITUDE

1. Objet du chapitre

Ce chapitre transforme les données gouvernées du Chapitre 2 en informations statistiques interprétables. Il structure les séries temporelles, distributions, tendances, saisonnalités, comparaisons, corrélations, indicateurs composites, ruptures et mesures d'incertitude qui alimenteront ensuite la détection d'anomalies, Watch System© et l'intelligence prédictive.

2. Principe de traçabilité statistique

Tout résultat statistique important doit pouvoir être relié à ses sources, à la population étudiée, à la période, aux filtres, aux transformations et à la méthode utilisée. Un graphique ou un indicateur ne doit jamais devenir une donnée sans origine identifiable.

3. Statistique descriptive

Moyenne, médiane, quantiles, dispersion, fréquence, proportion et autres mesures descriptives peuvent résumer un ensemble de données. Le choix de la mesure doit rester adapté à la distribution et au phénomène observé.

4. Distributions

L'analyse des distributions permet d'identifier concentration, dispersion, asymétrie, extrêmes et évolution de la structure d'une population ou d'un indicateur. Une moyenne stable peut masquer des changements importants dans la distribution sous-jacente.

5. Séries temporelles

Les séries temporelles organisent les observations selon le temps et permettent d'étudier niveau, évolution, cycles et ruptures. Date de mesure, fréquence, données manquantes et changements méthodologiques restent visibles.

6. Tendances

Une tendance décrit une évolution persistante observée sur une période donnée. Elle ne doit pas être extrapolée automatiquement au-delà de l'horizon où les données et hypothèses restent pertinentes.

7. Saisonnalité

Les variations récurrentes liées aux saisons, calendriers, cycles économiques, agricoles, scolaires ou autres rythmes peuvent être distinguées des tendances de fond. Une hausse saisonnière attendue ne doit pas être confondue avec une anomalie structurelle.

8. Cycles et régimes

Certains phénomènes évoluent par cycles ou régimes successifs. L'analyse peut identifier des phases d'expansion, ralentissement, tension ou normalisation sans supposer que les cycles futurs reproduiront exactement les cycles passés.

9. Comparaisons temporelles

Les comparaisons peuvent porter sur période précédente, année précédente, moyenne historique ou référence définie. La période de comparaison doit être explicitée pour éviter des conclusions produites par un choix arbitraire de base.

10. Comparaisons territoriales

Régions, wilayas, communes, zones économiques ou autres territoires peuvent être comparés lorsque les définitions et couvertures sont compatibles. Taille de population, structure économique, géographie et autres facteurs de contexte doivent être pris en compte.

11. Comparaisons sectorielles

Les secteurs peuvent être comparés selon production, emploi, prix, capacité, consommation, incidents ou autres indicateurs compatibles. Des métriques normalisées peuvent être nécessaires pour comparer des secteurs de tailles différentes.

12. Corrélations

Les corrélations mesurent des associations statistiques entre variables. Elles peuvent aider à identifier des relations à examiner, mais ne démontrent pas à elles seules qu'une variable cause l' autre.

13. Décalages temporels

Une variable peut précéder ou suivre une autre avec un délai. L'analyse des décalages aide à détecter des relations potentielles entre événements, mais exige une interprétation prudente des facteurs intermédiaires et du contexte.

14. Indicateurs composites

Plusieurs variables peuvent être combinées dans un indice ou score lorsque la méthode, les pondérations, les normalisations et les limites sont documentées. Un indice composite ne doit pas masquer les composantes qui expliquent son évolution.

15. Référentiels et seuils

Les résultats peuvent être comparés à des seuils réglementaires, historiques, statistiques, opérationnels ou définis par des experts compétents. L'origine du seuil et sa portée doivent être conservées.

16. Ruptures de tendance

Une rupture correspond à un changement significatif de niveau, pente, volatilité ou structure. Elle peut résulter d'un événement réel, d'une modification de collecte ou d'un changement méthodologique ; ces hypothèses doivent être distinguées.

17. Incertitude statistique

Échantillonnage, erreurs de mesure, données manquantes, révisions et modèles introduisent de l' incertitude. Lorsque cela est pertinent, les résultats présentent intervalles, marges, scénarios ou autres indications permettant de comprendre cette incertitude.

18. Qualité statistique et biais

Représentativité, couverture, biais de sélection, survivance, changements de définition et effets de composition peuvent influencer les conclusions. Une grande quantité de données ne garantit pas automatiquement une analyse représentative.

19. Deep Authenticity© et préparation de Watch System©

Deep Authenticity© peut vérifier la cohérence entre source, période, méthode, transformations et résultat publié. Les tendances, distributions, saisonnalités et ruptures établissent ensuite les références nécessaires au moteur de détection d'anomalies et à Watch System©.

20. Critères d'acceptation et conclusion

L'analyse statistique est acceptable si chaque résultat conserve sa provenance et sa méthode ; si corrélation et causalité restent distinctes ; si les comparaisons utilisent des bases compatibles ; si saisonnalité et tendance sont différenciées ; si les ruptures sont contextualisées ; et si l'incertitude et les biais significatifs restent visibles. Ce socle prépare le Chapitre 4 consacré à la détection d' anomalies.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME V — DONNÉES, IA ET INTELLIGENCE SYSTÉMIQUE

CHAPITRE 4 — DÉTECTION D'ANOMALIES

ANOMALIES PONCTUELLES, COLLECTIVES, TEMPORELLES ET GÉOGRAPHIQUES — CHANGEMENTS DE RÉGIME — SCORING — CONFIANCE — FAUX POSITIFS — VALIDATION HUMAINE

1. Objet du chapitre

Ce chapitre définit la couche de détection d'anomalies du Volume V. Elle transforme les références statistiques du Chapitre 3 en mécanismes capables de signaler des observations, groupes, trajectoires ou territoires qui s'écartent de comportements attendus, sans transformer automatiquement cet écart en diagnostic, fraude, panne ou crise.

2. Définition d'une anomalie

Une anomalie est un écart significatif par rapport à une référence définie : historique, statistique, saisonnière, territoriale, sectorielle, opérationnelle ou experte. La référence utilisée doit être conservée avec le signal.

3. Anomalies ponctuelles

Une observation isolée peut être inhabituelle par sa valeur, sa fréquence ou son contexte. Le système vérifie notamment unité, source, temporalité et qualité avant de considérer l'écart comme un signal exploitable.

4. Anomalies collectives

Un groupe d'observations peut devenir anormal alors qu'aucune valeur prise séparément ne dépasse un seuil. Cette détection permet d'identifier des configurations inhabituelles, concentrations ou combinaisons de facteurs.

5. Anomalies temporelles

Une variation peut être normale à une période et anormale à une autre. Les modèles tiennent compte des tendances, cycles, saisonnalités, jours particuliers et autres références temporelles disponibles.

6. Anomalies géographiques

La Cartographie Dynamique© peut identifier des écarts spatiaux : concentration inhabituelle, rupture territoriale, propagation ou différence persistante entre zones comparables. Les effets de population, taille et couverture des données doivent être normalisés.

7. Anomalies multivariées

Plusieurs variables peuvent former ensemble une configuration atypique. Le système conserve les variables principales ayant contribué au signal afin de faciliter son interprétation.

8. Changements de régime

Un changement durable de niveau, volatilité, relation entre variables ou structure peut signaler le passage à un nouveau régime. Le moteur distingue autant que possible rupture réelle, modification de collecte et changement méthodologique.

9. Références dynamiques

Les références peuvent évoluer lorsque le système dispose de nouvelles données. Toute mise à jour importante du référentiel ou du modèle reste versionnée afin qu'un ancien signal puisse être reproduit dans son contexte historique.

10. Méthodes de détection

Le moteur peut combiner règles, seuils statistiques, modèles temporels, méthodes multivariées et apprentissage automatique selon les cas. La méthode choisie doit être proportionnée à la donnée et à la conséquence potentielle du signal.

11. Score d'anomalie

Un score peut exprimer l'intensité de l'écart. Il ne représente pas automatiquement une probabilité de fraude ou de crise. Sa définition, son échelle et son interprétation doivent être documentées.

12. Niveau de confiance

Le niveau de confiance dépend notamment de la qualité des données, de la stabilité de la référence, du nombre de sources concordantes et de la robustesse du modèle. Intensité de l'anomalie et confiance dans le signal restent deux dimensions distinctes.

13. Criticité

La criticité combine le signal avec l'impact potentiel, le secteur, le territoire, l'horizon et les règles applicables. Une anomalie statistiquement forte peut avoir une faible criticité opérationnelle, et inversement.

14. Faux positifs

Le système doit mesurer et suivre les alertes finalement considérées comme normales ou explicables. Les faux positifs servent à améliorer règles et modèles, sans effacer l'historique des décisions prises.

15. Faux négatifs et événements manqués

Lorsque des événements réels n’ont pas été détectés, leur analyse peut révéler des limites de couverture, de seuil, de fréquence ou de modèle. La performance du système ne doit pas être évaluée uniquement sur les alertes émises.

16. Validation humaine ou experte

Les anomalies à conséquence significative sont examinées par les acteurs compétents selon le domaine. Le validateur peut confirmer, expliquer, reclasser ou rejeter le signal, avec conservation de la justification et de la date.

17. Explicabilité

Chaque alerte doit présenter les éléments utiles à sa compréhension : variables concernées, référence, période, territoire, amplitude, sources et facteurs principaux. Un signal impossible à expliquer doit être traité avec prudence.

18. Deep Authenticity©

Deep Authenticity© confronte provenance, versions, identités de sources, transformations et chronologies afin de distinguer autant que possible anomalie du phénomène et anomalie de la donnée elle-même. Une substitution ou rupture de provenance peut ainsi être signalée séparément.

19. Préparation de Watch System©

Les anomalies validées, seuils, niveaux de confiance et criticités alimentent Watch System©. Celui-ci organise la veille continue, la persistance des signaux, les escalades, les corrélations intersectorielles et la détection des signaux faibles.

20. Critères d’acceptation et conclusion

Le moteur est acceptable si anomalie et verdict restent distincts ; si la référence est identifiable ; si score, confiance et criticité ne sont pas confondus ; si les faux positifs et événements manqués sont suivis ; si les modèles restent versionnés ; et si les alertes importantes peuvent être expliquées et validées. Ce socle ouvre le Chapitre 5 consacré à Watch System©.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME V — DONNÉES, IA ET INTELLIGENCE SYSTÉMIQUE

CHAPITRE 5 — WATCH SYSTEM©

VEILLE CONTINUE — CONVERGENCE DES SIGNAUX — NIVEAUX D'ALERTE — PERSISTANCE — ESCALADE — SURVEILLANCE INTERSECTORIELLE — ANTICIPATION SYSTÉMIQUE

1. Objet du chapitre

Watch System© constitue la couche de veille continue du Volume V. Il transforme données, indicateurs, anomalies et événements authentifiés en un dispositif d'observation évolutif capable de détecter persistance, convergence et propagation de signaux dans le temps, entre territoires et entre secteurs.

2. Principe de veille continue

La veille n'implique pas une surveillance généralisée des personnes. Watch System© observe prioritairement des indicateurs, flux, capacités, ressources, événements et données agrégées ou autorisées, selon des finalités définies et des droits d'accès contrôlés.

3. Objets surveillés

Un objet de veille peut être un indicateur économique, social, environnemental, sanitaire, industriel, logistique, énergétique, agricole ou institutionnel, ainsi qu'un flux, une capacité, un stock, un territoire ou une combinaison documentée de variables.

4. Profil de veille

Chaque objet conserve son profil : sources, fréquence, référence, seuils, saisonnalité, modèle éventuel, criticité, responsables autorisés et règles d'escalade. Les modifications de profil sont versionnées.

5. Observation en temps réel et différé

Certaines sources peuvent être proches du temps réel tandis que d'autres sont quotidiennes, mensuelles ou trimestrielles. Watch System© respecte la fréquence réelle de chaque source et ne présente pas une donnée différée comme une observation instantanée.

6. Niveaux de signal

Les observations peuvent être classées selon des niveaux gradués : information, vigilance, anomalie, alerte et alerte critique, ou toute nomenclature institutionnelle autorisée. Le niveau reflète la situation analytique et non un verdict automatique.

7. Persistance

Une anomalie isolée peut être temporaire. La persistance mesure la durée ou la répétition d'un signal et permet de distinguer un événement ponctuel d'une évolution susceptible de devenir structurelle.

8. Convergence de signaux

Plusieurs signaux indépendants peuvent renforcer une même hypothèse. Watch System© conserve les sources et contributions séparément afin qu'une convergence apparente ne masque pas une dépendance entre données provenant en réalité de la même origine.

9. Propagation territoriale

La Cartographie Dynamique© peut suivre l'apparition, l'extension, la contraction ou le déplacement d' un signal entre territoires. La propagation observée reste distinguée d'une projection de propagation future.

10. Propagation intersectorielle

Un signal dans un secteur peut précéder des effets dans d'autres : transport et logistique peuvent affecter disponibilité et prix ; eau et énergie peuvent affecter agriculture ou industrie. Le système construit des relations à examiner sans imposer une causalité unique.

11. Corrélation des événements

Les événements peuvent être rapprochés selon temps, territoire, secteur, ressource, acteur institutionnel ou autre dimension autorisée. Une corrélation événementielle constitue une piste analytique et non une preuve causale.

12. Escalade

Lorsqu'un signal franchit des règles de persistance, confiance, criticité ou convergence, il peut être escaladé vers un niveau ou un acteur compétent. L'escalade conserve motif, date, version des règles et destinataire.

13. Désescalade et retour à la normale

Une alerte peut être abaissée ou clôturée lorsque les indicateurs se normalisent ou qu'une explication validée est disponible. L'historique reste conservé afin d'analyser les épisodes et la performance des mécanismes de veille.

14. Watchlists thématiques

Des vues spécialisées peuvent suivre alimentation, eau, énergie, santé, emploi, prix, transport, environnement, infrastructures ou autres domaines autorisés. Les watchlists partagent le socle commun tout en conservant leurs seuils et experts propres.

15. Watch System© intersectoriel

Une couche transversale rapproche les watchlists afin d'identifier des combinaisons de signaux susceptibles d'annoncer un phénomène systémique. Cette couche privilégie les relations explicables et la traçabilité des contributions.

16. Explicabilité de l'alerte

Chaque alerte importante doit pouvoir répondre à des questions simples : qu'est-ce qui a changé, depuis quand, où, par rapport à quelle référence, avec quelles sources, quel niveau de confiance et quels facteurs ont provoqué l'escalade.

17. Validation et responsabilité humaine

Les acteurs compétents peuvent confirmer, reclasser, commenter, suspendre ou clôturer une alerte. Les décisions à conséquence significative restent sous contrôle humain ou institutionnel et sont séparées du signal produit par le système.

18. Deep Authenticity©

Deep Authenticity© vérifie la provenance des sources, la cohérence des chronologies, les versions des règles et modèles et l'intégrité des éléments ayant contribué à l'alerte. Il aide à distinguer évolution réelle, erreur de donnée, manipulation ou rupture de chaîne nécessitant investigation.

19. AP Ledger, audit et mémoire des alertes

Les événements critiques de création, escalade, validation, désescalade et clôture peuvent être ancrés par empreintes minimales dans AP Ledger. Les contenus sensibles restent protégés tandis que l'audit peut reconstruire le cycle de vie d'une alerte.

20. Critères d'acceptation et conclusion

Watch System© est acceptable si veille et surveillance individuelle restent distinctes ; si chaque alerte conserve sources, référence et temporalité ; si persistance, convergence et criticité sont explicables ; si l'escalade reste gouvernée ; si les données sensibles sont minimisées ; et si l'humain conserve l' autorité décisionnelle. Cette architecture prépare le Chapitre 6 consacré aux signaux faibles et à la détection précoce.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME V — DONNÉES, IA ET INTELLIGENCE SYSTÉMIQUE

CHAPITRE 6 — SIGNAUX FAIBLES ET DÉTECTION PRÉCOCE

ÉMERGENCE — CONVERGENCE — PERSISTANCE — PRÉCURSEURS — HYPOTHÈSES — NIVEAUX DE CONFIANCE — ANTICIPATION

1. Objet du chapitre

Ce chapitre définit la détection des signaux faibles : indices précoces, dispersés ou encore insuffisants pour constituer une tendance établie, mais susceptibles d'annoncer une évolution significative. Il complète Watch System© en ajoutant une capacité d'anticipation avant le franchissement des seuils classiques.

2. Définition du signal faible

Un signal faible est une observation ou combinaison d'observations dont l'intensité est limitée, mais dont la nouveauté, la répétition, la convergence ou le contexte peut justifier une surveillance renforcée. Il reste une hypothèse analytique et non un événement confirmé.

3. Signal faible et anomalie

Une anomalie décrit un écart par rapport à une référence ; un signal faible peut au contraire rester dans les plages habituelles tout en révélant un changement émergent. Les deux mécanismes sont complémentaires et restent identifiés séparément.

4. Signal faible et tendance

Une tendance est déjà visible dans une série ou un ensemble d'indicateurs. Le signal faible intervient plus tôt, lorsque les éléments disponibles ne suffisent pas encore à établir une tendance robuste.

5. Sources précoces

Les signaux peuvent émerger de variations de stocks, délais, prix, flux, demandes, incidents, capacités, capteurs, publications institutionnelles, données sectorielles ou autres sources autorisées. La provenance de chaque contribution reste conservée.

6. Nouveauté

Un événement rare, une nouvelle combinaison de variables ou l'apparition d'un phénomène absent de l'historique peut recevoir un indice de nouveauté. La nouveauté seule ne suffit pas à conclure à l' importance du phénomène.

7. Persistance précoce

La répétition d’un petit écart sur plusieurs périodes peut devenir plus informative qu’une anomalie ponctuelle forte. Watch System© conserve la durée, la fréquence et la direction de ces micro-variations.

8. Convergence indépendante

Des signaux faibles issus de sources réellement indépendantes peuvent renforcer une hypothèse. Le système doit détecter les dépendances de source afin d’éviter de compter plusieurs fois une même information répliquée.

9. Précurseurs

Certains événements peuvent historiquement précéder des tensions, ruptures ou changements. Ils peuvent être utilisés comme précurseurs documentés, mais leur relation passée ne garantit pas la répétition future du phénomène.

10. Séquences émergentes

L’ordre des événements peut être significatif : hausse progressive des délais, baisse des stocks, augmentation des demandes puis tension sur les prix. Le moteur peut comparer ces séquences à des épisodes antérieurs sans imposer une causalité automatique.

11. Signaux intersectoriels

Un signal faible peut apparaître dans un secteur avant d’être visible dans un autre. Agriculture, eau, énergie, logistique, emploi, santé ou prix peuvent ainsi fournir des indices croisés d’une évolution systémique.

12. Signaux territoriaux

La Cartographie Dynamique© peut identifier l’apparition de micro-tendances dans plusieurs zones, leur rapprochement ou leur diffusion. Les différences de couverture et de population sont prises en compte avant comparaison.

13. Hypothèses analytiques

Les signaux faibles sont regroupés autour d’hypothèses explicites : tension d’approvisionnement possible, ralentissement, surplus émergent, pression territoriale ou autre scénario. Chaque hypothèse conserve les éléments qui la soutiennent et ceux qui la contredisent.

14. Score d’émergence

Un score d’émergence peut combiner nouveauté, persistance, convergence, extension territoriale, nombre de secteurs concernés et qualité des sources. Il ne constitue pas une probabilité certaine de réalisation.

15. Niveau de confiance

Le niveau de confiance augmente ou diminue avec la qualité des données, la répétition, l' indépendance des sources et la cohérence avec d'autres indicateurs. Il reste distinct de la gravité potentielle du phénomène.

16. Veille renforcée

Lorsqu'un signal faible atteint un niveau défini, Watch System© peut augmenter temporairement la fréquence d'analyse, ajouter des sources autorisées ou demander une validation experte, sans déclencher automatiquement une alerte publique ou une décision opérationnelle.

17. Confirmation, infirmation et extinction

Un signal peut devenir tendance, anomalie confirmée ou alerte ; il peut aussi être expliqué, infirmé ou disparaître. Tous ces résultats sont utiles pour améliorer les modèles et mesurer la capacité réelle de détection précoce.

18. Deep Authenticity©

Deep Authenticity© vérifie la provenance des éléments composant le signal, les transformations appliquées et les dépendances entre sources. Il contribue à empêcher qu'une donnée dupliquée, manipulée ou mal attribuée produise artificiellement une convergence.

19. Gouvernance et protection

La détection précoce privilégie les indicateurs agrégés et les données nécessaires à la finalité. Les hypothèses sensibles sont accessibles uniquement aux acteurs autorisés ; un signal faible concernant un territoire ou un groupe ne doit pas devenir un mécanisme de stigmatisation.

20. Critères d'acceptation et conclusion

Le système est acceptable si signal faible, anomalie, tendance et événement confirmé restent distincts ; si les hypothèses sont explicites ; si l'indépendance des sources est vérifiée ; si les signaux infirmés sont conservés pour l'apprentissage ; si la confiance et l'impact restent séparés ; et si toute escalade importante demeure gouvernée. Ce chapitre prépare les tableaux de bord économiques et sociaux prévisionnels.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME V — DONNÉES, IA ET INTELLIGENCE SYSTÉMIQUE

CHAPITRE 7 — TABLEAUX DE BORD ÉCONOMIQUES ET SOCIAUX PRÉVISIONNELS

VISION NATIONALE — RÉGIONALE — LOCALE — SECTORIELLE — INDICATEURS — TENDANCES — ALERTES — SCÉNARIOS — INCERTITUDE

1. Objet du chapitre

Ce chapitre définit les tableaux de bord économiques et sociaux prévisionnels du Volume V. Ils réunissent données qualifiées, statistiques, anomalies, signaux faibles, alertes et prévisions afin de fournir une lecture cohérente de la situation actuelle, des tendances et des trajectoires possibles.

2. Tableau de bord comme interface d'intelligence

Le tableau de bord n'est pas un simple écran d'indicateurs. Il relie valeur actuelle, historique, référence, tendance, anomalie, prévision, territoire, source et niveau de confiance afin de permettre une lecture contextualisée.

3. Vision nationale

Une vue nationale peut agréger les indicateurs structurants de production, prix, emploi, ressources, infrastructures, santé, mobilité, environnement ou autres domaines autorisés. Les agrégats nationaux restent reliés aux différences territoriales qu'ils peuvent masquer.

4. Vision régionale et locale

Les tableaux régionaux et locaux permettent d'identifier des évolutions qui disparaissent dans les moyennes nationales. Les comparaisons tiennent compte de la population, de la structure économique, de la géographie, de la couverture des données et des spécificités locales.

5. Vision sectorielle

Chaque secteur peut disposer d'un tableau spécialisé : agriculture, eau, énergie, industrie, transport, santé, emploi, commerce ou autre domaine. Les indicateurs sectoriels restent compatibles avec la couche transversale lorsque les définitions le permettent.

6. Hiérarchie des indicateurs

Les tableaux distinguent indicateurs stratégiques, opérationnels, contextuels et précurseurs. Cette hiérarchie évite qu'un grand nombre de mesures secondaires masque les phénomènes les plus importants.

7. Situation actuelle

La vue courante présente le dernier état disponible avec sa date réelle de mesure ou de publication. Une donnée mensuelle ou trimestrielle ne doit pas être affichée comme si elle décrivait la situation en temps réel.

8. Tendances

Les tendances présentent direction, vitesse d'évolution, durée et référence de comparaison. Elles peuvent être accompagnées de saisonnalité, volatilité et ruptures afin d'éviter une lecture simplifiée.

9. Alertes Watch System©

Les alertes actives peuvent apparaître avec niveau, durée, territoire, secteur, confiance, criticité et principaux facteurs. Le tableau permet de remonter jusqu'aux sources et à l'historique de l'alerte selon les droits.

10. Signaux faibles

Une zone spécifique peut présenter les hypothèses émergentes avant qu'elles ne deviennent des alertes. Elles sont clairement marquées comme signaux précoces et accompagnées des éléments qui les soutiennent ou les contredisent.

11. Prévisions

Les projections présentent horizon, scénario, modèle, date de calcul et incertitude. Les valeurs prévisionnelles sont visuellement et sémantiquement séparées des observations historiques.

12. Scénarios

Un tableau peut comparer scénario central, favorable, défavorable ou autres trajectoires définies. Les scénarios sont des hypothèses conditionnelles et non des promesses de résultat.

13. Indicateurs économiques

Selon les sources autorisées, les tableaux peuvent intégrer activité, production, commerce, prix, capacités, stocks, délais, emploi, investissement ou autres indicateurs pertinents, avec leurs définitions et périodicités.

14. Indicateurs sociaux

Des indicateurs agrégés relatifs à l'accès aux services, emploi, logement, mobilité, éducation, santé ou autres dimensions peuvent être présentés lorsque leur utilisation respecte confidentialité, représentativité et contexte.

15. Disparités

Les tableaux peuvent mettre en évidence des écarts territoriaux ou sectoriels, leur évolution et leur persistance. Ils ne doivent pas transformer automatiquement une disparité statistique en jugement sur une population ou une institution.

16. Drill-down et explicabilité

L’utilisateur autorisé peut passer d’un indicateur agrégé vers les composantes, périodes, territoires et sources qui l’expliquent. Cette capacité rend les tableaux auditables et limite l’effet de boîte noire.

17. Personnalisation par rôle

Décideur public, analyste, opérateur sectoriel ou autre acteur autorisé peut disposer de vues adaptées. La personnalisation modifie la présentation et le périmètre d’accès, mais ne modifie pas silencieusement les données de référence.

18. Deep Authenticity©

Deep Authenticity© vérifie la provenance des données, indicateurs, modèles, alertes et versions présentés. Un tableau doit pouvoir distinguer observation authentifiée, donnée transformée, estimation et prévision.

19. Gouvernance, audit et AP Ledger

Les changements importants de définition, indicateur, modèle, scénario ou alerte sont versionnés et auditables. AP Ledger peut ancrer des empreintes minimales des publications analytiques ou décisions critiques sans exposer les données sensibles.

20. Critères d’acceptation et conclusion

Le tableau de bord est acceptable si observation et prévision restent distinctes ; si chaque indicateur possède source, date et définition ; si l’incertitude est visible ; si les agrégats n’effacent pas les disparités pertinentes ; si les alertes restent explicables ; et si les accès sont proportionnés. Cette architecture prépare les chapitres consacrés aux pénuries, surplus et disparités.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME V — DONNÉES, IA ET INTELLIGENCE SYSTÉMIQUE

CHAPITRE 8 — PÉNURIES ET TENSIONS

STOCKS — CAPACITÉS — CONSOMMATION — FLUX — DÉPENDANCES — RISQUES DE RUPTURE — ANTICIPATION TERRITORIALE ET SECTORIELLE

1. Objet du chapitre

Ce chapitre définit les mécanismes permettant d'identifier, qualifier et anticiper les pénuries et tensions. L'objectif n'est pas seulement de constater une rupture après son apparition, mais de rapprocher stocks, capacités, consommation, flux, délais, dépendances et signaux faibles afin d' estimer les risques en amont.

2. Définition de la pénurie

Une pénurie correspond à une insuffisance effective de disponibilité par rapport à un besoin défini sur un territoire, une période et un segment donnés. Elle doit être distinguée d'une hausse de prix, d'un retard ponctuel, d'une perception de rareté ou d'une difficulté locale de distribution.

3. Tension avant pénurie

Une tension décrit une dégradation mesurable des conditions d'approvisionnement sans rupture nécessairement constatée : baisse de couverture des stocks, allongement des délais, saturation des capacités, concentration des fournisseurs ou hausse persistante de la demande.

4. Stocks et couverture

Le niveau absolu de stock ne suffit pas. Le système calcule lorsque les données le permettent une couverture en jours, semaines ou cycles de consommation, en tenant compte des entrées attendues, de la saisonnalité et de la variabilité de la demande.

5. Capacités de production

Capacité théorique, capacité disponible, capacité réellement utilisée et capacité mobilisable sont distinguées. Une capacité nominale élevée ne garantit pas une disponibilité immédiate si les matières, équipements, compétences ou infrastructures nécessaires manquent.

6. Consommation et demande

La demande est analysée selon tendance, saisonnalité, territoire, segment et éventuels événements exceptionnels. Une hausse ponctuelle ne doit pas être extrapolée automatiquement comme une nouvelle demande structurelle.

7. Flux et délais

Transport, logistique, importations, distribution, temps de transit et délais administratifs ou opérationnels peuvent influencer la disponibilité. Watch System© suit les changements persistants de délai et les ruptures de flux autorisées.

8. Dépendances critiques

Le système peut cartographier les dépendances envers un fournisseur, une région, une infrastructure, une matière, un composant ou un mode de transport. La concentration constitue un facteur de vulnérabilité, sans signifier qu'une rupture est certaine.

9. Produits et ressources substituables

Lorsque cela est pertinent, des alternatives ou capacités substituables peuvent être identifiées. La substituabilité doit être validée selon les exigences techniques, sanitaires, réglementaires ou professionnelles du secteur.

10. Seuils de tension

Des seuils peuvent combiner couverture de stock, utilisation des capacités, délais, volatilité de la demande et concentration des dépendances. Leur définition reste sectorielle, versionnée et révisable.

11. Signaux faibles de pénurie

Une baisse progressive des stocks, des retards répétés, une hausse des commandes, une contraction des capacités ou plusieurs micro-anomalies convergentes peuvent constituer un signal précoce avant franchissement des seuils de rupture.

12. Score de risque

Un score peut synthétiser probabilité estimée, horizon, exposition et robustesse des sources. Il reste un outil de priorisation et ne doit pas être présenté comme une certitude de pénurie.

13. Anticipation territoriale

La Cartographie Dynamique© permet de localiser les zones où couverture, flux ou capacités se dégradent. Une situation nationale équilibrée peut masquer une pénurie locale ; inversement, une tension locale ne doit pas être généralisée à tout un pays.

14. Anticipation sectorielle

Agriculture, alimentation, eau, énergie, pharmacie, santé, industrie, construction, transport ou autres secteurs peuvent avoir des dynamiques de pénurie différentes. Les indicateurs et horizons sont adaptés à chaque domaine.

15. Propagation systémique

Une pénurie peut produire des effets en chaîne : matière première vers industrie, énergie vers production, transport vers distribution, eau vers agriculture ou santé. L'intelligence systémique modélise ces dépendances comme scénarios d'impact et non comme causalités certaines.

16. Scénarios et stress tests

Le système peut simuler baisse d'approvisionnement, hausse de demande, interruption d'une infrastructure ou perte temporaire de capacité. Les scénarios indiquent hypothèses, durée, territoire et variables affectées.

17. Alertes et recommandations

Watch System© peut produire une alerte graduée et proposer des options d'analyse : vérifier une source, mobiliser une capacité autorisée, examiner une alternative ou renforcer la surveillance. Les décisions opérationnelles restent du ressort des acteurs compétents.

18. Deep Authenticity©

Deep Authenticity© vérifie la provenance des données de stocks, capacités, flux et événements utilisés. Il aide à détecter incohérences, doublons, ruptures de séries ou modifications susceptibles de créer artificiellement une impression de pénurie.

19. Gouvernance et prévention des effets pervers

Les informations sensibles sur stocks stratégiques, infrastructures ou capacités critiques sont compartimentées. La diffusion d'une prévision de pénurie doit être gouvernée afin d'éviter qu'une information incertaine provoque elle-même des comportements aggravant la tension.

20. Critères d'acceptation et conclusion

Le dispositif est acceptable si pénurie constatée, tension et risque prévisionnel restent distincts ; si les stocks sont rapportés aux besoins et aux délais ; si les dépendances sont explicables ; si les scénarios affichent leurs hypothèses ; si les données stratégiques sont protégées ; et si les recommandations restent sous autorité compétente. Le chapitre suivant traite le phénomène complémentaire : les surplus.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME V — DONNÉES, IA ET INTELLIGENCE SYSTÉMIQUE

CHAPITRE 9 — SURPLUS ET CAPACITÉS EXCÉDENTAIRES

EXCÉDENTS — SURPRODUCTION — CAPACITÉS INUTILISÉES — DÉSÉQUILIBRES TERRITORIAUX — REDISTRIBUTION — RÉALLOCATION — OPTIMISATION SYSTÉMIQUE

1. Objet du chapitre

Ce chapitre définit la détection et l'analyse des surplus, excédents et capacités sous-utilisées. Complémentaire au chapitre sur les pénuries, il cherche à identifier les ressources disponibles au-delà des besoins observés ou anticipés, tout en distinguant surplus réel, stock de sécurité, réserve stratégique et variation saisonnière.

2. Définition du surplus

Un surplus existe lorsqu'une quantité disponible dépasse un besoin ou une capacité d'absorption définis sur une période, un territoire ou un segment. La référence utilisée doit être explicite : consommation, commandes, capacité de stockage, objectif de réserve ou autre base documentée.

3. Surproduction

La production peut dépasser durablement la demande ou les capacités de transformation, stockage et distribution. Le système analyse volume, durée, saisonnalité et débouchés disponibles avant de qualifier une situation de surproduction structurelle.

4. Stocks excédentaires

Un stock élevé n'est pas automatiquement un surplus. Il peut correspondre à une constitution saisonnière, une réserve de sécurité ou une stratégie autorisée. L'analyse rapproche stock, consommation, durée de conservation, entrées futures et objectifs de couverture.

5. Capacités inutilisées

Des capacités industrielles, logistiques, agricoles, énergétiques, de stockage ou de service peuvent être partiellement inutilisées. Le système distingue capacité théorique, disponible, mobilisable et économiquement ou techniquement exploitable.

6. Inadéquation entre offre et demande

Un excédent peut résulter non d'une production excessive globale, mais d'une inadéquation de lieu, de calendrier, de qualité, de format ou de segment. L'intelligence systémique recherche ces écarts avant de conclure à un surplus général.

7. Déséquilibres territoriaux

Un territoire peut disposer d'un excédent alors qu'un autre connaît une tension. La Cartographie Dynamique© permet de visualiser simultanément zones excédentaires et déficitaires sans supposer qu'un transfert est automatiquement possible.

8. Déséquilibres sectoriels

Une capacité inutilisée dans un secteur peut parfois répondre à un besoin d'un autre secteur, sous réserve de compatibilité technique, réglementaire, économique et logistique. Les possibilités de réemploi restent des hypothèses à valider.

9. Signaux faibles de surplus

Hausse progressive des stocks, baisse persistante des commandes, ralentissement des sorties, augmentation des invendus ou sous-utilisation des capacités peuvent constituer des signaux précoces d'un excédent futur.

10. Score d'excédent

Un score peut combiner couverture des stocks, vitesse de rotation, capacité disponible, tendance de la demande, saisonnalité et durée de conservation. Il sert à prioriser l'analyse et ne constitue pas une instruction automatique de liquidation ou redistribution.

11. Produits périssables et temporalité

Pour les biens à durée de vie limitée, la valeur du surplus dépend fortement du temps restant avant dégradation ou expiration. Les alertes peuvent donc intégrer une fenêtre d'action plus courte et une criticité spécifique.

12. Coûts du surplus

Les excédents peuvent générer coûts de stockage, immobilisation, gaspillage, maintenance, dépréciation ou pression sur les prix. Ces effets sont analysés séparément afin de ne pas réduire le surplus à une simple quantité physique.

13. Redistribution

Lorsque les règles et conditions le permettent, le système peut identifier des zones ou acteurs présentant un besoin compatible. Il fournit une information d'aide à la décision ; il ne transfère pas automatiquement la propriété ni ne décide de l'affectation des ressources.

14. Réallocation de capacités

Des capacités sous-utilisées peuvent être proposées comme options dans des scénarios de tension ailleurs. Toute réallocation doit intégrer coûts, délais, compétences, sécurité, réglementation et impacts sur l'activité d'origine.

15. Optimisation logistique

Le rapprochement entre surplus et besoin peut inclure distance, transport, capacité de stockage, délais, coûts et contraintes. L'objectif est d'identifier des options réalistes plutôt qu'une correspondance purement quantitative.

16. Prévention du gaspillage

Dans les secteurs appropriés, la détection précoce peut aider à réduire pertes et destruction en favorisant transformation, réemploi, redistribution ou autres voies autorisées. Les choix restent soumis aux normes de qualité, sécurité et droit applicables.

17. Scénarios d'équilibrage

Le moteur peut simuler transfert territorial, réallocation, stockage supplémentaire, transformation ou ajustement de production. Chaque scénario présente hypothèses, contraintes, coûts estimés, horizon et effets possibles.

18. Deep Authenticity©

Deep Authenticity© vérifie la provenance des données de production, stocks, capacités, demandes et transferts. Il aide à distinguer surplus réel, erreur de saisie, double comptage, stock déjà engagé ou incohérence de chaîne.

19. Gouvernance et décision

Les informations commerciales, stratégiques ou relatives aux réserves peuvent être sensibles et compartimentées. L'IA peut recommander des options, mais la décision de produire, vendre, transférer, réserver, transformer ou détruire appartient aux acteurs compétents.

20. Critères d'acceptation et conclusion

Le dispositif est acceptable si stock élevé et surplus restent distincts ; si réserve stratégique et excédent sont différenciés ; si les déséquilibres territoriaux sont visibles ; si les possibilités de redistribution intègrent les contraintes réelles ; si les scénarios sont explicables ; et si aucune allocation n'est imposée automatiquement par l'IA. Le chapitre suivant approfondit les disparités.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME V — DONNÉES, IA ET INTELLIGENCE SYSTÉMIQUE

CHAPITRE 10 — DISPARITÉS

TERRITORIALES — ÉCONOMIQUES — SOCIALES — INFRASTRUCTURELLES — ACCÈS AUX SERVICES — MESURE — PERSISTANCE — ÉVOLUTION — CARTOGRAPHIE DYNAMIQUE©

1. Objet du chapitre

Ce chapitre définit l'analyse des disparités au sein du Volume V. Il vise à mesurer les écarts entre territoires, secteurs, infrastructures et niveaux d'accès aux services, à suivre leur évolution et leur persistance, puis à identifier les domaines nécessitant une analyse approfondie sans transformer automatiquement une différence statistique en jugement causal ou normatif.

2. Définition d'une disparité

Une disparité est un écart mesurable entre deux ou plusieurs ensembles comparables selon un indicateur défini. La population, le territoire, la période, l'unité et la méthode de comparaison doivent être explicités avant toute interprétation.

3. Disparités territoriales

Les différences entre régions, wilayas, communes, zones urbaines, rurales ou autres découpages peuvent concerner ressources, activité, infrastructures, capacités ou accès aux services. Les comparaisons doivent tenir compte des caractéristiques structurelles des territoires.

4. Disparités économiques

Production, emploi, investissement, prix, revenus agrégés, capacités, commerce ou autres indicateurs économiques peuvent révéler des écarts persistants. Le système distingue niveau absolu, évolution et position relative.

5. Disparités sociales

Des indicateurs agrégés relatifs à l'éducation, la santé, la mobilité, le logement, l'emploi ou l'accès aux services peuvent être analysés lorsque les données sont suffisamment représentatives et que leur usage respecte les règles de protection.

6. Disparités infrastructurelles

La disponibilité, capacité, qualité ou proximité d'infrastructures de transport, eau, énergie, télécommunications, santé, éducation ou autres services peut être cartographiée afin d'identifier les différences de couverture.

7. Accès aux services

L'existence d'une infrastructure ne garantit pas son accessibilité réelle. Distance, capacité, disponibilité, coût, horaires, continuité et autres facteurs pertinents peuvent être intégrés lorsque les données existent.

8. Normalisation des comparaisons

Les valeurs peuvent être rapportées à la population, superficie, activité, nombre d'usagers, production ou autre dénominateur pertinent. Le choix du dénominateur est conservé afin d'éviter les comparaisons trompeuses.

9. Références et benchmarks

Un territoire ou secteur peut être comparé à une moyenne nationale, un groupe comparable, son propre historique ou un objectif documenté. Aucun benchmark ne doit être présenté comme neutre si son choix influence fortement l'interprétation.

10. Mesure de l'écart

Le système peut utiliser écarts absolus, relatifs, ratios, distributions, quantiles ou indices composites. Les mesures restent accompagnées de leur définition et, pour les indices composites, de leurs pondérations.

11. Persistance

Une disparité ponctuelle peut résulter d'un événement temporaire. La persistance mesure la durée et la répétition de l'écart afin d'identifier les différences structurelles potentielles.

12. Convergence et divergence

L'évolution peut montrer un rapprochement entre territoires ou au contraire un accroissement des écarts. Le tableau de bord distingue le niveau actuel de la direction de l'évolution.

13. Disparités cachées par les moyennes

Une moyenne nationale ou régionale peut masquer des écarts internes importants. Le drill-down permet d'examiner les distributions et sous-territoires lorsque la granularité des données le permet et que la confidentialité est préservée.

14. Cartographie Dynamique©

La Cartographie Dynamique© représente les disparités dans l'espace et dans le temps. Elle peut superposer infrastructures, ressources, flux, capacités, tensions, surplus et autres indicateurs afin de faciliter l'analyse systémique.

15. Corrélations territoriales

Le système peut rechercher des associations entre disparités et facteurs contextuels : infrastructures, distance, activité, ressources ou autres variables disponibles. Une association spatiale ne démontre pas à elle seule une causalité.

16. Signaux faibles et évolution

Une divergence lente mais persistante peut devenir un signal faible avant qu'un seuil critique ne soit atteint. Watch System© peut suivre les écarts qui s'élargissent ou se déplacent dans le temps.

17. Scénarios de réduction d'écart

L'intelligence systémique peut simuler l'effet potentiel d'une capacité supplémentaire, d'une amélioration de flux ou d'autres hypothèses documentées. Ces scénarios constituent des outils d'aide à l'analyse, non des prescriptions automatiques de politique publique.

18. Deep Authenticity©

Deep Authenticity© vérifie provenance, période, couverture, définitions et transformations des données comparées. Il contribue à éviter qu'une différence de méthode, une rupture de série ou une couverture inégale soit interprétée comme une disparité réelle.

19. Protection contre la stigmatisation

Les analyses privilégient des niveaux agrégés adaptés et évitent de transformer un indicateur territorial ou social en jugement sur des individus ou groupes. Les données sensibles sont minimisées et les interprétations importantes doivent conserver leur contexte.

20. Critères d'acceptation et conclusion

L'analyse est acceptable si les ensembles comparés sont compatibles ; si dénominateurs et benchmarks sont explicites ; si niveau, persistance et évolution sont distingués ; si les moyennes peuvent être décomposées ; si corrélation et causalité restent séparées ; et si les résultats ne servent pas à stigmatiser des populations. Le chapitre suivant développera la Cartographie Dynamique© comme infrastructure spatiale du Volume V.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME V — DONNÉES, IA ET INTELLIGENCE SYSTÉMIQUE

CHAPITRE 11 — CARTOGRAPHIE DYNAMIQUE©

GÉOGRAPHIE — TEMPS — FLUX — RESSOURCES — PÉNURIES — SURPLUS — DISPARITÉS — ANOMALIES — SIGNAUX FAIBLES — PROJECTIONS

1. Objet du chapitre

La Cartographie Dynamique© constitue l'infrastructure spatiale du Volume V. Elle relie territoire, temps, ressources, flux, capacités, indicateurs, anomalies, pénuries, surplus, disparités, signaux faibles et projections afin de rendre visibles les relations géographiques de l'intelligence systémique.

2. La carte comme interface analytique

La carte n'est pas une simple représentation graphique. Chaque couche doit conserver source, période, unité, niveau de granularité, méthode de transformation, fraîcheur et droits d'accès afin que l' utilisateur puisse comprendre ce qu'il observe.

3. Référentiel géographique

Territoires administratifs, zones fonctionnelles, réseaux, sites, infrastructures et autres objets spatiaux peuvent être représentés selon des référentiels versionnés. Les changements de limites ou nomenclatures restent historisés.

4. Dimension temporelle

Toute information spatiale est associée à une période ou un instant. La carte peut ainsi reconstruire l' évolution historique, présenter l'état courant disponible et afficher séparément les projections futures.

5. Couches thématiques

Des couches peuvent représenter agriculture, eau, énergie, industrie, transport, santé, emploi, environnement, télécommunications, infrastructures ou autres secteurs autorisés. Elles restent activables selon le besoin et les droits.

6. Cartographie des ressources

Ressources disponibles, capacités, stocks, infrastructures et points de service peuvent être visualisés à une granularité appropriée. Les localisations stratégiques ou sensibles sont masquées, agrégées ou accessibles uniquement aux acteurs habilités.

7. Cartographie des flux

Les flux de marchandises, ressources, transport ou autres mouvements agrégés peuvent être représentés par origine, destination, volume, fréquence et période. La visualisation ne doit pas exposer inutilement les déplacements individuels.

8. Pénuries et tensions

Les zones en tension peuvent être affichées avec horizon, niveau de risque, couverture, facteurs principaux et confiance. Une prévision de pénurie est clairement distinguée d'une rupture effectivement observée.

9. Surplus

Les zones excédentaires peuvent être superposées aux zones déficitaires afin d'identifier des complémentarités potentielles. La carte ne suppose pas qu'un transfert est techniquement, juridiquement ou économiquement possible.

10. Disparités

Les écarts territoriaux peuvent être visualisés par niveau, persistance et évolution. Les valeurs sont normalisées lorsque nécessaire afin d'éviter que la taille d'un territoire ou de sa population produise une comparaison trompeuse.

11. Anomalies spatiales

Des concentrations inhabituelles, ruptures locales, clusters ou divergences entre zones comparables peuvent être signalés. Le moteur distingue autant que possible anomalie du phénomène, anomalie de couverture et anomalie de donnée.

12. Signaux faibles territoriaux

La Cartographie Dynamique© peut révéler plusieurs micro-signaux dispersés qui, pris ensemble, indiquent une émergence spatiale. Leur convergence reste accompagnée de la provenance et du niveau de confiance.

13. Propagation

Une séquence temporelle peut montrer apparition, extension, déplacement, contraction ou disparition d'un phénomène. La propagation observée est séparée des modèles qui estiment une propagation future.

14. Cartographie prédictive

Les projections peuvent représenter des zones de probabilité, intervalles, scénarios ou trajectoires. Elles utilisent une symbolique distincte des observations afin qu'une estimation future ne soit jamais confondue avec une réalité mesurée.

15. Cartographie des interdépendances

Les liens entre réseaux, ressources, infrastructures et secteurs peuvent être visualisés sous forme de dépendances. Cette représentation aide à comprendre les effets en chaîne possibles sans affirmer qu'ils se produiront nécessairement.

16. Drill-down et changement d'échelle

L'utilisateur autorisé peut passer du niveau national au régional, local ou sectoriel. La granularité disponible dépend de la qualité des données et des règles de confidentialité ; le zoom graphique ne crée pas artificiellement une précision absente des sources.

17. Watch System© géospatial

Watch System© peut surveiller des zones, corridors, bassins, réseaux ou autres périmètres autorisés et déclencher des signaux lorsque plusieurs indicateurs spatiaux convergent, persistent ou franchissent des seuils documentés.

18. Deep Authenticity©

Deep Authenticity© vérifie provenance, coordonnées, référentiels, temporalité, versions des couches et transformations. Il peut signaler incohérences de localisation, données obsolètes, ruptures de référentiel ou substitutions nécessitant investigation.

19. Gouvernance, souveraineté et sécurité

Les couches sensibles relatives aux infrastructures critiques, réserves, défense, personnes ou autres informations protégées sont compartimentées. La Cartographie Dynamique© applique minimisation, contrôle d'accès, journalisation et souveraineté des données.

20. Critères d'acceptation et conclusion

La Cartographie Dynamique© est acceptable si chaque couche possède source et date ; si historique, présent et prévision sont distingués ; si la granularité ne dépasse pas celle des données ; si les localisations sensibles sont protégées ; si les comparaisons territoriales sont normalisées ; et si la carte reste une interface d'analyse plutôt qu'une preuve autonome. Le chapitre suivant développera l' Intelligence Prédictive.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME V — DONNÉES, IA ET INTELLIGENCE SYSTÉMIQUE

CHAPITRE 12 — INTELLIGENCE PRÉDICTIVE

MODÈLES — HORIZONS — PROBABILITÉS — SCÉNARIOS — INCERTITUDE — BACKTESTING — DÉRIVE — RECALIBRAGE — PRÉVISIONS TERRITORIALES ET INTERSECTORIELLES

1. Objet du chapitre

Ce chapitre définit l'Intelligence Prédictive du Volume V. Elle utilise les données gouvernées, séries temporelles, anomalies, signaux faibles, alertes et interdépendances pour estimer des trajectoires futures possibles. Elle vise l'anticipation documentée et non la production de certitudes sur l'avenir.

2. Prévision et observation

Une observation décrit une information mesurée ou déclarée à une date donnée ; une prévision estime une valeur ou un état futur. Les interfaces, API, tableaux de bord et cartes doivent maintenir cette séparation de manière explicite.

3. Modèles prédictifs

L'architecture peut utiliser des modèles statistiques, temporels, probabilistes ou d'apprentissage automatique selon le problème. Le choix du modèle dépend des données disponibles, de l'horizon, de l'explicabilité requise et de la conséquence potentielle de son usage.

4. Registre des modèles

Chaque modèle important possède une identité, une version, une finalité, un propriétaire ou responsable, des données d'entraînement ou de calibration identifiables, des variables utilisées, une date de mise en service et un statut de validation.

5. Horizons temporels

Les prévisions sont distinguées selon leurs horizons : très court terme, court terme, moyen terme ou long terme selon le secteur. Plus l'horizon augmente, plus l'incertitude et la dépendance aux hypothèses doivent être visibles.

6. Prévisions ponctuelles et distributions

Une valeur centrale peut être fournie lorsqu'elle est utile, mais elle doit être complétée par une plage, une distribution ou plusieurs scénarios lorsque l'incertitude est significative. Un chiffre unique ne doit pas donner une illusion de précision.

7. Probabilités

Lorsqu'une probabilité est produite, sa signification doit être définie : probabilité conditionnelle à un modèle et à des données, non certitude objective. Les probabilités peuvent être recalibrées lorsque les performances observées montrent un écart.

8. Intervalles d'incertitude

Les prévisions peuvent inclure intervalles, quantiles ou bandes d'incertitude. Ces informations doivent s'élargir ou évoluer lorsque les données, l'horizon ou la volatilité rendent la projection moins certaine.

9. Variables explicatives

Les facteurs ayant contribué à une prévision importante doivent être identifiables dans une mesure appropriée : tendances, saisonnalité, stocks, capacités, prix, flux, événements, signaux faibles ou autres variables pertinentes.

10. Scénario central et scénarios alternatifs

L'architecture peut produire un scénario central accompagné de trajectoires favorables, défavorables ou conditionnelles. Les scénarios alternatifs permettent d'explorer l'effet de changements d' hypothèses sans prétendre prédire lequel se réalisera.

11. Prévisions de pénuries et surplus

Les modèles peuvent estimer l'évolution de la couverture des stocks, de la demande, des capacités et des flux afin d'anticiper tensions ou excédents. Les résultats restent reliés aux mécanismes définis dans les Chapitres 8 et 9.

12. Prévisions territoriales

La Cartographie Dynamique© peut afficher les trajectoires prévues par territoire. La granularité de la projection ne doit pas dépasser celle que permettent les données et la robustesse statistique.

13. Prévisions intersectorielles

L'intelligence systémique peut intégrer des variables provenant de plusieurs secteurs afin d'estimer des effets possibles en chaîne. Les dépendances utilisées doivent être explicites et les relations corrélatives ne sont pas automatiquement interprétées comme causales.

14. Backtesting

Les modèles sont évalués sur des périodes historiques non utilisées de manière inappropriée pour leur validation. Le backtesting compare les prévisions qu'aurait produites le système aux observations réellement survenues.

15. Mesure des erreurs

Erreur absolue, relative, biais, calibration ou autres métriques adaptées peuvent mesurer la performance. Une métrique unique ne suffit pas toujours : la performance doit être examinée selon horizon, territoire, secteur et régime.

16. Dérive des données et des modèles

Les relations historiques peuvent changer. Watch System© peut détecter dérive des distributions, baisse de performance, nouveaux comportements ou ruptures de régime indiquant qu'un modèle doit être réévalué.

17. Recalibrage et versioning

Lorsqu'un modèle est recalibré, la nouvelle version ne remplace pas silencieusement l'ancienne dans l'historique. Les prévisions passées restent liées au modèle et aux données disponibles au moment où elles ont été émises.

18. Deep Authenticity© et audit prédictif

Deep Authenticity© vérifie provenance des données, version du modèle, paramètres ou règles critiques, date de calcul et chaîne de transformation. AP Ledger peut ancrer des empreintes minimales de modèles validés et de prévisions critiques afin de préserver leur antériorité.

19. Contrôle humain et décision

Une prévision peut déclencher une analyse, un scénario ou une recommandation. Elle ne doit pas, à elle seule, imposer automatiquement une décision publique, économique, sociale ou opérationnelle à conséquence significative ; les acteurs compétents conservent l'autorité.

20. Critères d'acceptation et conclusion

L'Intelligence Prédictive est acceptable si prévision et observation restent distinctes ; si modèle, version, données, date et horizon sont traçables ; si l'incertitude est visible ; si les erreurs sont mesurées ; si la dérive déclenche une réévaluation ; si les scénarios conservent leurs hypothèses ; et si la décision reste gouvernée. Ce socle prépare l'Intelligence Systémique intersectorielle du Chapitre 13.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME V — DONNÉES, IA ET INTELLIGENCE SYSTÉMIQUE

CHAPITRE 13 — INTELLIGENCE SYSTÉMIQUE INTERSECTORIELLE

INTERDÉPENDANCES — EFFETS EN CHAÎNE — PROPAGATION — BOUCLES — VULNÉRABILITÉS — RÉSILIENCE — ANTICIPATION MULTISECTORIELLE

1. Objet du chapitre

Ce chapitre définit l'Intelligence Systémique intersectorielle : la capacité à analyser conjointement plusieurs secteurs afin d'identifier dépendances, transmissions, effets en chaîne, boucles de rétroaction, vulnérabilités communes et capacités de résilience. L'objectif est de dépasser la lecture en silos sans prétendre réduire les systèmes complexes à une causalité unique.

2. Du secteur au système

Chaque secteur conserve ses propres indicateurs, acteurs et règles. L'intelligence systémique ajoute une couche relationnelle qui étudie comment une variation dans un domaine peut modifier les contraintes ou opportunités d'un autre.

3. Graphe d'interdépendances

Les relations entre ressources, infrastructures, capacités, flux, secteurs et territoires peuvent être représentées dans un graphe versionné. Chaque relation conserve sa nature, sa source, son niveau de confiance et, lorsque disponible, son délai potentiel de transmission.

4. Dépendances directes et indirectes

Une dépendance directe relie immédiatement deux éléments ; une dépendance indirecte passe par plusieurs maillons. Le système peut explorer ces chaînes tout en signalant l'augmentation de l' incertitude à mesure que le nombre de relations s'accroît.

5. Eau, agriculture et alimentation

Une variation de disponibilité en eau peut influencer certaines capacités agricoles, lesquelles peuvent ensuite affecter volumes alimentaires, transformation, logistique ou prix. Cette chaîne constitue un exemple d'hypothèse systémique à tester avec des données, non une règle universelle.

6. Énergie, industrie et services

La disponibilité, le coût ou la qualité de l'énergie peuvent influencer production, stockage, transport et services. Les impacts dépendent de l'intensité énergétique, des capacités de substitution et de la résilience propre à chaque acteur ou territoire.

7. Transport, logistique et disponibilité

Les ruptures ou ralentissements de transport peuvent modifier délais, stocks et disponibilité de biens. L'analyse rapproche capacités logistiques, itinéraires, dépendances et alternatives sans conclure automatiquement qu'un retard produira une pénurie.

8. Prix, emploi et dynamiques sociales

Les évolutions de prix, activité et emploi peuvent être analysées avec d'autres indicateurs économiques et sociaux agrégés. Toute relation avec des dynamiques sociales reste contextualisée, probabiliste et protégée contre les interprétations simplistes ou stigmatisantes.

9. Santé et déterminants systémiques

Certains indicateurs de santé peuvent être étudiés avec environnement, accès aux services, mobilité ou disponibilité de ressources lorsque les données et règles le permettent. L'analyse systémique ne remplace jamais l'expertise médicale, épidémiologique ou institutionnelle.

10. Effets en cascade

Un événement initial peut se transmettre à plusieurs maillons. Le moteur identifie les chemins possibles, les délais, les facteurs amplificateurs et les points d'arrêt potentiels. Une cascade simulée reste distincte d'une cascade réellement observée.

11. Boucles de rétroaction

Certains phénomènes peuvent se renforcer ou s'atténuer mutuellement. Les boucles sont modélisées comme hypothèses dynamiques et doivent être confrontées aux observations avant d'être utilisées dans des décisions importantes.

12. Nœuds critiques

Le graphe peut révéler des ressources, infrastructures, capacités ou flux dont dépendent plusieurs secteurs. La criticité tient compte de la dépendance, de la substituabilité, du temps de récupération et des conséquences potentielles.

13. Points de substitution et résilience

L'analyse ne recherche pas uniquement les vulnérabilités. Elle identifie également alternatives, redondances, stocks de sécurité, itinéraires secondaires, capacités mobilisables et autres facteurs susceptibles d'absorber un choc.

14. Propagation territoriale et multisectorielle

La Cartographie Dynamique© superpose les dépendances au territoire afin d'identifier où un phénomène pourrait se propager ou être amorti. Observation, simulation et projection sont représentées séparément.

15. Signaux systémiques faibles

Plusieurs micro-signaux provenant de secteurs différents peuvent constituer ensemble un indice précoce. Watch System© évalue leur indépendance, persistance, proximité temporelle et cohérence avec le graphe d'interdépendances.

16. Score de vulnérabilité systémique

Un score peut combiner concentration des dépendances, substituabilité, exposition, criticité, délai de récupération et qualité des données. Il sert à prioriser l'analyse et ne constitue pas une prédiction certaine de défaillance.

17. Scénarios de propagation

Le moteur peut simuler la perte d'une capacité, la baisse d'une ressource, une hausse de demande ou un ralentissement de flux et observer les conséquences possibles sur plusieurs secteurs. Chaque scénario conserve hypothèses et incertitudes.

18. Deep Authenticity© et cohérence intersectorielle

Deep Authenticity© vérifie provenance, temporalité, versions et compatibilité des données croisées. Il aide à éviter qu'une relation apparente soit produite par des définitions incompatibles, des doublons ou des décalages temporels ignorés.

19. Gouvernance et contrôle humain

Les analyses systémiques peuvent influencer des choix importants ; elles doivent donc rester explicables, auditables et accessibles selon les rôles. L'IA propose relations, vulnérabilités et scénarios, tandis que l'autorité de décision demeure aux acteurs compétents.

20. Critères d'acceptation et conclusion

L'Intelligence Systémique est acceptable si chaque relation conserve sa source et son niveau de confiance ; si dépendance et causalité restent distinctes ; si l'incertitude augmente avec les chaînes complexes ; si vulnérabilités et capacités de résilience sont analysées ensemble ; si simulation et observation restent séparées ; et si les décisions importantes restent sous contrôle humain. Le chapitre suivant développera la simulation et les scénarios.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME V — DONNÉES, IA ET INTELLIGENCE SYSTÉMIQUE

CHAPITRE 14 — SIMULATION, SCÉNARIOS ET STRESS TESTS

WHAT IF? — CHOCS SIMPLES ET COMBINÉS — PROPAGATION — TRAJECTOIRES — RÉSILIENCE — OPTIONS D'ACTION — INCERTITUDE

1. Objet du chapitre

Ce chapitre définit la couche de simulation du Volume V. Elle permet d'explorer des questions de type « que se passerait-il si ? » en modifiant explicitement certaines hypothèses puis en observant les trajectoires possibles dans un ou plusieurs secteurs. Une simulation constitue un environnement d' analyse, non une prédiction certaine.

2. Simulation, prévision et décision

La prévision estime ce qui pourrait se produire à partir des données et modèles disponibles. La simulation examine ce qui pourrait se produire sous des hypothèses choisies. La décision sélectionne une action. Ces trois niveaux restent séparés.

3. Registre des scénarios

Chaque scénario possède une identité, une version, un auteur ou responsable, une date, un horizon, un périmètre, des hypothèses d'entrée et les modèles utilisés. Cette traçabilité permet de reproduire ou comparer les résultats.

4. Scénario de référence

Une trajectoire de référence sert de base de comparaison. Elle peut prolonger les conditions actuelles ou reprendre une prévision centrale, mais ses hypothèses doivent être explicites afin qu'elle ne soit pas interprétée comme un futur garanti.

5. Chocs simples

Le moteur peut simuler une variation isolée : baisse de production, hausse de demande, perte temporaire de capacité, allongement de délai ou autre perturbation documentée. L'effet est analysé sur les variables et secteurs concernés.

6. Chocs combinés

Plusieurs perturbations peuvent survenir simultanément ou successivement. Les scénarios combinés permettent d'examiner leurs interactions et d'identifier des effets qui ne seraient pas visibles dans des simulations séparées.

7. Temporalité des chocs

Amplitude, date de début, durée, vitesse d'apparition et rythme de récupération sont définis. Un choc bref et intense peut produire des effets différents d'une dégradation lente mais persistante.

8. Propagation intersectorielle

Le graphe d'interdépendances du Chapitre 13 permet de simuler la transmission possible d'un choc entre ressources, infrastructures et secteurs. À chaque maillon, les hypothèses et l'incertitude restent visibles.

9. Propagation territoriale

La Cartographie Dynamique© peut représenter les zones potentiellement affectées, les délais de propagation et les territoires disposant de capacités d'absorption ou de substitution. Une zone simulée n'est jamais affichée comme une zone effectivement touchée.

10. Contraintes et capacités

Les simulations intègrent, lorsque les données le permettent, stocks, capacités, flux, délais, substituabilité, infrastructures et règles opérationnelles. L'absence d'une contrainte importante doit être signalée comme limite du scénario.

11. Stress tests

Les stress tests appliquent des conditions défavorables définies afin d'évaluer la résistance d'un système. Leur objectif est d'identifier points de rupture, marges de sécurité, dépendances critiques et temps de récupération.

12. Résilience

La résilience est analysée selon capacité d'absorption, continuité, substitution, redondance, adaptation et récupération. Elle ne se résume pas à l'absence d'impact initial.

13. Points de rupture

Le moteur peut rechercher les seuils où une dégradation progressive entraîne un changement important de fonctionnement. Ces seuils sont des résultats de modèle et doivent être confrontés à l' expertise et aux observations.

14. Options d'action

Un scénario peut intégrer des options telles que mobilisation d'une capacité autorisée, modification d' un flux, recours à une alternative ou renforcement temporaire d'un stock. Ces options servent à comparer des conséquences potentielles et ne sont pas des ordres automatiques.

15. Comparaison multicritère

Les trajectoires peuvent être comparées selon disponibilité, délai, coût, continuité, impact territorial, résilience ou autres critères définis. Les pondérations doivent être explicites lorsque plusieurs critères sont agrégés.

16. Analyse de sensibilité

Le système fait varier les hypothèses importantes afin d'identifier celles qui influencent le plus les résultats. Une conclusion qui disparaît avec une petite variation d'hypothèse doit être présentée comme fragile.

17. Incertitude et scénarios extrêmes

Les simulations peuvent inclure plages d'incertitude et scénarios extrêmes plausibles. Un scénario extrême sert à tester la robustesse ; il ne constitue pas une annonce qu'un événement extrême va se produire.

18. Backtesting et validation

Lorsque des épisodes historiques comparables existent, les mécanismes de simulation peuvent être confrontés à ces événements pour mesurer leur capacité à reproduire certaines dynamiques observées. Les limites de comparabilité sont conservées.

19. Deep Authenticity©, AP Ledger et gouvernance

Deep Authenticity© vérifie données d'entrée, versions des modèles et hypothèses. Les scénarios critiques peuvent être ancrés par empreintes minimales dans AP Ledger. Les simulations sensibles sont accessibles selon les rôles et toute décision significative reste sous autorité humaine ou institutionnelle.

20. Critères d'acceptation et conclusion

La simulation est acceptable si hypothèses, modèles et versions sont traçables ; si référence, simulation, prévision et observation restent distinctes ; si l'incertitude et la sensibilité sont visibles ; si les contraintes importantes sont explicites ; si les options d'action restent des options ; et si les décisions demeurent gouvernées. Ce socle prépare le Chapitre 15 consacré à l'IA décisionnelle assistive.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME V — DONNÉES, IA ET INTELLIGENCE SYSTÉMIQUE

CHAPITRE 15 — IA DÉCISIONNELLE ASSISTIVE

ANALYSE — ALERTE — OPTIONS — RECOMMANDATION — ARBITRAGE HUMAIN — DÉCISION — TRAÇABILITÉ — ÉVALUATION

1. Objet du chapitre

Ce chapitre définit l'IA décisionnelle assistive du Volume V. Elle organise le passage des données, analyses, alertes, prévisions et simulations vers des options et recommandations explicables, sans transférer à l'IA l'autorité institutionnelle, juridique, économique ou opérationnelle attachée à la décision.

2. Principe d'assistance

L'IA assiste l'analyse et la préparation de décision. Elle peut synthétiser des éléments, comparer des scénarios, identifier des contraintes ou proposer des options. Elle ne doit pas être présentée comme l'autorité qui décide lorsque la décision relève d'un humain, d'une organisation ou d'une institution compétente.

3. Chaîne décisionnelle

La chaîne de référence est : observation → analyse → anomalie ou signal → alerte → prévision → simulation → options → recommandation → arbitrage → décision → exécution → suivi → évaluation. Chaque niveau conserve sa nature et sa provenance.

4. Contexte de décision

Avant toute recommandation, le système identifie objectif, périmètre, horizon, acteurs, contraintes, données disponibles et niveau d'urgence. Une recommandation produite hors contexte doit être considérée comme insuffisamment fondée.

5. Génération d'options

Le système peut produire plusieurs options compatibles avec les contraintes connues. Il doit éviter de réduire artificiellement un problème complexe à une seule solution lorsqu'il existe plusieurs trajectoires plausibles.

6. Critères d'évaluation

Les options peuvent être comparées selon disponibilité, délai, coût, continuité, résilience, impact territorial, contraintes réglementaires ou autres critères autorisés. Les critères et leurs pondérations sont explicites.

7. Recommandation

Une recommandation est une proposition argumentée issue de l'analyse des options. Elle conserve les données, hypothèses, modèles, critères et incertitudes qui ont contribué à son classement.

8. Alternatives

Même lorsqu'une option est classée première, les principales alternatives restent accessibles avec leurs avantages, limites et conditions. Le décideur peut ainsi comprendre le coût d'opportunité du choix.

9. Niveau de confiance

La confiance associée à une recommandation dépend de la qualité des données, de la stabilité des modèles, de la sensibilité des résultats et de la cohérence des sources. Elle ne mesure pas la légitimité politique, juridique ou institutionnelle d'une décision.

10. Explicabilité

Pour une décision importante, le système doit pouvoir expliquer pourquoi une option est proposée, quelles variables ont pesé, quelles hypothèses sont déterminantes et quelles informations pourraient modifier le résultat.

11. Incertitude et désaccord

Lorsque les modèles ou sources produisent des conclusions divergentes, le système ne masque pas ce désaccord. Il présente les écarts, leur origine et les conditions dans lesquelles chaque résultat pourrait devenir pertinent.

12. Arbitrage humain

Le décideur autorisé peut accepter, modifier, différer ou rejeter une recommandation. Lorsque cela est requis par la gouvernance, la justification de l'arbitrage est conservée afin de distinguer clairement recommandation algorithmique et décision finale.

13. Décisions à conséquence significative

Plus les conséquences potentielles sont importantes pour des personnes, des droits, des ressources critiques ou des politiques publiques, plus les exigences de validation, explicabilité, contrôle humain et audit doivent être élevées.

14. Exécution séparée

La production d'une recommandation ne doit pas déclencher silencieusement son exécution. Les systèmes d'exécution utilisent des autorisations, validations et contrôles distincts selon le domaine.

15. Suivi des résultats

Après décision et mise en œuvre, les indicateurs pertinents peuvent être suivis pour observer les résultats, effets secondaires et écarts par rapport aux hypothèses initiales.

16. Boucle d’apprentissage

Les résultats observés peuvent améliorer modèles, scénarios et critères, mais l’apprentissage ne doit pas réécrire l’historique. Les versions antérieures restent disponibles pour comprendre ce qui était connu au moment de la décision.

17. Biais et équité

Les recommandations sont évaluées pour détecter des biais liés aux données, à la couverture, aux objectifs ou aux critères. Une optimisation globale ne doit pas masquer des effets disproportionnés sur certains territoires ou ensembles de population.

18. Deep Authenticity©

Deep Authenticity© vérifie provenance des données, versions des modèles, scénarios, critères et recommandations. Il permet de reconstruire la chaîne ayant conduit d’une observation à une proposition décisionnelle.

19. AP Ledger, audit et responsabilité

Les décisions critiques, validations et versions de recommandations peuvent être ancrées par empreintes minimales dans AP Ledger. L’audit doit distinguer ce que l’IA a proposé, ce que le décideur a retenu et ce qui a réellement été exécuté.

20. Critères d’acceptation et conclusion

L’IA décisionnelle assistive est acceptable si recommandation et décision restent distinctes ; si plusieurs options peuvent être examinées ; si critères, hypothèses et incertitudes sont visibles ; si l’exécution possède ses propres autorisations ; si les résultats sont évalués ; et si l’autorité humaine ou institutionnelle demeure identifiable. Le chapitre suivant approfondira la gouvernance, la souveraineté et la sécurité des données et des modèles.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME V — DONNÉES, IA ET INTELLIGENCE SYSTÉMIQUE

CHAPITRE 16 — GOUVERNANCE, SOUVERAINETÉ ET SÉCURITÉ DES DONNÉES ET DES MODÈLES IA

CLASSIFICATION — ACCÈS — CONFIDENTIALITÉ — RÉSIDENCE — CYCLE DE VIE — CYBERSÉCURITÉ — AUDIT — SÉPARATION DES POUVOIRS — CONTINUITÉ SOUVERAINE

1. Objet du chapitre

Ce chapitre définit le cadre de gouvernance, de souveraineté et de sécurité applicable aux données, modèles, analyses, alertes, simulations et recommandations du Volume V. L'objectif est de permettre l'intelligence systémique sans créer une concentration incontrôlée de données, de pouvoir analytique ou d'autorité décisionnelle.

2. Gouvernance par finalité

Toute collecte, transformation, analyse ou utilisation de données doit correspondre à une finalité définie. Une donnée disponible techniquement n'est pas automatiquement disponible pour tout usage analytique.

3. Classification des données

Les données peuvent être classées selon leur sensibilité, criticité, origine, statut juridique et impact potentiel : ouvertes, internes, confidentielles, sensibles, stratégiques ou autres catégories définies par la gouvernance. La classification détermine les protections et droits associés.

4. Minimisation

L'architecture privilégie la quantité et la granularité minimales nécessaires à l'objectif. Lorsqu'un indicateur agrégé suffit, l'accès aux données individuelles sous-jacentes n'est pas requis.

5. Contrôle d'accès

Les droits sont attribués selon rôle, finalité, domaine, territoire, niveau de sensibilité et durée. Consultation, analyse, export, modification, administration et validation constituent des permissions distinctes.

6. Séparation des pouvoirs

La capacité d'administrer les sources, de modifier un modèle, de valider une alerte, d'autoriser une décision et d'auditer le système peut être répartie entre des rôles distincts. Cette séparation limite les conflits d'intérêts et les modifications non contrôlées.

7. Confidentialité et protection

Chiffrement, pseudonymisation, agrégation, compartimentation et autres mécanismes appropriés protègent les données sensibles. Les interfaces analytiques ne doivent pas exposer davantage d'information que le rôle utilisateur ne l'exige.

8. Souveraineté et résidence

Les politiques peuvent imposer des exigences de résidence, d'hébergement, de traitement ou de transfert selon la nature des données et les règles applicables. Les dépendances à des infrastructures externes doivent être identifiables et gouvernées.

9. Portabilité et réversibilité

Les données, schémas, configurations, historiques et éléments nécessaires à la continuité doivent pouvoir être exportés dans des formats documentés lorsque la gouvernance l'exige. La souveraineté implique la capacité de changer de composant sans perdre la mémoire analytique.

10. Registre des modèles IA

Chaque modèle important possède identité, version, finalité, propriétaire, statut, données de référence, métriques, limites connues et conditions d'utilisation. Un modèle retiré reste identifiable dans les analyses historiques qu'il a produites.

11. Cycle de vie des modèles

Développement, validation, mise en service, surveillance, recalibrage, suspension et retrait sont des états gouvernés. Le passage entre états peut exiger des validations différentes selon la criticité du modèle.

12. Validation avant mise en production

Les modèles destinés à des usages significatifs sont évalués sur performance, robustesse, biais, explicabilité, sécurité et adéquation à la finalité. Une performance moyenne élevée ne suffit pas si certaines situations critiques sont mal couvertes.

13. Surveillance des modèles

Watch System© peut suivre dérive des données, baisse de performance, anomalies d'entrée, changement de comportement ou autres signaux affectant la fiabilité. Une dégradation significative peut déclencher revue, limitation ou suspension.

14. Cybersécurité

Les composants analytiques sont protégés contre accès non autorisé, altération de données, substitution de modèles, exfiltration, compromission des connecteurs et autres menaces pertinentes. Les contrôles sont proportionnés à la criticité et au contexte.

15. Intégrité des chaînes analytiques

Une analyse critique doit conserver les versions des sources, transformations, modèles et paramètres essentiels. Toute modification d'un maillon doit être détectable afin d'empêcher une réécriture silencieuse du raisonnement historique.

16. Journalisation et audit

Les opérations importantes sont journalisées : accès sensibles, changements de source, publication de modèle, modification de seuil, création ou validation d'alerte, recommandation et décision. Les journaux eux-mêmes sont protégés contre l'altération.

17. Deep Authenticity© et AP Ledger

Deep Authenticity© vérifie cohérence, provenance, versions et intégrité des chaînes. AP Ledger peut ancrer des empreintes minimales d'événements critiques, modèles, jeux de données ou décisions sans exposer les contenus confidentiels.

18. Continuité souveraine

Des mécanismes de sauvegarde, redondance, reprise, fonctionnement dégradé et reconstruction permettent de maintenir les fonctions essentielles en cas d'incident. Les dépendances critiques et procédures de reprise sont documentées et testées.

19. Gouvernance de l'IA et responsabilité

Les responsabilités doivent rester identifiables : fournisseur de données, responsable de modèle, analyste, validateur, décideur, opérateur et auditeur. L'expression « l'IA a décidé » ne doit pas effacer la chaîne réelle de responsabilité.

20. Critères d'acceptation et conclusion

Le cadre est acceptable si finalité et droits sont explicites ; si les données sont minimisées et classifiées ; si les pouvoirs critiques sont séparés ; si modèles et versions sont gouvernés ; si la dérive est surveillée ; si l'intégrité et l'audit sont assurés ; si la continuité et la réversibilité sont possibles ; et si la responsabilité humaine ou institutionnelle demeure identifiable. Le chapitre suivant approfondira Deep Authenticity© appliqué aux données et aux modèles.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME V — DONNÉES, IA ET INTELLIGENCE SYSTÉMIQUE

CHAPITRE 17 — DEEP AUTHENTICITY© APPLIQUÉ AUX DONNÉES ET AUX MODÈLES IA

PROVENANCE — INTÉGRITÉ — VERSIONING — TRANSFORMATIONS — REPRODUCTIBILITÉ — CONTINUITÉ DE LA PREUVE ANALYTIQUE

1. Objet du chapitre

Ce chapitre applique Deep Authenticity© à l'ensemble de la chaîne analytique du Volume V. Son objectif est de préserver une continuité vérifiable entre source, dataset, transformation, modèle, exécution, résultat, prévision, recommandation et validation, afin qu'un résultat important puisse être replacé dans les conditions exactes de sa production.

2. Continuité de la preuve analytique

La chaîne de référence est : source → dataset → provenance → qualification → transformation → version → modèle IA → configuration → exécution → résultat → prévision ou recommandation → validation → trace d'audit. Chaque maillon important conserve son identité et ses relations avec les autres.

3. Authenticité et vérité

L'authenticité d'un dataset indique que son origine et son intégrité peuvent être vérifiées selon les mécanismes disponibles. Elle ne garantit pas que les observations soient exemptes d'erreur, complètes ou représentatives. De même, un modèle authentifié peut produire une prévision incorrecte.

4. Identité des sources

Chaque source importante possède une identité technique ou institutionnelle, un statut, un domaine, des conditions d'usage et un historique. Une modification d'émetteur, de connecteur ou de méthode doit pouvoir être détectée et contextualisée.

5. Empreinte des datasets

Les versions significatives d'un jeu de données peuvent recevoir une empreinte cryptographique ou un identifiant vérifiable. Cela permet de détecter une modification ultérieure sans nécessiter la publication du contenu confidentiel.

6. Versioning

Un dataset corrigé, enrichi ou mis à jour devient une version identifiable. Les analyses historiques restent attachées à la version réellement utilisée au moment de leur exécution.

7. Transformations

Nettoyage, normalisation, agrégation, jointure, filtrage, imputation ou enrichissement constituent des transformations distinctes. Les règles et versions critiques sont conservées afin de reconstruire la chaîne analytique.

8. Données manquantes et estimées

Une valeur imputée ou estimée ne doit jamais être transformée silencieusement en observation originale. Deep Authenticity© conserve la nature de la valeur et, lorsque pertinent, la méthode ayant permis de la produire.

9. Lignage des données

Le lignage relie un résultat aux données amont et permet de remonter d'un indicateur vers ses sources. Il peut également identifier quels résultats ou modèles sont affectés lorsqu'une source est corrigée ou invalidée.

10. Identité des modèles

Chaque modèle IA ou statistique important possède identité, version, finalité, responsable, statut de validation et environnement d'utilisation. Deux versions d'un même modèle sont traitées comme des objets analytiques distincts.

11. Origine et validation des modèles

Lorsque cela est applicable, le système conserve l'origine du modèle, ses conditions de validation, métriques principales, limites connues et données de référence. Cette documentation accompagne son statut d'utilisation.

12. Configuration et paramètres

Les paramètres, seuils, variables et configurations ayant un effet significatif sur un résultat doivent être versionnés ou enregistrés selon la criticité. Une modification de configuration ne doit pas être invisible dans l'historique.

13. Identité de l'exécution

Une exécution analytique importante peut recevoir un identifiant reliant date, modèle, version, données d'entrée, configuration et résultat. Cela permet de distinguer deux calculs effectués à des moments ou dans des conditions différentes.

14. Reproductibilité

Lorsque les données et composants sont disponibles, une analyse doit pouvoir être reproduite ou, à défaut, reconstruite suffisamment pour comprendre ses conditions de production. Les dépendances non reproductibles sont documentées comme limites.

15. Détection d'altération

Une divergence d'empreinte, une rupture de provenance, une version inattendue ou une transformation non autorisée peut déclencher un signal. Le système distingue suspicion d'altération, erreur opérationnelle et changement légitime en attente de validation.

16. Résultats, prévisions et recommandations

Chaque résultat important conserve la chaîne qui l'a produit. Une recommandation peut ainsi être reliée à la prévision, au scénario, au modèle, aux données et aux hypothèses qui ont contribué à sa formulation.

17. Révisions et corrections

Lorsqu'une erreur est découverte, une nouvelle version corrige l'information sans effacer silencieusement la version antérieure. L'historique permet de savoir quelles analyses ou décisions ont été produites avant la correction.

18. AP Ledger et ancrage minimal

AP Ledger peut enregistrer des empreintes minimales, horodatages, identifiants de version et événements critiques afin de préserver antériorité et intégrité sans exposer les datasets, modèles ou résultats confidentiels.

19. Audit et responsabilité

L'auditeur autorisé peut reconstruire qui a fourni ou validé une source, quelle version a été utilisée, quel modèle a produit un résultat, quelles transformations ont été appliquées et quelle autorité a finalement pris une décision. La responsabilité reste attribuable aux rôles réels.

20. Critères d'acceptation et conclusion

Deep Authenticity© appliqué à l'IA est acceptable si source, dataset, transformation, modèle, exécution et résultat restent identifiables ; si les corrections ne réécrivent pas l'historique ; si les valeurs estimées restent distinguées des observations ; si les altérations sont détectables ; si l'audit peut reconstruire la chaîne ; et si authenticité, exactitude, performance et vérité prédictive ne sont jamais confondues. Ce socle prépare le Chapitre 18 consacré à AP Ledger et à la mémoire analytique.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME V — DONNÉES, IA ET INTELLIGENCE SYSTÉMIQUE

CHAPITRE 18 — AP LEDGER ET MÉMOIRE ANALYTIQUE

ANTÉRIORITÉ — EMPREINTES — VERSIONS — ALERTES — PRÉVISIONS — DÉCISIONS — AUDIT — MÉMOIRE SYSTÉMIQUE VÉRIFIABLE

1. Objet du chapitre

Ce chapitre définit le rôle d'AP Ledger dans la mémoire analytique du Volume V. AP Ledger ne remplace ni les bases de données ni les systèmes analytiques : il peut ancrer des preuves minimales d'existence, d'antériorité, de version et d'intégrité pour les événements critiques de la chaîne analytique.

2. Principe de mémoire analytique

L'intelligence systémique doit pouvoir se souvenir de ce qui était connu, calculé, prévu, recommandé et décidé à un moment donné. Cette mémoire permet de comparer prévisions et résultats, d'analyser les erreurs et de reconstruire le contexte historique sans réécrire le passé.

3. AP Ledger comme couche d'ancrage

AP Ledger conserve des empreintes, identifiants, horodatages et relations minimales lorsque cela est nécessaire. Les contenus volumineux ou sensibles restent dans leurs systèmes gouvernés ; le Ledger fournit un point de vérification et non un entrepôt universel.

4. Antériorité

L'ancrage peut établir qu'une version de dataset, modèle, scénario, alerte, prévision ou décision existait à une date donnée. Cette antériorité est particulièrement importante lorsqu'une analyse est révisée ultérieurement.

5. Empreintes des datasets

Une empreinte cryptographique d'une version significative de dataset peut être enregistrée avec son identifiant et sa date. Une vérification ultérieure permet de déterminer si le contenu correspondant a changé.

6. Empreintes des modèles

Les modèles et configurations critiques peuvent recevoir des empreintes associées à leurs versions. Une prévision historique peut ainsi rester liée au modèle réellement utilisé plutôt qu'à sa version actuelle.

7. Transformations et pipelines

Les versions critiques des règles de transformation ou pipelines analytiques peuvent être référencées. L'objectif est de conserver les éléments nécessaires pour comprendre comment les données d'entrée sont devenues un résultat.

8. Mémoire des alertes

Création, escalade, validation, reclassification, désescalade et clôture d'une alerte peuvent constituer des événements de mémoire. L'historique permet de savoir ce que Watch System© signalait à chaque étape.

9. Mémoire des signaux faibles

Les hypothèses émergentes peuvent être versionnées afin de conserver leur évolution : apparition, renforcement, contradiction, confirmation ou extinction. Les signaux infirmés restent utiles à l' évaluation du système.

10. Mémoire des prévisions

Une prévision critique conserve date, horizon, modèle, version, données de référence et résultat. Lorsque le futur devient observable, la prévision originale reste inchangée afin de permettre une mesure honnête de la performance.

11. Mémoire des scénarios

Les simulations et stress tests peuvent être ancrés avec leurs hypothèses, versions et résultats principaux. Deux scénarios portant le même nom mais utilisant des hypothèses différentes restent distinguables.

12. Mémoire des recommandations

Une recommandation importante peut être reliée aux options examinées, critères, prévisions et scénarios disponibles au moment de sa production. Elle ne doit pas être reconstruite a posteriori avec des informations inconnues à cette date.

13. Mémoire des décisions

Lorsque la gouvernance l'exige, la décision finale peut être reliée à la recommandation, au décideur ou rôle autorisé, à la date et à la justification disponible. L'audit distingue clairement proposition algorithmique et décision institutionnelle.

14. Mémoire de l'exécution

La décision et son exécution sont deux événements différents. Le système peut conserver si, quand et dans quelles conditions une décision a réellement été mise en œuvre, afin d'éviter d'attribuer à une recommandation des résultats liés à une exécution différente.

15. Évaluation a posteriori

La mémoire analytique permet de comparer données initiales, prévision, décision, exécution et résultat observé. Cette chaîne soutient le backtesting, l'apprentissage institutionnel et l'amélioration des modèles.

16. Corrections sans effacement

Une erreur ou correction produit une nouvelle version et un lien avec l'élément antérieur. Le système évite la suppression silencieuse d'une prévision ou d'une donnée qui avait réellement influencé une décision passée.

17. Confidentialité et minimisation

AP Ledger n'a pas vocation à exposer données personnelles, secrets commerciaux, informations stratégiques ou modèles confidentiels. Les ancrages utilisent des éléments minimaux permettant la vérification tout en conservant les contenus protégés hors Ledger.

18. Deep Authenticity© et reconstruction

Deep Authenticity© utilise les identités, empreintes, versions et relations pour reconstruire la continuité de la preuve analytique. Il peut détecter un maillon absent, une version incohérente ou une tentative de substitution nécessitant investigation.

19. Audit et mémoire systémique

La mémoire analytique dépasse l'audit technique : elle permet d'étudier comment le système a perçu une situation, quelles alertes ont été émises, quelles hypothèses ont été retenues et comment les décisions ont évolué. Elle devient une mémoire institutionnelle vérifiable.

20. Critères d'acceptation et conclusion

AP Ledger est acceptable si les ancrages restent minimaux ; si les contenus sensibles demeurent protégés ; si les versions historiques ne sont pas réécrites ; si prévision, recommandation, décision et exécution restent distinctes ; si les corrections sont traçables ; et si l'audit peut reconstruire le contexte temporel. Ce socle prépare le Chapitre 19 consacré au Centre d'Intelligence Systémique.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME V — DONNÉES, IA ET INTELLIGENCE SYSTÉMIQUE

CHAPITRE 19 — CENTRE D'INTELLIGENCE SYSTÉMIQUE

OBSERVATION — WATCH SYSTEM© — CARTOGRAPHIE DYNAMIQUE© — PRÉVISION — SIMULATION — ALERTE — COORDINATION — AIDE À LA DÉCISION

1. Objet du chapitre

Le Centre d'Intelligence Systémique constitue la couche opérationnelle de convergence du Volume V. Il réunit, sans confondre leurs fonctions, données gouvernées, analyse statistique, Watch System©, signaux faibles, tableaux de bord, Cartographie Dynamique©, intelligence prédictive, simulations et IA décisionnelle assistive.

2. Centre logique plutôt que centralisation absolue

Le Centre n'impose pas que toutes les données soient physiquement regroupées dans une base unique. Il peut fonctionner selon une architecture fédérée où les données restent dans des domaines souverains tandis que les indicateurs, preuves, autorisations et résultats nécessaires sont orchestrés selon les droits.

3. Mission d'observation

La première fonction est de fournir une représentation cohérente de la situation disponible : indicateurs, tendances, ressources, capacités, flux, pénuries, surplus, disparités et événements significatifs, avec leur temporalité et leur niveau de confiance.

4. Mission d'anticipation

La deuxième fonction est d'identifier anomalies, signaux faibles, trajectoires possibles et risques émergents. Les projections restent explicitement séparées des observations afin que l'anticipation ne soit pas confondue avec le constat.

5. Mission de coordination analytique

Le Centre rapproche les analyses produites par plusieurs domaines sans supprimer l'expertise sectorielle. Les responsables de l'eau, de l'énergie, de l'agriculture, de la santé, du transport, de l'économie ou d'autres secteurs conservent leur compétence métier.

6. Watch System© intégré

Watch System© constitue la couche de veille continue du Centre. Il consolide les alertes autorisées, mesure leur persistance, rapproche les signaux indépendants et identifie les phénomènes susceptibles de devenir intersectoriels.

7. Cartographie Dynamique© intégrée

La carte opérationnelle permet de visualiser indicateurs, ressources, infrastructures, flux, tensions, surplus, disparités, alertes et projections. Les couches sensibles sont filtrées selon les rôles et la granularité autorisée.

8. Tableaux de bord intégrés

Les tableaux de bord fournissent des vues nationales, régionales, locales et sectorielles adaptées aux rôles. Chaque indicateur conserve source, date, définition et possibilité de remonter vers les éléments explicatifs disponibles.

9. Intelligence prédictive intégrée

Les modèles fournissent des trajectoires et probabilités selon différents horizons. Le Centre présente modèle, version, date, incertitude et principaux facteurs afin d'éviter une consommation aveugle de la prévision.

10. Simulation et salle de scénarios

Les acteurs autorisés peuvent comparer scénario de référence, chocs, stress tests et options d'action. Les hypothèses sont visibles et les résultats de simulation sont clairement distingués des données observées.

11. Gestion des alertes

Une alerte possède un cycle de vie : création, qualification, validation, escalade, coordination, suivi, désescalade et clôture. Le Centre ne doit pas multiplier les alertes sans hiérarchie ; il organise priorité, confiance, criticité et responsabilité.

12. Cellules sectorielles et transversales

Des cellules ou vues spécialisées peuvent traiter un secteur tandis qu'une fonction transversale examine les interdépendances. Cette organisation limite le risque qu'une alerte systémique soit invisible parce que ses premiers éléments sont dispersés entre plusieurs domaines.

13. Coordination territoriale

Les niveaux national, régional et local peuvent partager une situation commune tout en conservant leurs responsabilités et droits. Un territoire peut enrichir une analyse par des informations locales sans modifier silencieusement les données d'un autre niveau.

14. Dossier analytique d'événement

Pour un événement important, le Centre peut constituer un dossier réunissant chronologie, sources, indicateurs, alertes, cartes, prévisions, scénarios, recommandations, validations et décisions. Ce dossier devient l'unité cohérente d'analyse et d'audit.

15. IA décisionnelle assistive

L'IA peut synthétiser le dossier, comparer les options, identifier des contraintes ou signaler des contradictions. Elle ne remplace pas les autorités compétentes et ne transforme pas automatiquement une recommandation en ordre d'exécution.

16. Modes normal, vigilance et crise

L'interface et les procédures peuvent s'adapter à la situation : fonctionnement normal, vigilance renforcée ou gestion de crise. Le passage d'un mode à l'autre suit des règles gouvernées et reste journalisé.

17. Continuité opérationnelle

Le Centre prévoit fonctionnement dégradé, redondance, reprise, sauvegarde et procédures manuelles lorsque certains composants ou réseaux sont indisponibles. L'intelligence systémique ne doit pas devenir un point unique de défaillance.

18. Deep Authenticity© et AP Ledger

Deep Authenticity© vérifie la continuité entre sources, modèles, alertes, scénarios et décisions. AP Ledger peut ancrer les événements critiques et versions significatives, créant une mémoire analytique vérifiable sans exposer les contenus sensibles.

19. Protection des citoyens et limites

Le Centre est conçu pour comprendre des systèmes, ressources, territoires et phénomènes, non pour établir une surveillance généralisée des citoyens. Minimisation, agrégation, finalité, contrôle d'accès et séparation des rôles limitent les usages disproportionnés.

20. Critères d'acceptation et conclusion

Le Centre d'Intelligence Systémique est acceptable si convergence ne signifie pas centralisation absolue ; si expertise sectorielle et coordination transversale coexistent ; si observation, prévision, simulation et décision restent distinctes ; si les alertes sont hiérarchisées et auditables ; si la continuité opérationnelle est prévue ; si les citoyens sont protégés contre la surveillance disproportionnée ; et si l'autorité décisionnelle demeure identifiable. Le Chapitre 20 pourra désormais synthétiser et clôturer le Volume V.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME V — DONNÉES, IA ET INTELLIGENCE SYSTÉMIQUE

CHAPITRE 20 — SYNTHÈSE GÉNÉRALE, CRITÈRES D'ACCEPTATION ET CLÔTURE DU VOLUME V

DONNÉES — ANALYSE — WATCH SYSTEM© — SIGNAUX FAIBLES — PRÉVISION — CARTOGRAPHIE DYNAMIQUE© — INTELLIGENCE SYSTÉMIQUE — DÉCISION ASSISTÉE — SOUVERAINETÉ

1. Objet du chapitre

Ce chapitre clôture le Volume V en réunissant ses composantes dans une architecture cohérente de Données, IA et Intelligence Systémique. L'objectif est de fixer les principes d'ensemble, les frontières fonctionnelles et les critères permettant d'évaluer la conformité d'une mise en œuvre à l'architecture définie.

2. Finalité du Volume V

Le Volume V transforme des données internes et externes gouvernées en capacités d'observation, d'analyse, d'anticipation, de simulation et d'aide à la décision. Il cherche à améliorer la compréhension des phénomènes économiques, sociaux, territoriaux et sectoriels sans confondre calcul analytique, autorité institutionnelle et réalité observée.

3. Chaîne d'intelligence systémique

La chaîne générale peut être résumée ainsi : sources → données qualifiées → analyse statistique → anomalies → Watch System© → signaux faibles → tableaux de bord → pénuries, surplus et disparités → Cartographie Dynamique© → intelligence prédictive → intelligence systémique intersectorielle → simulation → recommandation → arbitrage humain → décision → suivi → mémoire analytique.

4. Données internes et externes

Les sources internes et externes restent identifiées, qualifiées et gouvernées. Provenance, temporalité, couverture, définition, droits d'usage et transformations conditionnent la valeur analytique de la donnée.

5. Analyse statistique et détection d'anomalies

L'analyse statistique établit références, distributions, tendances et variabilité. La détection d'anomalies identifie les écarts nécessitant investigation, sans assimiler automatiquement une anomalie à une fraude, une panne ou une crise.

6. Watch System© et signaux faibles

Watch System© organise la veille continue, la persistance, la convergence et l'escalade des signaux. La détection précoce complète les seuils classiques en identifiant des indices émergents encore insuffisants pour constituer une tendance ou une alerte confirmée.

7. Tableaux de bord prévisionnels

Les tableaux de bord réunissent état observé, tendances, alertes, signaux faibles et projections. Observation historique, estimation et prévision restent visuellement et sémantiquement distinctes.

8. Pénuries, surplus et disparités

Le système analyse simultanément insuffisances, excédents et écarts territoriaux ou sectoriels. Tension, pénurie constatée et risque prévisionnel sont séparés ; stock élevé et surplus sont séparés ; disparité statistique et causalité sont séparées.

9. Cartographie Dynamique©

La Cartographie Dynamique© relie géographie, temps, ressources, flux, infrastructures, tensions, surplus, disparités, anomalies et projections. La granularité de la représentation ne doit jamais dépasser la précision réellement supportée par les données.

10. Intelligence prédictive

Les modèles produisent des trajectoires conditionnelles accompagnées d'horizon, version, hypothèses et incertitude. Prévision et certitude restent distinctes ; les performances sont mesurées par backtesting, erreurs, calibration et surveillance de dérive.

11. Intelligence systémique intersectorielle

Le graphe d'interdépendances rapproche ressources, infrastructures, secteurs et territoires afin d' examiner les effets en chaîne et capacités de résilience. Interdépendance, corrélation et causalité ne sont jamais assimilées automatiquement.

12. Simulation et stress tests

Les simulations explorent des hypothèses explicites et permettent de comparer des trajectoires, chocs, contraintes et options. Simulation, prévision, observation et décision constituent quatre objets différents.

13. IA décisionnelle assistive

L'IA peut produire des synthèses, options et recommandations explicables. Elle ne possède pas, par défaut, l'autorité institutionnelle de décider ou d'exécuter. Les décisions à conséquence significative restent soumises à une autorité humaine ou institutionnelle identifiable.

14. Gouvernance et souveraineté

Finalité, classification, minimisation, contrôle d’accès, résidence, portabilité, réversibilité, séparation des pouvoirs et continuité opérationnelle encadrent l’ensemble. L’architecture peut être fédérée afin que convergence analytique ne signifie pas centralisation absolue des données.

15. Deep Authenticity©

Deep Authenticity© assure la continuité vérifiable entre sources, datasets, transformations, modèles, configurations, exécutions, résultats, prévisions, recommandations et validations. Authenticité, exactitude, performance et vérité prédictive restent des notions distinctes.

16. AP Ledger et mémoire analytique

AP Ledger peut ancrer des preuves minimales d’antériorité, de version et d’intégrité. La mémoire analytique conserve ce qui était réellement connu, prévu, recommandé, décidé et exécuté à un moment donné, sans réécriture silencieuse de l’historique.

17. Centre d’Intelligence Systémique

Le Centre d’Intelligence Systémique constitue la couche opérationnelle de convergence. Il coordonne observation, veille, cartographie, prévision, simulation et aide à la décision tout en maintenant expertise sectorielle, droits territoriaux, continuité et responsabilités.

18. Critères d’acceptation transversaux

Une mise en œuvre conforme doit notamment assurer : provenance et date des données ; distinction observation/estimation/prévision ; traçabilité des modèles et versions ; visibilité de l’incertitude ; séparation recommandation/décision/exécution ; contrôle humain des décisions significatives ; protection des données sensibles ; auditabilité ; réversibilité ; continuité opérationnelle ; et prévention d’une surveillance disproportionnée des citoyens.

19. Principe de responsabilité

L’intelligence systémique n’efface jamais la responsabilité. Les rôles de fournisseur de données, responsable de modèle, analyste, validateur, décideur, opérateur et auditeur doivent rester identifiables. La technologie augmente la capacité d’analyse ; elle ne dissout pas l’autorité ni l’ obligation de rendre compte.

20. Clôture officielle du Volume V

Le Volume V — Données, IA et Intelligence Systémique — établit ainsi une architecture complète allant de la donnée brute gouvernée à la mémoire vérifiable de la décision. Son principe directeur est une intelligence augmentée mais maîtrisée : observer sans confondre, anticiper sans prétendre savoir avec certitude, simuler sans imposer, recommander sans usurper la décision, et conserver une preuve vérifiable de la chaîne analytique. Le Volume V est, à ce stade, structurellement clôturé.

Principes de clôture — Formule synthétique

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VI — JUMEAU NUMÉRIQUE NATIONAL ET SIMULATION INSTITUTIONNELLE

CHAPITRE 1 — FONDEMENTS ET ARCHITECTURE DU JUMEAU NUMÉRIQUE NATIONAL©

IDENTITÉ — ÉTAT — ÉVÉNEMENTS — RELATIONS — TEMPORALITÉ — SYNCHRONISATION — FÉDÉRATION — PROVENANCE — GOUVERNANCE

1. Objet du chapitre

Ce chapitre définit les fondements du Jumeau Numérique National© : une représentation numérique gouvernée, évolutive et vérifiable d'objets, organisations, secteurs, territoires, infrastructures et institutions. Sa finalité est de permettre observation, compréhension, simulation et comparaison de trajectoires sans confondre la représentation numérique avec le réel.

2. Principe de non-confusion

Le jumeau numérique représente un état du réel à partir de données disponibles, de règles et de modèles. Il peut être incomplet, différé ou incertain. L'architecture maintient donc la distinction : objet réel ≠ état numérique ≠ estimation ≠ simulation ≠ décision ≠ exécution réelle.

3. Échelle des jumeaux

L'architecture suit une progression fédérée : Jumeau Numérique du Produit → de l'Entreprise → du Secteur → du Territoire → Jumeau Numérique National© → Jumeau Numérique Institutionnel. Chaque niveau conserve ses responsabilités, son périmètre et ses règles d'accès.

4. Identité numérique

Tout objet représenté possède une identité numérique stable ou versionnée selon sa nature. Cette identité permet de relier états, événements, documents, ressources, dépendances et historiques sans imposer une centralisation physique de toutes les données.

5. État du jumeau

L’état décrit les propriétés connues à un instant ou une période : statut, capacité, localisation, disponibilité, configuration, indicateurs ou autres attributs pertinents. Chaque valeur conserve sa date, sa source et, lorsque nécessaire, son niveau de confiance.

6. Événements

Les événements décrivent les changements : production, transfert, incident, mise à jour, décision, exécution ou modification institutionnelle. Ils permettent de reconstruire comment un état a évolué dans le temps.

7. Relations et dépendances

Les jumeaux peuvent être reliés par appartenance, composition, approvisionnement, flux, dépendance, autorité, responsabilité ou autres relations gouvernées. Ces relations constituent la base des simulations multisectorielles.

8. Temporalité

Le système distingue temps de l’événement, temps de collecte, temps de réception et temps de traitement lorsque cela est pertinent. Cette séparation empêche qu’une information ancienne reçue tardivement soit interprétée comme un événement actuel.

9. Synchronisation avec le réel

Le jumeau est synchronisé selon la fréquence appropriée à chaque objet : temps réel, quasi temps réel, périodique ou événementiel. Une absence de mise à jour est visible et ne doit pas être interprétée comme une stabilité certaine du réel.

10. États observés, estimés et simulés

Un état observé provient d’une source ; un état estimé résulte d’un calcul destiné à combler ou interpréter une information ; un état simulé appartient à un scénario. Ces trois catégories sont explicitement marquées.

11. Architecture fédérée

Le Jumeau Numérique National© peut agréger des représentations distribuées sans copier systématiquement leurs données sources. Les domaines souverains exposent uniquement les informations, indicateurs ou preuves nécessaires selon les droits et finalités.

12. Interopérabilité

Des schémas, identifiants, vocabulaires et interfaces documentés permettent aux jumeaux de communiquer. Les correspondances entre modèles sectoriels sont versionnées afin que les changements de définition restent traçables.

13. Granularité

Le niveau de détail dépend de la finalité, de la qualité des données et de la sensibilité. Une représentation nationale n'exige pas nécessairement l'accès à la granularité individuelle ; l'agrégation est privilégiée lorsqu'elle suffit.

14. Provenance et Deep Authenticity©

Deep Authenticity© relie chaque état et événement aux sources, transformations et versions ayant contribué à sa représentation. Il permet de distinguer donnée authentifiée, donnée transformée, estimation et résultat de modèle.

15. Jumeau du produit et de l'entreprise

Les premiers niveaux permettent de représenter cycle de vie, capacités, stocks, flux, équipements ou autres propriétés autorisées d'un produit ou d'une entreprise. Ils constituent des briques possibles des niveaux sectoriels supérieurs.

16. Jumeau sectoriel et territorial

Le niveau sectoriel agrège acteurs, capacités, ressources et dépendances d'un domaine. Le niveau territorial rapproche plusieurs secteurs sur une zone afin d'étudier ressources, infrastructures, flux, pénuries, surplus, disparités et résilience.

17. Jumeau National©

Le niveau national relie les jumeaux sectoriels et territoriaux dans une vue systémique. Il ne prétend pas reproduire chaque détail du pays ; il maintient les états et relations nécessaires à l'analyse nationale, à l'anticipation et à la simulation.

18. Jumeau Numérique Institutionnel

Le jumeau institutionnel représente structures, compétences, processus, règles, décisions et capacités d'exécution d'une institution selon un périmètre gouverné. Il prépare la simulation institutionnelle profonde sans substituer le modèle à l'autorité réelle.

19. Gouvernance, sécurité et responsabilité

Finalité, minimisation, classification, contrôle d'accès, souveraineté, séparation des rôles et audit encadrent chaque niveau. Le jumeau national est conçu pour modéliser des systèmes et institutions, non pour constituer une surveillance généralisée des citoyens.

20. Critères d'acceptation et conclusion

L'architecture est acceptable si réel et représentation restent distincts ; si identité, état, événement, relation et temporalité sont traçables ; si états observés, estimés et simulés sont séparés ; si la fédération préserve la souveraineté des domaines ; si la granularité est proportionnée ; et si la responsabilité institutionnelle demeure identifiable. Le Chapitre 2 développera le modèle d'identité, d' état et de synchronisation des jumeaux.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VI — JUMEAU NUMÉRIQUE NATIONAL ET SIMULATION INSTITUTIONNELLE

CHAPITRE 2 — IDENTITÉ, ÉTAT, ÉVÉNEMENTS ET SYNCHRONISATION DU JUMEAU

IDENTITÉ PERSISTANTE — ÉTAT COURANT — HISTORIQUE — ÉVÉNEMENTS — TEMPORALITÉ — FRAÎCHEUR — RÉCONCILIATION — VERSIONING

1. Objet du chapitre

Ce chapitre formalise le mécanisme par lequel un jumeau numérique conserve son identité, représente un état, enregistre ses changements et se synchronise avec les systèmes ou phénomènes réels qu'il représente. Il fournit le socle temporel nécessaire aux simulations et aux comparaisons futures.

2. Identité persistante

Chaque jumeau possède un identifiant stable dans son périmètre de gouvernance. Les changements de nom, de statut, de propriétaire, de rattachement ou de classification ne doivent pas créer artificiellement un nouvel objet lorsque l'identité réelle demeure la même.

3. Cycle de vie

Création, activation, modification, suspension, fusion, séparation, archivage ou retrait sont représentés comme des états ou événements gouvernés. Le cycle de vie numérique doit rester relié au cycle de vie réel sans effacer les étapes antérieures.

4. État courant

L'état courant est la meilleure représentation disponible à un instant donné selon les données reçues et les règles de réconciliation. Il conserve une date de validité, une date de dernière mise à jour et la provenance des attributs importants.

5. Historique des états

Le système conserve les états antérieurs ou les événements permettant de les reconstruire. Cette capacité est indispensable pour savoir ce que le jumeau représentait avant une décision, une simulation ou un incident.

6. Événements de changement

Un événement décrit une transition : modification de capacité, déplacement, changement de statut, production, consommation, transfert, incident, décision ou autre fait pertinent. L'événement conserve type, temps, source et relation avec l'objet concerné.

7. Temporalité multiple

Le système peut distinguer le moment où un fait s'est produit, celui où il a été observé, celui où il a été transmis et celui où il a été intégré. Cette temporalité multiple évite de confondre retard d'information et retard du phénomène réel.

8. Horodatage et ordre des événements

Les événements sont ordonnés selon des règles explicites. Lorsque plusieurs sources fournissent des temps différents ou incomplets, l'incertitude temporelle est conservée plutôt que masquée par un ordre artificiellement précis.

9. Fraîcheur de l'état

Chaque attribut ou ensemble d'attributs peut porter une mesure de fraîcheur. Un état ancien peut rester la dernière information disponible, mais il doit être identifiable comme potentiellement obsolète.

10. Synchronisation

La synchronisation peut être continue, périodique, événementielle ou manuelle selon le type de jumeau. La fréquence est proportionnée à la vitesse réelle du phénomène et aux besoins opérationnels.

11. Retards et données tardives

Une donnée reçue tardivement peut modifier la compréhension d'un état historique. Le système l' intègre sans réécrire silencieusement ce qui était connu précédemment : temps du fait et temps de connaissance restent distincts.

12. Sources multiples

Plusieurs sources peuvent décrire le même attribut. Le jumeau conserve leur provenance et applique des règles de priorité, confiance ou validation sans supprimer les divergences utiles à l'audit.

13. Conflits de sources

Lorsque deux sources crédibles se contredisent, le système peut marquer l'état comme contesté, conserver plusieurs valeurs candidates ou solliciter une validation. Il ne fabrique pas une certitude par simple moyenne si les valeurs décrivent des réalités incompatibles.

14. Réconciliation

La réconciliation transforme plusieurs observations en un état de référence selon des règles versionnées : autorité de source, fraîcheur, qualité, cohérence ou validation humaine. Le résultat reste relié aux observations ayant contribué à sa production.

15. États observés, estimés et simulés

Les valeurs observées proviennent de sources ; les valeurs estimées complètent ou interprètent l' information ; les valeurs simulées appartiennent à une trajectoire hypothétique. Leur nature est conservée au niveau des attributs et des interfaces.

16. Branches de simulation

Une simulation crée une branche logique à partir d'un état de référence. Les événements simulés ne modifient jamais l'état réel du jumeau tant qu'une action n'a pas été autorisée puis exécutée dans le monde réel.

17. Versioning et snapshots

Des snapshots peuvent figer l'état d'un ensemble de jumeaux à une date donnée. Ils permettent de reproduire une simulation, comparer deux décisions ou reconstruire le contexte exact d'une analyse.

18. Deep Authenticity© et continuité temporelle

Deep Authenticity© relie identité, état, événements, sources, transformations et versions. Il permet de vérifier qu'un état historique n'a pas été remplacé silencieusement et que les corrections restent distinguables des données initiales.

19. Monitoring de synchronisation

Watch System© peut surveiller les retards, pertes de flux, divergences persistantes, changements de schéma ou ruptures de synchronisation. Une alerte de synchronisation concerne la qualité du jumeau et ne doit pas être confondue avec une alerte sur le phénomène réel.

20. Critères d'acceptation et conclusion

Le mécanisme est acceptable si l'identité reste stable et traçable ; si les états historiques sont reconstructibles ; si temps du fait et temps de connaissance sont distingués ; si fraîcheur et conflits de sources sont visibles ; si les simulations restent isolées du réel ; si les corrections sont versionnées ; et si la synchronisation elle-même est surveillée. Le Chapitre 3 développera le Jumeau Numérique du Produit.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VI — JUMEAU NUMÉRIQUE NATIONAL ET SIMULATION INSTITUTIONNELLE

CHAPITRE 3 — JUMEAU NUMÉRIQUE DU PRODUIT

IDENTITÉ — COMPOSITION — CYCLE DE VIE — ÉTAT — TRAÇABILITÉ — FLUX — QUALITÉ — SIMULATION — AGRÉGATION

1. Objet du chapitre

Ce chapitre définit le Jumeau Numérique du Produit comme première unité concrète de l'architecture du Volume VI. Il représente, selon la finalité autorisée, l'identité, la composition, les états, les événements, la provenance, les transformations et le cycle de vie d'un produit ou d'une catégorie de produits.

2. Produit unitaire et produit agrégé

Le jumeau peut représenter une unité individualisée lorsque cela est nécessaire ou une référence, un lot, une famille ou une catégorie lorsque l'agrégation suffit. Le niveau de granularité est proportionné à la finalité et aux exigences de confidentialité.

3. Identité du produit

L'identité peut relier référence, version, lot, série, catégorie, fabricant ou autres attributs pertinents. Une modification de conditionnement ou de statut n'implique pas automatiquement la création d'une nouvelle identité métier.

4. Composition

Lorsque cela est pertinent, le jumeau représente composants, matières, sous-ensembles, quantités et relations de composition. Chaque composant peut lui-même être relié à un jumeau ou à une référence vérifiable.

5. Origine et provenance

Le produit peut être relié à son origine, aux étapes de transformation et aux acteurs autorisés de sa chaîne. Deep Authenticity© permet de conserver la provenance des informations sans exposer inutilement des données commerciales sensibles.

6. État du produit

L'état peut inclure disponibilité, localisation agrégée ou autorisée, qualité, statut logistique, condition, conformité ou autre propriété pertinente. Chaque valeur conserve sa temporalité et sa source.

7. Cycle de vie

Conception, fabrication, transformation, stockage, distribution, utilisation, maintenance, retour, recyclage ou retrait peuvent constituer des phases selon la nature du produit. Le modèle reste adaptable aux différents secteurs.

8. Événements de cycle de vie

Production, contrôle, transfert, réception, transformation, changement de statut ou retrait sont enregistrés comme événements lorsqu'ils sont pertinents. Ils permettent de reconstruire l'évolution du jumeau.

9. Qualité et conformité

Le jumeau peut référencer contrôles, certificats, statuts de conformité et anomalies autorisées. Il distingue la présence d'une preuve de conformité de l'évaluation technique ou réglementaire elle-même.

10. Stocks et disponibilité

Les jumeaux produits agrégés peuvent contribuer à représenter quantités disponibles, réservées, en transit, transformées ou indisponibles. Ces états alimentent les analyses de pénuries et de surplus sans double comptage.

11. Flux logistiques

Les transferts entre entreprises, sites ou territoires peuvent être représentés sous forme d'événements ou flux agrégés. Le modèle distingue expédition, transit, réception et disponibilité réelle.

12. Temporalité et péremption

Pour les produits sensibles au temps, dates de fabrication, durée de vie, expiration ou fenêtres d'utilisation peuvent influencer l'état. Une quantité physiquement présente n'est pas nécessairement une quantité réellement disponible.

13. Maintenance et produits durables

Pour les équipements ou biens durables, le jumeau peut représenter usage, maintenance, indisponibilité, composants remplacés et capacité restante selon les données autorisées.

14. Anomalies et rappels

Une anomalie de qualité, une incohérence de provenance ou un rappel peut être propagé vers les jumeaux concernés. Le système doit pouvoir identifier le périmètre affecté sans généraliser à des produits non concernés.

15. Simulation du produit

Le jumeau peut simuler évolution de stock, consommation, vieillissement, disponibilité, transformation ou maintenance. Les états simulés sont isolés des états observés et n'altèrent jamais la représentation réelle.

16. Scénarios de substitution

Lorsque plusieurs produits sont techniquement substituables, le système peut tester des scénarios de remplacement. La compatibilité doit être validée selon les contraintes sectorielles, réglementaires, sanitaires ou techniques applicables.

17. Agrégation vers l'entreprise

Les jumeaux produits peuvent alimenter le Jumeau Numérique de l'Entreprise par des indicateurs de production, stocks, capacités, commandes, flux et qualité. L'entreprise n'a pas besoin de centraliser chaque détail si des agrégats gouvernés suffisent.

18. Deep Authenticity© et AP Ledger

Deep Authenticity© relie identité, composition, événements et preuves. AP Ledger peut ancrer des empreintes minimales de versions, lots, contrôles ou événements critiques sans transformer le Ledger en base de données de produits.

19. Gouvernance et confidentialité

Secrets industriels, prix contractuels, fournisseurs sensibles ou informations stratégiques sont compartimentés. Le partage entre niveaux du jumeau suit la finalité, les droits et le principe de minimisation.

20. Critères d'acceptation et conclusion

Le Jumeau Numérique du Produit est acceptable si identité, composition, état et événements sont traçables ; si la granularité est proportionnée ; si stock physique et disponibilité réelle sont distingués ; si les simulations restent isolées ; si la provenance est vérifiable ; et si l'agrégation vers les niveaux supérieurs respecte confidentialité et souveraineté. Le Chapitre 4 développera le Jumeau Numérique de l'Entreprise.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VI — JUMEAU NUMÉRIQUE NATIONAL ET SIMULATION INSTITUTIONNELLE

CHAPITRE 4 — JUMEAU NUMÉRIQUE DE L'ENTREPRISE

PRODUITS — SITES — ÉQUIPEMENTS — STOCKS — CAPACITÉS — RESSOURCES — PRODUCTION — FLUX — DÉPENDANCES — SCÉNARIOS — RÉSILIENCE

1. Objet du chapitre

Ce chapitre définit le Jumeau Numérique de l'Entreprise comme représentation dynamique et gouvernée de ses capacités opérationnelles, ressources, produits, sites, équipements, stocks, flux, engagements, dépendances et événements pertinents. Il constitue le niveau d'agrégation permettant de passer des jumeaux produits au jumeau sectoriel.

2. Entreprise comme système dynamique

Le jumeau ne se limite pas à une fiche administrative. Il représente, selon la finalité autorisée, la manière dont ressources, équipements, stocks, commandes, capacités et contraintes interagissent dans le temps.

3. Identité et périmètre

L’entreprise, ses établissements, sites, unités ou fonctions peuvent disposer d’identités reliées. Le périmètre du jumeau précise quelles entités juridiques, opérationnelles ou géographiques sont incluses afin d’éviter les doubles comptages.

4. Agrégation des jumeaux produits

Les produits, lots, familles ou catégories peuvent alimenter des indicateurs de production, stock, qualité, commandes et flux. L’agrégation conserve les règles de calcul et ne nécessite pas de transmettre chaque détail produit aux niveaux supérieurs.

5. Sites et infrastructures

Usines, entrepôts, plateformes, bureaux, installations ou autres sites pertinents peuvent être représentés avec leurs fonctions, capacités et dépendances. Les localisations sensibles restent protégées selon les règles applicables.

6. Équipements et actifs

Les équipements critiques peuvent être reliés à disponibilité, état, maintenance, capacité ou contraintes. Une capacité nominale d’équipement est distinguée de la capacité réellement mobilisable.

7. Capacités de production et de service

Le jumeau distingue capacité théorique, installée, disponible, utilisée et mobilisable. Les contraintes en ressources, maintenance, approvisionnement, compétences ou infrastructures peuvent expliquer l’ écart entre ces niveaux.

8. Stocks et ressources

Matières, composants, produits, ressources énergétiques ou autres intrants peuvent être représentés selon quantité, disponibilité, réservation, transit et couverture. Les réserves stratégiques ou contractuellement engagées sont distinguées des stocks libres.

9. Commandes, engagements et demande

Les commandes reçues, engagements de livraison, prévisions internes ou autres signaux de demande peuvent influencer la charge future. Une prévision commerciale reste distincte d’une commande ferme.

10. Production et opérations

Les activités peuvent être représentées par cycles, ordres, volumes, rendement, disponibilité ou autres indicateurs adaptés. Le jumeau permet de relier production observée, capacité disponible et contraintes actives.

11. Flux entrants et sortants

Approvisionnements, livraisons, transferts et autres flux autorisés relient l'entreprise à ses fournisseurs, clients, sites et territoires. Expédition, transit, réception et disponibilité réelle restent des états distincts.

12. Dépendances externes

Le jumeau peut représenter dépendances envers fournisseurs, énergie, eau, transport, télécommunications, compétences, infrastructures ou autres ressources. Leur criticité dépend notamment de la concentration, de la substituabilité et du délai de remplacement.

13. Contraintes et goulots d'étranglement

Une capacité globale peut être limitée par un maillon particulier. Le système peut identifier équipements, ressources, flux ou processus susceptibles de devenir des goulots d'étranglement, sans transformer une estimation en certitude opérationnelle.

14. Indicateurs et état synthétique

Des indicateurs agrégés décrivent activité, capacité, disponibilité, charge, stocks, délais, qualité ou résilience. Chaque indicateur conserve définition, période, provenance et méthode d'agrégation.

15. Événements et anomalies

Panne, retard, rupture d'approvisionnement, variation de capacité, incident qualité ou autre événement pertinent peut modifier l'état. Watch System© peut suivre les anomalies et leur persistance sans confondre alerte technique et situation réelle confirmée.

16. Simulation d'entreprise

Le jumeau peut tester hausse de demande, perte de fournisseur, indisponibilité d'équipement, variation de stock ou autre scénario. Les branches simulées restent séparées de l'état opérationnel réel.

17. Résilience et alternatives

Les scénarios peuvent identifier stocks de sécurité, fournisseurs alternatifs, capacités redondantes, itinéraires secondaires ou autres moyens d'absorption. La résilience est évaluée selon continuité, substitution, adaptation et temps de récupération.

18. Agrégation vers le secteur

Le Jumeau Numérique du Secteur reçoit uniquement les indicateurs, capacités, flux, dépendances ou événements nécessaires à la finalité sectorielle et autorisés par la gouvernance. L'agrégation peut préserver confidentialité commerciale et secrets industriels.

19. Deep Authenticity©, AP Ledger et gouvernance

Deep Authenticity© relie les indicateurs d'entreprise aux données, événements et transformations autorisés. AP Ledger peut ancrer des versions ou événements critiques. Accès, export, simulation et partage sont contrôlés selon rôle, finalité et sensibilité.

20. Critères d'acceptation et conclusion

Le Jumeau Numérique de l'Entreprise est acceptable si l'entreprise est représentée comme système dynamique ; si capacités nominales et mobilisables sont distinguées ; si commandes et prévisions restent séparées ; si les dépendances sont explicables ; si les simulations n'altèrent pas l'état réel ; si les données sensibles sont minimisées ; et si l'agrégation sectorielle ne nécessite pas une centralisation exhaustive. Le Chapitre 5 développera le Jumeau Numérique du Secteur.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VI — JUMEAU NUMÉRIQUE NATIONAL ET SIMULATION INSTITUTIONNELLE

CHAPITRE 5 — JUMEAU NUMÉRIQUE DU SECTEUR

ENTREPRISES — CHAÎNES DE VALEUR — CAPACITÉS — RESSOURCES — INFRASTRUCTURES — FLUX — DÉPENDANCES — ÉQUILIBRES — RÉSILIENCE

1. Objet du chapitre

Ce chapitre définit le Jumeau Numérique du Secteur comme représentation dynamique et gouvernée d'un domaine économique, productif, social ou de service. Il agrège les informations nécessaires provenant des entreprises, infrastructures, ressources et acteurs du secteur afin d'analyser capacités, flux, dépendances, équilibres, tensions et résilience.

2. Périmètre sectoriel

Chaque jumeau sectoriel possède un périmètre explicite : agriculture, eau, énergie, industrie, transport, santé, commerce, télécommunications ou autre domaine défini. Les frontières peuvent évoluer, mais leurs versions doivent rester traçables pour préserver la comparabilité historique.

3. Agrégation des entreprises

Les Jumeaux Numériques des Entreprises contribuent par des indicateurs, capacités, stocks, flux, dépendances ou événements autorisés. Le niveau sectoriel ne nécessite pas l'accès systématique aux données détaillées de chaque entreprise.

4. Acteurs et rôles

Producteurs, fournisseurs, transformateurs, distributeurs, opérateurs d'infrastructure, institutions ou autres catégories peuvent être représentés selon leur fonction dans le secteur. Les relations sont modélisées sans exposer inutilement des informations sensibles.

5. Chaînes de valeur

Le jumeau représente les principales étapes reliant ressources, production, transformation, stockage, transport, distribution et consommation ou utilisation finale. Cette représentation permet d'identifier les maillons dont dépend la continuité du secteur.

6. Capacités sectorielles

Les capacités théoriques, disponibles, utilisées et mobilisables peuvent être agrégées par activité, territoire ou catégorie. Les règles d'agrégation évitent de compter comme mobilisable une capacité indisponible ou dépendante d'une ressource absente.

7. Ressources et intrants

Matières, eau, énergie, composants, compétences, capacités financières ou autres ressources pertinentes peuvent être reliées aux activités qui en dépendent. Le jumeau distingue disponibilité nationale, importée, locale, contractuelle ou stratégique lorsque les données le permettent.

8. Infrastructures sectorielles

Réseaux, plateformes, installations, capacités de stockage, transport ou autres infrastructures sont intégrés comme objets structurants. Leur disponibilité et criticité peuvent influencer plusieurs acteurs simultanément.

9. Flux sectoriels

Les flux agrégés d'approvisionnement, production, transformation et distribution permettent d' observer la circulation des ressources et produits. Origine, destination, volume, période et délai sont conservés à la granularité autorisée.

10. Offre, demande et équilibre

Le jumeau rapproche capacités, production, stocks, commandes, consommation ou besoins afin d' estimer l'équilibre sectoriel. Un équilibre national peut masquer des tensions territoriales ou des inadéquations de qualité, calendrier ou segment.

11. Pénuries et surplus sectoriels

Les mécanismes du Volume V sont intégrés au jumeau : tensions, couverture, risques de rupture, excédents et capacités inutilisées. Les états observés sont distingués des risques et scénarios futurs.

12. Dépendances critiques

Le système peut identifier concentration de fournisseurs, dépendance à une ressource, infrastructure ou importation, ainsi que substituabilité et délai de remplacement. La criticité dépend du contexte et ne se réduit pas au nombre de dépendances.

13. Interdépendances internes

Les sous-secteurs peuvent dépendre les uns des autres. Une difficulté en amont peut se transmettre à la transformation, au transport ou à la distribution ; les chemins de propagation sont modélisés comme hypothèses explicables.

14. Territorialisation du secteur

Le jumeau sectoriel peut être décliné par territoire afin de comparer capacités, ressources, infrastructures, flux et besoins. Cette territorialisation prépare le Jumeau Numérique du Territoire en rapprochant plusieurs secteurs sur une même zone.

15. Watch System© sectoriel

Watch System© surveille anomalies, retards, capacités, stocks, flux, dépendances et signaux faibles du secteur. Les alertes conservent source, persistance, criticité et niveau de confiance.

16. Simulation sectorielle

Le jumeau peut simuler variation de demande, baisse de capacité, rupture d'approvisionnement, changement de flux, mobilisation de stocks ou substitution. Chaque scénario reste une branche séparée de l'état observé.

17. Résilience sectorielle

La résilience est évaluée selon diversité des acteurs, redondance, substituabilité, stocks, capacités de réserve, alternatives logistiques et temps de récupération. Le système analyse vulnérabilités et capacités d'absorption conjointement.

18. Agrégation vers le territoire et le national

Le jumeau sectoriel expose aux niveaux territorial et national les indicateurs, états, capacités, dépendances et alertes nécessaires selon les droits. La fédération permet une vision systémique sans centralisation exhaustive des données sources.

19. Deep Authenticity©, AP Ledger et gouvernance

Deep Authenticity© vérifie provenance, agrégations, versions et relations. AP Ledger peut ancrer les événements ou versions critiques. Les secrets commerciaux, informations stratégiques et données sensibles restent compartimentés.

20. Critères d'acceptation et conclusion

Le Jumeau Numérique du Secteur est acceptable si son périmètre est explicite ; si les agrégations sont traçables ; si capacités et disponibilités réelles sont distinguées ; si les chaînes de valeur et dépendances sont explicables ; si les simulations restent séparées du réel ; si la confidentialité des entreprises est préservée ; et si l'agrégation vers les niveaux supérieurs demeure gouvernée. Le Chapitre 6 développera le Jumeau Numérique du Territoire.

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VI — JUMEAU NUMÉRIQUE NATIONAL ET SIMULATION INSTITUTIONNELLE

CHAPITRE 6 — JUMEAU NUMÉRIQUE DU TERRITOIRE

POPULATION AGRÉGÉE — RESSOURCES — INFRASTRUCTURES — SERVICES — ÉCONOMIE — FLUX — ENVIRONNEMENT — DISPARITÉS — RISQUES — RÉSILIENCE

1. Objet du chapitre

Ce chapitre définit le Jumeau Numérique du Territoire comme représentation dynamique, multisectorielle et gouvernée d'un espace géographique. Il rapproche ressources, infrastructures, services, activités économiques, flux, indicateurs sociaux agrégés, environnement, risques et capacités de résilience afin de comprendre les interactions territoriales.

2. Identité et périmètre territorial

Chaque territoire possède une identité, des limites et un niveau administratif ou fonctionnel explicites. Les changements de découpage sont versionnés afin de préserver la comparabilité historique et d' éviter d'attribuer artificiellement une évolution statistique à un changement de frontière.

3. Articulation des échelles

Le jumeau peut fonctionner aux niveaux local, communal, régional ou autre échelle autorisée. Les agrégations et désagrégations respectent la précision des données ; un zoom cartographique ne crée jamais une information plus fine que celle réellement disponible.

4. Population et besoins agrégés

Les indicateurs démographiques et sociaux utiles sont représentés à une granularité agrégée et proportionnée. Le jumeau vise à comprendre besoins, accès et dynamiques territoriales, non à suivre individuellement les citoyens.

5. Ressources territoriales

Eau, énergie, ressources agricoles, capacités de stockage, foncier ou autres ressources pertinentes peuvent être représentés selon disponibilité, capacité, saisonnalité, qualité et contraintes d'accès.

6. Infrastructures

Réseaux de transport, énergie, eau, télécommunications, santé, logistique et autres infrastructures structurantes sont reliés aux secteurs et services qu'ils soutiennent. Leur état et criticité contribuent à l'analyse de continuité territoriale.

7. Services essentiels

Le jumeau peut représenter capacités et accessibilité agrégées de services essentiels selon les données autorisées. Capacité théorique, disponibilité réelle, charge et accessibilité sont distinguées.

8. Activité économique

Entreprises et secteurs contribuent par des indicateurs agrégés de capacité, production, emploi, stocks, flux ou activité. Les secrets commerciaux et informations stratégiques restent dans leurs domaines gouvernés.

9. Flux territoriaux

Entrées, sorties et flux internes de personnes agrégées, marchandises, ressources, énergie ou services peuvent être analysés lorsque la finalité le justifie. Origine, destination, volume, période et dépendance sont représentés à la granularité appropriée.

10. Environnement et contraintes naturelles

Les données environnementales pertinentes peuvent être intégrées pour comprendre disponibilité des ressources, contraintes physiques, saisonnalité et exposition. Une relation spatiale n’est pas automatiquement interprétée comme une causalité.

11. Pénuries et surplus

Le jumeau territorial rapproche stocks, capacités, besoins et flux pour identifier tensions, pénuries ou surplus. Un équilibre national peut ainsi être décomposé afin de révéler des déséquilibres locaux.

12. Disparités territoriales

Les indicateurs permettent de comparer accès, capacités, ressources, activité et services entre territoires. Les disparités sont contextualisées et ne doivent pas être utilisées pour stigmatiser des populations ou attribuer une cause sans preuve.

13. Cartographie Dynamique©

La Cartographie Dynamique© constitue l’interface spatiale du jumeau. Elle superpose état observé, historique, alertes, dépendances, flux et projections tout en maintenant une séparation visuelle entre réel, estimation et simulation.

14. Risques et vulnérabilités

Le jumeau peut analyser exposition, dépendances critiques, concentration des capacités, substituabilité, temps de récupération et autres facteurs de vulnérabilité. Un score de risque sert à prioriser l’analyse, non à déclarer qu’un événement va nécessairement se produire.

15. Résilience territoriale

La résilience inclut redondance des infrastructures, alternatives logistiques, capacités locales, stocks, coopération interterritoriale et vitesse de récupération. Les ressources d'adaptation sont analysées conjointement aux vulnérabilités.

16. Watch System© territorial

Watch System© rapproche anomalies et signaux faibles issus de plusieurs secteurs sur un même territoire. Il peut identifier une convergence multisectorielle tout en conservant source, confiance, temporalité et statut de validation.

17. Simulation territoriale

Le jumeau peut tester perte d'infrastructure, hausse de demande, baisse de ressource, rupture logistique, redistribution de flux ou mobilisation de capacités. Chaque scénario constitue une branche isolée de l'état observé.

18. Interterritorialité

Les territoires sont reliés par ressources, réseaux, chaînes logistiques, services et dépendances. Une simulation peut donc analyser la propagation d'un choc ou l'effet d'une coopération entre plusieurs territoires.

19. Agrégation vers le Jumeau Numérique National©

Les jumeaux territoriaux exposent au niveau national les indicateurs, états, alertes, capacités et dépendances nécessaires selon les droits. La vue nationale résulte de cette fédération et non d'une duplication exhaustive de toutes les données locales.

20. Critères d'acceptation et conclusion

Le Jumeau Numérique du Territoire est acceptable si les frontières et échelles sont versionnées ; si la granularité respecte les données ; si les citoyens ne font pas l'objet d'un suivi individuel disproportionné ; si ressources, infrastructures, services et flux sont reliés ; si disparités et causalité restent distinctes ; si les simulations n'altèrent pas le réel ; et si l'agrégation nationale demeure fédérée et gouvernée. Le Chapitre 7 développera le Jumeau Numérique National©.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VI — JUMEAU NUMÉRIQUE NATIONAL ET SIMULATION INSTITUTIONNELLE

CHAPITRE 7 — JUMEAU NUMÉRIQUE NATIONAL©

SYSTÈME DE SYSTÈMES — FÉDÉRATION — ÉTAT NATIONAL — SNAPSHOTS — INTERDÉPENDANCES — RÉSILIENCE — SIMULATION

1. Objet du chapitre

Livre Blanc 2026 — Authenticity Plus© / Deep Authenticity© — Document Maître Définitif

Ce chapitre définit le Jumeau Numérique National© comme système fédéré de représentations permettant d'observer, relier et simuler les principales dynamiques nationales. Il orchestre les jumeaux Produit, Entreprise, Secteur et Territoire sans exiger la centralisation exhaustive de leurs données.

2. Système de systèmes

Le niveau national est un système de systèmes. Chaque jumeau composant conserve identité, gouvernance et responsabilités, tandis que le niveau national maintient les relations, indicateurs et dépendances nécessaires à une compréhension multisectorielle.

3. Architecture fédérée

Les domaines sectoriels et territoriaux exposent des états, indicateurs, événements ou preuves selon les droits. Le Jumeau Numérique National© coordonne ces contributions au moyen d'interfaces et de modèles communs plutôt que par copie systématique des données sources.

4. État National Observé

L'État National Observé rassemble les informations effectivement connues et qualifiées à une date donnée. Chaque composante conserve source, temporalité, granularité, fraîcheur et niveau de confiance.

5. État National Estimé

Lorsque certaines informations sont incomplètes, des estimations peuvent compléter la représentation. Elles restent explicitement marquées, reliées aux méthodes utilisées et séparées des observations.

6. Branches Nationales Simulées

Une ou plusieurs branches peuvent être créées à partir d'un état de référence afin d'explorer des scénarios. Les événements et états simulés n'altèrent jamais l'État National Observé.

7. Snapshot national temporel

Un snapshot fige la représentation connue à un instant : états, versions, modèles, données de référence et dépendances. Il permet de reproduire une simulation et d'éviter l'utilisation rétroactive d' informations inconnues au moment étudié.

8. Ressources et capacités nationales

Le jumeau rapproche ressources, capacités installées, disponibles et mobilisables, stocks, infrastructures et services. L'agrégation nationale conserve les différences sectorielles et territoriales nécessaires à l'interprétation.

9. Flux nationaux et internationaux

Les flux internes et externes de ressources, produits, énergie, services ou autres éléments pertinents peuvent être représentés à la granularité autorisée. Importation, transit, disponibilité et consommation restent des états distincts.

10. Besoins et équilibres

Le système rapproche besoins, demande, capacités, stocks et flux pour analyser les équilibres. Un équilibre agrégé national ne doit jamais masquer automatiquement des pénuries, surplus ou disparités territoriales.

11. Interdépendances multisectorielles

Le graphe national relie secteurs, territoires, ressources et infrastructures. Les relations conservent nature, source et confiance ; interdépendance et causalité ne sont pas assimilées.

12. Infrastructures critiques

Les infrastructures dont dépendent plusieurs secteurs peuvent être identifiées selon criticité, concentration, substituabilité et temps de récupération. Les informations sensibles sont compartimentées et accessibles selon les rôles.

13. Vulnérabilités nationales

Le jumeau peut identifier concentration de dépendances, absence d'alternative, tensions de capacité, exposition territoriale ou autres fragilités. Ces résultats servent à prioriser l'analyse et non à déclarer une crise certaine.

14. Résilience nationale

La résilience est représentée par redondances, stocks, capacités de réserve, alternatives, coopération territoriale, substituabilité et vitesse de récupération. Vulnérabilités et capacités d'absorption sont analysées ensemble.

15. Watch System© national

Watch System© rapproche anomalies, alertes et signaux faibles sectoriels ou territoriaux afin d' identifier les phénomènes convergents. Une alerte nationale doit conserver les éléments qui ont contribué à son escalade.

16. Cartographie Dynamique© nationale

La carte nationale représente ressources, capacités, infrastructures, flux, disparités, alertes et projections à des niveaux adaptés. Observation, estimation et simulation restent visuellement distinctes.

17. Simulation nationale

Le jumeau peut simuler chocs simples ou combinés, propagation multisectorielle, redistribution de flux, mobilisation de capacités ou autres hypothèses. Chaque scénario conserve son snapshot initial, ses paramètres et son incertitude.

18. Comparaison simulation-réalité

Après exécution réelle et observation des résultats, le système peut comparer trajectoire simulée et trajectoire observée. Les écarts servent au backtesting, au recalibrage et à l'apprentissage sans modifier rétroactivement la simulation originale.

19. Deep Authenticity©, AP Ledger et souveraineté

Deep Authenticity© assure la continuité entre sources, jumeaux, agrégations, modèles et résultats. AP Ledger peut ancrer snapshots, versions et événements critiques. La souveraineté repose sur fédération, minimisation, réversibilité et contrôle des accès.

20. Critères d'acceptation et conclusion

Le Jumeau Numérique National© est acceptable s'il demeure un système de systèmes ; si observation, estimation et simulation sont séparées ; si les snapshots empêchent la réécriture du contexte historique ; si les disparités ne sont pas masquées par les agrégats ; si les dépendances sont explicables ; si les simulations restent isolées du réel ; et si la souveraineté des domaines est préservée. Le Chapitre 8 développera le Jumeau Numérique Institutionnel.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VI — JUMEAU NUMÉRIQUE NATIONAL ET SIMULATION INSTITUTIONNELLE

CHAPITRE 8 — JUMEAU NUMÉRIQUE INSTITUTIONNEL

STRUCTURES — COMPÉTENCES — RESPONSABILITÉS — PROCESSUS — RÈGLES — RESSOURCES — DÉLAIS — DÉCISIONS — EXÉCUTION — RÉSULTATS

1. Objet du chapitre

Ce chapitre définit le Jumeau Numérique Institutionnel comme représentation gouvernée des structures, compétences, responsabilités, processus, règles, ressources, décisions et capacités d'exécution d'une institution. Il permet d'étudier son fonctionnement et de préparer la Simulation Institutionnelle Profonde© sans substituer le modèle à l'institution réelle.

2. Institution réelle et représentation

Le jumeau institutionnel décrit certains mécanismes de l'institution à partir de données, règles et modèles. Il reste distinct de l'institution, de ses agents, de ses autorités et de ses actes juridiques réels.

3. Identité et périmètre institutionnel

Chaque institution, organisme, direction, service ou unité représentée possède une identité et un périmètre versionnés. Les réorganisations, fusions, transferts de compétence ou changements de rattachement sont conservés dans l'historique.

4. Structures organisationnelles

Le jumeau représente les unités et leurs relations fonctionnelles ou hiérarchiques lorsque cela est nécessaire. Une structure formelle peut être distinguée des circuits opérationnels effectivement observés.

5. Compétences et mandats

Les compétences attribuées à chaque niveau sont modélisées selon les références applicables et leur période de validité. Une capacité technique à effectuer une action ne signifie pas que le rôle possède l'autorité institutionnelle pour la décider.

6. Responsabilités

Les responsabilités de préparation, validation, décision, exécution, contrôle et audit sont identifiées. Cette séparation permet de simuler les processus sans effacer la responsabilité des acteurs réels.

7. Processus institutionnels

Les processus sont représentés par étapes, entrées, sorties, acteurs, règles, délais et dépendances. Le modèle peut décrire aussi bien un processus nominal que certaines variantes autorisées ou situations exceptionnelles.

8. Règles et contraintes

Les règles juridiques, réglementaires, budgétaires, procédurales ou opérationnelles pertinentes peuvent être représentées comme contraintes versionnées. Le moteur de simulation ne doit pas traiter une règle ancienne comme encore applicable sans signaler sa période de validité.

9. Ressources institutionnelles

Budgets agrégés, effectifs autorisés, capacités techniques, infrastructures, systèmes d'information ou autres ressources peuvent être représentés à la granularité nécessaire. Disponibilité théorique et disponibilité réellement mobilisable restent distinctes.

10. Délais et files d'attente

Le jumeau peut représenter temps de traitement, délais de validation, files d'attente, dépendances et goulets d'étranglement. Ces éléments permettent de comprendre pourquoi une décision formellement simple peut avoir un temps d'exécution important.

11. Entrées et dossiers

Les demandes, alertes, dossiers ou événements déclencheurs peuvent entrer dans un processus institutionnel. Leur contenu sensible reste protégé et la simulation peut utiliser des catégories ou données synthétiques lorsque le détail réel n'est pas nécessaire.

12. Décisions institutionnelles

Le jumeau distingue proposition, avis, validation, arbitrage et décision. Une décision simulée n'a aucune valeur institutionnelle réelle et ne peut être exécutée comme un acte officiel.

13. Exécution réelle

Après une décision réelle autorisée, le système peut suivre son exécution : action lancée, ressources mobilisées, délais, obstacles et état d'avancement. Décision et exécution restent deux événements distincts.

14. Résultats et effets

Le jumeau peut rapprocher objectifs, décisions, exécution et résultats observés. Les effets attribués à une décision doivent être analysés avec prudence lorsque plusieurs facteurs externes ont pu contribuer au résultat.

15. Interactions entre institutions

Plusieurs institutions peuvent être reliées par compétence, transmission, autorisation, financement, contrôle ou coordination. Le modèle permet d'identifier les dépendances institutionnelles et les délais de passage entre organisations.

16. Scénarios institutionnels

Le jumeau peut simuler changement de règle, variation de charge, réallocation de ressources, accélération d'une validation, indisponibilité d'un service ou autre hypothèse. Chaque scénario conserve ses paramètres et reste isolé du fonctionnement réel.

17. Performance et résilience institutionnelles

Les simulations peuvent comparer capacité de traitement, continuité, délai, qualité de service, redondance, adaptabilité et temps de récupération. La performance ne doit pas être réduite à un indicateur unique lorsque les missions sont multiples.

18. Deep Authenticity© et AP Ledger

Deep Authenticity© relie structures, règles, versions, décisions et exécutions aux sources autorisées. AP Ledger peut ancrer des versions de processus, règles ou événements critiques afin de préserver l'antériorité et l'intégrité.

19. Gouvernance, droits et limites

Le Jumeau Numérique Institutionnel est soumis à des droits stricts. Il ne doit pas devenir un mécanisme de surveillance individuelle des agents ou citoyens. Les analyses privilégient processus, capacités et résultats agrégés selon la finalité.

20. Critères d'acceptation et conclusion

Le Jumeau Numérique Institutionnel est acceptable si institution réelle et modèle restent distincts ; si compétences et responsabilités sont versionnées ; si décision simulée et décision réelle sont séparées ; si les ressources mobilisables et théoriques sont distinguées ; si les interactions interinstitutionnelles sont explicables ; si la confidentialité est préservée ; et si l'autorité institutionnelle demeure hors du moteur de simulation. Le Chapitre 9 développera la modélisation multisectorielle et multi-institutionnelle.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VI — JUMEAU NUMÉRIQUE NATIONAL ET SIMULATION INSTITUTIONNELLE

CHAPITRE 9 — MODÉLISATION MULTISECTORIELLE ET MULTI-INSTITUTIONNELLE

INTERDÉPENDANCES — MATRICES — FLUX — CONTRAINTES CROISÉES — PROPAGATION — BOUCLES — TEMPORALITÉ — COORDINATION

1. Objet du chapitre

Ce chapitre définit la modélisation multisectorielle et multi-institutionnelle qui relie les différents niveaux du Volume VI. Elle permet de représenter simultanément produits, entreprises, secteurs, territoires, infrastructures et institutions afin d'étudier leurs dépendances, leurs contraintes croisées et les trajectoires possibles d'un système complexe.

2. Modèle fédéré de relations

La modélisation ne fusionne pas nécessairement tous les jumeaux dans un modèle monolithique. Elle maintient des modèles spécialisés reliés par des interfaces, variables d'échange et règles de correspondance versionnées.

3. Graphe multisectoriel

Les ressources, capacités, infrastructures, flux, secteurs et territoires sont représentés comme des nœuds et relations. Chaque relation conserve sa nature, sa direction éventuelle, sa source, sa temporalité et son niveau de confiance.

4. Graphe multi-institutionnel

Les institutions sont reliées par compétences, transmissions, validations, financements, contrôles, coordinations ou autres dépendances. Cette couche permet de modéliser comment une réponse opérationnelle peut dépendre de plusieurs autorités ou processus.

5. Matrices d'interdépendances

Des matrices peuvent synthétiser les dépendances entre secteurs, territoires ou institutions. Elles servent à identifier concentrations, dépendances réciproques et points de propagation, tout en restant des représentations simplifiées du système réel.

6. Variables d'interface

Les modèles échangent uniquement les variables nécessaires : disponibilité, capacité, demande, délai, flux, statut, contrainte ou autre indicateur défini. Les unités, définitions et périodes doivent être compatibles ou explicitement converties.

7. Contraintes croisées

Une décision ou variation dans un secteur peut être limitée par les capacités d'un autre secteur ou par une contrainte institutionnelle. Le moteur conserve ces contraintes afin d'éviter des scénarios techniquement possibles mais institutionnellement ou matériellement irréalisables.

8. Propagation des effets

Un choc peut se transmettre par plusieurs chemins : ressource → entreprise → secteur → territoire → institution, ou selon d'autres séquences. Chaque étape conserve son mécanisme supposé et l'incertitude associée.

9. Temporalité de propagation

Les effets n'apparaissent pas tous au même moment. Délais physiques, logistiques, administratifs, budgétaires ou décisionnels sont intégrés afin d'éviter une propagation instantanée artificielle.

10. Boucles de rétroaction

Le système peut comporter des boucles amplificatrices ou stabilisatrices. Une décision institutionnelle peut modifier un flux économique, lequel peut ensuite modifier la demande ou les ressources disponibles et influencer de nouvelles décisions.

11. Capacités et seuils

Les modèles peuvent intégrer limites de capacité, seuils de saturation, stocks minimaux, délais incompressibles ou autres contraintes. Les seuils issus d'estimations restent distingués des limites réglementaires ou physiques établies.

12. Substitution et adaptation

Lorsque des alternatives existent, la modélisation peut représenter substitution de produit, fournisseur, itinéraire, capacité, territoire ou procédure. Les conditions de compatibilité et le temps nécessaire à l'adaptation restent explicites.

13. Coordination interinstitutionnelle

Une réponse multisectorielle peut exiger plusieurs validations ou actions coordonnées. Le modèle représente séquences, dépendances et parallélisations possibles sans attribuer à la simulation une autorité sur les institutions réelles.

14. Résolution des conflits de modèles

Deux modèles peuvent produire des hypothèses incompatibles. Le système conserve les divergences, compare les hypothèses et peut demander arbitrage ou validation plutôt que de fusionner silencieusement des résultats contradictoires.

15. Granularité et cohérence

Les modèles peuvent fonctionner à des granularités différentes. L'agrégation ou la désagrégation respecte les limites des données ; un modèle national ne doit pas créer artificiellement une précision locale absente des sources.

16. Calibration multisectorielle

Les paramètres d'interaction peuvent être calibrés à partir de données historiques, expertise ou autres méthodes gouvernées. La provenance et la version des paramètres sont conservées afin de rendre les simulations reproductibles.

17. Validation et backtesting

Lorsque des épisodes historiques sont disponibles, le système peut tester sa capacité à reproduire certaines propagations, délais et effets observés. Une bonne reproduction historique ne garantit pas qu'un futur choc suivra exactement la même trajectoire.

18. Deep Authenticity© et reproductibilité

Deep Authenticity© relie modèles, variables d'interface, paramètres, données, versions et résultats. Un scénario important doit pouvoir être reconstruit à partir du snapshot initial et des composants effectivement utilisés.

19. Gouvernance et limites

Les modèles multisectoriels sont gouvernés selon leur criticité. Les hypothèses sensibles, données confidentielles et informations d'infrastructure sont compartimentées. La modélisation sert à éclairer les décisions, non à produire une autorité automatique.

20. Critères d'acceptation et conclusion

La modélisation est acceptable si les modèles restent fédérés et traçables ; si les interfaces sont définies ; si les contraintes croisées et délais sont représentés ; si les divergences entre modèles restent visibles ; si la granularité respecte les données ; si les paramètres sont versionnés ; et si les simulations demeurent reproductibles. Le Chapitre 10 développera la construction des scénarios nationaux et institutionnels.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VI — JUMEAU NUMÉRIQUE NATIONAL ET SIMULATION INSTITUTIONNELLE

CHAPITRE 10 — CONSTRUCTION DES SCÉNARIOS NATIONAUX ET INSTITUTIONNELS

SNAPSHOT INITIAL — HYPOTHÈSES — CHOCS — DÉCISIONS CANDIDATES — BRANCHES — HORIZONS — TRAJECTOIRES — COMPARABILITÉ

1. Objet du chapitre

Ce chapitre définit la méthode de construction des scénarios nationaux et institutionnels. Un scénario est une branche hypothétique, traçable et reproductible créée à partir d'un état de référence afin d' explorer les conséquences possibles d'événements, contraintes, décisions candidates et réactions du système.

2. Snapshot initial

Tout scénario important commence par un snapshot identifié du Jumeau Numérique National© et, lorsque nécessaire, des jumeaux institutionnels concernés. Ce point de départ fixe ce qui était connu, estimé, versionné et disponible au moment de la simulation.

3. Scénario de référence

Une branche de référence représente l'évolution retenue comme base de comparaison en l'absence des changements spécifiques testés. Elle n'est pas un futur certain et conserve elle aussi ses hypothèses.

4. Hypothèses explicites

Les hypothèses portent notamment sur demande, ressources, comportements agrégés, capacités, délais, règles ou contexte externe. Elles sont enregistrées séparément des données observées afin que le résultat puisse être interprété correctement.

5. Événements exogènes

Un scénario peut introduire des événements externes au système simulé : variation de disponibilité, choc climatique modélisé, changement de marché, perturbation logistique ou autre facteur pertinent. Leur amplitude, durée et calendrier sont explicites.

6. Événements endogènes

Certains événements résultent du fonctionnement simulé lui-même : saturation d'une capacité, épuisement d'un stock, retard accumulé, déclenchement d'un seuil ou propagation d'une dépendance. Leur mécanisme est relié au modèle qui les produit.

7. Chocs simples et combinés

Les scénarios peuvent tester un choc isolé ou plusieurs chocs simultanés ou successifs. Les scénarios combinés permettent d'étudier des interactions non visibles dans des analyses séparées.

8. Décisions candidates

Plusieurs décisions possibles peuvent être introduites comme branches alternatives : réallocation autorisée, mobilisation de capacité, modification de calendrier, changement de procédure ou autre option gouvernée. Une décision candidate reste une hypothèse de simulation.

9. Branches alternatives

À partir du même snapshot, le système peut créer plusieurs branches afin de comparer « sans action », « option A », « option B » ou d'autres alternatives. Les branches ne partagent pas leurs événements simulés après leur séparation.

10. Horizons temporels

Chaque scénario possède un horizon : immédiat, court, moyen ou long terme selon la finalité. Les modèles et incertitudes peuvent différer selon l'horizon ; une précision excessive à long terme doit être évitée.

11. Pas de temps

La simulation peut évoluer par minutes, heures, jours, semaines, mois ou autres pas appropriés. Le pas de temps doit correspondre aux phénomènes étudiés et ne pas donner une impression artificielle de précision.

12. Contraintes institutionnelles

Les branches intègrent les compétences, validations, budgets, délais et règles applicables lorsqu'ils influencent la faisabilité. Une option matériellement possible peut rester institutionnellement impossible dans le scénario considéré.

13. Réactions multisectorielles

Les changements se propagent entre secteurs et territoires selon le modèle du Chapitre 9. Les réactions peuvent inclure adaptation, substitution, saturation, déplacement de flux ou autres mécanismes documentés.

14. Réactions institutionnelles

Les institutions simulées peuvent traiter alertes, dossiers, validations et décisions selon leurs processus modélisés. Ces réactions représentent le fonctionnement du jumeau institutionnel, non les décisions réelles de personnes ou autorités.

15. Trajectoires

Chaque branche produit une trajectoire temporelle d'états, indicateurs, événements, contraintes et résultats. Les trajectoires permettent de comparer non seulement le résultat final, mais également la vitesse, les transitions et les effets intermédiaires.

16. Critères de comparaison

Les branches peuvent être comparées selon continuité, délai, disponibilité, coût agrégé, résilience, effets territoriaux, utilisation des ressources ou autres critères autorisés. Les pondérations et priorités doivent être explicites.

17. Incertitude et sensibilité

Chaque scénario conserve les principales sources d'incertitude. L'analyse de sensibilité fait varier les hypothèses déterminantes afin d'identifier les conclusions robustes et celles qui dépendent fortement d'un paramètre.

18. Reproductibilité et versioning

Snapshot, modèles, paramètres, règles, hypothèses et événements d'entrée sont versionnés. Une simulation historique reste attachée aux composants effectivement utilisés et n'est pas recalculée silencieusement avec des versions nouvelles.

19. Deep Authenticity© et AP Ledger

Deep Authenticity© relie le scénario à son état initial, ses hypothèses, modèles et résultats. AP Ledger peut ancrer l'identité, l'antériorité et les versions des scénarios critiques sans exposer leurs contenus sensibles.

20. Critères d'acceptation et conclusion

Un scénario est acceptable si son snapshot initial est identifiable ; si observations et hypothèses restent séparées ; si décisions candidates ne sont pas confondues avec décisions réelles ; si branches et horizons sont comparables ; si contraintes institutionnelles et multisectorielles sont prises en compte ; si l'incertitude est visible ; et si la simulation est reproductible. Le Chapitre 11 développera la Simulation Institutionnelle Profonde©.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VI — JUMEAU NUMÉRIQUE NATIONAL ET SIMULATION INSTITUTIONNELLE

CHAPITRE 11 — SIMULATION INSTITUTIONNELLE PROFONDE©

PROCESSUS — COMPÉTENCES — VALIDATIONS — DÉLAIS — RESSOURCES — COORDINATION — DÉCISIONS CANDIDATES — EFFETS — APPRENTISSAGE

1. Objet du chapitre

Ce chapitre définit la Simulation Institutionnelle Profonde© comme l'utilisation coordonnée des Jumeaux Numériques Institutionnels et du Jumeau Numérique National© pour explorer, avant toute exécution réelle, les conséquences possibles de chaînes de décision, contraintes, délais, allocations de ressources et interactions interinstitutionnelles.

2. Principe de simulation profonde

La simulation ne teste pas seulement le résultat final d'une décision. Elle reproduit, au niveau de détail autorisé, les étapes susceptibles de conditionner son efficacité : saisine, instruction, expertise, validation, arbitrage, mobilisation de ressources, coordination, exécution et suivi.

3. Point de départ vérifiable

Toute simulation profonde commence par un snapshot identifié. Les structures, compétences, règles, ressources, capacités et données disponibles au moment de départ sont figées ou référencées afin que la simulation puisse être reproduite.

4. Chaîne institutionnelle simulée

Le moteur peut représenter une séquence telle que : signal → analyse → saisine → proposition → expertise → validation → arbitrage → décision candidate → préparation d'exécution → effets simulés. Chaque étape conserve ses conditions et délais.

5. Compétences et autorisations

Le moteur vérifie quelles institutions ou fonctions sont compétentes pour chaque étape. Une action techniquement faisable mais hors compétence ne doit pas être considérée comme une décision institutionnellement exécutable.

6. Règles et procédures

Les règles applicables, versions et exceptions gouvernées sont intégrées au scénario. Le moteur peut comparer plusieurs procédures autorisées sans inventer un pouvoir ou une dérogation absente du modèle.

7. Délais institutionnels

Délais de transmission, instruction, consultation, validation, mobilisation et exécution sont modélisés. Le système peut identifier lorsqu'une option pertinente sur le fond arrive trop tard pour produire l'effet recherché.

8. Ressources et capacités d'exécution

Budget disponible, capacités techniques, infrastructures, stocks, personnels agrégés ou autres ressources pertinentes peuvent limiter l'exécution. Décider une action ne crée pas automatiquement les ressources nécessaires à sa réalisation.

9. Files d'attente et saturation

Lorsque plusieurs dossiers ou événements sollicitent les mêmes capacités, le modèle peut simuler files d'attente, priorisation et saturation. Ces mécanismes permettent d'évaluer la robustesse institutionnelle sous charge.

10. Coordination interinstitutionnelle

Les scénarios peuvent inclure plusieurs institutions agissant en parallèle ou en séquence. Le moteur représente dépendances, transmissions, validations croisées et points de synchronisation nécessaires.

11. Décisions candidates concurrentes

Plusieurs options peuvent être simulées à partir du même snapshot. Chacune conserve sa chaîne institutionnelle, ses délais, ressources nécessaires, effets attendus et contraintes.

12. Propagation multisectorielle

Une décision institutionnelle simulée peut modifier capacités, flux, demande, ressources ou règles et produire des effets dans plusieurs secteurs et territoires. Les effets indirects sont reliés aux modèles du Chapitre 9.

13. Effets de second ordre

La Simulation Institutionnelle Profonde© examine, lorsque les modèles le permettent, les conséquences secondaires : déplacement de contrainte, saturation ailleurs, modification de comportement agrégé, coût d'opportunité ou nouvelle dépendance.

14. Boucles de rétroaction institutionnelles

Les résultats intermédiaires peuvent modifier la suite du scénario : une alerte peut déclencher une nouvelle validation, une saturation peut provoquer une réallocation, ou un effet inattendu peut conduire à reconsidérer une option.

15. Comparaison des trajectoires décisionnelles

Les options sont comparées non seulement sur leur résultat final, mais sur temps de décision, délai d'exécution, ressources mobilisées, continuité, effets territoriaux, résilience, réversibilité et autres critères gouvernés.

16. Points de non-retour et réversibilité

Le système peut signaler les étapes après lesquelles une option devient difficile ou coûteuse à inverser. Cette information aide à distinguer décisions réversibles, partiellement réversibles et fortement engageantes.

17. Incertitude et limites

Les résultats conservent incertitudes liées aux données, modèles, hypothèses et réactions du système. La simulation institutionnelle ne prétend pas reproduire parfaitement les comportements humains, politiques ou sociaux.

18. Simulation et exécution réelle

Aucune décision candidate simulée ne devient automatiquement un acte réel. La transition vers l'exécution exige une décision réelle, prise par l'autorité compétente, puis des autorisations et mécanismes opérationnels distincts.

19. Deep Authenticity©, AP Ledger et audit

Deep Authenticity© relie snapshot, règles, modèles, décisions candidates et résultats. AP Ledger peut ancrer les versions et événements critiques. L'audit peut reconstruire ce que le système a simulé avant qu'une décision réelle ne soit prise.

20. Critères d'acceptation et conclusion

La Simulation Institutionnelle Profonde© est acceptable si son point de départ est vérifiable ; si compétences, règles, délais et ressources sont représentés ; si les effets multisectoriels et secondaires restent explicables ; si l'incertitude est visible ; si les décisions candidates restent distinctes des actes réels ; et si l'autorité institutionnelle demeure extérieure au moteur. Le Chapitre 12 développera la comparaison multicritère des décisions et trajectoires.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VI — JUMEAU NUMÉRIQUE NATIONAL ET SIMULATION INSTITUTIONNELLE

CHAPITRE 12 — COMPARAISON MULTICRITÈRE DES DÉCISIONS ET DES TRAJECTOIRES

OPTIONS — CRITÈRES — PONDÉRATIONS — DÉLAIS — RESSOURCES — IMPACTS — RISQUES — RÉVERSIBILITÉ — INCERTITUDE — ARBITRAGE

1. Objet du chapitre

Ce chapitre définit la comparaison multicritère des décisions candidates et des trajectoires produites par la Simulation Institutionnelle Profonde©. Son objectif est de rendre visibles les compromis entre plusieurs options sans réduire une décision complexe à un score unique ni transférer l'arbitrage à l' algorithme.

2. Ensemble d'options comparables

Les options sont comparées à partir d'un même snapshot ou de conditions initiales rendues explicitement comparables. Une option utilisant des informations, ressources ou règles différentes doit signaler cette différence avant toute comparaison.

3. Trajectoire de référence

La branche de référence sert de point de comparaison : absence d'action spécifique, continuité des mesures existantes ou autre hypothèse documentée. Elle ne représente pas nécessairement l'inaction absolue ni un futur certain.

4. Familles de critères

Les critères peuvent couvrir résultats attendus, délais, ressources, coûts agrégés, continuité, résilience, couverture territoriale, faisabilité institutionnelle, réversibilité, risques et autres dimensions autorisées. Leur définition précède le classement.

5. Résultats et efficacité

Le système mesure dans quelle mesure chaque trajectoire atteint les objectifs du scénario. L' efficacité simulée reste conditionnelle aux hypothèses, modèles et comportements représentés.

6. Délais

Temps de décision, préparation, mobilisation, exécution, apparition des premiers effets et atteinte d' un objectif peuvent être comparés séparément. Une option plus efficace à terme peut être insuffisamment rapide dans une situation urgente.

7. Ressources nécessaires

Les besoins en capacités, budgets agrégés, infrastructures, stocks, compétences ou autres ressources sont comparés à leur disponibilité simulée. Une option exigeant des ressources inexistantes ou indisponibles est signalée comme contrainte.

8. Coûts et coûts d'opportunité

Lorsque les données le permettent, les scénarios peuvent comparer coûts directs et ressources détournées d'autres usages. Le coût d'opportunité est présenté comme une dimension de l'arbitrage, non comme une valeur automatiquement exhaustive.

9. Impacts sectoriels

Une option favorable à un secteur peut déplacer une contrainte vers un autre. La comparaison multisectorielle rend visibles ces transferts afin d'éviter une optimisation locale qui dégrade le système global.

10. Impacts territoriaux

Les résultats peuvent varier selon les territoires. Les agrégats nationaux sont accompagnés, lorsque pertinent, d'une lecture territoriale afin qu'un bénéfice moyen ne masque pas des disparités importantes.

11. Continuité et résilience

Les options sont évaluées sur leur capacité à maintenir les fonctions essentielles, absorber les perturbations, utiliser des alternatives et récupérer après un choc. Résilience et performance immédiate sont deux dimensions distinctes.

12. Risques et effets secondaires

Chaque trajectoire peut présenter des risques directs, indirects ou de second ordre. Le système distingue risques identifiés, incertitudes et conséquences hypothétiques insuffisamment étayées.

13. Réversibilité

Les décisions réversibles, partiellement réversibles et fortement engageantes sont distinguées. Le coût, le délai et les conditions de retour peuvent constituer des critères à part entière.

14. Robustesse

Une option robuste conserve des résultats acceptables lorsque certaines hypothèses varient. La robustesse peut être préférée à une performance maximale obtenue uniquement dans un scénario très précis.

15. Incertitude

Les intervalles, distributions ou niveaux de confiance disponibles accompagnent les critères. Une petite différence entre deux options ne doit pas être présentée comme décisive si elle est inférieure à l'incertitude des modèles.

16. Pondérations

Lorsque des pondérations sont utilisées, leur origine, valeur, version et autorité de validation sont explicites. Le système peut afficher plusieurs jeux de pondérations pour montrer comment les priorités modifient le classement.

17. Analyse de dominance et compromis

Une option peut être dominée si une autre est au moins aussi favorable sur tous les critères retenus et meilleure sur certains. Lorsque les options impliquent des compromis, le système présente un front de choix plutôt qu'un faux optimum universel.

18. Explicabilité de la comparaison

Pour chaque option, le décideur peut consulter les critères déterminants, hypothèses sensibles, contraintes, effets sectoriels et territoriaux ainsi que les raisons d'un éventuel classement. Les données et modèles restent traçables.

19. Arbitrage institutionnel et audit

La comparaison éclaire l'arbitrage mais ne le remplace pas. L'autorité compétente peut retenir une option différente du classement algorithmique et documenter sa justification. Deep Authenticity© et AP Ledger peuvent conserver versions, pondérations, résultats et décision finale.

20. Critères d'acceptation et conclusion

La comparaison est acceptable si les options partent de conditions comparables ; si les critères et pondérations sont explicites ; si délais, ressources, impacts, risques, résilience et réversibilité sont visibles ; si l'incertitude empêche les faux écarts de précision ; si les compromis sont présentés sans faux optimum ; et si l'arbitrage demeure institutionnel. Le Chapitre 13 développera la décision réelle, l' autorisation et le passage contrôlé de la simulation à l'exécution.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VI — JUMEAU NUMÉRIQUE NATIONAL ET SIMULATION INSTITUTIONNELLE

CHAPITRE 13 — DÉCISION RÉELLE, AUTORISATION ET PASSAGE CONTRÔLÉ À L' EXÉCUTION

SIMULATION — ARBITRAGE — AUTORITÉ — VALIDATION — AUTORISATION — PLAN D'EXÉCUTION — CONTRÔLES — TRAÇABILITÉ — RÉEL

1. Objet du chapitre

Ce chapitre définit la frontière critique entre la simulation et l'action réelle. Il formalise le passage d' une ou plusieurs décisions candidates issues des scénarios vers une décision institutionnelle réelle, puis vers une exécution contrôlée, traçable et réversible lorsque cela est possible.

2. Frontière simulation-réalité

Aucun résultat de simulation, classement multicritère ou recommandation d'IA ne constitue par lui-même une décision réelle. Le passage au réel exige une autorité compétente, une validation explicite et un acte identifiable.

3. Dossier de décision

Avant arbitrage, un dossier peut réunir snapshot initial, situation observée, hypothèses, scénarios comparés, critères, incertitudes, contraintes, effets attendus, risques, réversibilité et recommandations. Il conserve les versions utilisées.

4. Autorité compétente

La décision réelle appartient au rôle, organe ou institution disposant du mandat applicable. Le système vérifie les droits et compétences représentés mais ne s'attribue jamais lui-même l'autorité.

5. Arbitrage humain et institutionnel

L'autorité peut retenir, modifier ou écarter une option simulée. Elle peut également demander un scénario complémentaire. L'écart entre recommandation algorithmique et décision retenue peut être documenté sans être traité automatiquement comme une erreur.

6. Validation et signatures

Les validations nécessaires sont enregistrées selon le niveau de criticité. Identité, rôle, date, portée et version du dossier approuvé doivent être traçables afin d'éviter qu'une validation ancienne soit appliquée à une décision modifiée.

7. Conditions préalables

Avant exécution, le système vérifie les conditions connues : disponibilité des ressources, autorisations, dépendances, calendrier, contraintes et éventuelles validations complémentaires. Une condition non satisfaite peut bloquer ou renvoyer l'action vers arbitrage.

8. Transformation en plan d'exécution

La décision réelle est traduite en actions, responsables, ressources, séquences, délais, critères de réussite, points de contrôle et conditions d'arrêt. Cette traduction constitue une étape distincte de la décision elle-même.

9. Principe du moindre privilège

Les systèmes et acteurs d'exécution ne reçoivent que les droits nécessaires aux actions autorisées. Une décision générale ne doit pas ouvrir un accès technique illimité aux systèmes concernés.

10. Séparation des rôles

Préparation, simulation, recommandation, validation, décision, exécution et audit peuvent être séparés selon la criticité. Cette séparation réduit le risque qu'un même composant puisse proposer, approuver et exécuter seul une action significative.

11. Exécution progressive

Lorsque la nature de l’action le permet, l’exécution peut être découpée en phases, pilotes, paliers ou périmètres limités. Les résultats intermédiaires peuvent conditionner la poursuite, l’adaptation ou l’ arrêt.

12. Points de contrôle

Des checkpoints vérifient ressources, effets observés, conformité aux conditions initiales et apparition de risques nouveaux. Le franchissement d’un point de contrôle peut nécessiter une nouvelle validation.

13. Conditions d’arrêt et rollback

Les plans définissent, lorsque possible, des seuils d’arrêt, procédures de suspension et mécanismes de retour. La réversibilité simulée doit être confirmée dans les conditions réelles avant d’être considérée comme disponible.

14. Gestion des écarts

Si l’environnement réel diverge fortement du scénario — ressource indisponible, délai différent, événement externe ou effet inattendu — l’exécution peut être suspendue, adaptée ou renvoyée vers une nouvelle simulation.

15. Événements d’exécution réelle

Chaque action significative produit des événements réels distincts : ordre autorisé, démarrage, progression, modification, suspension, achèvement ou échec. Ces événements alimentent le jumeau sans être confondus avec les événements simulés.

16. Mise à jour du jumeau

Le Jumeau Numérique National© et les jumeaux concernés sont synchronisés avec les résultats observés de l’exécution. Les nouvelles données mettent à jour l’état courant mais ne réécrivent pas les branches simulées historiques.

17. Monitoring continu

Watch System© surveille l’exécution, les écarts, dépendances, effets secondaires et signaux faibles. Une alerte peut déclencher analyse ou réévaluation, mais ne doit pas modifier automatiquement une décision institutionnelle sans mécanisme autorisé.

18. Deep Authenticity© et AP Ledger

Deep Authenticity© relie dossier, scénarios, validations, décision, plan d’exécution et événements réels. AP Ledger peut ancrer les empreintes et horodatages des étapes critiques afin d’établir une chaîne d’antériorité vérifiable.

19. Audit et responsabilité

L’audit doit pouvoir reconstruire : ce qui était connu, ce qui a été simulé, ce qui a été recommandé, qui a décidé, ce qui a été autorisé, ce qui a réellement été exécuté et quels résultats ont été observés. La responsabilité reste attachée aux rôles institutionnels réels.

20. Critères d’acceptation et conclusion

Le passage au réel est acceptable si simulation et décision sont séparées ; si l’autorité compétente est identifiable ; si le dossier et ses versions sont figés ; si les conditions préalables sont vérifiées ; si l’exécution suit un plan contrôlé ; si checkpoints, arrêt et rollback sont prévus lorsque possibles ; si les écarts peuvent provoquer une réévaluation ; et si toute la chaîne est auditée. Le Chapitre 14 développera l’exécution réelle et le monitoring continu.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VI — JUMEAU NUMÉRIQUE NATIONAL ET SIMULATION INSTITUTIONNELLE

CHAPITRE 14 — EXÉCUTION RÉELLE ET MONITORING CONTINU

DÉCISION AUTORISÉE — ACTIONS RÉELLES — SYNCHRONISATION — TRAJECTOIRES — ÉCARTS — WATCH SYSTEM© — ADAPTATION — AUDIT

1. Objet du chapitre

Ce chapitre définit le suivi de l’exécution réelle après une décision institutionnelle autorisée. Il organise la remontée des événements, la synchronisation des jumeaux, la comparaison continue entre trajectoires prévues et observées, la détection des écarts et les mécanismes de réévaluation.

2. Quatre trajectoires distinctes

Le système maintient séparément la trajectoire simulée, la trajectoire autorisée, la trajectoire effectivement exécutée et la trajectoire observée dans le réel. Cette séparation permet d’identifier précisément l’origine d’un écart.

3. Ordre et plan d’exécution

La décision autorisée est traduite en actions, responsables, séquences, ressources, délais et critères de contrôle. Le plan d’exécution conserve la version approuvée et les modifications ultérieures.

4. Événements d’exécution

Démarrage, progression, mobilisation de ressources, changement d’état, suspension, reprise, achèvement ou échec sont enregistrés comme événements réels. Ils ne sont jamais confondus avec les événements produits par une simulation.

5. Synchronisation des jumeaux

Les jumeaux Produit, Entreprise, Secteur, Territoire, National et Institutionnel concernés sont mis à jour à partir des informations réelles autorisées. Les fréquences de synchronisation dépendent du phénomène et de la criticité.

6. État attendu et état observé

À chaque point de contrôle, le système peut comparer l'état attendu selon la trajectoire autorisée avec l'état réellement observé. L'écart est daté, contextualisé et relié aux données disponibles.

7. Écarts de calendrier

Un retard peut provenir d'une validation, d'une ressource, d'une dépendance, d'une difficulté opérationnelle ou d'un événement extérieur. Le monitoring cherche à localiser l'écart sans attribuer automatiquement une cause.

8. Écarts de ressources

Les ressources effectivement mobilisées peuvent différer du plan. Le système compare disponibilité prévue, mobilisation réelle, consommation et éventuelles contraintes nouvelles.

9. Écarts de résultat

Les effets observés peuvent être inférieurs, supérieurs ou différents de ceux simulés. Ces écarts sont conservés pour l'analyse ultérieure sans réécrire les prévisions initiales.

10. Écarts de périmètre

Une action peut être exécutée sur un périmètre différent de celui prévu en raison de contraintes ou adaptations autorisées. La comparaison doit alors tenir compte de cette différence au lieu de produire un faux écart de performance.

11. Watch System© d'exécution

Watch System© surveille progression, retards, anomalies, dépendances, seuils et signaux faibles pendant l'exécution. Il peut escalader une situation mais ne modifie pas de lui-même une décision institutionnelle.

12. Seuils et niveaux d'escalade

Les écarts peuvent être classés selon tolérance, vigilance, alerte ou criticité selon des règles gouvernées. Les seuils sont versionnés et adaptés au contexte plutôt qu'appliqués uniformément à tous les processus.

13. Points de contrôle dynamiques

Les checkpoints peuvent être déclenchés par calendrier, événement ou dépassement de seuil. Ils permettent de confirmer la poursuite, demander une analyse complémentaire, suspendre ou renvoyer vers arbitrage.

14. Adaptation contrôlée

Une adaptation mineure peut être autorisée dans les limites du plan. Au-delà de ces limites, le système crée une nouvelle proposition ou simulation et requiert la validation de l'autorité compétente.

15. Nouvelle simulation en cours d'exécution

Si le réel diverge fortement du scénario initial, un nouveau snapshot peut être créé à partir de l'état courant. Les options restantes sont alors resimulées sans effacer la trajectoire initiale.

16. Monitoring des effets secondaires

Le suivi porte aussi sur les secteurs, territoires, ressources ou institutions susceptibles de subir des effets indirects. Une amélioration locale ne doit pas masquer une dégradation déplacée ailleurs.

17. Continuité et résilience

Le monitoring mesure la continuité des fonctions essentielles, la capacité d'absorption et le temps de récupération. Les mécanismes de secours et alternatives réellement utilisés sont comparés à ceux prévus.

18. Deep Authenticity© et AP Ledger

Deep Authenticity© relie décision, plan, événements d'exécution, états observés, alertes et adaptations. AP Ledger peut ancrer les versions et événements critiques pour préserver une chronologie vérifiable.

19. Dossier d'exécution et audit

Le dossier d'exécution rassemble décision, plan approuvé, actions réalisées, écarts, alertes, adaptations, validations et résultats. Il permet de reconstruire la séquence réelle et de la comparer aux simulations antérieures.

20. Critères d'acceptation et conclusion

Le monitoring est acceptable si les quatre trajectoires restent distinctes ; si les événements réels sont traçables ; si les écarts de temps, ressources, périmètre et résultat sont visibles ; si Watch System© n' exerce pas d'autorité décisionnelle ; si les adaptations importantes repassent par validation ; si les nouvelles simulations conservent l'historique ; et si le dossier d'exécution est auditable. Le Chapitre 15 développera la comparaison Simulation / Réalité et l'analyse structurée des écarts.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VI — JUMEAU NUMÉRIQUE NATIONAL ET SIMULATION INSTITUTIONNELLE

CHAPITRE 15 — COMPARAISON SIMULATION / RÉALITÉ ET ANALYSE STRUCTURÉE DES ÉCARTS

PRÉVU — AUTORISÉ — EXÉCUTÉ — OBSERVÉ — ÉCARTS — ATTRIBUTION — BACKTESTING — RECALIBRAGE — APPRENTISSAGE

1. Objet du chapitre

Ce chapitre définit la comparaison structurée entre les trajectoires simulées et les résultats réellement observés. Son objectif n'est pas seulement de mesurer une erreur finale, mais de comprendre à quel moment, dans quelle dimension et pour quelles raisons possibles la trajectoire réelle s'est écartée de la trajectoire simulée.

2. Préservation de la simulation originale

La simulation initiale, ses modèles, paramètres, hypothèses et données de départ restent figés. Les résultats réels ultérieurs ne sont jamais injectés rétroactivement dans cette simulation historique.

3. Alignement temporel

La comparaison aligne les trajectoires sur des dates, événements ou jalons comparables. Un décalage de calendrier est distingué d'une erreur d'amplitude ou d'un résultat structurellement différent.

4. Alignement de périmètre

Les comparaisons tiennent compte des différences de territoire, population agrégée, secteur, ressource ou périmètre d'exécution. Une action réalisée sur un périmètre réduit ne doit pas être comparée naïvement à un scénario national complet.

5. Écart simulation-autorisation

Le système identifie les différences entre l'option simulée et la décision réellement autorisée : paramètres modifiés, ressources réduites, calendrier différent, conditions ajoutées ou périmètre adapté.

6. Écart autorisation-exécution

Le système compare ensuite le plan autorisé avec ce qui a réellement été exécuté. Retards, actions non réalisées, adaptations, ressources différentes ou changements de séquence sont conservés.

7. Écart exécution-observation

Enfin, le système compare les actions effectivement réalisées aux effets observés. Cette étape permet de distinguer une mauvaise exécution d'une hypothèse de modèle insuffisante ou d'un événement externe.

8. Taxonomie des écarts

Les écarts peuvent être classés notamment en données initiales, hypothèses, paramètres, modèle, calendrier, ressources, périmètre, exécution, dépendances, comportement agrégé, événement externe ou observation. Plusieurs catégories peuvent contribuer simultanément.

9. Erreur de données initiales

Une donnée initiale inexacte, tardive ou incomplète peut expliquer une divergence. La correction améliore les simulations futures sans modifier ce que le système connaissait au moment de la simulation originale.

10. Erreur d'hypothèse

Une hypothèse peut se révéler trop optimiste, pessimiste ou inadaptée. Le système conserve l' hypothèse originale et mesure sa sensibilité afin de comprendre son influence sur le résultat.

11. Erreur ou limite de modèle

Un modèle peut sous-représenter une dépendance, un délai, une saturation ou une rétroaction. L' analyse documente la limite avant toute modification du modèle et évite d'attribuer automatiquement chaque écart au modèle.

12. Événements externes

Certains écarts résultent d'événements qui n'étaient ni connus ni raisonnablement représentés dans le scénario. Ils sont distingués des erreurs de simulation afin de ne pas pénaliser artificiellement le modèle.

13. Attribution prudente

La présence d'un écart et d'un facteur concomitant ne prouve pas une causalité. L'analyse peut proposer des facteurs explicatifs avec niveaux de confiance, mais les conclusions causales exigent des éléments suffisants.

14. Mesures d'écart

Selon les variables, le système peut utiliser erreur absolue, relative, temporelle, de couverture, de trajectoire ou autres métriques appropriées. Aucune métrique unique ne résume nécessairement la qualité d'une simulation complexe.

15. Backtesting institutionnel et multisectoriel

Les simulations historiques peuvent être rejouées avec les composants d'époque afin de comparer propagation, délais, décisions candidates et résultats. Le backtesting évalue la performance passée sans garantir la performance future.

16. Calibration et recalibrage

Les écarts récurrents peuvent conduire à recalibrer paramètres, délais, relations ou distributions. Toute modification est versionnée, testée et comparée à la version précédente avant déploiement.

17. Détection de dérive

Watch System© peut surveiller la dégradation progressive des performances d'un modèle ou d'une relation. Une dérive déclenche investigation, validation ou recalibrage selon les règles de gouvernance.

18. Apprentissage institutionnel

Les enseignements ne concernent pas seulement les modèles : ils peuvent révéler des délais réels, contraintes d'exécution, dépendances, procédures ou capacités différentes de celles représentées. Le jumeau institutionnel peut ainsi être amélioré sans réécrire son historique.

19. Deep Authenticity©, AP Ledger et mémoire

Deep Authenticity© relie simulation originale, décision, exécution, observations, analyse des écarts et nouvelle version éventuelle. AP Ledger peut ancrer les étapes critiques afin de démontrer l'antériorité des prévisions et l'intégrité de l'apprentissage.

20. Critères d'acceptation et conclusion

L'analyse est acceptable si la simulation originale reste intacte ; si temps et périmètres sont alignés ; si les écarts simulation-autorisation, autorisation-exécution et exécution-observation sont séparés ; si les causes restent prudentes et traçables ; si recalibrage et dérive sont versionnés ; et si l'apprentissage améliore les versions futures sans réécrire le passé. Le Chapitre 16 développera la boucle d'apprentissage continu et l'évolution gouvernée du Jumeau Numérique National©.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VI — JUMEAU NUMÉRIQUE NATIONAL ET SIMULATION INSTITUTIONNELLE

CHAPITRE 16 — BOUCLE D'APPRENTISSAGE CONTINU ET ÉVOLUTION GOUVERNÉE DU JUMEAU NUMÉRIQUE NATIONAL©

ÉCARTS — ENSEIGNEMENTS — DONNÉES — MODÈLES — PROCESSUS — VALIDATION — VERSIONING — DÉPLOIEMENT — MÉMOIRE — AMÉLIORATION CONTINUE

1. Objet du chapitre

Ce chapitre définit la boucle d'apprentissage continu du Jumeau Numérique National©. Elle transforme les écarts observés, résultats d'exécution, retours institutionnels et performances des modèles en propositions d'amélioration gouvernées, testées, versionnées et auditables.

2. Apprendre sans réécrire

L’apprentissage ne modifie jamais rétroactivement les simulations, décisions ou états historiques. Chaque amélioration produit une nouvelle version reliée à la précédente afin de conserver la mémoire de ce que le système savait et représentait à chaque époque.

3. Sources d’apprentissage

Les enseignements peuvent provenir des écarts simulation-réalité, incidents, changements de contexte, dérives, retours d’experts, nouvelles données, modifications institutionnelles ou performances observées lors d’exécutions réelles.

4. Classification des enseignements

Les enseignements sont classés selon leur cible : qualité des données, schéma, paramètre, modèle, dépendance, scénario, règle institutionnelle, délai, ressource, interface ou processus. Cette classification évite de corriger le mauvais composant.

5. Amélioration des données

Les erreurs récurrentes de fraîcheur, couverture, définition ou qualité peuvent conduire à améliorer les sources, contrôles, fréquences de synchronisation ou règles de réconciliation. Les corrections restent traçables.

6. Amélioration des modèles

Un modèle peut nécessiter recalibrage, ajout de variable, modification de structure ou remplacement. Toute évolution est testée sur des cas historiques et scénarios de référence avant adoption.

7. Amélioration des interdépendances

Les propagations réellement observées peuvent révéler des relations manquantes, surestimées ou devenues obsolètes. Le graphe multisectoriel évolue par versions avec provenance et justification.

8. Amélioration du jumeau institutionnel

Les délais réels, files d’attente, séquences de validation ou capacités d’exécution peuvent différer du modèle initial. Ces observations permettent d’améliorer la représentation des processus sans transformer automatiquement une pratique observée en règle officielle.

9. Évolution des scénarios

Les bibliothèques de scénarios peuvent être enrichies par des événements réellement rencontrés, combinaisons de chocs ou réactions inattendues. Un scénario historique reste figé tandis qu’un nouveau scénario réutilisable peut être créé.

10. Proposition de changement

Toute évolution significative est formalisée par une proposition décrivant problème observé, composant concerné, changement envisagé, preuves, impacts, risques et méthode de validation.

11. Environnement de test

Les nouvelles versions sont évaluées hors production sur des snapshots, scénarios historiques, stress tests et jeux de validation appropriés. Une amélioration sur un cas ne doit pas masquer une dégradation sur d'autres situations.

12. Comparaison des versions

Ancienne et nouvelle versions sont comparées selon précision, robustesse, stabilité, explicabilité, ressources nécessaires et effets sur les scénarios. Les gains et régressions restent visibles.

13. Validation humaine et institutionnelle

Les changements significatifs de modèle, règle, processus ou interface passent par les responsables compétents. L'apprentissage automatique ne dispose pas d'un droit autonome de modifier les composants critiques en production.

14. Déploiement contrôlé

Une version validée peut être déployée progressivement, avec surveillance renforcée, capacité de rollback et conservation de la version précédente selon les règles de criticité.

15. Compatibilité et migration

Les changements de schéma, identifiant, relation ou modèle doivent prévoir compatibilité, migration ou coexistence de versions. Les anciennes simulations doivent rester interprétables même après évolution de l'architecture.

16. Monitoring post-déploiement

Après mise en production, Watch System© surveille performances, dérive, anomalies et effets inattendus. Une dégradation peut déclencher rollback, investigation ou nouvelle boucle d' amélioration.

17. Mémoire des générations

Le système conserve une généalogie des versions : données, modèles, règles, processus, interfaces et scénarios. Cette mémoire permet de comprendre pourquoi une génération du jumeau diffère d'une autre.

18. Deep Authenticity© et AP Ledger

Deep Authenticity© relie enseignement, preuve, proposition, tests, validation, version et déploiement. AP Ledger peut ancrer les changements critiques et leur antériorité, créant une mémoire d'évolution vérifiable.

19. Gouvernance de l’apprentissage

L’apprentissage continu reste soumis à finalité, responsabilité, sécurité, souveraineté, explicabilité et audit. Le système apprend sous contrôle ; il ne s’auto-transforme pas silencieusement dans les fonctions institutionnelles critiques.

20. Critères d’acceptation et conclusion

La boucle est acceptable si le passé reste intact ; si les enseignements sont reliés aux écarts observés ; si les changements sont testés et comparés ; si les versions sont conservées ; si les modifications critiques exigent validation ; si rollback et monitoring sont prévus ; et si la généalogie du jumeau est vérifiable. Le Chapitre 17 développera la gouvernance, la sécurité et la souveraineté du Jumeau Numérique National©.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VI — JUMEAU NUMÉRIQUE NATIONAL ET SIMULATION INSTITUTIONNELLE

CHAPITRE 17 — GOUVERNANCE, SÉCURITÉ ET SOUVERAINETÉ DU JUMEAU NUMÉRIQUE NATIONAL©

FÉDÉRATION — FINALITÉ — ACCÈS — SÉPARATION DES POUVOIRS — SÉCURITÉ — CONFIDENTIALITÉ — RÉSILIENCE — RÉVERSIBILITÉ — SOUVERAINETÉ

1. Objet du chapitre

Ce chapitre fixe les principes de gouvernance, de sécurité et de souveraineté applicables au Jumeau Numérique National© et à la Simulation Institutionnelle Profonde©. L’objectif est de permettre une intelligence systémique nationale sans créer une concentration incontrôlée des données, des droits ou du pouvoir décisionnel.

2. Fédération comme principe de souveraineté

Le Jumeau Numérique National© reste un système desystèmes. Les domaines sectoriels, territoriaux et institutionnels conservent leurs responsabilités et leurs données selon les règles applicables, tandis que le niveau national accède uniquement aux états, indicateurs, relations ou preuves nécessaires.

3. Finalité et proportionnalité

Toute collecte, synchronisation, agrégation, simulation ou consultation doit correspondre à une finalité définie. Le niveau de détail et la durée de conservation sont proportionnés au besoin opérationnel, analytique, institutionnel ou d’audit.

4. Classification des informations

Les données, modèles, scénarios, infrastructures, dépendances et résultats sont classifiés selon leur sensibilité. Les politiques d'accès, d'export, de partage et de conservation découlent de cette classification.

5. Contrôle d'accès

Les accès sont attribués selon identité, rôle, mission, finalité et contexte. Le principe du moindre privilège limite chaque acteur et composant aux fonctions et informations nécessaires.

6. Séparation des pouvoirs

Les capacités d'administration technique, alimentation des données, développement des modèles, simulation, validation, décision, exécution et audit peuvent être séparées. Aucun composant critique ne doit pouvoir concentrer silencieusement toutes ces fonctions.

7. Séparation simulation-exécution

Les environnements et autorisations de simulation sont distincts des systèmes d'exécution réelle. Une branche simulée ne peut franchir cette frontière qu'au travers du processus institutionnel d' autorisation défini au Chapitre 13.

8. Sécurité des interfaces fédérées

Les interfaces entre jumeaux authentifient les systèmes, contrôlent les droits, valident les schémas et journalisent les échanges pertinents. Une interface compromise doit pouvoir être isolée sans arrêter nécessairement l'ensemble du système national.

9. Intégrité des données et modèles

Les versions, signatures, empreintes, contrôles de provenance et mécanismes Deep Authenticity© contribuent à détecter altérations, substitutions ou incohérences. L'intégrité technique ne garantit toutefois pas à elle seule l'exactitude métier.

10. Confidentialité et compartimentation

Secrets industriels, informations stratégiques, données institutionnelles sensibles et détails d' infrastructures critiques sont compartimentés. Les vues nationales privilégient agrégation, abstraction et indicateurs lorsque le détail n'est pas nécessaire.

11. Protection des citoyens

Le Jumeau Numérique National© est conçu pour représenter systèmes, ressources, infrastructures, territoires et dynamiques agrégées. Il ne constitue pas un dispositif de surveillance généralisée ou de profilage individuel des citoyens.

12. Traçabilité des accès sensibles

Les consultations, exports, changements de droits et opérations critiques peuvent être journalisés selon leur niveau de sensibilité. Les journaux eux-mêmes sont protégés contre l'altération et les accès abusifs.

13. Sécurité des scénarios

Les scénarios peuvent révéler vulnérabilités, dépendances ou capacités sensibles. Leur accès, partage et conservation suivent des règles spécifiques afin qu'un outil de résilience ne devienne pas une source d'exposition.

14. Résilience cyber et opérationnelle

L'architecture prévoit segmentation, redondance, sauvegardes, reprise, fonctionnement dégradé et procédures manuelles. Le Jumeau Numérique National© ne doit pas devenir un point unique de défaillance de l'action institutionnelle.

15. Continuité sans jumeau

Les institutions doivent conserver des capacités minimales de fonctionnement lorsque certaines composantes du jumeau sont indisponibles. Le système augmente la capacité d'analyse ; il ne doit pas rendre l'État incapable d'agir sans lui.

16. Souveraineté technologique

Formats documentés, portabilité, maîtrise des clés, capacité d'hébergement adaptée, interopérabilité et absence de dépendance irréversible à un fournisseur contribuent à la souveraineté. Les composants critiques doivent pouvoir être remplacés ou migrés selon une stratégie maîtrisée.

17. Réversibilité

Les données, modèles, configurations, historiques et preuves nécessaires peuvent être exportés ou migrés dans des formats gouvernés. Les procédures de sortie sont testées avant qu'une dépendance technologique ne devienne critique.

18. Gouvernance des changements

Toute modification significative de schéma, modèle, droit, interface ou politique suit proposition, analyse d'impact, validation, versioning et monitoring. Les changements d'urgence sont eux aussi tracés et revus a posteriori.

19. Deep Authenticity© et AP Ledger

Deep Authenticity© assure la continuité vérifiable entre identités, données, modèles, simulations, validations et exécutions. AP Ledger peut ancrer des événements critiques, versions et preuves d' antériorité sans stocker les contenus sensibles eux-mêmes.

20. Critères d'acceptation et conclusion

La gouvernance est acceptable si l'architecture demeure fédérée ; si finalité et proportionnalité encadrent les usages ; si les pouvoirs sont séparés ; si simulation et exécution sont isolées ; si les informations sensibles sont compartimentées ; si les citoyens sont protégés d'une surveillance disproportionnée ; si continuité, réversibilité et souveraineté technologique sont prévues ; et si les changements restent auditables. Le Chapitre 18 développera la résilience, la continuité nationale et les modes dégradés du jumeau.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VI — JUMEAU NUMÉRIQUE NATIONAL ET SIMULATION INSTITUTIONNELLE

CHAPITRE 18 — RÉSILIENCE, CONTINUITÉ NATIONALE ET MODES DÉGRADÉS

PANNE — ISOLEMENT — AUTONOMIE LOCALE — DONNÉES INCOMPLÈTES — SYNCHRONISATION DIFFÉRÉE — REPRISE — RECONSTRUCTION — RETOUR NOMINAL

1. Objet du chapitre

Ce chapitre définit les mécanismes permettant au Jumeau Numérique National©, à ses jumeaux fédérés et aux institutions utilisatrices de continuer à fonctionner de manière maîtrisée lors de pannes, pertes de connectivité, indisponibilités de données, défaillances de composants ou autres situations dégradées.

2. Principe de continuité

La continuité nationale ne dépend pas de la disponibilité permanente d'un composant unique. Les fonctions essentielles disposent de procédures, capacités locales et mécanismes de reprise adaptés à leur criticité.

3. Classification des fonctions critiques

Les fonctions sont classées selon leur importance et leurs objectifs de continuité. Les fonctions de représentation, simulation, consultation, décision ou exécution peuvent avoir des exigences différentes.

4. Modes de fonctionnement

Le système distingue au minimum fonctionnement nominal, fonctionnement dégradé, isolement local, reprise et retour au nominal. Le passage entre modes est gouverné, visible et journalisé.

5. Perte partielle de connectivité

Un territoire, secteur ou institution isolé peut continuer certaines opérations localement selon les droits et données disponibles. L'absence de connexion au niveau national ne doit pas entraîner automatiquement l'arrêt des fonctions locales essentielles.

6. Autonomie locale contrôlée

Les nœuds autorisés peuvent conserver des snapshots, règles, modèles ou référentiels nécessaires à leur fonctionnement dégradé. Les limites d'autonomie sont définies avant la crise et ne créent pas de pouvoirs institutionnels nouveaux.

7. Données indisponibles

Lorsqu'une source devient indisponible, le jumeau marque la donnée comme non actualisée et affiche sa fraîcheur. La dernière valeur connue ne doit pas être présentée comme une observation actuelle certaine.

8. Données incomplètes et estimations

Des estimations peuvent être utilisées dans certaines fonctions si la gouvernance le permet. Elles restent explicitement identifiées et accompagnées de leur incertitude ; elles ne remplacent pas silencieusement les observations manquantes.

9. Défaillance d'un modèle

Si un modèle critique devient indisponible ou invalide, le système peut basculer vers une version validée antérieure, un modèle simplifié ou une procédure manuelle selon le plan de continuité.

10. Défaillance d'une interface fédérée

Une interface compromise ou instable peut être isolée. Les autres domaines continuent de fonctionner lorsque leurs dépendances le permettent, limitant la propagation d'une panne à l' ensemble du système.

11. Synchronisation différée

Pendant l'isolement, les événements locaux sont conservés avec leurs horodatages et provenance. Lors du rétablissement, ils sont synchronisés sans perdre la distinction entre temps du fait, temps de transmission et temps d'intégration.

12. Réconciliation après reconnexion

Des conflits peuvent apparaître entre états locaux et nationaux. La réconciliation applique des règles explicites de provenance, autorité, temporalité et validation plutôt qu'un simple écrasement de la dernière valeur reçue.

13. Files d'événements et reprise progressive

Les flux accumulés sont réintégrés progressivement afin d'éviter saturation, double traitement ou désordre temporel. Les événements critiques peuvent être priorisés selon des règles gouvernées.

14. Reconstruction de l'état

Après incident, le système peut reconstruire l'état courant à partir de snapshots, événements, journaux et sources disponibles. La reconstruction conserve les zones d'incertitude ou les périodes pour lesquelles les informations restent manquantes.

15. Continuité de la décision institutionnelle

Les institutions conservent des procédures de décision et d'autorisation indépendantes du moteur de simulation lorsque celui-ci est indisponible. Les décisions prises en mode dégradé sont enregistrées puis réconciliées avec le jumeau lors de la reprise.

16. Continuité de l'exécution

Les systèmes opérationnels essentiels ne doivent pas dépendre d'une commande permanente du Jumeau Numérique National©. Les plans d'exécution autorisés peuvent prévoir des modes locaux, manuels ou autonomes limités.

17. Exercices et tests de résilience

Les scénarios de panne, isolement, perte de données, indisponibilité de modèle et reprise sont testés régulièrement. Les résultats alimentent la boucle d'apprentissage du Chapitre 16.

18. Retour contrôlé au nominal

Le retour au fonctionnement nominal exige vérification de l'intégrité, synchronisation, réconciliation, validation des composants et surveillance renforcée. Une reconnexion technique ne suffit pas à déclarer la reprise complète.

19. Deep Authenticity© et AP Ledger

Deep Authenticity© relie snapshots, événements locaux, périodes d'isolement, réconciliations et versions de reprise. AP Ledger peut ancrer des preuves minimales des étapes critiques afin de préserver une chronologie vérifiable malgré les interruptions.

20. Critères d'acceptation et conclusion

La résilience est acceptable si les fonctions critiques sont identifiées ; si les modes dégradés sont définis ; si les nœuds autorisés peuvent fonctionner localement ; si données anciennes et estimations restent visibles ; si la synchronisation différée préserve la temporalité ; si la reprise traite les conflits explicitement ; si les institutions peuvent décider sans dépendance absolue au jumeau ; et si le retour au nominal est contrôlé. Le Chapitre 19 développera le Centre National de Simulation et d'Intelligence Institutionnelle.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VI — JUMEAU NUMÉRIQUE NATIONAL ET SIMULATION INSTITUTIONNELLE

CHAPITRE 19 — CENTRE NATIONAL DE SIMULATION ET D'INTELLIGENCE INSTITUTIONNELLE

JUMEAU NATIONAL — SCÉNARIOS — SIMULATION PROFONDE — COMPARAISON — DÉCISION ASSISTÉE — EXÉCUTION — MONITORING — APPRENTISSAGE

1. Objet du chapitre

Ce chapitre définit le Centre National de Simulation et d'Intelligence Institutionnelle comme la couche opérationnelle de convergence du Volume VI. Il réunit le Jumeau Numérique National©, les Jumeaux Numériques Institutionnels, la modélisation multisectorielle, les scénarios, la Simulation Institutionnelle Profonde©, la comparaison des décisions, le monitoring réel et l'apprentissage continu.

2. Centre de convergence, non centre de pouvoir

Le Centre organise l'information, la simulation et l'aide à la décision. Il ne concentre pas l'autorité institutionnelle : les compétences, validations, décisions et responsabilités demeurent attachées aux institutions et rôles légalement ou réglementairement compétents.

3. Architecture fédérée

Le Centre fonctionne sur une architecture fédérée. Il orchestre des jumeaux sectoriels, territoriaux et institutionnels sans exiger la copie exhaustive de leurs données, et accède uniquement aux informations nécessaires selon les droits et finalités.

4. Salle de situation nationale

Une vue de situation peut réunir état national observé, estimations, alertes, ressources, capacités, flux, infrastructures, dépendances et disparités. Les informations sensibles sont filtrées selon les rôles et la granularité autorisée.

5. Salle de scénarios

Les analystes autorisés peuvent créer des branches à partir de snapshots vérifiables, introduire hypothèses et chocs, puis comparer plusieurs trajectoires. Les scénarios restent isolés du jumeau réel.

6. Simulation Institutionnelle Profonde© intégrée

Le Centre permet de simuler non seulement les effets physiques ou économiques, mais aussi les chaînes institutionnelles : saisine, instruction, validation, arbitrage, délais, ressources, coordination et préparation de l'exécution.

7. Comparaison des décisions

Les options candidates peuvent être comparées selon efficacité, délais, ressources, impacts sectoriels et territoriaux, résilience, risques, réversibilité, robustesse et incertitude. Le Centre expose les compromis sans produire un faux optimum universel.

8. Dossier d'aide à la décision

Pour chaque situation significative, le Centre peut constituer un dossier réunissant snapshot, données, alertes, scénarios, hypothèses, critères, résultats, incertitudes, recommandations et validations. Chaque version reste identifiable.

9. Interface avec l'autorité réelle

Le dossier est transmis aux autorités compétentes selon les processus institutionnels. Le Centre peut éclairer, expliquer et comparer ; il ne transforme jamais automatiquement une recommandation en décision officielle.

10. Passage contrôlé à l'exécution

Lorsqu'une décision réelle est prise, le Centre peut contribuer à la préparation du plan d'exécution, aux checkpoints et au suivi. Les environnements de simulation et d'exécution restent techniquement et institutionnellement séparés.

11. Monitoring continu

Le Centre rapproche trajectoire simulée, trajectoire autorisée, trajectoire exécutée et trajectoire observée. Les écarts sont détectés, contextualisés et transmis aux acteurs compétents.

12. Watch System© intégré

Watch System© surveille anomalies, retards, dépendances, signaux faibles, ruptures de synchronisation et effets secondaires. L'escalade d'une alerte déclenche analyse ou procédure ; elle n' accorde pas au système une autorité autonome.

13. Cartographie Dynamique© intégrée

La Cartographie Dynamique© permet de visualiser territoires, ressources, infrastructures, flux, alertes, trajectoires et scénarios. Observation, estimation, décision autorisée et simulation disposent de représentations distinctes.

14. Cellules sectorielles, territoriales et institutionnelles

Le Centre peut comporter des cellules spécialisées travaillant sur des périmètres différents tout en partageant un cadre commun. Cette organisation conserve l'expertise métier et évite qu'une vision nationale efface les réalités locales ou sectorielles.

15. Coordination interinstitutionnelle

Les situations nécessitant plusieurs institutions peuvent être suivies dans une vue commune des responsabilités, dépendances, validations, délais et actions. Le Centre facilite la coordination sans modifier la répartition réelle des compétences.

16. Modes normal, vigilance, crise et reprise

Les interfaces, fréquences de synchronisation et procédures peuvent s'adapter aux modes normal, vigilance, crise, dégradé et reprise. Les transitions entre modes sont gouvernées, explicites et auditables.

17. Apprentissage opérationnel

Après l'exécution, le Centre organise la comparaison simulation-réalité, l'analyse des écarts et les propositions d'amélioration. Les modèles, processus et paramètres ne sont modifiés qu'après test, validation et versioning.

18. Deep Authenticity© et AP Ledger

Deep Authenticity© assure la continuité vérifiable entre snapshot, données, modèles, scénarios, recommandations, validations, décision, exécution et résultats. AP Ledger peut ancrer les versions et événements critiques sans centraliser les contenus sensibles.

19. Gouvernance, sécurité et protection

Le Centre applique moindre privilège, séparation des pouvoirs, compartimentation, continuité, réversibilité et souveraineté. Il vise l'intelligence des systèmes et des institutions, non la surveillance généralisée des citoyens ou des agents.

20. Critères d'acceptation et conclusion

Le Centre est acceptable s'il demeure une couche d'intelligence et non une autorité autonome ; si l'architecture reste fédérée ; si simulation, décision et exécution sont séparées ; si les expertises sectorielles et territoriales sont préservées ; si le monitoring compare les quatre trajectoires ; si l'apprentissage est gouverné ; si la continuité en mode dégradé est assurée ; et si la chaîne complète reste vérifiable. Le Chapitre 20 synthétisera et clôturera le Volume VI.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VI — JUMEAU NUMÉRIQUE NATIONAL ET SIMULATION INSTITUTIONNELLE

CHAPITRE 20 — SYNTHÈSE, ARCHITECTURE INTÉGRÉE ET CONCLUSION DU VOLUME VI

PRODUIT → ENTREPRISE → SECTEUR → TERRITOIRE → NATIONAL → INSTITUTIONNEL → SIMULATION → DÉCISION → EXÉCUTION → MONITORING → APPRENTISSAGE

1. Objet du chapitre

Ce chapitre synthétise l'architecture du Volume VI et clôt la construction du Jumeau Numérique National© et de la Simulation Institutionnelle Profonde©. L'ensemble forme une chaîne fédérée reliant le réel observable, la représentation numérique, la simulation, l'arbitrage institutionnel, l'exécution réelle, le monitoring et l'apprentissage gouverné.

2. Chaîne des jumeaux

L'architecture progresse du Jumeau Numérique du Produit vers le Jumeau Numérique de l'Entreprise, du Secteur, du Territoire, puis vers le Jumeau Numérique National©. Chaque niveau agrège uniquement les informations nécessaires et conserve les responsabilités, droits et granularités de ses domaines sources.

3. Jumeau Numérique Institutionnel

Le Jumeau Numérique Institutionnel ajoute structures, compétences, responsabilités, processus, règles, ressources, délais et capacités d'exécution. Il permet de représenter comment une institution peut traiter une situation sans confondre modèle institutionnel et institution réelle.

4. Système de systèmes fédéré

Le niveau national n'est pas une base centrale exhaustive. Il constitue un système de systèmes reliant jumeaux spécialisés par interfaces, identités, indicateurs, événements, relations et preuves gouvernés.

5. Trois états fondamentaux

L'architecture distingue État Observé, État Estimé et États Simulés. Cette séparation empêche une estimation ou une projection d'être présentée comme un fait et protège l'intégrité du jumeau de référence.

6. Temps, snapshots et mémoire

Les snapshots temporels figent ce qui était connu à un instant donné. Ils rendent les scénarios reproductibles, permettent le backtesting et empêchent l'introduction rétroactive d'informations inconnues au moment d'une décision.

7. Modélisation multisectorielle

Les secteurs, territoires, ressources, infrastructures et institutions sont reliés par graphes, matrices d' interdépendances, variables d'interface, contraintes croisées, délais et boucles de rétroaction. Les divergences entre modèles restent visibles.

8. Construction des scénarios

Les scénarios partent d'un snapshot, explicitent hypothèses, événements et chocs, puis créent des branches alternatives. Chaque trajectoire conserve ses paramètres, son horizon, ses contraintes et son incertitude.

9. Simulation Institutionnelle Profonde©

La simulation reproduit les chaînes de traitement : signal, analyse, saisine, proposition, expertise, validation, arbitrage, décision candidate, mobilisation de ressources et effets simulés. Elle explore la faisabilité institutionnelle autant que les conséquences multisectorielles.

10. Comparaison des décisions

Les options sont comparées selon plusieurs critères : efficacité, délais, ressources, coûts, impacts sectoriels et territoriaux, résilience, risques, robustesse, réversibilité et incertitude. Les compromis sont exposés sans transformer un score en décision.

11. Frontière décisionnelle

La simulation s'arrête avant l'autorité réelle. Une décision candidate, une recommandation d'IA ou un classement ne devient jamais automatiquement un acte institutionnel. La décision appartient à l' autorité compétente et reste identifiable et auditable.

12. Passage contrôlé à l'exécution

Une décision réelle autorisée est traduite en plan d'exécution avec responsables, ressources, séquences, checkpoints, conditions d'arrêt et mécanismesde rollback lorsque possibles. Les environnements de simulation et d'exécution restent séparés.

13. Quatre trajectoires

Le système conserve distinctement trajectoire simulée, trajectoire autorisée, trajectoire exécutée et trajectoire observée. Cette architecture permet de localiser les écarts et d'éviter d'attribuer automatiquement toute divergence au modèle.

14. Monitoring continu

Watch System© surveille progression, anomalies, retards, dépendances, effets secondaires et signaux faibles. Cartographie Dynamique© spatialise les états, flux, risques et trajectoires tout en distinguant réel, estimation et simulation.

15. Comparaison Simulation / Réalité

Les écarts sont analysés entre simulation et autorisation, autorisation et exécution, puis exécution et observation. Données, hypothèses, paramètres, modèles, ressources, périmètres, délais et événements externes peuvent être examinés séparément.

16. Apprentissage continu gouverné

Les enseignements produisent des propositions d'amélioration des données, modèles, interdépendances, scénarios ou processus institutionnels. Les nouvelles versions sont testées, validées, déployées progressivement et surveillées sans réécrire les générations antérieures.

17. Gouvernance, sécurité et souveraineté

L'architecture applique fédération, finalité, proportionnalité, moindre privilège, séparation des pouvoirs, compartimentation, réversibilité et souveraineté technologique. Elle vise l'intelligence des systèmes et non une surveillance généralisée des citoyens.

18. Résilience et modes dégradés

Le système prévoit perte de connectivité, données incomplètes, défaillance de modèle, autonomie locale contrôlée, synchronisation différée, réconciliation et reprise. Les institutions conservent une capacité de décision et d'action même lorsque le jumeau est indisponible.

19. Centre National de Simulation et d'Intelligence Institutionnelle

Le Centre constitue la couche opérationnelle de convergence : situation nationale, scénarios, simulation profonde, comparaison, dossiers d'aide à la décision, monitoring et apprentissage. Il demeure un centre d'intelligence et de coordination, non une autorité autonome.

20. Conclusion générale du Volume VI

Le Volume VI établit une architecture dans laquelle la donnée devient représentation, la représentation devient compréhension systémique, la compréhension devient scénario, le scénario éclaire la décision, la décision autorisée devient exécution, l'exécution devient observation et l'observation devient apprentissage. Deep Authenticity© assure la continuité vérifiable de cette chaîne et AP Ledger peut en ancrer les étapes critiques. Le Jumeau Numérique National© n'a donc pas vocation à prédire un futur unique, mais à rendre plusieurs futurs comparables, leurs hypothèses explicites, leurs conséquences observables et leurs décisions auditables.

Architecture intégrée — chaîne de référence

RÉEL → DONNÉES → DEEP AUTHENTICITY© → JUMEAUX FÉDÉRÉS → JUMEAU NUMÉRIQUE NATIONAL© → SCÉNARIOS → SIMULATION INSTITUTIONNELLE PROFONDE© → COMPARAISON → ARBITRAGE INSTITUTIONNEL → DÉCISION RÉELLE → EXÉCUTION → WATCH SYSTEM© / MONITORING → COMPARAISON SIMULATION-RÉALITÉ → APPRENTISSAGE → NOUVELLE VERSION

1. Principe fondamental

Le Passeport Numérique Universel fournit une continuité vérifiable du réel : identité, état, provenance et événements autorisés. Le Jumeau Numérique organise une représentation structurée de ce réel. La Simulation Institutionnelle Profonde explore ensuite des scénarios possibles à partir de cette représentation. Ces trois niveaux sont complémentaires mais ne doivent jamais être confondus.

2. Passeport et Jumeau Numérique du produit

Le Passeport Numérique Universel constitue la mémoire d'identité et de cycle de vie du produit. Le Jumeau Numérique du produit peut exploiter ces événements pour représenter son état, ses relations,

son comportement et son évolution. Le passeport répond principalement à « qui est-il et que lui est-il arrivé ? » ; le jumeau à « quel est son état systémique et comment évolue-t-il ? ».

3. De l'unité à l'entreprise

Des événements autorisés issus de nombreux passeports peuvent être agrégés pour alimenter le Jumeau Numérique d'une entreprise : production, circulation, maintenance, retours, stocks, rappels ou seconde main. L'agrégation préserve provenance, temporalité, confidentialité et niveau d'assurance.

4. Du secteur au territoire

Les données agrégées de plusieurs entreprises et chaînes de valeur peuvent contribuer aux représentations sectorielles et territoriales. Le Passeport Numérique Universel fournit des événements ancrés dans les actifs réels ; le jumeau les relie à d'autres données économiques, sociales, logistiques ou institutionnelles.

5. Jumeau Numérique National et Institutionnel

À l'échelle nationale, le Jumeau Numérique National et Institutionnel ne constitue pas une copie intégrale de tous les passeports individuels. Il exploite les informations nécessaires, autorisées et généralement agrégées afin de représenter les interactions entre secteurs, territoires, institutions, flux et ressources.

6. Chaîne de montée en abstraction

Actif réel → mécanisme natif de vérité → Passeport Numérique Universel → événements vérifiables → agrégation gouvernée → Jumeau Numérique du produit ou de l'organisation → jumeaux sectoriels et territoriaux → Jumeau Numérique National et Institutionnel. Chaque niveau ajoute de l'abstraction sans effacer l'origine des données.

7. Simulation Institutionnelle Profonde

La Simulation Institutionnelle Profonde utilise le modèle du jumeau pour tester des hypothèses et comparer des scénarios avant une décision. Un scénario simulé ne modifie jamais le Passeport Numérique Universel ni l'état réel tant qu'une décision autorisée et une exécution réelle n'ont pas eu lieu.

8. Séparation simulation-exécution

Les environnements de simulation restent distincts des systèmes d'exécution. Une branche simulée ne peut devenir une action réelle qu'au travers du processus institutionnel d'autorisation compétent. Le Centre National de Simulation organise l'information et l'aide à la décision sans concentrer l' autorité institutionnelle.

9. Monitoring continu

Après exécution d'une décision, le monitoring continu recueille les événements réels et indicateurs gouvernés. Ils peuvent mettre à jour le Jumeau Numérique et être comparés aux trajectoires simulées. L'écart entre scénario et réalité devient une information d'apprentissage.

10. Boucle institutionnelle

Réalité vérifiable → Passeport Numérique Universel → Jumeau Numérique → scénarios → Simulation Institutionnelle Profonde → décision humaine/institutionnelle → exécution autorisée → monitoring réel → nouveaux événements vérifiables → mise à jour du jumeau → apprentissage.

11. Gouvernance et souveraineté

Le Jumeau Numérique National reste un système de systèmes. Les domaines sectoriels, territoriaux et institutionnels conservent leurs responsabilités et leurs données selon les règles applicables. Le niveau national accède uniquement aux états, indicateurs, relations ou preuves nécessaires.

12. Confidentialité

Le Passeport d'un actif ou d'une personne ne doit pas devenir automatiquement visible dans le Jumeau Numérique National. Finalité, proportionnalité, classification, moindre privilège et agrégation gouvernent les accès et représentations.

13. Résilience

Le système doit préserver la distinction entre données observées, données anciennes, estimations et scénarios même en mode dégradé. Les institutions doivent conserver des procédures de décision indépendantes du moteur de simulation lorsque celui-ci est indisponible.

14. AP Ledger et mémoire vérifiable

AP Ledger peut ancrer des preuves minimales de snapshots, décisions, exécutions, réconciliations et étapes critiques. Il complète la continuité du Passeport et du Jumeau sans transformer le registre en dépôt exhaustif de toutes les données.

15. Invariant doctrinal

Passeport Numérique Universel = continuité vérifiable du réel. Jumeau Numérique = représentation structurée du réel. Simulation Institutionnelle Profonde = exploration de futurs possibles. Monitoring = confrontation des résultats au réel exécuté. Aucun de ces niveaux ne doit se substituer aux autres.

16. Règle d'intégration dans le DMC

Cette mise à niveau doit être absorbée dans les chapitres correspondants du Volume VI lors de l'assemblage final. Elle complète le DMC existant sans reproduire le chapitre fondateur du Passeport Numérique Universel.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VII — GOUVERNANCE, SOUVERAINETÉ ET DÉPLOIEMENT INTERNATIONAL

CHAPITRE 1 — FONDEMENTS DE LA GOUVERNANCE DE DEEP AUTHENTICITY©

CONFIANCE — RESPONSABILITÉ — FÉDÉRATION — SOUVERAINETÉ — PROPORTIONNALITÉ — CONTRÔLE — AUDIT — COOPÉRATION

1. Objet du chapitre

Ce chapitre définit les fondements de la gouvernance de Deep Authenticity©. La gouvernance organise les responsabilités, droits, contrôles, preuves, décisions et mécanismes d'audit nécessaires pour qu'une infrastructure de confiance puisse fonctionner à l'échelle des entreprises, secteurs, territoires, institutions, États et échanges internationaux.

2. Gouverner la confiance plutôt que centraliser le pouvoir

Deep Authenticity© vise à rendre vérifiables identités, données, événements, transformations, certifications et décisions sans créer une autorité technique unique contrôlant l'ensemble des participants. La gouvernance doit distribuer les responsabilités et préserver les autorités légitimes de chaque domaine.

3. Principe de fédération

Chaque organisation, secteur, territoire ou État conserve la maîtrise de ses systèmes et de ses données selon les règles applicables. La coopération repose sur des interfaces, preuves, référentiels et mécanismes de reconnaissance communs plutôt que sur une centralisation exhaustive.

4. Principe de souveraineté

La participation à une infrastructure commune de confiance ne doit pas entraîner l'abandon de la souveraineté numérique, économique ou institutionnelle. Les droits d'accès, d'hébergement, de traitement, de certification et de décision restent gouvernés par les autorités compétentes.

5. Finalité et proportionnalité

Toute collecte, vérification, partage ou conservation d'information répond à une finalité identifiée. Le niveau de détail, la durée de conservation et l'étendue des contrôles sont proportionnés au risque, au besoin et au cadre applicable.

6. Responsabilités explicites

Les rôles de producteur de données, détenteur, vérificateur, certificateur, opérateur, autorité, auditeur et utilisateur sont distingués. Une même organisation peut exercer plusieurs rôles uniquement lorsque la gouvernance autorise cette combinaison et prévoit les contrôles nécessaires.

7. Séparation des pouvoirs

La création d'une donnée, sa validation, sa certification, son utilisation décisionnelle et son audit ne doivent pas être confondus lorsque leur criticité exige une séparation. La gouvernance limite les situations dans lesquelles un acteur pourrait produire seul la preuve de sa propre conformité.

8. Identité, mandat et autorité

Toute action significative est reliée à une identité et, lorsque nécessaire, à un rôle, un mandat et une période de validité. Une identité authentifiée ne prouve pas à elle seule que son titulaire possède l' autorité pour effectuer une action.

9. Gouvernance des données

Les données restent attachées à leur provenance, leur classification, leurs droits d'usage, leur temporalité et leur niveau de confiance. La gouvernance définit ce qui peut être partagé, sous quelle forme, avec qui et pour quelle finalité.

10. Gouvernance des modèles et de l'IA

Les modèles utilisés pour analyser, estimer, détecter, recommander ou simuler sont versionnés et soumis à des niveaux de contrôle adaptés. Une sortie d'IA ne devient pas automatiquement une preuve, une certification ou une décision institutionnelle.

11. Gouvernance des preuves

Les preuves Deep Authenticity© doivent permettre de vérifier origine, intégrité, antériorité et chaîne de transformations selon le besoin. La preuve technique reste distincte de l'interprétation juridique, réglementaire ou métier qui lui est appliquée.

12. Gouvernance de la certification

Les mécanismes AP Certified© reposent sur des critères définis, des versions identifiables, des organismes ou rôles autorisés, des périodes de validité et des procédures de suspension ou retrait. La certification n'est pas un statut irrévocable.

13. Gouvernance des accès

Le moindre privilège, la nécessité d'en connaître, la classification et le contexte déterminent les accès. Les consultations et opérations sensibles peuvent être journalisées et soumises à contrôle renforcé.

14. Gouvernance des changements

Les référentiels, schémas, règles, modèles, niveaux de certification et interfaces évoluent par versions. Les changements significatifs suivent proposition, analyse d'impact, validation, publication et période de transition.

15. Gestion des conflits et contestations

Un participant doit pouvoir contester une donnée, une preuve, une certification ou une décision de gouvernance selon une procédure définie. Les corrections conservent l'historique et ne suppriment pas silencieusement les états antérieurs.

16. Audit et redevabilité

L’audit doit permettre de reconstruire qui a produit, validé, modifié, certifié, consulté ou utilisé un élément critique. La traçabilité soutient la responsabilité mais ne remplace pas les mécanismes institutionnels ou juridiques de responsabilité.

17. Gouvernance multiniveau

La gouvernance peut être organisée aux niveaux organisationnel, sectoriel, territorial, national et international. Les niveaux supérieurs définissent des cadres d’interopérabilité sans absorber automatiquement les compétences des niveaux inférieurs.

18. Coopération et reconnaissance mutuelle

Deux organisations ou États peuvent reconnaître certains référentiels, certificats ou preuves sans harmoniser l’ensemble de leurs systèmes. La reconnaissance mutuelle devient ainsi un mécanisme de coopération compatible avec la souveraineté.

19. Deep Authenticity© et AP Ledger

Deep Authenticity© assure la continuité entre identités, données, transformations, validations et certifications. AP Ledger peut ancrer des empreintes, versions, statuts et événements critiques afin d’ établir une mémoire vérifiable sans imposer la publication des contenus sensibles.

20. Critères d’acceptation et conclusion

La gouvernance de Deep Authenticity© est acceptable si elle distribue les responsabilités ; préserve souveraineté et fédération ; applique finalité et proportionnalité ; sépare les pouvoirs critiques ; relie actions, identités et mandats ; gouverne données, IA, preuves et certifications ; permet contestation et audit ; et rend possible la coopération sans centralisation du pouvoir. Le Chapitre 2 développera l’ architecture de gouvernance nationale.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VII — GOUVERNANCE, SOUVERAINETÉ ET DÉPLOIEMENT INTERNATIONAL

CHAPITRE 2 — ARCHITECTURE DE GOUVERNANCE NATIONALE

ÉTAT — INSTITUTIONS — TERRITOIRES — SECTEURS — ENTREPRISES — OPÉRATEURS DE CONFIANCE — CERTIFICATION — AUDIT

1. Objet du chapitre

Ce chapitre définit l'architecture de gouvernance nationale de Deep Authenticity©. Elle organise la répartition des responsabilités entre État, institutions, territoires, secteurs, entreprises, opérateurs de confiance, organismes de certification et fonctions d'audit, dans une logique fédérée et souveraine.

2. Principe d'architecture multiniveau

La gouvernance nationale ne repose pas sur une administration unique de toutes les données et décisions. Chaque niveau conserve ses compétences, tandis que des règles communes assurent identité, interopérabilité, preuve, sécurité et audit.

3. Rôle stratégique de l'État

L'État définit le cadre souverain, les objectifs nationaux, les exigences de sécurité, les domaines critiques et les conditions de reconnaissance. Il organise la cohérence générale sans se substituer systématiquement aux responsabilités opérationnelles des acteurs.

4. Institutions nationales

Les institutions appliquent le cadre dans leurs domaines de compétence. Elles gouvernent leurs données, processus, modèles, certifications ou décisions selon leurs mandats et exposent uniquement les éléments nécessaires aux mécanismes nationaux de confiance.

5. Gouvernance territoriale

Les territoires conservent la gouvernance des informations et capacités relevant de leurs compétences. Les échanges avec le niveau national respectent granularité, finalité, proportionnalité et règles de souveraineté.

6. Gouvernance sectorielle

Chaque secteur peut disposer de référentiels, risques, exigences et niveaux de certification spécifiques. La gouvernance nationale fournit un socle commun sans effacer les particularités industrielles, économiques ou réglementaires.

7. Entreprises et opérateurs économiques

Les entreprises restent responsables de leurs données sources, processus, produits et déclarations selon le cadre applicable. Deep Authenticity© permet de produire des preuves vérifiables sans exiger la divulgation de l'ensemble de leurs informations internes.

8. Opérateurs de confiance

Des opérateurs autorisés peuvent fournir identité, horodatage, vérification, certification, infrastructure ou autres services de confiance. Leurs mandats, obligations, périmètres et mécanismes de supervision sont explicitement définis.

9. Autorités de gouvernance

Une ou plusieurs autorités peuvent administrer référentiels, accréditations, règles d'interopérabilité ou mécanismes de reconnaissance. Leur rôle doit rester distinct de celui des acteurs qu'elles supervisent lorsque la criticité l'exige.

10. AP Certified©

AP Certified© s'intègre à l'architecture nationale comme mécanisme de certification gouverné. Les critères, niveaux, périodes de validité, preuves nécessaires, organismes autorisés, renouvellements, suspensions et retraits sont versionnés.

11. Accréditation des certificateurs

Les organismes ou fonctions habilités à certifier doivent démontrer compétence, indépendance adaptée, sécurité, traçabilité et capacité d'audit. L'accréditation peut être limitée à un secteur, un territoire, un niveau ou une famille de certifications.

12. Référentiels nationaux

Les identifiants, vocabulaires, schémas, niveaux de confiance, classifications et règles de preuve nécessaires à l'interopérabilité sont gouvernés comme des référentiels nationaux versionnés.

13. Fédération des registres et preuves

Les registres et systèmes de preuve peuvent rester distribués. Le niveau national assure leur reconnaissance et leur interopérabilité sans imposer qu'un registre central contienne toutes les données ou tous les événements.

14. Gouvernance des droits

Les droits sont attribués selon identité, mandat, mission, finalité et classification. Les accès transversaux ou exceptionnels sont encadrés, temporisés lorsque nécessaire et soumis à traçabilité renforcée.

15. Gestion des incidents de confiance

Fraude présumée, compromission, certificat contesté, identité compromise ou incohérence de preuve déclenchent des procédures d'investigation, limitation, suspension, correction et notification selon la criticité.

16. Contestation, recours et correction

Les acteurs disposent de mécanismes permettant de contester une donnée, un statut ou une certification. Une correction produit un nouvel état traçable ; elle ne supprime pas silencieusement l'existence de l'état antérieur.

17. Audit indépendant

Les fonctions d'audit évaluent conformité des processus, sécurité, respect des mandats, qualité des preuves et application des règles. L'audit doit pouvoir accéder aux éléments nécessaires sans devenir propriétaire des données contrôlées.

18. Comité de gouvernance et évolution

Les changements structurants de référentiels, certification, interopérabilité ou sécurité sont examinés selon un processus documenté associant les expertises concernées. Les décisions et versions applicables restent publiables ou consultables selon leur classification.

19. Deep Authenticity© et AP Ledger

Deep Authenticity© relie acteurs, mandats, données, preuves, certifications et décisions de gouvernance. AP Ledger peut ancrer accréditations, versions, statuts, suspensions et événements critiques afin de préserver une mémoire vérifiable.

20. Critères d'acceptation et conclusion

L'architecture nationale est acceptable si les compétences restent distribuées ; si État, institutions, territoires, secteurs et entreprises conservent leurs responsabilités ; si les opérateurs de confiance sont supervisés ; si certification et accréditation sont traçables ; si contestation et audit existent ; si les registres peuvent rester fédérés ; et si aucun acteur n'acquiert par défaut un contrôle total du système. Le Chapitre 3 développera la souveraineté numérique.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VII — GOUVERNANCE, SOUVERAINETÉ ET DÉPLOIEMENT INTERNATIONAL

CHAPITRE 3 — SOUVERAINETÉ NUMÉRIQUE

DONNÉES — IDENTITÉS — CLÉS — INFRASTRUCTURES — CLOUD — IA — LOGICIELS — INTEROPÉRABILITÉ — PORTABILITÉ — RÉVERSIBILITÉ

1. Objet du chapitre

Ce chapitre définit la souveraineté numérique comme la capacité d'un État, de ses institutions et de ses acteurs stratégiques à maîtriser les actifs numériques nécessaires à leur continuité, leur sécurité et leur autonomie de décision. Cette souveraineté ne signifie pas l'isolement technologique : elle exige la capacité de choisir, contrôler, substituer, migrer et coopérer selon des règles maîtrisées.

2. Souveraineté par la maîtrise

La souveraineté numérique repose moins sur l'origine nationale de chaque composant que sur la maîtrise effective des dépendances critiques. Une technologie externe peut être utilisée lorsque ses conditions d'accès, de contrôle, de continuité, de sortie et d'audit sont compatibles avec les exigences souveraines.

3. Souveraineté des données

Les données stratégiques restent soumises à des règles de classification, localisation, accès, traitement, partage, conservation et destruction. La maîtrise des données inclut également les métadonnées, historiques, journaux, modèles dérivés et copies nécessaires à la continuité.

4. Identités numériques souveraines

Les identités des institutions, entreprises, systèmes, agents autorisés et objets critiques doivent pouvoir être vérifiées dans un cadre gouverné. Les mécanismes nationaux conservent la capacité d' émettre, suspendre, révoquer ou reconnaître les identités nécessaires.

5. Maîtrise des clés cryptographiques

Les clés utilisées pour signer, chiffrer ou authentifier les actifs critiques sont gouvernées selon des politiques de génération, stockage, rotation, sauvegarde, révocation et récupération. La dépendance à un tiers ne doit pas empêcher l'État ou l'autorité compétente d'exercer les contrôles prévus.

6. Infrastructures numériques critiques

Centres de données, réseaux, capacités de calcul, stockage, services d'identité, synchronisation et autres infrastructures nécessaires sont cartographiés selon leur criticité, redondance, localisation, dépendances et capacités de reprise.

7. Cloud et services externalisés

Le recours au cloud ou à des services externes est évalué selon contrôle des données, juridictions applicables, chiffrement, portabilité, disponibilité, dépendances techniques et conditions de sortie. L'externalisation d'une fonction ne transfère pas automatiquement la responsabilité de gouvernance.

8. Souveraineté de l'intelligence artificielle

Les modèles d'IA critiques sont gouvernés selon provenance, données d'entraînement ou de calibration disponibles, versions, hébergement, dépendances, capacités d'audit et alternatives. Une dépendance à un modèle unique non substituable constitue un risque stratégique à identifier.

9. Modèles ouverts, propriétaires et hybrides

La souveraineté n'impose pas un modèle économique ou logiciel unique. Les solutions ouvertes, propriétaires ou hybrides sont évaluées selon contrôlabilité, sécurité, performance, capacité de maintenance, portabilité et risque de verrouillage.

10. Logiciels et composants critiques

Les composants logiciels nécessaires aux fonctions souveraines disposent d'un inventaire, de versions maîtrisées, de procédures de mise à jour et de solutions de continuité. Les dépendances transitives critiques doivent être identifiées autant que raisonnablement possible.

11. Interopérabilité

Les interfaces et formats documentés permettent de connecter plusieurs fournisseurs, systèmes et générations technologiques. L'interopérabilité réduit la dépendance sans exiger que tous les acteurs utilisent une plateforme unique.

12. Portabilité des données et configurations

Les données, schémas, configurations, historiques, preuves et paramètres nécessaires doivent pouvoir être exportés dans des formats gouvernés. La portabilité théorique est insuffisante si les volumes, coûts ou délais rendent la migration impraticable.

13. Réversibilité

Tout service numérique critique doit disposer, selon son niveau de risque, d'une stratégie de sortie : migration vers un autre fournisseur, retour vers une infrastructure maîtrisée, coexistence temporaire ou fonctionnement dégradé. Ces stratégies sont testées périodiquement.

14. Dépendances stratégiques numériques

Le système cartographie fournisseurs uniques, technologies non substituables, composants étrangers critiques, licences, réseaux, capacités de calcul et compétences rares. Chaque dépendance est évaluée selon criticité, concentration, substituabilité et délai de remplacement.

15. Capacités nationales minimales

La souveraineté peut nécessiter des capacités minimales nationales ou maîtrisées : identité, cryptographie, stockage, calcul, sauvegarde, supervision, compétences, reprise et continuité. Le niveau requis dépend de la criticité des fonctions.

16. Résilience et fonctionnement dégradé

Les fonctions essentielles prévoient des modes dégradés en cas de perte d'un fournisseur, d'un réseau ou d'un service externe. La continuité institutionnelle ne doit pas dépendre d'une connectivité permanente avec une infrastructure non maîtrisée.

17. Coopération technologique souveraine

Plusieurs États ou partenaires peuvent mutualiser standards, infrastructures ou capacités tout en conservant leurs autorités et leurs données. La coopération devient un multiplicateur de souveraineté lorsqu'elle réduit une dépendance sans en créer une nouvelle incontrôlée.

18. Mesure de la souveraineté numérique

Des indicateurs peuvent suivre concentration des fournisseurs, couverture des plans de sortie, capacité de migration, disponibilité des alternatives, localisation des actifs, maîtrise des clés, délais de récupération et niveau de dépendance des fonctions critiques.

19. Deep Authenticity© et AP Ledger

Deep Authenticity© relie identités, données, composants, versions, fournisseurs, transformations et preuves. AP Ledger peut ancrer versions, changements de contrôle, migrations et événements critiques afin de conserver une mémoire vérifiable de la souveraineté numérique.

20. Critères d'acceptation et conclusion

La souveraineté numérique est acceptable si les données et identités critiques restent gouvernées ; si les clés et infrastructures essentielles sont maîtrisées ; si cloud, IA et logiciels sont évalués selon leurs dépendances ; si interopérabilité, portabilité et réversibilité sont réelles et testées ; si des capacités minimales de continuité existent ; et si la coopération technologique n'entraîne pas une perte d'autorité. Le Chapitre 4 développera la souveraineté économique.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VII — GOUVERNANCE, SOUVERAINETÉ ET DÉPLOIEMENT INTERNATIONAL

CHAPITRE 4 — SOUVERAINETÉ ÉCONOMIQUE

CAPACITÉS PRODUCTIVES — RESSOURCES — CHAÎNES DE VALEUR — DÉPENDANCES — STOCKS — SUBSTITUTION — RÉSILIENCE — AUTONOMIE STRATÉGIQUE

1. Objet du chapitre

Ce chapitre définit la souveraineté économique comme la capacité d'un État et de son économie à préserver les fonctions essentielles, ses marges de décision et sa capacité d'adaptation face aux dépendances, ruptures ou transformations externes. Elle ne signifie ni autarcie ni fermeture des échanges, mais maîtrise des vulnérabilités critiques.

2. Souveraineté économique et ouverture

Une économie souveraine peut être fortement intégrée aux échanges internationaux. La question centrale est de savoir si une interruption, une concentration de fournisseur ou une contrainte extérieure peut empêcher durablement l'exercice d'une fonction essentielle sans alternative disponible.

3. Cartographie des capacités productives

Les capacités nationales sont représentées par secteur, territoire, niveau de production, disponibilité, flexibilité et dépendances. Capacité installée, capacité réellement mobilisable et capacité mobilisable en situation exceptionnelle restent distinctes.

4. Ressources stratégiques

Les ressources essentielles sont identifiées selon disponibilité nationale, importations, concentration géographique, saisonnalité, stocks, alternatives et délais de remplacement. Leur criticité dépend de leur rôle dans les fonctions économiques et institutionnelles.

5. Chaînes de valeur

Deep Authenticity© permet de relier matières, composants, transformations, entreprises, secteurs, territoires et marchés. Cette représentation aide à identifier les étapes dont la défaillance pourrait interrompre plusieurs chaînes en aval.

6. Dépendances extérieures

Les dépendances sont analysées selon fournisseur, pays, technologie, ressource, infrastructure, financement, compétence ou autre facteur pertinent. Une forte importation n'est pas automatiquement une vulnérabilité si des alternatives rapides et crédibles existent.

7. Concentration et points critiques

Le système identifie fournisseurs uniques, capacités fortement concentrées, infrastructures irremplaçables et étapes de production sans alternative immédiate. La criticité combine importance, probabilité de rupture, substituabilité et temps de récupération.

8. Stocks stratégiques

Les stocks peuvent absorber certaines perturbations mais leur efficacité dépend de volume, rotation, localisation, qualité, accessibilité et durée probable de la rupture. Le stock stratégique est traité comme un mécanisme de transition, non comme une solution permanente.

9. Substitution

La substitution peut concerner produit, matière, fournisseur, technologie, itinéraire, capacité ou processus. Chaque alternative possède des conditions de compatibilité, de certification, de coût et de délai qui doivent être intégrées aux scénarios.

10. Diversification

La diversification réduit certaines concentrations en répartissant fournisseurs, territoires, routes logistiques ou technologies. Elle doit toutefois être évaluée sur les dépendances sous-jacentes afin d'éviter plusieurs fournisseurs reposant en réalité sur le même point critique.

11. Capacités de réserve et montée en puissance

Certains secteurs peuvent disposer de capacités de réserve ou de mécanismes permettant une augmentation temporaire de production. Les délais, ressources, personnels, énergie, composants et autorisations nécessaires à cette montée en puissance sont explicités.

12. Relocalisation et capacités souveraines

Lorsqu'une dépendance est jugée critique et difficilement substituable, une capacité nationale ou maîtrisée peut être développée. Les décisions de relocalisation sont évaluées selon criticité, faisabilité, coût, délai, compétences et résilience créée.

13. Infrastructures économiques critiques

Énergie, transport, logistique, paiements, télécommunications et autres infrastructures peuvent conditionner plusieurs chaînes de valeur. Leur résilience est analysée conjointement aux capacités productives.

14. Compétences stratégiques

Certaines capacités dépendent de compétences rares, savoir-faire industriels, maintenance, ingénierie ou certification. La souveraineté économique inclut donc la conservation, la transmission et le renouvellement de ces compétences.

15. Simulation des ruptures

Le Jumeau Numérique National© peut simuler interruption d'importation, perte de capacité, hausse de demande, blocage logistique ou combinaison de chocs. Les scénarios évaluent propagation, stocks, substitution, délais et récupération.

16. Arbitrage économique

Les mesures de souveraineté peuvent avoir des coûts et effets d'opportunité. Les décisions comparent résilience obtenue, coût, impact concurrentiel, délais, innovation et risques de nouvelles dépendances.

17. Coopération économique souveraine

Des partenariats fiables peuvent renforcer la souveraineté par diversification, capacités partagées, reconnaissance mutuelle ou accords de continuité. La coopération doit réduire les vulnérabilités plutôt que déplacer une dépendance critique vers un partenaire unique.

18. Indicateurs de souveraineté économique

Des indicateurs peuvent suivre concentration des fournisseurs, couverture des stocks, temps de substitution, part de capacité maîtrisée, dépendances critiques, délais de montée en puissance, diversification et temps estimé de récupération.

19. Deep Authenticity© et AP Ledger

Deep Authenticity© relie produits, entreprises, capacités, origines, transformations, certifications et dépendances. AP Ledger peut ancrer les preuves et changements critiques nécessaires à la continuité des chaînes de confiance économiques.

20. Critères d'acceptation et conclusion

La souveraineté économique est acceptable si les capacités et dépendances critiques sont connues ; si stocks, diversification et substitution sont évalués avec leurs délais ; si les infrastructures et compétences sont intégrées ; si les mesures de résilience restent proportionnées ; si la coopération réduit réellement les vulnérabilités ; et si l'ouverture internationale demeure compatible avec la capacité nationale de décision et de continuité. Le Chapitre 5 développera la protection des données et la souveraineté informationnelle.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VII — GOUVERNANCE, SOUVERAINETÉ ET DÉPLOIEMENT INTERNATIONAL

CHAPITRE 5 — PROTECTION DES DONNÉES ET SOUVERAINETÉ INFORMATIONNELLE

CLASSIFICATION — MINIMISATION — LOCALISATION — ACCÈS — CHIFFREMENT — FÉDÉRATION — PARTAGE — CONSERVATION — TRAÇABILITÉ — CONTRÔLE SOUVERAIN

1. Objet du chapitre

Ce chapitre définit la protection des données et la souveraineté informationnelle comme la capacité à maîtriser le cycle de vie des informations stratégiques, institutionnelles, économiques et personnelles selon leur finalité, leur sensibilité et les règles applicables. L'objectif est de permettre l'usage et la coopération sans perte de contrôle sur les données.

2. Donnée comme actif gouverné

Une donnée n'est pas considérée comme un objet isolé. Elle est reliée à une source, une finalité, un propriétaire ou responsable, une classification, des droits d'usage, une temporalité, une qualité et des obligations de conservation ou suppression.

3. Classification

Les informations sont classifiées selon leur sensibilité et leur impact potentiel en cas de divulgation, altération, indisponibilité ou usage abusif. Les niveaux de classification déterminent les exigences de stockage, accès, partage, chiffrement et audit.

4. Minimisation

Seules les données nécessaires à une finalité définie sont collectées, transmises ou exposées. Une preuve ou un indicateur agrégé est privilégié lorsqu'il permet d'atteindre l'objectif sans communiquer la donnée détaillée.

5. Localisation et juridiction

La localisation physique ou logique des données, sauvegardes et traitements est connue lorsque la criticité l'exige. Les juridictions applicables et les conditions d'accès par des tiers sont intégrées à l' évaluation de souveraineté.

6. Contrôle des accès

Les accès reposent sur identité, rôle, mandat, finalité, classification et contexte. Les droits permanents sont limités et les accès exceptionnels peuvent être temporaires, justifiés et soumis à une journalisation renforcée.

7. Chiffrement et maîtrise des clés

Les données sensibles sont protégées selon leur criticité pendant stockage et transmission. La gouvernance des clés doit préserver les capacités d'accès légitimes, de rotation, de révocation, de récupération et de continuité.

8. Fédération plutôt que centralisation

Les données peuvent rester auprès de leurs détenteurs légitimes tandis que le système échange preuves, indicateurs, requêtes ou résultats autorisés. La fédération réduit la nécessité de constituer des bases centrales contenant des informations qui n'ont pas besoin d'y être copiées.

9. Partage interinstitutionnel

Le partage entre institutions est fondé sur une finalité, un cadre d'autorisation, une granularité et une durée définis. La capacité technique d'accéder à une donnée ne constitue jamais, à elle seule, une autorisation de l'utiliser.

10. Données économiques et secrets d'affaires

Les informations commerciales, industrielles et stratégiques des entreprises sont compartimentées. Deep Authenticity© permet de vérifier certains attributs ou certifications sans exiger la divulgation des procédés, contrats ou données internes non nécessaires.

11. Données personnelles

Les données relatives aux personnes sont traitées selon finalité, proportionnalité et protection renforcée. Les architectures nationales privilégient les données agrégées ou pseudonymisées lorsque l'identification individuelle n'est pas nécessaire à la fonction.

12. Données dérivées et inférences

Les indicateurs, scores, estimations et inférences peuvent être sensibles même lorsqu'ils ne reproduisent pas les données sources. Leur provenance, finalité, droits d'usage et durée de conservation sont donc également gouvernés.

13. Conservation et cycle de vie

Les durées de conservation sont adaptées aux obligations, besoins opérationnels, preuve et audit. Les données arrivées au terme de leur durée sont supprimées, anonymisées ou archivées selon des procédures gouvernées.

14. Sauvegardes et réplications

Les sauvegardes, caches, réplications et environnements de reprise sont inclus dans la gouvernance. Une donnée supprimée du système principal ne doit pas rester indéfiniment accessible dans des copies non maîtrisées.

15. Traçabilité

Les accès, modifications, exports et partages sensibles peuvent être journalisés. La traçabilité permet de reconstruire les opérations critiques tout en appliquant elle-même des règles de minimisation et de protection aux journaux.

16. Transferts transfrontaliers

Un transfert international est évalué selon finalité, classification, partenaire, juridiction, sécurité, durée, réutilisation autorisée et conditions de retour ou suppression. La coopération ne suppose pas la libre circulation de toutes les données.

17. Preuves transfrontalières minimales

Lorsqu'un partenaire a besoin de vérifier un fait, le système privilégie, lorsque possible, une preuve ou attestation vérifiable plutôt que le transfert de l'ensemble des données sources. Ce principe prépare les Corridors de Confiance©.

18. Incident et compromission

Une fuite, un accès abusif, une altération ou une perte de disponibilité déclenche confinement, investigation, évaluation d'impact, correction et notification selon les règles applicables. Les preuves de l'incident restent préservées.

19. Deep Authenticity© et AP Ledger

Deep Authenticity© relie données, provenance, classifications, droits, transformations, partages et preuves. AP Ledger peut ancrer consentements ou autorisations pertinentes, versions, transferts et événements critiques sans publier les contenus protégés.

20. Critères d'acceptation et conclusion

La souveraineté informationnelle est acceptable si les données sont classifiées et minimisées ; si localisation et juridictions critiques sont connues ; si accès et clés restent maîtrisés ; si la fédération limite les copies inutiles ; si données personnelles et économiques sont protégées ; si transferts internationaux sont gouvernés ; si le cycle de vie est maîtrisé ; et si la coopération peut reposer sur des preuves minimales. Le Chapitre 6 développera la Résilience Nationale©.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VII — GOUVERNANCE, SOUVERAINETÉ ET DÉPLOIEMENT INTERNATIONAL

CHAPITRE 6 — RÉSILIENCE NATIONALE©

ANTICIPATION — ABSORPTION — CONTINUITÉ — ADAPTATION — COORDINATION — RÉCUPÉRATION — APPRENTISSAGE — SOUVERAINETÉ

1. Objet du chapitre

Ce chapitre définit la Résilience Nationale© comme la capacité d'un État, de ses institutions, territoires, secteurs et acteurs économiques à anticiper une perturbation, en absorber les effets, maintenir les fonctions essentielles, adapter l'organisation collective, récupérer puis apprendre de l' événement.

2. Résilience systémique

La résilience nationale ne se réduit ni à la cybersécurité ni aux stocks d'urgence. Elle relie dimensions institutionnelle, numérique, économique, productive, énergétique, logistique, territoriale et informationnelle dans une lecture commune des dépendances et capacités de continuité.

3. Fonctions essentielles

Les fonctions dont l'interruption aurait des conséquences majeures sont identifiées et hiérarchisées. Pour chacune, le système décrit capacités minimales, dépendances critiques, délais tolérables, alternatives et conditions de reprise.

4. Anticipation

Watch System©, Cartographie Dynamique© et le Jumeau Numérique National© peuvent contribuer à détecter signaux faibles, tensions, concentrations et dégradations progressives. L'anticipation améliore le temps de préparation sans prétendre supprimer l'incertitude.

5. Préparation

Plans de continuité, ressources de réserve, procédures, compétences, moyens alternatifs et chaînes de décision sont préparés avant les crises. Leur existence documentaire ne suffit pas : leur faisabilité doit être testée.

6. Capacité d'absorption

Une architecture résiliente limite la propagation d'un choc grâce à redondance, segmentation, stocks, diversification, capacités locales, alternatives et priorisation des fonctions essentielles.

7. Continuité institutionnelle

Les institutions conservent des procédures permettant de décider, autoriser et coordonner même lorsque certains systèmes numériques, données ou infrastructures deviennent indisponibles. Les responsabilités en mode dégradé sont définies à l'avance.

8. Continuité numérique

Identités, communications, données essentielles, sauvegardes, calcul et services critiques disposent de solutions de continuité proportionnées. Les dépendances externes importantes sont accompagnées de mécanismes de substitution ou de fonctionnement dégradé.

9. Continuité économique et productive

Les secteurs critiques évaluent capacités de production, stocks, fournisseurs alternatifs, ressources, énergie, transport et compétences nécessaires au maintien d'un niveau minimal d'activité.

10. Résilience logistique

Les routes, plateformes, capacités de transport, entrepôts et corridors alternatifs sont intégrés aux scénarios. La résilience logistique mesure aussi le temps nécessaire pour réorienter les flux lorsque le chemin nominal devient indisponible.

11. Résilience territoriale

Les territoires disposent de profils de vulnérabilité et de capacités propres. L'architecture nationale évite qu'une moyenne nationale masque un territoire fortement exposé ou dépourvu d'alternative.

12. Coordination intersectorielle

Une crise dans un secteur peut créer des effets en cascade ailleurs. Les mécanismes de coordination identifient les dépendances, priorités concurrentes et arbitrages nécessaires entre énergie, transport, production, communications et autres fonctions.

13. Priorisation en situation de contrainte

Lorsque les ressources deviennent insuffisantes, des règles institutionnelles déterminent les fonctions prioritaires. Le système peut éclairer les conséquences de plusieurs allocations, mais l' arbitrage réel demeure attaché aux autorités compétentes.

14. Modes dégradés

Les organisations et infrastructures critiques définissent des niveaux de fonctionnement dégradé : services maintenus, fonctionnalités suspendues, données disponibles, procédures manuelles et limites de durée.

15. Récupération

La reprise ne consiste pas seulement à restaurer un composant. Elle vise à rétablir progressivement les fonctions, synchroniser les états, vérifier l'intégrité, traiter les retards accumulés et réduire les risques de rechute.

16. Reconstruction et adaptation

Après une perturbation majeure, le retour exact à l'état antérieur peut être insuffisant ou impossible. La reconstruction peut intégrer diversification, nouvelles capacités, nouvelles procédures ou réduction structurelle d'une dépendance.

17. Exercices nationaux et stress tests

Les scénarios de rupture sont testés à différents niveaux : institution, secteur, territoire et national. Les exercices vérifient décisions, communications, ressources, continuité, synchronisation et temps de récupération.

18. Indicateurs de résilience

Des indicateurs peuvent suivre couverture des plans de continuité, temps de détection, durée d' absorption, capacité minimale maintenue, temps de substitution, temps de récupération, redondance et évolution des dépendances critiques.

19. Deep Authenticity© et AP Ledger

Deep Authenticity© relie plans, capacités, dépendances, exercices, décisions, événements et résultats. AP Ledger peut ancrer versions de plans, validations, déclenchements et étapes critiques de reprise afin de préserver une mémoire vérifiable.

20. Critères d'acceptation et conclusion

La Résilience Nationale© est acceptable si les fonctions essentielles sont identifiées ; si leurs dépendances et capacités minimales sont connues ; si les modes dégradés sont préparés ; si la continuité couvre institutions, numérique, économie, production, logistique et territoires ; si les arbitrages restent institutionnels ; si exercices et indicateurs mesurent la capacité réelle ; et si chaque crise nourrit un apprentissage gouverné. Le Chapitre 7 développera les Dépendances Stratégiques©.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VII — GOUVERNANCE, SOUVERAINETÉ ET DÉPLOIEMENT INTERNATIONAL

CHAPITRE 7 — DÉPENDANCES STRATÉGIQUES©

IDENTIFICATION — CARTOGRAPHIE — CRITICITÉ — CONCENTRATION — SUBSTITUABILITÉ — PROFONDEUR — DÉLAI — RÉDUCTION — MONITORING

1. Objet du chapitre

Ce chapitre définit les Dépendances Stratégiques© comme les dépendances dont la rupture, l'indisponibilité, la concentration ou la perte de maîtrise pourrait affecter durablement une fonction essentielle, une capacité souveraine ou une chaîne de valeur critique. L'objectif est de les identifier, les mesurer, les simuler et les réduire de manière proportionnée.

2. Dépendance et vulnérabilité

Toute dépendance n'est pas une vulnérabilité. Elle devient stratégique lorsque son importance se combine à une faible substituabilité, une forte concentration, un délai de remplacement élevé ou une capacité limitée à fonctionner sans elle.

3. Typologie des dépendances

Les dépendances peuvent concerner matières premières, énergie, composants, technologies, logiciels, données, infrastructures, fournisseurs, compétences, financement, logistique, certification ou partenaires institutionnels. Une même fonction peut dépendre simultanément de plusieurs catégories.

4. Cartographie multi-niveaux

La cartographie relie produit, entreprise, secteur, territoire, infrastructure et niveau national. Elle permet d'identifier les dépendances visibles directement et celles qui apparaissent seulement à travers plusieurs niveaux de sous-traitance ou d'intermédiation.

5. Profondeur de chaîne

Une dépendance critique peut se situer plusieurs rangs en amont. L'analyse cherche, lorsque les données le permettent, à dépasser le fournisseur direct afin d'identifier matières, composants, technologies ou infrastructures communes à plusieurs chaînes.

6. Concentration

La concentration est évaluée selon fournisseurs, pays, territoires, technologies, infrastructures ou routes. Plusieurs fournisseurs apparents peuvent partager une même dépendance sous-jacente et ne pas constituer une diversification réelle.

7. Criticité

La criticité combine l'importance de la fonction dépendante, l'impact potentiel d'une rupture, la durée tolérable, la disponibilité d'alternatives et le temps de récupération. Les critères et pondérations restent explicites.

8. Substituabilité

Une alternative n'est considérée comme crédible que si elle peut satisfaire les exigences techniques, réglementaires, logistiques, économiques et temporelles. Une substitution théorique mais impossible à déployer dans le délai utile ne réduit pas réellement la dépendance.

9. Temps de remplacement

Le délai de remplacement inclut recherche d'alternative, qualification, certification, adaptation industrielle, contractualisation, transport, intégration et montée en capacité. Il peut être plus déterminant que le coût de l'alternative.

10. Dépendances croisées

Deux secteurs peuvent dépendre l'un de l'autre ou partager un même point critique. L'analyse systémique recherche ces dépendances croisées afin d'identifier les risques de propagation et de boucle de rétroaction.

11. Dépendances numériques et technologiques

Les plateformes, modèles d'IA, composants logiciels, capacités de calcul, réseaux, licences et clés technologiques sont intégrés à la cartographie. Les risques de verrouillage et de perte de support sont traités comme des dépendances potentielles.

12. Dépendances économiques et industrielles

Capacités de production, ressources, fournisseurs, équipements, maintenance et savoir-faire sont analysés conjointement. Une capacité nationale peut elle-même dépendre d'intrants ou technologies extérieurs critiques.

13. Dépendances logistiques

Ports, routes, plateformes, capacités de transport, entrepôts et corridors sont reliés aux chaînes de valeur. Une diversification des fournisseurs sans diversification logistique peut laisser subsister un point unique de rupture.

14. Dépendances de compétences

Certaines fonctions reposent sur un nombre limité de compétences ou de savoir-faire. Le risque est évalué selon disponibilité, transmission, formation, mobilité, renouvellement et temps nécessaire pour reconstituer la capacité.

15. Scénarios de rupture

Le Jumeau Numérique National© peut simuler perte d'un fournisseur, d'un pays, d'une technologie, d'une infrastructure ou d'une combinaison de dépendances. Les scénarios évaluent propagation, stocks, alternatives, délais et effets territoriaux.

16. Stratégies de réduction

Les réponses peuvent inclure diversification, substitution, stocks, redondance, relocalisation ciblée, capacités de réserve, coopération avec plusieurs partenaires ou développement de compétences. La stratégie dépend du profil réel de la dépendance.

17. Arbitrage et proportionnalité

Réduire toute dépendance à zéro serait irréaliste et potentiellement contre-productif. Les mesures sont priorisées selon criticité, coût, délai, faisabilité, bénéfice de résilience et risque de créer une nouvelle dépendance.

18. Watch System© des dépendances

Watch System© peut surveiller concentration, disponibilité, délais, incidents fournisseurs, tensions logistiques et évolution des alternatives. Les seuils d'alerte sont gouvernés et les signaux faibles déclenchent analyse plutôt qu'action automatique.

19. Deep Authenticity© et AP Ledger

Deep Authenticity© relie dépendances, origines, fournisseurs, composants, certifications, alternatives et changements de statut. AP Ledger peut ancrer les preuves et versions critiques afin de conserver une mémoire vérifiable de l'évolution des dépendances.

20. Critères d'acceptation et conclusion

La gestion des Dépendances Stratégiques© est acceptable si les dépendances sont cartographiées au-delà du premier niveau lorsque nécessaire ; si criticité, concentration, substituabilité et temps de remplacement sont distingués ; si les dépendances croisées et logistiques sont visibles ; si les stratégies de réduction restent proportionnées ; et si le monitoring détecte leur évolution. Le Chapitre 8 développera l'autonomie stratégique et les capacités souveraines.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VII — GOUVERNANCE, SOUVERAINETÉ ET DÉPLOIEMENT INTERNATIONAL

CHAPITRE 8 — AUTONOMIE STRATÉGIQUE ET CAPACITÉS SOUVERAINES

CAPACITÉS MINIMALES — RÉSERVES — SUBSTITUTION — DIVERSIFICATION — MONTÉE EN PUISSANCE — COMPÉTENCES — COOPÉRATION — CONTINUITÉ

1. Objet du chapitre

Ce chapitre définit l'autonomie stratégique comme la capacité à préserver une liberté réelle de décision et d'action dans les domaines essentiels. Elle repose sur des capacités souveraines minimales, des alternatives crédibles, des mécanismes de continuité et une maîtrise suffisante des dépendances identifiées au Chapitre 7.

2. Autonomie et interdépendance

L'autonomie stratégique n'exige pas l'indépendance absolue. Un État peut rester profondément interconnecté avec ses partenaires tout en conservant la capacité de poursuivre ses fonctions essentielles lorsqu'une relation, une technologie, un fournisseur ou un corridor devient temporairement indisponible.

3. Identification des capacités souveraines

Les capacités souveraines sont déterminées à partir des fonctions essentielles, des dépendances stratégiques et des scénarios de rupture. Elles peuvent concerner production, énergie, numérique, logistique, données, certification, maintenance, compétences ou capacités institutionnelles.

4. Niveau minimal de capacité

Pour chaque fonction critique, un niveau minimal de capacité peut être défini : volume, durée, couverture territoriale, délai de mobilisation ou niveau de service. Ce seuil constitue une capacité de continuité et non nécessairement la capacité économique normale du pays.

5. Capacités permanentes et mobilisables

Certaines capacités doivent être disponibles en permanence ; d'autres peuvent être mobilisées ou augmentées lorsque nécessaire. Les délais et ressources de mobilisation sont intégrés à l'évaluation de leur crédibilité.

6. Réserves stratégiques

Les réserves de matières, composants, équipements, données, capacités numériques ou autres ressources peuvent soutenir la continuité pendant une rupture. Leur gouvernance inclut dimensionnement, rotation, qualité, localisation, accès et renouvellement.

7. Capacités de substitution

Les alternatives sont préparées avant la crise lorsque la criticité l'exige. Produits, technologies, fournisseurs, routes ou processus de substitution peuvent être préqualifiés afin de réduire le temps de bascule.

8. Diversification structurée

La diversification vise à réduire les concentrations réelles. Elle analyse les dépendances sous-jacentes afin d'éviter que plusieurs solutions supposées indépendantes reposent sur le même composant, pays, infrastructure ou technologie.

9. Montée en puissance

La capacité à augmenter rapidement une production ou un service est modélisée selon équipements, intrants, énergie, personnels, autorisations, maintenance et logistique. La montée en puissance est mesurée en délai autant qu'en volume.

10. Capacités industrielles souveraines

Lorsque la criticité le justifie, certaines capacités de production, transformation, réparation ou maintenance peuvent être maintenues ou développées nationalement, même si elles ne représentent pas en permanence l'option économique la moins coûteuse.

11. Capacités numériques souveraines

Identité, cryptographie, données essentielles, calcul, stockage, communications, sauvegardes et supervision peuvent nécessiter des capacités maîtrisées permettant la continuité ou la reprise sans dépendance absolue à un acteur externe.

12. Compétences et savoir-faire

Une capacité souveraine sans compétences disponibles reste théorique. Formation, transmission, maintien des savoir-faire, documentation, exercices et renouvellement des équipes font partie intégrante de l'autonomie stratégique.

13. Capacité institutionnelle

L'autonomie repose aussi sur la capacité des institutions à analyser, arbitrer, autoriser, coordonner et agir. Les outils numériques assistent cette capacité mais ne doivent pas devenir une condition unique de son existence.

14. Préqualification et certification

Les alternatives stratégiques peuvent être testées et certifiées avant une crise. AP Certified© peut contribuer à établir des statuts vérifiables de compatibilité, conformité ou capacité, selon des référentiels gouvernés.

15. Coopération souveraine

Des capacités peuvent être partagées entre États ou partenaires fiables lorsqu'aucun participant ne perd la maîtrise de ses fonctions essentielles. Les accords précisent priorités, disponibilité, conditions d'accès, continuité et mécanismes de sortie.

16. Scénarios de mobilisation

Le Jumeau Numérique National© peut simuler mobilisation de réserves, substitution, augmentation de capacité, changement de corridor ou activation d'un partenariat. Les scénarios mesurent délais, goulots d'étranglement et effets secondaires.

17. Arbitrage coût-résilience

Les capacités souveraines ont un coût. Leur dimensionnement compare criticité, probabilité de rupture, impact, coût de maintien, délai de reconstruction et valeur de la continuité obtenue.

18. Indicateurs d'autonomie stratégique

Les indicateurs peuvent suivre couverture des capacités minimales, délai de mobilisation, durée des réserves, nombre d'alternatives préqualifiées, temps de substitution, capacité de montée en puissance et part des fonctions critiques disposant d'un plan de continuité.

19. Deep Authenticity© et AP Ledger

Deep Authenticity© relie capacités, ressources, certifications, alternatives, exercices et états de préparation. AP Ledger peut ancrer validations, versions, certifications et événements de mobilisation critiques afin de conserver une mémoire vérifiable.

20. Critères d'acceptation et conclusion

L'autonomie stratégique est acceptable si les capacités souveraines découlent des fonctions essentielles et dépendances réelles ; si les niveaux minimaux sont définis ; si réserves, substitution et diversification sont crédibles ; si la montée en puissance est testée ; si compétences et capacités institutionnelles sont intégrées ; si la coopération ne crée pas une nouvelle dépendance incontrôlée ; et si les coûts sont arbitrés avec la résilience obtenue. Le Chapitre 9 développera la gouvernance internationale de Deep Authenticity©.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VII — GOUVERNANCE, SOUVERAINETÉ ET DÉPLOIEMENT INTERNATIONAL

CHAPITRE 9 — GOUVERNANCE INTERNATIONALE DE DEEP AUTHENTICITY©

SOUVERAINETÉ — FÉDÉRATION — RECONNAISSANCE MUTUELLE — INTEROPÉRABILITÉ — CONFIANCE — PREUVES — CERTIFICATION — COOPÉRATION

1. Objet du chapitre

Ce chapitre définit la gouvernance internationale de Deep Authenticity© comme un cadre de coopération permettant à plusieurs États, institutions et écosystèmes économiques de vérifier des preuves, certifications et statuts communs sans transférer leur souveraineté à une autorité supranationale unique.

2. Coopérer sans centraliser

L'architecture internationale repose sur la fédération. Chaque État conserve ses autorités, données, infrastructures et mécanismes de décision, tandis que les partenaires conviennent des éléments nécessaires à l'interopérabilité et à la reconnaissance mutuelle.

3. Souveraineté des participants

L'adhésion à un cadre Deep Authenticity© international ne modifie pas, par elle-même, les compétences institutionnelles d'un État. Les engagements, droits et obligations résultent des instruments et accords effectivement adoptés par les participants.

4. Niveaux de coopération

La coopération peut être bilatérale, régionale, sectorielle, plurilatérale ou plus large. Les participants peuvent commencer par un périmètre limité avant d'étendre progressivement les catégories de preuves, certifications ou échanges reconnus.

5. Référentiels communs minimaux

L'interopérabilité internationale repose sur un noyau de définitions, identifiants, statuts, formats de preuve, niveaux de confiance et règles de validation suffisamment communs pour permettre la vérification entre systèmes.

6. Reconnaissance mutuelle

Deux partenaires peuvent reconnaître l'équivalence ou l'acceptabilité de certaines certifications ou preuves sans harmoniser l'ensemble de leurs réglementations. La portée, les exceptions et la durée de cette reconnaissance sont explicites.

7. Autorités de confiance nationales

Chaque participant désigne les autorités, organismes ou mécanismes habilités à émettre ou reconnaître les éléments couverts par l'accord. Le partenaire vérifie le mandat de l'émetteur autant que l'intégrité technique de la preuve.

8. Registre fédéré des autorités

Les informations nécessaires pour identifier les autorités reconnues, leurs mandats, statuts, clés ou périmètres peuvent être publiées ou fédérées selon des mécanismes gouvernés. Le registre ne doit pas devenir une base mondiale de données sensibles.

9. Preuves transfrontalières

Les échanges privilégient les preuves nécessaires à la transaction : origine, conformité, certification, transformation, statut ou autre attribut convenu. Les données sources restent auprès de leur détenteur lorsque leur transfert n'est pas nécessaire.

10. AP Certified© à l'international

AP Certified© peut être reconnu selon des niveaux, secteurs et juridictions déterminés. Une certification nationale n'acquiert pas automatiquement une portée universelle ; son acceptation dépend des cadres de reconnaissance applicables.

11. Interopérabilité technique

Les protocoles de vérification, formats, schémas, mécanismes cryptographiques et interfaces doivent permettre la coexistence de plusieurs infrastructures nationales. L'interopérabilité ne doit pas exiger l' utilisation d'un fournisseur unique.

12. Interopérabilité institutionnelle

Au-delà de la technique, les partenaires doivent comprendre qui est compétent pour émettre, suspendre, révoquer ou contester une preuve. Les changements de mandat doivent pouvoir être propagés aux partenaires concernés.

13. Protection des données

Les échanges internationaux appliquent minimisation, classification, finalité et règles de transfert. La vérification d'un attribut ne justifie pas l'accès à l'ensemble du dossier ayant permis de l'établir.

14. Contestation et révocation

Les accords prévoient comment signaler une preuve contestée, un certificat suspendu, une identité compromise ou une autorité révoquée. Les partenaires doivent pouvoir actualiser rapidement le statut de confiance sans effacer l'historique.

15. Gestion des divergences

Des différences de normes, droit, terminologie ou niveau d'exigence peuvent subsister. Le système les rend explicites et peut représenter des équivalences partielles plutôt que d'imposer une harmonisation artificielle.

16. Gouvernance des changements internationaux

Toute évolution des référentiels communs suit une procédure de proposition, consultation, validation, versioning et transition. Les participants conservent la possibilité de gérer les versions selon leurs engagements.

17. Résilience de la confiance internationale

La vérification transfrontalière doit pouvoir continuer malgré l'indisponibilité temporaire d'un participant ou d'un service central. Caches gouvernés, preuves signées, mécanismes de révocation et synchronisation différée peuvent soutenir la continuité.

18. Audit et transparence institutionnelle

Les mécanismes d'audit portent sur les processus de confiance, mandats, certifications et échanges concernés. La transparence est adaptée au niveau de sensibilité : auditabilité ne signifie pas publication universelle des contenus.

19. Deep Authenticity© et AP Ledger

Deep Authenticity© relie autorités, identités, preuves, certifications, accords et statuts de reconnaissance. AP Ledger peut ancrer les versions, accréditations, suspensions et événements critiques afin de fournir une chronologie vérifiable entre partenaires.

20. Critères d'acceptation et conclusion

La gouvernance internationale est acceptable si chaque État conserve sa souveraineté ; si la coopération repose sur fédération et reconnaissance mutuelle ; si les référentiels communs restent minimaux et versionnés ; si les preuves transfrontalières appliquent la minimisation ; si contestation, révocation et divergences sont gérées ; et si aucune infrastructure unique n'est indispensable à l' exercice de la confiance. Le Chapitre 10 développera AP Global Secure Trade Programme©.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VII — GOUVERNANCE, SOUVERAINETÉ ET DÉPLOIEMENT INTERNATIONAL

CHAPITRE 10 — AP GLOBAL SECURE TRADE PROGRAMME©

IDENTITÉ — ORIGINE — CONFORMITÉ — CERTIFICATION — TRAÇABILITÉ — RISQUE — INTEROPÉRABILITÉ — CORRIDORS — CONFIANCE COMMERCIALE

1. Objet du programme

AP Global Secure Trade Programme© définit un cadre fédéré de confiance pour sécuriser et fluidifier les échanges internationaux. Il vise à permettre aux partenaires autorisés de vérifier l'identité des acteurs, l'origine des produits, certaines transformations, certifications et statuts de conformité sans exiger la centralisation de toutes les données commerciales.

2. Principe de commerce vérifiable

Le programme remplace, lorsque cela est approprié, une logique fondée uniquement sur des déclarations documentaires par une chaîne de preuves vérifiables. Chaque preuve conserve son émetteur, son mandat, sa temporalité, son périmètre et son statut.

3. Participation souveraine

Chaque État ou juridiction conserve ses autorités, règles, systèmes de contrôle et décisions d' admission. La participation au programme facilite la vérification et la reconnaissance ; elle ne supprime pas les compétences douanières, réglementaires ou institutionnelles nationales.

4. Identité des acteurs

Exportateurs, importateurs, producteurs, transformateurs, transporteurs, certificateurs et autres acteurs pertinents peuvent disposer d'identités vérifiables reliées à leurs mandats et statuts. Une identité valide ne remplace pas les autorisations requises pour une opération donnée.

5. Identité du produit et du lot

Produits, lots, unités logistiques ou autres objets commerciaux peuvent être reliés à des identifiants persistants ou contextuels. Les relations entre produit, lot, origine, transformation et certification sont conservées selon le niveau de traçabilité nécessaire.

6. Origine et provenance

Les preuves d'origine peuvent être reliées aux producteurs, lieux, matières ou transformations nécessaires au référentiel applicable. Le système distingue origine déclarée, origine vérifiée et origine certifiée selon les niveaux de preuve.

7. Transformations et chaîne de valeur

Les transformations significatives peuvent être enregistrées comme événements vérifiables : production, assemblage, traitement, conditionnement ou changement de statut. Les secrets industriels non nécessaires restent protégés.

8. Conformité et exigences d'entrée

Le pays ou marché destinataire conserve ses exigences. Le programme permet de vérifier plus rapidement si les preuves disponibles correspondent aux exigences reconnues, sans transformer cette vérification technique en décision automatique d'admission.

9. AP Certified© dans le commerce international

AP Certified© peut attester des niveaux ou attributs définis pour un produit, une entreprise, un processus ou une chaîne. Les certificats sont limités par leur périmètre, version, validité et juridictions ou partenaires qui les reconnaissent.

10. Dossier commercial de confiance

Une transaction peut être accompagnée d'un dossier numérique réunissant uniquement les preuves nécessaires : identités, origine, certifications, statuts, événements logistiques et autres attributs autorisés. Les données sources détaillées restent fédérées lorsque leur transfert n'est pas requis.

11. Vérification avant expédition

Lorsque les partenaires le permettent, certaines preuves peuvent être vérifiées avant le départ des marchandises. Les incohérences peuvent ainsi être détectées plus tôt et corrigées avant d'atteindre un point de contrôle frontalier.

12. Vérification en transit et à destination

Les événements de transport, changements de garde, intégrité des unités logistiques ou statuts peuvent être mis à jour selon les capacités disponibles. Les autorités destinataires conservent la possibilité d'effectuer leurs propres contrôles.

13. Approche fondée sur le risque

Le programme peut aider à distinguer flux disposant de preuves cohérentes, flux nécessitant vérification complémentaire et anomalies. Les règles de risque restent gouvernées par les autorités compétentes et ne doivent pas produire une exemption automatique de contrôle.

14. Gestion des anomalies

Preuve absente, certificat expiré, incohérence d'origine, rupture de chaîne ou identité contestée déclenchent une demande de clarification, un contrôle renforcé ou une procédure selon les règles applicables. L'anomalie reste distincte d'une conclusion de fraude.

15. Interopérabilité douanière et commerciale

Le programme s'intègre aux systèmes existants par interfaces et schémas gouvernés. Il n'exige pas le remplacement simultané des infrastructures nationales et peut être déployé progressivement par catégories de produits ou corridors.

16. Corridors de Confiance©

Des partenaires peuvent établir des Corridors de Confiance© pour certains flux, secteurs ou opérateurs répondant à des exigences reconnues. Le corridor organise la reconnaissance des preuves et la coordination des contrôles sans supprimer la souveraineté frontalière.

17. Continuité et résilience des échanges

Les preuves signées, caches gouvernés, synchronisations différées et mécanismes de statut permettent de maintenir certaines vérifications lors d'indisponibilités temporaires. Les procédures de secours restent définies par les participants.

18. Mesure de performance

Les indicateurs peuvent suivre temps de vérification, taux de dossiers complets, anomalies détectées avant expédition, délais de traitement, taux de reconnaissance des certifications et résilience des flux. La performance ne doit pas être mesurée uniquement par la vitesse.

19. Deep Authenticity© et AP Ledger

Deep Authenticity© relie identités, produits, lots, origines, transformations, certifications et événements commerciaux. AP Ledger peut ancrer empreintes, statuts et événements critiques afin d' établir une continuité vérifiable entre partenaires sans publier les contenus commerciaux sensibles.

20. Critères d'acceptation et conclusion

AP Global Secure Trade Programme© est acceptable si les États conservent leurs compétences ; si les échanges reposent sur des preuves vérifiables et minimisées ; si identité, origine, conformité et certification restent distinguées ; si les contrôles fondés sur le risque demeurent gouvernés ; si l' interopérabilité permet un déploiement progressif ; et si les Corridors de Confiance© fluidifient les échanges sans supprimer les contrôles souverains. Le Chapitre 11 développera AP Certified©.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VII — GOUVERNANCE, SOUVERAINETÉ ET DÉPLOIEMENT INTERNATIONAL

CHAPITRE 11 — AP CERTIFIED©

OBJETS CERTIFIABLES — RÉFÉRENTIELS — PREUVES — ÉVALUATION — CERTIFICATEURS — ACCRÉDITATION — VALIDITÉ — SURVEILLANCE — SUSPENSION — RÉVOCATION — RECONNAISSANCE

1. Objet du chapitre

Ce chapitre définit AP Certified© comme un cadre de certification gouverné permettant d'attester, dans un périmètre explicite, qu'un produit, un processus, un service, une organisation, une capacité ou un autre objet défini satisfait des exigences vérifiables. La certification reste distincte de l'identité, de la simple traçabilité et de toute autorisation institutionnelle.

2. Principe de certification vérifiable

Une certification AP Certified© repose sur un référentiel identifié, des preuves suffisantes, une méthode d'évaluation, une décision de certification, une durée de validité et un statut vérifiable. Le certificat ne doit jamais être interprété au-delà du périmètre effectivement évalué.

3. Objets certifiables

Selon le programme applicable, peuvent être certifiés des produits, processus, services, entreprises, sites, capacités, chaînes ou autres objets définis. Chaque catégorie dispose de critères et de méthodes adaptés ; une certification d'un objet n'entraîne pas automatiquement celle des objets qui lui sont liés.

4. Référentiels de certification

Chaque certification est reliée à une version précise d'un référentiel. Celui-ci décrit exigences, preuves attendues, méthodes d'évaluation, règles de décision, exceptions, durée de validité, surveillance et conditions de suspension ou retrait.

5. Niveaux et portées

AP Certified© peut prévoir plusieurs niveaux ou portées afin de distinguer profondeur de vérification, périmètre couvert ou exigences satisfaites. Les niveaux doivent rester compréhensibles et ne pas créer une impression de garantie absolue.

6. Dossier de preuve

Le dossier rassemble les preuves nécessaires : identités, provenance, documents, mesures, résultats d'essais, événements Deep Authenticity© ou autres éléments autorisés. La minimisation s'applique : seules les informations nécessaires à l'évaluation sont exposées.

7. Évaluation de conformité

L'évaluation peut combiner revue documentaire, essais, inspection, audit, vérification de preuves ou autres méthodes prévues par le référentiel. Les méthodes sont proportionnées au risque et suffisamment documentées pour permettre une décision reproductible.

8. Décision de certification

La décision de délivrer, maintenir, étendre, réduire, suspendre ou retirer une certification est prise par un rôle ou organisme autorisé selon le schéma applicable. La collecte de preuves et la décision peuvent être séparées afin de renforcer l'impartialité.

9. Organismes certificateurs

Les certificateurs doivent démontrer compétence, impartialité, confidentialité, sécurité, traçabilité et capacité de traitement des plaintes ou recours. Leur périmètre d'autorisation précise les secteurs, objets, référentiels et niveaux qu'ils peuvent certifier.

10. Accréditation

Lorsque le schéma l'exige, les organismes certificateurs sont évalués par une fonction ou un organisme d'accréditation distinct. L'accréditation atteste la compétence pour des activités déterminées et ne transforme pas l'organisme d'accréditation en certificateur des objets finaux.

11. Identité numérique du certificat

Chaque certificat possède un identifiant, un émetteur, un titulaire ou objet, un référentiel, une version, une portée, une date d'émission, une échéance éventuelle et un statut. La vérification doit permettre de détecter un certificat expiré, suspendu, retiré ou remplacé.

12. Validité et renouvellement

La validité dépend de la nature de l'objet et du risque. Le renouvellement peut exiger nouvelles preuves, réévaluation, surveillance ou confirmation que les conditions ayant fondé la certification restent satisfaites.

13. Surveillance continue ou périodique

Certains schémas peuvent prévoir une surveillance entre deux renouvellements. Les changements significatifs, anomalies ou événements définis peuvent déclencher une réévaluation sans transformer AP Certified© en surveillance permanente non proportionnée.

14. Modification du périmètre

Une modification de produit, processus, site, fournisseur, technologie ou autre élément critique peut nécessiter extension, réduction ou nouvelle évaluation. Le certificat conserve l'historique de ses versions et de son périmètre.

15. Suspension et révocation

Une certification peut être suspendue lorsque des conditions deviennent incertaines ou temporairement non satisfaites, puis retirée lorsque les exigences ou obligations ne sont plus remplies. Le statut doit être propagé rapidement aux partenaires qui s'y fient.

16. Plaintes, recours et contestation

Les titulaires et parties habilitées disposent de procédures de plainte ou recours. La contestation est instruite de manière traçable, avec séparation appropriée des responsabilités et conservation de l'état antérieur.

17. Reconnaissance nationale et internationale

Un certificat AP Certified© n'est reconnu que dans les périmètres, secteurs ou juridictions où un mécanisme de reconnaissance existe. La reconnaissance peut être totale, conditionnelle ou limitée à certains attributs.

18. Alignement avec les principes de conformité

Le cadre AP Certified© est conçu pour pouvoir s'articuler avec les principes internationaux de certification et d'accréditation applicables, notamment compétence, impartialité, cohérence, confidentialité et gestion des recours, tout en conservant ses mécanismes propres de preuve numérique.

19. Deep Authenticity© et AP Ledger

Deep Authenticity© relie objet, référentiel, preuves, évaluations, décisions et statut du certificat. AP Ledger peut ancrer émission, renouvellement, modification, suspension et retrait afin de préserver une chronologie vérifiable sans publier les dossiers confidentiels.

20. Critères d'acceptation et conclusion

AP Certified© est acceptable si l'objet et le périmètre sont explicites ; si le référentiel est versionné ; si les preuves et méthodes sont définies ; si les certificateurs sont compétents et supervisés ; si validité, surveillance, modification, suspension et retrait sont gouvernés ; si les recours existent ; si la reconnaissance internationale reste explicite ; et si la preuve numérique ne remplace pas l'évaluation de conformité. Le Chapitre 12 développera la normalisation et les référentiels internationaux.

Note d'alignement : l'architecture proposée distingue certification et accréditation et retient les principes de compétence et d'impartialité afin de rester compatible avec les cadres internationaux d' évaluation de la conformité, sans prétendre qu'AP Certified© constitue à ce stade une certification ISO/IEC.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VII — GOUVERNANCE, SOUVERAINETÉ ET DÉPLOIEMENT INTERNATIONAL

CHAPITRE 12 — NORMALISATION ET RÉFÉRENTIELS INTERNATIONAUX

VOCABULAIRES — SCHÉMAS — EXIGENCES — CONFORMITÉ — INTEROPÉRABILITÉ — VERSIONING — ÉQUIVALENCE — RECONNAISSANCE MUTUELLE

1. Objet du chapitre

Ce chapitre définit la normalisation comme le mécanisme permettant de transformer les principes de Deep Authenticity© en référentiels compréhensibles, testables et interopérables. L'objectif n'est pas d'imposer un système technique unique, mais de rendre compatibles les preuves, certifications et mécanismes de confiance entre organisations, secteurs et États.

2. Normalisation et souveraineté

Un référentiel international commun ne doit pas effacer les règles nationales. Il définit les éléments nécessaires à la coopération tandis que chaque juridiction conserve la capacité de fixer des exigences supplémentaires, des exceptions et des conditions d'application.

3. Architecture des référentiels

Les référentiels peuvent être organisés en couches : principes communs, terminologie, modèles de données, formats de preuve, exigences de sécurité, règles d'évaluation de conformité, profils sectoriels et profils nationaux. Cette structure limite les duplications tout en permettant l'adaptation.

4. Terminologie commune

Les concepts essentiels — identité, preuve, origine, transformation, certification, statut, révocation, autorité, mandat et autres notions du système — disposent de définitions suffisamment précises pour éviter que deux partenaires attribuent des significations différentes au même terme.

5. Schémas et modèles de données

Les échanges utilisent des schémas versionnés décrivant champs, identifiants, relations, unités, temporalité et statuts. Les extensions nationales ou sectorielles sont possibles sans casser le noyau d'interopérabilité.

6. Exigences vérifiables

Les exigences destinées à soutenir une certification ou une évaluation doivent être formulées de façon claire, observable et suffisamment non ambiguë pour permettre une évaluation cohérente. Les critères de décision restent séparés des simples recommandations.

7. Référentiels adaptés à l’évaluation de conformité

Les documents normatifs destinés à AP Certified© doivent préciser objet, portée, exigences, méthodes ou catégories d’évaluation pertinentes, preuves attendues et règles de décision. Cette approche facilite l’articulation avec les pratiques internationales d’évaluation de conformité.

8. Interopérabilité technique

Les standards d’échange doivent permettre plusieurs implémentations, fournisseurs et infrastructures. L’interopérabilité est vérifiée par conformité aux interfaces et comportements attendus plutôt que par obligation d’utiliser un logiciel unique.

9. Interopérabilité sémantique

Deux systèmes techniquement connectés ne sont réellement interopérables que s’ils interprètent les informations de manière compatible. Vocabulaires, codes, unités, relations et règles de transformation doivent donc être gouvernés.

10. Profils nationaux et sectoriels

Un standard commun peut être décliné en profils définissant les options et exigences applicables à un pays, un secteur ou un corridor. Le profil indique explicitement les écarts par rapport au noyau commun.

11. Versioning et compatibilité

Chaque référentiel possède une version identifiable, une date d’entrée en vigueur et, lorsque nécessaire, une période de transition. Les mécanismes de compatibilité permettent à plusieurs versions de coexister temporairement sans ambiguïté.

12. Gouvernance des changements

Les évolutions suivent proposition, justification, consultation, analyse d’impact, validation et publication. Les changements incompatibles font l’objet de mécanismes de migration afin d’éviter une rupture brutale des chaînes de confiance.

13. Tests de conformité et d’interopérabilité

Des suites de tests peuvent vérifier schémas, signatures, statuts, interfaces et comportements attendus. La réussite technique à ces tests ne remplace pas une certification lorsque celle-ci exige également une évaluation métier, réglementaire ou organisationnelle.

14. Équivalence

Deux référentiels différents peuvent être reconnus comme équivalents sur certaines exigences sans être identiques. L’équivalence est documentée exigence par exigence ou attribut par attribut afin d’ éviter une reconnaissance plus large que ce qui a réellement été comparé.

15. Reconnaissance mutuelle

La reconnaissance internationale peut s'appuyer sur des accords ou arrangements acceptant certains résultats d'essais, inspections, certifications ou accréditations. La confiance repose sur des critères communs, la compétence des organismes et la clarté du périmètre reconnu.

16. Articulation avec les standards internationaux

Deep Authenticity© et AP Certified© sont conçus pour pouvoir s'articuler avec des normes internationales existantes lorsqu'elles sont pertinentes. L'objectif est d'éviter de recréer des exigences déjà reconnues et de concentrer les spécifications propres à Deep Authenticity© sur ses mécanismes distinctifs.

17. Gouvernance du catalogue de référentiels

Un catalogue versionné peut identifier référentiels actifs, versions retirées, profils, dépendances, équivalences et juridictions de reconnaissance. Le catalogue facilite la vérification sans transformer l' organisation qui le maintient en autorité universelle.

18. Stratégie de normalisation internationale

La progression peut suivre plusieurs étapes : spécifications internes stabilisées, pilotes multi-acteurs, profils sectoriels, coopération avec organismes compétents, propositions de normalisation et reconnaissance progressive. La maturité technique précède la revendication de statut normatif.

19. Deep Authenticity© et AP Ledger

Deep Authenticity© relie référentiels, versions, profils, preuves et certifications. AP Ledger peut ancrer publication, remplacement, retrait, équivalence et reconnaissance de versions critiques afin de préserver une chronologie vérifiable.

20. Critères d'acceptation et conclusion

La normalisation est acceptable si les référentiels sont clairs, versionnés et testables ; si les exigences sont adaptées à l'évaluation de conformité ; si interopérabilité technique et sémantique sont distinguées ; si les profils préservent les besoins nationaux et sectoriels ; si équivalence et reconnaissance restent limitées à leur périmètre réel ; et si Deep Authenticity© s'articule avec les standards internationaux sans revendiquer une reconnaissance non obtenue. Le Chapitre 13 développera les Corridors de Confiance©.

Note d'alignement international

Cette architecture tient compte des principes de l'ISO/CASCO : les normes de la série ISO/IEC 17000 constituent une boîte à outils pour l'évaluation de conformité, tandis que les accords de reconnaissance mutuelle peuvent soutenir l'acceptation internationale de résultats d'essais, d' inspections, de certifications ou d'accréditations. ISO/IEC 17007:2026 fournit en outre des orientations pour rédiger des documents normatifs adaptés à l'évaluation de conformité. Cette

référence d’alignement ne signifie pas que Deep Authenticity© ou AP Certified© bénéficient actuellement d’une reconnaissance ISO/IEC.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VII — GOUVERNANCE, SOUVERAINETÉ ET DÉPLOIEMENT INTERNATIONAL

CHAPITRE 13 — CORRIDORS DE CONFIANCE©

ÉTATS PARTENAIRES — AUTORITÉS — OPÉRATEURS — AP CERTIFIED© — PRODUITS — PREUVES — LOGISTIQUE — CONTRÔLES — INTEROPÉRABILITÉ — RÉSILIENCE

1. Objet du chapitre

Ce chapitre définit les Corridors de Confiance© comme des cadres opérationnels de coopération entre États, autorités, opérateurs économiques et infrastructures de confiance. Leur objectif est de rendre certains flux commerciaux, industriels ou logistiques plus vérifiables, plus prévisibles et plus résilients, sans supprimer les compétences souveraines de contrôle.

2. Principe du corridor

Un Corridor de Confiance© ne constitue ni une frontière parallèle ni une zone d'exemption générale. Il organise un ensemble convenu de preuves, identités, certifications, contrôles et mécanismes de reconnaissance permettant aux participants de mieux préparer et vérifier les échanges.

3. Périmètre

Un corridor peut être défini par pays partenaires, secteur, catégorie de produits, route logistique, opérateurs éligibles ou combinaison de ces dimensions. Son périmètre, ses exclusions et sa durée sont explicitement gouvernés.

4. Accord entre partenaires

Les partenaires définissent objectifs, autorités compétentes, référentiels reconnus, données ou preuves échangées, mécanismes de contestation, règles de sécurité, continuité et conditions de suspension. L'accord ne transfère pas automatiquement de compétence réglementaire.

5. Autorités reconnues

Chaque État identifie les autorités ou organismes habilités à émettre, vérifier, reconnaître, suspendre ou révoquer les statuts utilisés dans le corridor. Le mandat de l'émetteur fait partie de la chaîne de confiance.

6. Éligibilité des opérateurs

Exportateurs, importateurs, producteurs, logisticiens ou autres opérateurs peuvent être admis selon des critères définis : identité, conformité, historique, certifications, capacités de traçabilité ou autres exigences proportionnées.

7. AP Certified© dans le corridor

AP Certified© peut contribuer à démontrer certains attributs ou niveaux de conformité lorsque le référentiel et la certification sont reconnus par les partenaires. Le corridor n'étend pas automatiquement la portée d'un certificat au-delà de sa reconnaissance formelle.

8. Identité et traçabilité des produits

Produits, lots ou unités logistiques peuvent être reliés à des identifiants et événements vérifiables. L' objectif est de maintenir une continuité suffisante entre origine, transformations pertinentes, certification, expédition, transit et réception.

9. Dossier numérique de corridor

Un dossier numérique peut réunir les preuves minimales requises pour un flux : identité des acteurs, origine, certificats, statuts, documents ou événements logistiques. Les informations confidentielles restent auprès de leurs détenteurs lorsque leur transfert n'est pas nécessaire.

10. Pré-vérification

Les preuves peuvent être contrôlées avant l'expédition ou avant l'arrivée afin d'identifier plus tôt les dossiers incomplets, incohérences ou certificats non valides. La pré-vérification améliore la préparation sans garantir automatiquement l'admission finale.

11. Contrôles coordonnés

Les partenaires peuvent coordonner certains contrôles afin de réduire les duplications inutiles lorsqu' une confiance suffisante existe dans les résultats de conformité. Les autorités conservent néanmoins leur droit d'effectuer les contrôles requis par leur cadre applicable.

12. Approche fondée sur le risque

Les informations du corridor peuvent soutenir une priorisation des contrôles selon la qualité des preuves, les anomalies et les règles de risque applicables. Le statut de corridor ne doit pas devenir une immunité contre les contrôles.

13. Gestion des anomalies

Une rupture de traçabilité, un certificat suspendu, une identité contestée ou une incohérence déclenche une procédure définie : clarification, contrôle complémentaire, suspension d'un flux ou autre mesure relevant de l'autorité compétente. Une anomalie n'est pas automatiquement une preuve de fraude.

14. Interopérabilité

Le corridor doit pouvoir relier plusieurs systèmes nationaux et commerciaux grâce à des formats, identifiants, statuts et protocoles communs ou convertibles. Aucun fournisseur technique unique ne doit être indispensable au fonctionnement du cadre.

15. Performance et facilitation

La performance peut être mesurée par temps de traitement, taux de dossiers pré-vérifiés, réduction des duplications, taux d'anomalies détectées en amont, fiabilité des statuts et continuité des flux. La rapidité reste subordonnée à l'intégrité des contrôles.

16. Résilience du corridor

Des itinéraires alternatifs, procédures de secours, caches gouvernés, preuves signées et synchronisation différée peuvent soutenir la continuité en cas d'indisponibilité d'un système ou d'une liaison. Les modes dégradés restent explicitement encadrés.

17. Suspension et sortie

Un partenaire, opérateur, certification ou flux peut être suspendu selon les conditions prévues. Les mécanismes de sortie garantissent que la fin d'un corridor ou d'une participation n'entraîne ni perte des preuves historiques ni dépendance technique irréversible.

18. Extension progressive

Un corridor peut commencer par un produit, un secteur ou un nombre limité d'opérateurs, puis s' étendre après évaluation. Les résultats des pilotes alimentent l'évolution des référentiels, contrôles, interfaces et mécanismes de reconnaissance.

19. Deep Authenticity© et AP Ledger

Deep Authenticity© relie accords, autorités, opérateurs, produits, preuves, certifications et événements du corridor. AP Ledger peut ancrer versions, statuts, validations, suspensions et événements critiques afin de préserver une chronologie vérifiable entre partenaires.

20. Critères d'acceptation et conclusion

Un Corridor de Confiance© est acceptable si son périmètre et ses autorités sont explicites ; si les preuves échangées sont minimisées ; si les certifications sont reconnues dans une portée définie ; si la pré-vérification ne remplace pas la décision souveraine ; si les contrôles coordonnés reposent sur une confiance démontrée ; si anomalies, résilience et sortie sont gouvernées ; et si l'interopérabilité évite la dépendance à une plateforme unique. Le Chapitre 14 développera le passeport numérique et les preuves transfrontalières.

Note d'alignement international

Les Corridors de Confiance© sont conçus pour pouvoir s'articuler avec les mécanismes internationaux de reconnaissance des résultats d'évaluation de conformité. Les travaux ISO/CASCO indiquent que les accords ou arrangements de reconnaissance mutuelle peuvent soutenir l' acceptation de résultats d'essais, d'inspections, de certifications ou d'accréditations entre juridictions, tandis qu'ISO 22373:2025 propose un cadre d'authenticité, d'intégrité et de confiance pour les chaînes de produits et de valeur. Cet alignement constitue une orientation d'interopérabilité et ne vaut pas reconnaissance normative automatique du programme.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VII — GOUVERNANCE, SOUVERAINETÉ ET DÉPLOIEMENT INTERNATIONAL

CHAPITRE 14 — PASSEPORT NUMÉRIQUE ET PREUVES TRANSFRONTALIÈRES

IDENTITÉ — ORIGINE — PRODUIT — PROPRIÉTÉ — CERTIFICATION — PREUVES — FRONTIÈRES — INTEROPÉRABILITÉ — SOUVERAINETÉ — TRAÇABILITÉ

1. Objet du chapitre

Ce chapitre définit le passeport numérique de Deep Authenticity© comme un ensemble structuré de références, statuts et preuves permettant d'accompagner unproduit, un actif ou un droit au cours de son cycle de vie et, lorsque cela est nécessaire, au-delà des frontières nationales. Il vise à maintenir une continuité vérifiable entre identité, origine, authenticité, événements significatifs et autorités compétentes sans transformer le passeport en registre universel contenant toutes les données.

2. Principe du passeport numérique

Le passeport numérique constitue une représentation vérifiable associée à un objet déterminé. Il ne remplace ni le produit physique, ni les documents réglementaires, ni les registres souverains qui possèdent une valeur juridique propre. Il fournit une couche de liaison permettant de retrouver les preuves nécessaires, leur origine, leur statut, leur période de validité et, lorsque cela est autorisé, leur historique.

3. Identité persistante

Chaque passeport doit être rattaché à une identité suffisamment stable pour éviter qu'un changement de système, de propriétaire, de territoire ou d'opérateur rompe la continuité de vérification. L' identifiant ne constitue toutefois pas, à lui seul, une preuve d'authenticité : sa valeur dépend de la chaîne d'émission, des contrôles, des événements associés et des autorités ou opérateurs qui ont produit les preuves correspondantes.

4. Périmètre informationnel

Le passeport peut référencer, selon le secteur et les exigences applicables : origine, fabricant, lot, unité, caractéristiques essentielles, certifications, contrôles, propriété, maintenance, réparations, transformations, rappels, restrictions ou autres événements pertinents. Le principe de minimisation demeure applicable : seules les informations nécessaires à la fonction considérée doivent être exposées.

5. Séparation entre donnée et preuve

Deep Authenticity© distingue la donnée source de la preuve permettant d'en vérifier certaines propriétés. Une administration, une entreprise ou un organisme de certification peut conserver ses

informations sensibles dans son propre environnement tout en fournissant une preuve signée, une empreinte, un statut ou une attestation vérifiable. Le passeport n'impose donc pas la duplication systématique des bases de données.

6. Autorité de l'émetteur

Toute information significative doit pouvoir être reliée à son émetteur et à la capacité dans laquelle celui-ci intervient. Un fabricant peut attester certains éléments de production ; un organisme compétent peut émettre une certification ; une autorité publique peut établir un statut réglementaire ; un propriétaire peut déclencher certaines opérations relevant de ses droits. La plateforme ne confond pas ces niveaux d'autorité.

7. Authenticity Plus© et l'identité physique

Pour les produits physiques protégés par Authenticity Plus©, le passeport numérique s'articule avec l' architecture fondamentale des trois QR codes : consommateur, revendeur/professionnel et contrôle/douanes. Ces accès fonctionnellement distincts permettent aux différents acteurs d' interroger ou d'alimenter le système conformément à leur rôle. L'interprétation fondamentale reste : VERT — original ; JAUNE — original mais déjà vérifié ou vendu ; ROUGE — contrefaçon ou code inexistant dans le système Authenticity Plus©. Le passeport numérique enrichit cette architecture ; il ne s'y substitue pas.

8. Cycle de vie

Le passeport accompagne les événements pertinents depuis la création ou l'enregistrement initial jusqu'à la fin de vie, lorsque le cadre applicable l'exige. Production, certification, expédition, importation, vente, transfert de propriété, maintenance, réparation, seconde main, rappel, recyclage ou destruction peuvent constituer des événements vérifiables. Tous les événements possibles ne sont pas nécessairement obligatoires pour tous les secteurs.

9. Preuves transfrontalières

Lorsqu'un produit traverse une frontière, certaines preuves doivent pouvoir être comprises et vérifiées par des acteurs appartenant à des juridictions différentes. Une preuve transfrontalière doit donc préciser au minimum son origine, son émetteur, sa portée, son statut, sa période de validité et les éléments nécessaires à sa vérification. Sa lisibilité technique ne signifie pas automatiquement qu'elle possède une valeur juridique identique dans tous les États.

10. Reconnaissance et souveraineté

La reconnaissance d'une preuve étrangère relève des règles applicables, des accords entre partenaires et des autorités compétentes. Deep Authenticity© peut faciliter la transmission, l' authentification et la vérification technique d'une preuve ; il ne peut pas imposer à un État de reconnaître juridiquement une certification, un document ou une décision provenant d'une autre juridiction. Cette distinction protège la souveraineté réglementaire.

11. Connexion aux Corridors de Confiance©

Les Corridors de Confiance© définis au Chapitre 13 constituent un environnement privilégié pour l'utilisation des passeports numériques transfrontaliers. Les partenaires peuvent convenir des catégories de preuves reconnues, des autorités habilitées, des formats, des contrôles, des niveaux d'assurance et des procédures applicables aux anomalies. Le passeport devient ainsi un support opérationnel du corridor sans remplacer l'accord qui le gouverne.

12. Contrôles douaniers et réglementaires

Les autorités de contrôle peuvent disposer d'un accès adapté aux informations nécessaires à leur mission. Dans l'architecture Authenticity Plus©, le QR de contrôle/douanes constitue un canal fonctionnel distinct destiné aux acteurs habilités. Les informations accessibles peuvent contribuer à vérifier identité, origine, statut, certifications, événements logistiques ou anomalies connues. La décision d'admission, d'inspection, de blocage ou de mainlevée demeure toutefois de la compétence de l'autorité concernée.

13. Transfert de propriété

Lorsque le produit change légitimement de propriétaire, le passeport peut enregistrer ou référencer l'événement de transfert selon les règles du système. Le transfert ne doit pas effacer l'historique antérieur ni permettre au nouveau détenteur de modifier rétroactivement les preuves établies. Les informations personnelles associées aux propriétaires successifs restent soumises aux règles de confidentialité et ne deviennent pas automatiquement accessibles aux utilisateurs ultérieurs.

14. Produits d'occasion

Le passeport numérique prend une importance particulière sur le marché de seconde main. Il peut permettre de vérifier qu'un produit correspond toujours à une identité connue, de consulter les statuts autorisés, de constater certains transferts ou événements pertinents et de réduire la réintroduction de produits frauduleux dans les circuits légitimes. L'absence d'un événement intermédiaire ne doit toutefois pas être interprétée automatiquement comme une preuve de contrefaçon.

15. Interopérabilité

Le passeport doit pouvoir fonctionner dans un environnement composé de multiples systèmes publics, industriels, commerciaux et internationaux. Formats ouverts ou documentés, identifiants résolvables, signatures vérifiables, vocabulaires contrôlés, API et mécanismes de conversion peuvent permettre cette interopérabilité. Deep Authenticity© doit éviter qu'un passeport devienne inutilisable simplement parce qu'un fournisseur, un logiciel ou une infrastructure particulière disparaît.

16. Confidentialité et divulgation sélective

Le caractère transfrontalier d'une preuve ne justifie pas la circulation indiscriminée des données. Le passeport applique une logique de divulgation proportionnée : consommateur, revendeur, transporteur, certificateur, douane, administration ou propriétaire peuvent disposer de vues différentes selon leur rôle. Lorsque cela est techniquement et juridiquement approprié, une propriété peut être démontrée sans révéler l'ensemble du dossier source.

17. Révocation, correction et historique

Une certification peut expirer, une autorisation être retirée, une erreur être corrigée ou un produit faire l'objet d'un rappel. Le passeport doit donc gérer les changements de statut sans réécrire silencieusement l'histoire. Les versions, corrections, suspensions et révocations importantes doivent conserver une chronologie permettant de comprendre quel statut était applicable à un moment donné.

18. Résilience et vérification en environnement dégradé

Les échanges internationaux peuvent traverser des zones où la connectivité est limitée ou momentanément indisponible. Des preuves signées, données minimales vérifiables localement, caches gouvernés ou mécanismes de synchronisation différée peuvent soutenir certains contrôles en mode dégradé. Toute décision prise à partir d'informations non synchronisées doit cependant respecter des règles explicites de fraîcheur, de portée et de réconciliation ultérieure.

19. Deep Authenticity© et AP Ledger

Deep Authenticity© fournit le cadre de relation entre produit, identité, acteurs, preuves, droits et événements. AP Ledger peut conserver ou ancrer les éléments probants nécessaires à la chronologie : émission, certification, transfert, validation, modification de statut, suspension, révocation ou autre événement critique. Le registre probant n'a pas vocation à recevoir indistinctement toutes les données du passeport ; il conserve les éléments nécessaires à l'intégrité, à l'auditabilité et à la preuve.

20. Critères d'acceptation et conclusion

Un passeport numérique transfrontalier est acceptable si son identité est persistante ; si l'autorité de chaque émetteur peut être déterminée ; si données et preuves restent distinguées ; si les informations exposées sont minimisées ; si les changements de statut sont traçables ; si les preuves peuvent être vérifiées entre systèmes ; si la confidentialité est préservée ; si la reconnaissance étrangère respecte la souveraineté des États ; si les modes dégradés sont gouvernés ; et si aucune dépendance technique unique ne compromet la continuité du passeport. Le passeport numérique devient ainsi une continuité de preuve accompagnant l'objet au-delà des organisations, des systèmes et, lorsque les accords applicables le permettent, des frontières. Le Chapitre 15 développera la continuité internationale de confiance et les mécanismes d'extension multinationale.

Note d'alignement international

Le passeport numérique et les preuves transfrontalières sont conçus pour pouvoir s'articuler avec des cadres internationaux d'interopérabilité. ISO 22373:2025 établit un cadre relatif à l'authenticité, à l'intégrité et à la confiance pour les produits et documents au sein des chaînes de valeur, tandis que le W3C Verifiable Credentials Data Model v2.0 fournit un modèle pour exprimer des justificatifs numériques de manière vérifiable par machine, avec des mécanismes de sécurité et de respect de la vie privée. Ces références constituent des orientations d'interopérabilité ; elles ne valent ni conformité automatique, ni reconnaissance réglementaire du programme Deep Authenticity©.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VII — GOUVERNANCE, SOUVERAINETÉ ET DÉPLOIEMENT INTERNATIONAL

CHAPITRE 15 — CONTINUITÉ INTERNATIONALE DE CONFIANCE

ÉTATS — JURIDICTIONS — AUTORITÉS — IDENTITÉS — PREUVES — RECONNAISSANCE — INTEROPÉRABILITÉ — SOUVERAINETÉ — RÉSILIENCE — COOPÉRATION

1. Objet du chapitre

Ce chapitre définit la continuité internationale de confiance comme la capacité de préserver la vérifiabilité d'une identité, d'un produit, d'un document, d'une certification, d'un droit ou d'un événement lorsqu'il traverse plusieurs organisations, systèmes ou juridictions. L'objectif n'est pas d' uniformiser les souverainetés, mais de rendre les preuves compréhensibles, vérifiables et gouvernables au-delà de leur environnement d'origine.

2. Principe de continuité

Une chaîne de confiance internationale ne doit pas être interrompue simplement parce qu'un actif change de territoire, d'opérateur ou de système informatique. Chaque transition doit conserver suffisamment d'éléments pour établir l'origine de la preuve, son intégrité, son statut et l'autorité qui l'a émise. La continuité porte sur la preuve ; elle n'implique pas une continuité automatique des effets juridiques.

3. Fédération plutôt que centralisation

Deep Authenticity© privilégie une architecture fédérée dans laquelle les États, institutions et opérateurs conservent leurs propres systèmes et responsabilités. L'infrastructure internationale fournit des mécanismes communs de vérification, de résolution d'identités, d'échange de preuves et d'interopérabilité. Aucune base mondiale unique contenant l'ensemble des données souverainesn'est nécessaire à ce modèle.

4. Domaines de confiance

La continuité internationale peut concerner les trois domaines fondamentaux de Deep Authenticity© : physique, numérique et administratif. Dans le domaine physique, elle accompagne produits et chaînes de valeur. Dans le domaine numérique, elle concerne provenance, intégrité, signature et statut des contenus ou actifs numériques. Dans le domaine administratif, elle peut soutenir la vérification de documents, certificats, autorisations ou autres actes lorsque les cadres juridiques concernés le permettent.

5. Identité des autorités

Une preuve internationale n’est interprétable que si son émetteur peut être identifié. Le système doit permettre de déterminer quelle autorité, institution, entreprise ou entité a produit la preuve, dans quelle capacité, sous quel mandat et pour quelle période. La vérification technique d’une signature ne suffit pas à établir la compétence juridique de son émetteur.

6. Niveaux de confiance

Toutes les preuves ne possèdent pas le même niveau d’assurance. Deep Authenticity© peut distinguer différents niveaux selon la méthode d’identification, la qualité de l’émetteur, la certification, les contrôles effectués, la fraîcheur des informations et la solidité cryptographique. Le niveau de confiance doit rester explicite afin d’éviter qu’une preuve faible soit interprétée comme une garantie absolue.

7. Reconnaissance entre juridictions

Deux ou plusieurs juridictions peuvent définir les conditions dans lesquelles certaines preuves sont reconnues. Cette reconnaissance peut concerner des catégories déterminées de certificats, contrôles, identités, produits ou opérateurs. Elle doit préciser sa portée, ses exclusions, ses autorités compétentes, sa durée et ses conditions de suspension ou de révision. Deep Authenticity© facilite l’ exécution technique de cette reconnaissance sans se substituer à l’accord qui la fonde.

8. Continuité du passeport numérique

Le passeport numérique défini au Chapitre 14 devient l’un des supports principaux de la continuité internationale. Il permet de relier les preuves successives sans imposer leur stockage dans un système unique. Un produit peut ainsi conserver une continuité d’identité et d’historique tout en traversant plusieurs opérateurs et territoires.

9. Authenticity Plus© et les flux physiques

Pour les produits physiques, la continuité internationale demeure reliée au mécanisme fondamental d’ Authenticity Plus© fondé sur les trois QR codes fonctionnellement distincts : consommateur, revendeur/professionnel et contrôle/douanes. Les acteurs interrogent la même identité de produit selon des droits et finalités différents. Les statuts VERT, JAUNE et ROUGE conservent leur signification fondamentale dans l’écosystème Authenticity Plus©, tandis que les autorités compétentes conservent leurs propres pouvoirs de décision.

10. Corridors de Confiance©

Les Corridors de Confiance© constituent une modalité concrète de mise en œuvre de la continuité internationale. Ils permettent de commencer par des relations limitées entre partenaires, secteurs ou routes logistiques avant une extension plus large. Chaque corridor devient ainsi un environnement contrôlé permettant de tester interopérabilité, reconnaissance, sécurité, gouvernance et performance.

11. Réseau de confiance

Plusieurs corridors compatibles peuvent progressivement former un réseau de confiance. Cette évolution ne signifie pas qu'un partenaire reconnu par un État devient automatiquement reconnu par tous les autres. Les relations doivent rester explicitement gouvernées afin d'éviter une propagation incontrôlée de la confiance. Le réseau se construit donc par fédération de relations démontrables plutôt que par confiance universelle implicite.

12. Interopérabilité sémantique

L'échange technique d'une preuve ne garantit pas que tous les partenaires lui donnent la même signification. La continuité internationale exige donc également une interopérabilité sémantique : définitions, statuts, catégories, unités, vocabulaires et règles d'interprétation doivent être suffisamment compatibles ou convertibles. Une preuve correctement transmise mais incorrectement interprétée constitue une rupture de confiance.

13. Gouvernance des anomalies

Une preuve contestée, un certificat révoqué, une signature invalide, une incohérence de traçabilité ou une autorité non reconnue doit déclencher une procédure gouvernée. Selon le contexte, celle-ci peut conduire à une vérification complémentaire, une suspension, une demande d'information ou une décision relevant de l'autorité compétente. Une anomalie reste un signal nécessitant qualification et ne constitue pas automatiquement une preuve de fraude.

14. Révocation transfrontalière

La confiance internationale exige que les partenaires puissent connaître les changements critiques de statut. Lorsqu'une certification, une autorité, un identifiant ou une habilitation est révoqué, les systèmes concernés doivent pouvoir obtenir cette information dans des délais compatibles avec le niveau de risque. La révocation doit être authentifiée, datée et reliée à l'autorité compétente.

15. Souveraineté et localisation

Chaque partenaire conserve le droit de définir les conditions de stockage, de traitement, d'accès et de transfert applicables aux données relevant de sa juridiction. Deep Authenticity© doit permettre des architectures dans lesquelles les preuves circulent sans imposer la circulation intégrale des données sources. Cette séparation entre vérification et centralisation constitue une condition essentielle de souveraineté.

16. Résilience internationale

La continuité de confiance doit survivre aux interruptions techniques, cyberincidents, défaillances de partenaires ou ruptures de connectivité. Redondance, mécanismes de secours, preuves signées, synchronisation différée, procédures de récupération et voies alternatives peuvent soutenir la continuité. Les modes dégradés doivent rester limités, documentés et réconciliés après rétablissement.

17. Suspension et découplage

Un État, une autorité, un opérateur ou une relation de reconnaissance doit pouvoir être suspendu sans provoquer l'effondrement de l'ensemble du réseau. L'architecture doit permettre un découplage contrôlé : les nouvelles transactions peuvent être limitées tandis que les preuves historiques nécessaires à l'audit restent vérifiables. La fédération doit donc éviter les dépendances irréversibles.

18. Extension progressive

La continuité internationale ne doit pas être déployée simultanément à l'échelle mondiale. Elle peut progresser par secteurs, partenaires, familles de produits, catégories documentaires ou corridors. Chaque étape fournit des données permettant d'évaluer sécurité, performance, acceptabilité, interopérabilité et gouvernance avant extension.

19. Deep Authenticity© et AP Ledger

Deep Authenticity© relie les identités, autorités, accords, preuves, passeports numériques, produits et événements constituant le réseau international de confiance. AP Ledger peut ancrer les éléments probants nécessaires à la continuité : émission, reconnaissance, validation, modification, révocation, suspension et autres événements critiques. L'objectif n'est pas de créer un registre mondial contenant toutes les informations, mais de préserver une chronologie vérifiable des événements qui nécessitent une preuve durable.

20. Critères d'acceptation et conclusion

Une architecture de continuité internationale de confiance est acceptable si les autorités participantes sont identifiables ; si les niveaux de confiance sont explicites ; si la reconnaissance entre juridictions reste gouvernée ; si la vérification n'implique pas une centralisation systématique des données ; si les passeports numériques restent interopérables ; si les anomalies et révocations peuvent circuler de manière fiable ; si chaque partenaire conserve ses compétences souveraines ; si la résilience et la sortie sont prévues ; et si l'extension du réseau repose sur une confiance démontrée plutôt que présumée. La continuité internationale transforme ainsi Deep Authenticity© en une infrastructure capable de préserver la vérifiabilité au-delà des frontières tout en maintenant la séparation entre preuve technique, reconnaissance institutionnelle et décision souveraine. Le Chapitre 16 développera les mécanismes de déploiement international progressif de Deep Authenticity©, depuis les pilotes nationaux et sectoriels jusqu'aux architectures multinationales interopérables.

Note d'alignement international

L'architecture de continuité internationale de confiance est conçue pour pouvoir s'articuler avec les standards et mécanismes internationaux applicables à l'identité, à la signature électronique, à l' évaluation de conformité, aux chaînes de valeur, aux échanges de données et à la reconnaissance entre juridictions. Cet alignement vise l'interopérabilité et la compatibilité progressive. Il ne doit pas être interprété comme une reconnaissance réglementaire ou normative automatique de Deep Authenticity© ou d'Authenticity Plus© par une organisation internationale.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VII — GOUVERNANCE, SOUVERAINETÉ ET DÉPLOIEMENT INTERNATIONAL

CHAPITRE 16 — DÉPLOIEMENT INTERNATIONAL PROGRESSIF DE DEEP AUTHENTICITY©

PILOTES — SECTEURS — ÉTATS — CORRIDORS — INTEROPÉRABILITÉ — SOUVERAINETÉ — ÉVALUATION — EXTENSION — RÉSILIENCE — GOUVERNANCE

1. Objet du chapitre

Ce chapitre définit une méthode de déploiement international progressif de Deep Authenticity©. L'objectif n'est pas d'imposer simultanément une infrastructure mondiale, mais de construire la confiance par étapes mesurables : expérimentation, validation, extension sectorielle, interconnexion nationale, coopération bilatérale ou multilatérale, puis fédération progressive des environnements compatibles.

2. Principe de progressivité

Le déploiement suit une logique d'élargissement contrôlé. Chaque étape doit démontrer sa valeur, sa sécurité, son interopérabilité et sa gouvernabilité avant de servir de base à l'étape suivante. Une extension géographique rapide ne constitue pas un objectif en elle-même : la qualité de la confiance établie prime sur le nombre de territoires connectés.

3. Phase préparatoire

Avant tout pilote, l'environnement concerné doit être cartographié : autorités compétentes, systèmes existants, catégories de produits ou documents, opérateurs, exigences réglementaires, flux de données, infrastructures de confiance et risques. Cette cartographie évite qu'un déploiement technique précède la définition des responsabilités institutionnelles.

4. Pilote sectoriel

Le premier niveau opérationnel peut concerner un secteur, une catégorie de produits, une chaîne de valeur ou un processus administratif clairement délimité. Le pilote dispose d'objectifs mesurables, d'un périmètre explicite, d'une durée, de responsables identifiés et de critères permettant de déterminer s'il peut être étendu, corrigé ou interrompu.

5. Sélection des cas d'usage

Les premiers cas d'usage privilégient les situations dans lesquelles la vérification apporte une valeur identifiable : lutte contre la contrefaçon, traçabilité critique, certification, contrôle réglementaire, transfert de propriété, rappel de produits ou vérification documentaire. La priorité tient également compte de la capacité à produire des résultats évaluables.

6. Déploiement d’Authenticity Plus©

Pour les produits physiques, Authenticity Plus© constitue le mécanisme fondamental d’ authentification et de lutte contre la contrefaçon. Le déploiement conserve les trois QR codes fonctionnellement distincts : consommateur, revendeur/professionnel et contrôle/douanes. Les statuts restent VERT — original ; JAUNE — original mais déjà vérifié ou vendu ; ROUGE — contrefaçon ou code inexistant dans le système Authenticity Plus©. Les couches de Deep Authenticity© enrichissent cette architecture sans la remplacer.

7. Évaluation du pilote

Chaque pilote produit une évaluation documentée. Les indicateurs peuvent inclure taux d’ authentification, anomalies détectées, temps de vérification, disponibilité, incidents, qualité des données, adoption, intégration aux systèmes existants et coûts opérationnels. Les résultats négatifs ou incomplets sont conservés au même titre que les succès afin d’éviter une extension fondée sur uneévaluation biaisée.

8. Extension sectorielle

Après validation, le périmètre peut être étendu à d’autres opérateurs, territoires ou catégories du même secteur. Cette extension vérifie que les mécanismes restent efficaces lorsque le nombre d’ acteurs, le volume de transactions et la diversité des situations augmentent. Les critères d’ acceptation sont réévalués à chaque changement significatif d’échelle.

9. Interconnexion nationale

Plusieurs déploiements sectoriels peuvent progressivement être reliés dans une architecture nationale. Deep Authenticity© devient alors une couche d’interopérabilité de confiance entre systèmes existants plutôt qu’une application isolée. Les autorités nationales conservent leurs responsabilités, leurs registres et leurs compétences réglementaires.

10. Gouvernance nationale

Le passage à l’échelle nationale exige une gouvernance explicite : responsabilités institutionnelles, gestion des identités, cybersécurité, règles d’accès, audit, continuité, protection des données, certification et procédures de contestation. La gouvernance doit précéder l’interconnexion généralisée des secteurs.

11. Passage aux Corridors de Confiance©

Lorsque deux partenaires disposent d’environnements suffisamment matures, un Corridor de Confiance© peut être établi sur un périmètre limité. Produits, opérateurs, preuves, certifications et procédures reconnues sont définis dans un accord de coopération. Le corridor constitue une étape intermédiaire entre infrastructure nationale et réseau international.

12. Passeports numériques transfrontaliers

Les passeports numériques définis au Chapitre 14 accompagnent l'extension internationale. Ils permettent aux produits ou actifs concernés de conserver une continuité d'identité et de preuve au-delà de leur système d'origine. Les partenaires déterminent les attributs vérifiables, les autorités reconnues et les informations nécessaires aux contrôles.

13. Fédération des corridors

Plusieurs Corridors de Confiance© peuvent progressivement devenir interopérables lorsque leurs exigences, identités et mécanismes de preuve sont suffisamment compatibles. Cette fédération ne crée pas automatiquement une reconnaissance universelle. Chaque relation reste gouvernée par les accords et compétences applicables.

14. Modèle multiniveau

Le déploiement international peut être organisé selon plusieurs niveaux : local → sectoriel → national → bilatéral → régional → multilatéral → international. Chaque niveau conserve son périmètre de décision. L'infrastructure supérieure ne doit pas supprimer les compétences légitimes des niveaux inférieurs.

15. Interopérabilité technologique

L'expansion internationale nécessite des interfaces suffisamment ouvertes pour éviter une dépendance irréversible à une technologie unique. API documentées, formats structurés, signatures vérifiables, identifiants interopérables, mécanismes d'export et protocoles de migration permettent aux partenaires d'intégrer Deep Authenticity© à leurs infrastructures.

16. Localisation et souveraineté des données

Le déploiement doit pouvoir s'adapter aux règles nationales relatives à l'hébergement, au traitement et au transfert des données. Certaines informations peuvent demeurer dans les infrastructures nationales tandis que des preuves ou attributs minimaux sont échangés. L'internationalisation ne doit pas être assimilée à une centralisation mondiale des données.

17. Sécurité et résilience à l'échelle

L'augmentation du nombre de partenaires accroît simultanément la surface d'attaque et les risques de dépendance. Chaque phase d'extension intègre tests de sécurité, gestion des clés, surveillance, segmentation, continuité d'activité, reprise après incident et procédures de suspension. Un incident local doit pouvoir être isolé sans compromettre automatiquement l'ensemble du réseau.

18. Gouvernance de l'évolution

Deep Authenticity© doit pouvoir évoluer sans rompre les preuves historiques ou l'interopérabilité existante. Les standards, protocoles, politiques et référentiels sont versionnés. Les modifications importantes suivent des procédures documentées permettant aux partenaires de tester, accepter, différer ou contester une évolution selon les règles établies.

19. Deep Authenticity© et AP Ledger

Deep Authenticity© organise la progression du réseau entre pilotes, secteurs, États, corridors et environnements internationaux. AP Ledger peut ancrer les événements critiques liés au déploiement : versions, validations, certifications, reconnaissances, modifications de périmètre, suspensions et transitions entre phases. Cette chronologie permet de démontrer l'état du réseau et la manière dont celui-ci a évolué.

20. Critères d'acceptation et conclusion

Un déploiement international de Deep Authenticity© est acceptable s'il progresse par étapes évaluables ; si chaque phase possède des responsabilités explicites ; si les résultats des pilotes sont mesurés ; si l'architecture physique d'Authenticity Plus© reste préservée ; si les systèmes nationaux restent souverains ; si l'interopérabilité évite les dépendances irréversibles ; si la fédération des corridors repose sur des relations gouvernées ; si sécurité et résilience augmentent avec l'échelle ; et si une extension peut être suspendue ou corrigée sans compromettre les preuves historiques.

Deep Authenticity© doit devenir internationale par accumulation progressive de confiance démontrée : PILOTE → VALIDATION → SECTEUR → ÉTAT → CORRIDOR → FÉDÉRATION → RÉSEAU INTERNATIONAL.

Le Chapitre 17 développera la gouvernance du réseau international de Deep Authenticity©, notamment la répartition des responsabilités, les mécanismes de représentation, la gestion des évolutions et la prévention de toute concentration excessive du pouvoir.

Note d'alignement international

Le déploiement progressif de Deep Authenticity© est conçu pour permettre une articulation avec les cadres internationaux existants de coopération, d'interopérabilité, d'identité, de commerce, d'évaluation de conformité, de cybersécurité, de protection des données et de facilitation des échanges. L'intégration à de tels cadres devra être établie au cas par cas par les autorités et organisations compétentes. La compatibilité technique ou conceptuelle ne constitue pas, en elle-même, une reconnaissance institutionnelle ou normative.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VII — GOUVERNANCE, SOUVERAINETÉ ET DÉPLOIEMENT INTERNATIONAL

CHAPITRE 17 — GOUVERNANCE DU RÉSEAU INTERNATIONAL DEEP AUTHENTICITY©

SOUVERAINETÉ — REPRÉSENTATION — RESPONSABILITÉS — FÉDÉRATION — RÈGLES — AUDIT — ÉVOLUTION — CONTESTATION — RÉSILIENCE — NEUTRALITÉ

1. Objet du chapitre

Ce chapitre définit les principes de gouvernance applicables à un réseau international Deep Authenticity© composé d'États, d'autorités, d'institutions, d'opérateurs et d'infrastructures interopérables. L'objectif est de permettre la coopération sans créer une autorité technique unique capable de se substituer aux compétences souveraines, réglementaires ou juridictionnelles des participants.

2. Principe de gouvernance fédérée

Le réseau repose sur une gouvernance fédérée. Chaque participant conserve ses compétences, ses systèmes, ses responsabilités et son droit de déterminer les conditions dans lesquelles il reconnaît ou utilise les preuves provenant d'autres environnements. Le niveau international organise l' interopérabilité et les règles communes nécessaires au fonctionnement du réseau ; il ne constitue pas un gouvernement supranational.

3. Séparation des responsabilités

La gouvernance distingue définition des règles, exploitation technique, certification, contrôle, audit, résolution des incidents et décision réglementaire. Ces fonctions ne doivent pas être concentrées sans mécanismes de contrôle appropriés. Une infrastructure de vérité crédible doit pouvoir démontrer qui définit une règle, qui l'exécute, qui la contrôle et qui peut la contester.

4. Représentation des participants

Les mécanismes de représentation tiennent compte de la diversité du réseau : États, autorités compétentes, secteurs économiques, organismes techniques et autres catégories de participants légitimes. La représentation ne doit pas être confondue avec l'accès aux données : participer à la gouvernance d'un référentiel ne confère pas automatiquement un droit d'accès aux informations opérationnelles des autres membres.

5. Souveraineté des États

Chaque État conserve son pouvoir de déterminer la valeur juridique des preuves, certifications, identités, documents ou statuts utilisés sur son territoire. Deep Authenticity© peut fournir les moyens

techniques permettant de vérifier l'origine et l'intégrité d'une preuve. La décision de reconnaître ses effets appartient à l'autorité compétente.

6. Gouvernance d'Authenticity Plus©

Dans le domaine physique, la gouvernance internationale préserve le mécanisme fondamental d' Authenticity Plus© fondé sur trois QR codes fonctionnellement distincts : consommateur, revendeur/professionnel et contrôle/douanes. Les règles internationales d'interopérabilité ne doivent pas supprimer cette séparation fonctionnelle. Les significations restent VERT — original ; JAUNE — original mais déjà vérifié ou vendu ; ROUGE — contrefaçon ou code inexistant dans le système Authenticity Plus©.

7. Référentiels communs

Le réseau peut établir des référentiels communs concernant identifiants, formats de preuve, statuts, signatures, niveaux de confiance, procédures d'interopérabilité ou autres éléments nécessaires. Chaque référentiel dispose d'une version identifiable, d'une autorité de maintenance, d'un historique et de procédures d'évolution. Une règle non versionnée compromet la compréhension des preuves historiques.

8. Processus de décision

Les décisions relatives au fonctionnement commun du réseau suivent des procédures documentées. Selon leur nature, elles peuvent nécessiter consultation, expertise technique, analyse juridique, évaluation de sécurité, période d'observation ou vote selon les règles établies. Les décisions critiques ne doivent pas pouvoir être modifiées discrétionnairement par un acteur technique isolé.

9. Gestion des droits

Les droits sont attribués selon les rôles, mandats et besoins légitimes. Un opérateur technique ne reçoit pas automatiquement des compétences réglementaires ; une autorité nationale ne reçoit pas automatiquement accès aux données souveraines d'un autre État ; un organisme de certification ne peut agir au-delà de la portée reconnue de son mandat.

10. Transparence institutionnelle

Les éléments essentiels de gouvernance doivent pouvoir être identifiés : responsabilités, règles applicables, versions, procédures de décision, mécanismes d'audit et voies de contestation. La transparence ne signifie pas publication de secrets techniques, données personnelles ou informations de sécurité sensibles ; elle signifie que la structure du pouvoir et des responsabilités doit pouvoir être comprise et contrôlée.

11. Audit indépendant

Les composants critiques, processus de gouvernance et mécanismes de sécurité doivent pouvoir faire l'objet d'audits indépendants adaptés à leur niveau de risque. Les audits peuvent porter sur conformité aux référentiels, cybersécurité, gestion des accès, continuité, intégrité des preuves ou

application des procédures. Les résultats sensibles peuvent être communiqués selon des niveaux de confidentialité appropriés.

12. Gestion des conflits

Des désaccords peuvent apparaître concernant une preuve, une certification, une autorité, une règle ou une décision du réseau. Des mécanismes de contestation doivent permettre d'identifier le niveau compétent pour traiter le différend. Deep Authenticity© fournit les éléments probants nécessaires à l'analyse mais ne remplace pas les mécanismes juridiques ou institutionnels compétents.

13. Suspension

Une autorité, un opérateur, une certification, une clé, un corridor ou une relation de confiance peut devoir être suspendu. La procédure précise l'autorité habilitée, les motifs, la portée, la durée, les conséquences et les conditions éventuelles de rétablissement. La suspension doit pouvoir être appliquée sans détruire les preuves historiques nécessaires à l'audit.

14. Gestion de crise

Un incident majeur peut exiger une coordination internationale : compromission cryptographique, cyberattaque, fraude systémique, corruption d'un référentiel ou indisponibilité d'une infrastructure critique. Le réseau doit pouvoir partager rapidement les informations nécessaires, isoler les composants concernés et maintenir les fonctions essentielles sans supprimer les limites de compétence au-delà de ce qui est strictement nécessaire.

15. Gouvernance de l'évolution technologique

Les technologies cryptographiques, standards, protocoles et architectures évoluent. La gouvernance permet leur remplacement ou leur migration sans invalider arbitrairement les preuves historiques. Des périodes de coexistence, mécanismes de conversion, calendriers de migration et procédures de dépréciation peuvent être nécessaires.

16. Prévention de la concentration

Une infrastructure internationale de vérité ne doit pas dépendre d'un acteur unique pour l'identité, l'hébergement, la certification, l'audit, la décision et la conservation des preuves. La séparation des responsabilités, la fédération, l'interopérabilité et les possibilités de sortie constituent des protections structurelles contre une concentration excessive, qu'elle soit publique ou privée.

17. Neutralité et non-discrimination

Les règles techniques communes doivent être appliquées selon des critères explicites et vérifiables. L'accès au réseau, la certification ou l'interopérabilité ne doivent pas dépendre de décisions arbitraires dissimulées dans les mécanismes techniques. Les différences de traitement justifiées par le risque, la réglementation ou les accords applicables doivent pouvoir être expliquées.

18. Sortie et réversibilité

Tout participant doit disposer de mécanismes permettant une sortie gouvernée du réseau ou d'un service déterminé. La sortie préserve la capacité de vérifier les preuves historiques nécessaires et permet, lorsque cela est applicable, la récupération ou migration des informations. Aucun participant ne doit être maintenu uniquement parce qu'une dépendance technique rendrait son départ impossible.

19. Deep Authenticity© et AP Ledger

Deep Authenticity© fournit le cadre de gouvernance reliant participants, mandats, règles, référentiels, décisions, certifications et relations de confiance. AP Ledger peut ancrer les versions, décisions, habilitations, suspensions, révocations et événements critiques nécessaires à l'auditabilité. Il fournit une chronologie probante sans transformer automatiquement chaque décision en vérité juridique.

20. Critères d'acceptation et conclusion

La gouvernance internationale de Deep Authenticity© est acceptable si les compétences souveraines restent explicites ; si les responsabilités sont séparées ; si les règles et référentiels sont versionnés ; si les décisions critiques sont gouvernées ; si les accès sont proportionnés aux mandats ; si les audits sont possibles ; si les contestations, suspensions et crises disposent de procédures ; si l'évolution technologique préserve les preuves historiques ; si la concentration excessive est structurellement limitée ; et si les participants disposent de mécanismes de sortie et de réversibilité.

L'objectif n'est pas de créer une autorité mondiale de la vérité. Il est de construire une infrastructure dans laquelle la confiance internationale peut être établie, vérifiée, contestée, auditée et révoquée selon des règles connues, tout en maintenant la pluralité des souverainetés.

UNE INFRASTRUCTURE COMMUNE DE VÉRIFICATION N'IMPLIQUE PAS UNE AUTORITÉ POLITIQUE COMMUNE.

Le Chapitre 18 développera la diplomatie de la confiance et la coopération avec les organisations internationales.

Note d'alignement international

La gouvernance proposée est conçue pour pouvoir s'articuler avec les principes internationaux applicables à la coopération institutionnelle, à la reconnaissance mutuelle, à la cybersécurité, à la protection des données, à l'identité numérique, à l'évaluation de conformité et à l'interopérabilité. Toute participation, reconnaissance ou intégration institutionnelle demeure soumise aux décisions, procédures et compétences propres des États et organisations concernés.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VII — GOUVERNANCE, SOUVERAINETÉ ET DÉPLOIEMENT INTERNATIONAL

CHAPITRE 18 — DIPLOMATIE DE LA CONFIANCE ET COOPÉRATION AVEC LES ORGANISATIONS INTERNATIONALES

ÉTATS — DIPLOMATIE — ORGANISATIONS INTERNATIONALES — COOPÉRATION — CONFIANCE — SOUVERAINETÉ — PILOTES — RECONNAISSANCE — INTEROPÉRABILITÉ — NEUTRALITÉ

1. Objet du chapitre

Ce chapitre définit la diplomatie de la confiance comme l'ensemble des mécanismes permettant aux États, organisations internationales, institutions régionales et acteurs habilités de coopérer autour de preuves vérifiables sans transférer automatiquement leurs compétences souveraines. Deep Authenticity© peut fournir une infrastructure technique et institutionnelle de confiance au service de cette coopération.

2. Principe de diplomatie de la confiance

La coopération internationale repose traditionnellement sur des accords, documents, certifications, déclarations et mécanismes de reconnaissance. Deep Authenticity© vise à compléter ces instruments par une capacité de vérification de l'origine, de l'intégrité, du statut et de l'historique des preuves échangées. La confiance diplomatique demeure politique et juridique ; l'infrastructure en renforce la dimension vérifiable.

3. Souveraineté et coopération

La participation à un mécanisme Deep Authenticity© ne doit pas être interprétée comme un transfert général de souveraineté. Chaque État conserve ses compétences réglementaires, administratives, douanières et juridictionnelles. La coopération porte sur des périmètres explicitement convenus et peut être limitée par secteur, type de preuve, territoire, durée ou catégorie d'acteurs.

4. Dialogue bilatéral

Le déploiement international peut commencer par des dialogues bilatéraux entre États ou autorités compétentes. Ceux-ci permettent d'identifier les preuves prioritaires, les exigences juridiques, les autorités habilitées, les systèmes existants et les conditions d'un pilote. L'objectif est de construire une confiance démontrable avant toute extension multilatérale.

5. Coopération régionale

Les organisations et ensembles régionaux peuvent constituer un niveau intermédiaire entre coopération bilatérale et architecture mondiale. Des référentiels compatibles, procédures communes

ou mécanismes de reconnaissance peuvent être expérimentés dans un espace régional tout en préservant les compétences de ses membres.

6. Organisations internationales

Les organisations internationales peuvent contribuer à la convergence des principes, à la définition de standards, à la coopération technique, au renforcement des capacités ou à l'évaluation de certains mécanismes. Deep Authenticity© doit pouvoir dialoguer avec ces cadres sans revendiquer une reconnaissance institutionnelle qui n'aurait pas été formellement accordée.

7. Neutralité de l'infrastructure

Pour devenir un support crédible de coopération internationale, Deep Authenticity© doit être utilisable sans imposer l'alignement politique sur un État, une entreprise ou un bloc particulier. La neutralité recherchée est fonctionnelle : règles explicites, interopérabilité, séparation des responsabilités, auditabilité et absence de discrimination technique arbitraire.

8. Authenticity Plus© dans les échanges internationaux

Dans le domaine physique, Authenticity Plus© conserve son architecture fondamentale des trois QR codes fonctionnellement distincts : consommateur, revendeur/professionnel et contrôle/douanes. Les statuts restent VERT — original ; JAUNE — original mais déjà vérifié ou vendu ; ROUGE — contrefaçon ou code inexistant dans le système Authenticity Plus©. Les coopérations internationales peuvent reconnaître des modalités de vérification sans supprimer les pouvoirs des autorités nationales.

9. Pilotes diplomatiques et institutionnels

Un pilote international peut être établi entre un nombre limité de partenaires afin de tester identité des autorités, échanges de preuves, certification, contrôles, protection des données et procédures d' incident. Son périmètre, ses objectifs, sa durée et ses critères d'évaluation doivent être formalisés avant le lancement.

10. Corridors de Confiance©

Les Corridors de Confiance© constituent un instrument opérationnel de diplomatie économique et institutionnelle. Ils permettent à des partenaires de convenir d'un ensemble limité de preuves, opérateurs, certifications et procédures reconnues. Leur réussite peut servir de fondement à une coopération plus large sans créer de reconnaissance universelle automatique.

11. Reconnaissance progressive

La reconnaissance internationale doit être graduelle. Une preuve peut être techniquement vérifiable sans être juridiquement reconnue ; une certification peut être reconnue pour un secteur mais pas pour un autre ; un accord peut être bilatéral sans produire d'effet pour des tiers. Deep Authenticity© conserve ces distinctions afin d'éviter une propagation implicite de la confiance.

12. Diplomatie économique

La confiance vérifiable peut contribuer à réduire certaines frictions liées aux échanges : duplications documentaires, incertitude sur l'origine, difficulté de vérifier une certification ou rupture de traçabilité. La plateforme peut ainsi soutenir la diplomatie économique, la facilitation des échanges et la protection des chaînes de valeur, sous réserve des règles applicables.

13. Diplomatie numérique

La coopération numérique exige des mécanismes permettant d'établir provenance, intégrité et autorité sans centraliser toutes les données. Deep Authenticity© peut soutenir des échanges de preuves entre infrastructures souveraines, y compris pour des documents et contenus numériques, lorsque les partenaires définissent les règles de reconnaissance et d'accès.

14. Renforcement des capacités

Tous les partenaires ne disposent pas du même niveau d'infrastructure, de cybersécurité ou d' expertise. Les programmes de coopération peuvent inclure formation, assistance technique, outils de conformité, référentiels communs et accompagnement à l'interopérabilité. Le renforcement des capacités évite que la confiance numérique internationale accentue les écarts technologiques.

15. Protection des données et confidentialité

La diplomatie de la confiance ne doit pas conduire à l'échange systématique des données sources. Les partenaires déterminent quelles preuves sont nécessaires, qui peut les consulter et pendant combien de temps. La minimisation, la divulgation sélective et la conservation locale des informations sensibles constituent des principes structurants.

16. Gouvernance des différends

Un désaccord peut porter sur l'authenticité d'une preuve, sa reconnaissance, l'autorité de l'émetteur, une suspension ou l'interprétation d'un accord. Les mécanismes diplomatiques, administratifs ou juridiques compétents conservent leur rôle. Deep Authenticity© fournit les éléments probants et la chronologie nécessaires à l'analyse sans se substituer aux procédures de règlement.

17. Résilience géopolitique

Une infrastructure internationale doit pouvoir continuer à fonctionner malgré tensions diplomatiques, sanctions applicables, ruptures de coopération, cyberincidents ou retrait d'un partenaire. La segmentation, la réversibilité, la conservation des preuves historiques et la possibilité de suspendre certaines relations limitent la propagation des crises.

18. Extension multilatérale

Après validation de plusieurs coopérations bilatérales ou régionales, des mécanismes multilatéraux peuvent être envisagés. Leur extension doit rester conditionnée à des règles de gouvernance

explicites, des standards suffisamment interopérables et des procédures de reconnaissance définies. L'échelle ne doit jamais remplacer la démonstration de confiance.

19. Deep Authenticity© et AP Ledger

Deep Authenticity© relie accords, autorités, organisations, corridors, passeports numériques, preuves et décisions de coopération. AP Ledger peut ancrer les versions, reconnaissances, habilitations, suspensions et événements critiques nécessaires à une chronologie vérifiable. Cette fonction probante ne transforme pas un accord technique en traité ou en obligation juridique internationale.

20. Critères d'acceptation et conclusion

Une diplomatie de la confiance fondée sur Deep Authenticity© est acceptable si la souveraineté des participants reste explicite ; si la coopération repose sur des périmètres convenus ; si les organisations internationales interviennent selon leurs mandats ; si la neutralité fonctionnelle est protégée ; si la reconnaissance demeure progressive et non automatique ; si les données sont minimisées ; si les différends disposent de voies de traitement ; si la résilience géopolitique est prévue ; et si l'extension multilatérale repose sur des résultats démontrés.

Deep Authenticity© peut ainsi devenir un langage commun de vérification entre systèmes souverains sans devenir une autorité diplomatique supérieure aux États.

La diplomatie de la confiance repose sur un principe central : COOPÉRER SUR LA PREUVE SANS ABANDONNER LA SOUVERAINETÉ.

Le Chapitre 19 développera les mécanismes de partenariats stratégiques, de financement et de soutenabilité du déploiement international de Deep Authenticity©.

Note d'alignement international

La diplomatie de la confiance proposée est conçue pour pouvoir s'articuler avec les cadres internationaux de coopération, de facilitation des échanges, d'évaluation de conformité, d'identité numérique, de cybersécurité, de protection des données et de reconnaissance mutuelle. Toute référence à ces cadres constitue une orientation d'interopérabilité et de coopération ; elle ne vaut ni approbation, ni certification, ni reconnaissance institutionnelle automatique de Deep Authenticity© ou d'Authenticity Plus©.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VII — GOUVERNANCE, SOUVERAINETÉ ET DÉPLOIEMENT INTERNATIONAL

CHAPITRE 19 — PARTENARIATS STRATÉGIQUES, FINANCEMENT ET SOUTENABILITÉ

ÉTATS — PARTENARIATS — FINANCEMENT — SOUVERAINETÉ — INVESTISSEMENT — MODÈLE ÉCONOMIQUE — INDÉPENDANCE — INFRASTRUCTURES — RISQUES — SOUTENABILITÉ

1. Objet du chapitre

Ce chapitre définit les principes permettant de financer, déployer et maintenir Deep Authenticity© à l'échelle nationale et internationale sans compromettre sa mission de confiance, sa neutralité fonctionnelle ni la souveraineté des participants. La soutenabilité doit couvrir simultanément les dimensions économique, institutionnelle, technique et opérationnelle.

2. Principe de soutenabilité

Une infrastructure de confiance ne peut dépendre durablement d'un financement exceptionnel ou d'un acteur unique. Son modèle doit couvrir conception, exploitation, cybersécurité, maintenance, certification, audit, évolution technologique, assistance et continuité. Les revenus et financements doivent rester compatibles avec les obligations de service et de gouvernance.

3. Partenariats avec les États

Les États peuvent intervenir comme utilisateurs institutionnels, partenaires de déploiement, autorités compétentes ou financeurs d'infrastructures relevant de leur souveraineté. Les accords précisent les responsabilités, niveaux de service, données concernées, conditions de réversibilité et limites de compétence. Le financement public ne doit pas être confondu avec un transfert de propriété sur les données souveraines.

4. Partenariats institutionnels

Administrations, organismes de normalisation, structures de certification, autorités sectorielles, universités et organismes de recherche peuvent contribuer selon leurs mandats. Les partenariats doivent distinguer expertise, validation, exploitation et décision réglementaire afin d'éviter qu'une coopération technique soit présentée comme une reconnaissance institutionnelle non accordée.

5. Partenariats industriels

Producteurs, distributeurs, logisticiens, intégrateurs et opérateurs technologiques peuvent contribuer au déploiement d'Authenticity Plus© et de Deep Authenticity©. Les accords industriels définissent interfaces, responsabilités, niveaux de sécurité, propriété intellectuelle, confidentialité, réversibilité et

obligations de continuité. Aucun partenaire ne doit devenir indispensable au fonctionnement global sans solution de remplacement.

6. Financement des pilotes

Les premières expérimentations peuvent être financées par l'entité porteuse, des partenaires publics ou privés, des programmes d'innovation ou des mécanismes de coopération. Chaque pilote dispose d'un budget identifié et d'indicateurs permettant d'évaluer coût, valeur créée, adoption, sécurité et capacité de passage à l'échelle.

7. Modèle économique

La soutenabilité peut combiner licences, abonnements de services, intégration, certification, prestations institutionnelles ou autres mécanismes compatibles avec les règles applicables. Le modèle économique doit rester lisible et éviter que la vérification essentielle d'un produit ou d'une preuve soit artificiellement rendue inaccessible par une tarification disproportionnée.

8. Royalties et licences

Les royalties ou licences peuvent contribuer au financement de l'innovation et de l'exploitation lorsqu' elles sont définies contractuellement de manière transparente. Leur assiette, leur taux, leur durée et leur périmètre doivent être explicites. Les projections économiques restent distinctes des revenus effectivement constatés et doivent présenter clairement leurs hypothèses.

9. Infrastructure souveraine

Un État ou une institution peut exiger que certaines composantes soient hébergées ou exploitées dans un environnement souverain. Le modèle financier doit permettre cette configuration sans imposer un hébergement mondial unique. Les coûts de redondance, sécurité, exploitation et mise à niveau doivent être intégrés dès la conception.

10. Financement de la cybersécurité

La cybersécurité constitue une dépense structurelle et non une option ponctuelle. Budgets de tests, audits, gestion des vulnérabilités, renouvellement cryptographique, surveillance, réponse aux incidents et reprise d'activité doivent être prévus sur toute la durée de vie de l'infrastructure.

11. AP Certified© et économie de la conformité

AP Certified© peut soutenir des services de certification ou d'évaluation lorsque les référentiels, compétences et responsabilités sont clairement établis. La certification ne doit pas devenir un mécanisme de dépendance commerciale obligatoire lorsque d'autres preuves reconnues sont acceptables. Sa valeur repose sur la qualité du référentiel et la confiance dans son processus.

12. Accessibilité économique

L'adoption internationale exige que petites entreprises, artisans, producteurs, créateurs et acteurs disposant de ressources limitées puissent accéder à des modalités proportionnées. Des offres

différenciées, architectures légères ou programmes d'accompagnement peuvent éviter que l' infrastructure de confiance ne soit réservée aux grandes organisations.

13. Financement du renforcement des capacités

Le déploiement dans des environnements moins équipés peut nécessiter formation, assistance technique, intégration et amélioration des infrastructures locales. États, institutions de développement et partenaires peuvent financer ces capacités selon des programmes définis. L' objectif est de renforcer l'autonomie locale plutôt que de créer une dépendance permanente.

14. Prévention de la capture économique

Aucun investisseur, fournisseur, partenaire ou financeur ne doit pouvoir utiliser sa contribution financière pour obtenir un contrôle disproportionné sur les règles de confiance, les données souveraines ou les décisions institutionnelles. Les droits économiques, techniques et de gouvernance doivent être séparés lorsque leur concentration créerait un risque systémique.

15. Transparence financière

Les coûts, obligations contractuelles et mécanismes de rémunération ayant un effet significatif sur la gouvernance ou l'accès au système doivent être documentés selon les règles applicables. La transparence ne requiert pas la publication de toutes les informations commerciales confidentielles, mais elle doit permettre d'identifier les conflits d'intérêts et dépendances critiques.

16. Continuité financière

Les fonctions critiques doivent pouvoir continuer à fonctionner en cas de retrait d'un financeur, de défaillance d'un prestataire ou de changement de modèle économique. Réserves, redondance contractuelle, plans de transition et mécanismes de reprise peuvent réduire ce risque. La continuité technique doit être accompagnée d'une continuité financière.

17. Mesure de la valeur créée

La performance économique ne se limite pas au chiffre d'affaires de la plateforme. Les évaluations peuvent considérer réduction de la fraude, diminution des duplications, amélioration des contrôles, accélération des vérifications, protection des recettes, meilleure traçabilité et réduction de certains coûts de litige ou de rappel. Les méthodes de calcul et leurs hypothèses doivent rester explicites.

18. Partage de valeur

Le développement international peut nécessiter un partage de valeur entre concepteur, opérateurs locaux, intégrateurs, partenaires institutionnels et autres acteurs. Les mécanismes retenus doivent préserver l'incitation à investir tout en évitant une accumulation de rentes qui réduirait l'accessibilité ou la concurrence. Le partage économique ne modifie pas automatiquement la propriété des données ou les compétences publiques.

19. Deep Authenticity© et gouvernance économique

Deep Authenticity© peut relier contrats, licences, services, niveaux de responsabilité et événements économiques pertinents. AP Ledger peut ancrer les versions contractuelles ou événements critiques lorsque cela est nécessaire à la preuve. La gouvernance économique doit rester séparée de la décision d'authenticité afin qu'un intérêt financier ne puisse déterminer arbitrairement le statut d'une preuve.

20. Critères d'acceptation et conclusion

Le modèle de partenariats et de financement est acceptable si les sources de financement sont identifiables ; si les responsabilités sont explicites ; si la cybersécurité et la maintenance disposent de ressources durables ; si les mécanismes économiques préservent l'accessibilité ; si les infrastructures souveraines restent possibles ; si les partenaires disposent de solutions de sortie ; si la capture économique est limitée ; si la valeur créée est mesurable ; et si les intérêts financiers ne peuvent altérer les règles d'authenticité.

La soutenabilité de Deep Authenticity© doit permettre à l'infrastructure de croître sans transformer la confiance en dépendance économique. Son modèle doit financer l'innovation, la sécurité et le déploiement tout en protégeant la neutralité, la souveraineté et la capacité de réversibilité.

Le principe directeur est : FINANCER L'INFRASTRUCTURE SANS PRIVATISER LA VÉRITÉ.

Le Chapitre 20 développera la feuille de route stratégique internationale, les étapes de consolidation et les conditions de passage vers une infrastructure de confiance à portée mondiale.

Note d'alignement international

Les modèles de financement et de partenariat de Deep Authenticity© sont conçus pour pouvoir s'articuler avec les cadres applicables aux marchés publics, partenariats public-privé, investissements, concurrence, propriété intellectuelle, coopération au développement et financement des infrastructures numériques. Toute structure concrète devra être adaptée au droit applicable et ne vaut pas validation préalable par une institution financière ou internationale.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VII — GOUVERNANCE, SOUVERAINETÉ ET DÉPLOIEMENT INTERNATIONAL

CHAPITRE 20 — FEUILLE DE ROUTE STRATÉGIQUE INTERNATIONALE ET PASSAGE À L'ÉCHELLE MONDIALE

VISION — PHASAGE — PILOTES — ÉTATS — CORRIDORS — FÉDÉRATION — GOUVERNANCE — INTEROPÉRABILITÉ — RÉSILIENCE — ÉCHELLE MONDIALE

1. Objet du chapitre

Ce chapitre établit la feuille de route stratégique permettant à Deep Authenticity© de progresser d' expérimentations maîtrisées vers une infrastructure internationale de confiance à grande échelle. La trajectoire proposée repose sur des étapes vérifiables, des critères de passage explicites et le maintien de la souveraineté des participants.

2. Principe de passage à l'échelle

Le passage à l'échelle ne doit pas être confondu avec une croissance rapide du nombre d'utilisateurs ou de territoires. Il suppose que sécurité, gouvernance, interopérabilité, capacité opérationnelle et soutenabilité progressent avec le volume. Une phase ne doit être étendue que lorsque ses limites sont suffisamment comprises et maîtrisées.

3. Phase 1 — Consolidation du socle

La première phase consolide l'architecture fondamentale, les responsabilités, les interfaces, les mécanismes cryptographiques, la traçabilité et les règles de gouvernance. Pour le domaine physique, elle préserve le cœur d'Authenticity Plus© fondé sur les trois QR codes fonctionnellement distincts et leurs statuts VERT, JAUNE et ROUGE.

4. Phase 2 — Pilotes nationaux

Des pilotes limités permettent de valider les cas d'usage dans un cadre institutionnel réel. Ils portent sur des secteurs ou flux présentant une valeur mesurable et disposent de critères de sécurité, adoption, performance, coût et qualité des preuves. Les résultats déterminent les corrections nécessaires avant extension.

5. Phase 3 — Extension sectorielle

Les mécanismes validés peuvent être étendus à plusieurs opérateurs et catégories d'un même secteur. Cette phase teste l'augmentation des volumes, la diversité des systèmes, la gouvernance des anomalies et la capacité d'intégration. Elle prépare l'interconnexion entre secteurs sans imposer une architecture monolithique.

6. Phase 4 — Architecture nationale

Les déploiements sectoriels matures peuvent être fédérés dans une architecture nationale de confiance. Les administrations, entreprises et infrastructures existantes restent responsables de leurs systèmes, tandis que Deep Authenticity© fournit les mécanismes communs d'identité, de preuve, d' interopérabilité et de traçabilité nécessaires.

7. Phase 5 — Premier Corridor de Confiance©

Une coopération bilatérale ou limitée peut ensuite relier deux environnements nationaux suffisamment matures. Le Corridor de Confiance© définit produits, autorités, opérateurs, certifications, preuves et procédures reconnues. Son succès doit être évalué avant toute réplication vers de nouveaux partenaires.

8. Phase 6 — Réseau de corridors

Plusieurs corridors compatibles peuvent former un réseau fédéré. Chaque relation conserve ses propres bases juridiques et institutionnelles. Le réseau ne doit pas créer de confiance transitive automatique : une reconnaissance entre deux partenaires ne s'étend à un troisième que si les conditions applicables le prévoient explicitement.

9. Phase 7 — Interopérabilité régionale

Lorsque plusieurs États ou institutions d'une région disposent de mécanismes compatibles, des référentiels communs peuvent faciliter les échanges. L'interopérabilité régionale doit préserver les différences réglementaires et permettre des profils nationaux lorsque ceux-ci sont nécessaires à la souveraineté ou à la conformité.

10. Phase 8 — Coopération multilatérale

La maturité régionale et bilatérale peut ouvrir la voie à des cadres multilatéraux. Organisations internationales, institutions spécialisées et États partenaires peuvent alors examiner les mécanismes de preuve, d'identité, de conformité et de gouvernance. Toute reconnaissance demeure formelle, explicite et limitée au mandat de l'organisation concernée.

11. Phase 9 — Fédération internationale

Une fédération internationale peut relier plusieurs réseaux compatibles sans créer une base mondiale unique. Les identités, preuves et statuts restent vérifiables entre environnements selon des règles communes ou des mécanismes de conversion. La fédération repose sur la compatibilité et la gouvernance plutôt que sur la centralisation.

12. Phase 10 — Infrastructure à portée mondiale

À maturité, Deep Authenticity© peut fonctionner comme une infrastructure de confiance à portée mondiale couvrant progressivement les domaines physique, numérique et administratif. Cette portée

ne signifie ni monopole, ni autorité politique mondiale : elle signifie capacité d'interopérer avec des systèmes souverains multiples.

13. Critères de passage entre phases

Chaque transition doit être conditionnée par des critères documentés : sécurité, stabilité, qualité des données, disponibilité, capacité d'audit, interopérabilité, conformité, gouvernance, réversibilité et soutenabilité économique. Une phase peut être prolongée ou réduite lorsque les critères ne sont pas atteints.

14. Indicateurs stratégiques

Le suivi peut inclure nombre de secteurs intégrés, organismes connectés, produits ou actifs vérifiables, taux de vérification, anomalies détectées, disponibilité, incidents, délais de traitement, corridors actifs, preuves transfrontalières et niveaux d'adoption. Les indicateurs doivent distinguer volume, qualité et impact réel.

15. Gouvernance de la croissance

L'augmentation de l'échelle exige une capacité de décision adaptée. Les mécanismes de représentation, versionnement, audit, gestion des incidents et évolution des référentiels doivent être renforcés avant que la croissance ne crée une complexité incontrôlable. La gouvernance doit précéder, et non suivre, l'expansion.

16. Souveraineté et architecture mondiale

Une infrastructure mondiale de confiance n'exige pas une infrastructure mondiale de données. Les États et institutions peuvent conserver localement leurs informations sensibles et partager uniquement les preuves ou attributs nécessaires. Cette séparation constitue l'un des fondements de l' acceptabilité internationale de Deep Authenticity©.

17. Résilience systémique

À grande échelle, Deep Authenticity© doit pouvoir isoler les incidents, fonctionner en mode dégradé, remplacer certains composants et maintenir la vérification des preuves historiques. La segmentation, la redondance, la diversité des opérateurs et les mécanismes de sortie réduisent le risque qu'une défaillance locale devienne mondiale.

18. Horizon stratégique

La finalité n'est pas de remplacer les infrastructures nationales, sectorielles ou internationales existantes, mais de leur fournir une couche commune de vérité vérifiable. L'expansion doit rester compatible avec les évolutions technologiques, juridiques et géopolitiques afin que le système puisse s'adapter sans perdre son identité fondamentale.

19. Deep Authenticity© et AP Ledger

Deep Authenticity© organise la continuité entre les différentes étapes de la feuille de route. AP Ledger peut ancrer les versions, validations, reconnaissances, transitions, suspensions et événements critiques afin de conserver une chronologie vérifiable de la construction du réseau. L'historique du déploiement devient ainsi lui-même auditable.

20. Critères d'acceptation et conclusion

La feuille de route est acceptable si chaque phase possède un périmètre et des critères de passage explicites ; si l'architecture fondamentale d'Authenticity Plus© est préservée dans le domaine physique ; si la croissance reste mesurable ; si la souveraineté et la localisation des données demeurent possibles ; si l'interopérabilité évite la centralisation obligatoire ; si la gouvernance précède l'expansion ; si les incidents peuvent être isolés ; et si l'infrastructure conserve sa réversibilité.

La trajectoire stratégique peut être résumée ainsi : SOCLE → PILOTE → SECTEUR → ÉTAT → CORRIDOR → RÉSEAU → RÉGION → MULTILATÉRAL → FÉDÉRATION → PORTÉE MONDIALE.

Deep Authenticity© ne devient pas universelle parce qu'elle centralise le monde, mais parce qu'elle permet à des systèmes différents de partager une capacité commune : établir et vérifier la provenance, l'intégrité, le statut et l'histoire des éléments critiques.

Cette trajectoire prépare la conclusion stratégique du Volume VII et son articulation avec les volumes suivants du Livre Blanc 2026.

Note d'alignement international

La feuille de route internationale est conçue comme un cadre stratégique adaptable aux exigences nationales, régionales et multilatérales. Les étapes proposées peuvent s'articuler avec les standards et mécanismes internationaux applicables à l'identité, à la conformité, à la cybersécurité, à la protection des données, aux chaînes de valeur et à la facilitation des échanges. Cette compatibilité constitue une orientation d'interopérabilité et ne vaut pas reconnaissance institutionnelle automatique.

1. Principe de gouvernance

Le Passeport Numérique Universel est universel par son principe d'identité et de continuité vérifiable, mais gouverné selon les compétences, droits et souverainetés applicables. Deep Authenticity© ne suppose ni une autorité mondiale unique ni une base centrale détenant toutes les données.

2. Universalité et souveraineté

Un actif peut conserver une identité vérifiable lorsqu'il traverse organisations, secteurs ou frontières, tandis que chaque autorité compétente conserve la maîtrise des données, clés, registres, règles et décisions relevant de sa juridiction.

3. Nœuds Souverains Nationaux

Les Nœuds Souverains Nationaux permettent à chaque pays de participer à Deep Authenticity© sans abandonner la maîtrise de ses actifs informationnels stratégiques. Ils peuvent héberger ou contrôler les composants, preuves, clés et politiques nécessaires aux passeports relevant de leur périmètre.

4. Fédération plutôt que centralisation

Une juridiction peut confirmer un statut ou une preuve minimale à une autre sans transférer l'ensemble du dossier sous-jacent. La confiance repose sur des protocoles communs, des autorités identifiables et des règles de reconnaissance explicites.

5. Corridors de Confiance

Les Corridors de Confiance organisent l'échange contrôlé de preuves entre organisations ou États : attributs vérifiables, autorités habilitées, niveau d'assurance, protocoles, données autorisées, révocations et responsabilités. Les données sensibles restent dans leurs environnements souverains lorsque leur transfert n'est pas nécessaire.

6. Confiance interinstitutionnelle

Une institution n'a pas à faire confiance aveuglément à toute l'infrastructure d'une autre. Elle doit pouvoir vérifier l'origine, l'autorité, l'intégrité et le statut de la preuve nécessaire. Le Passeport Numérique Universel devient ainsi un support de confiance vérifiable.

7. Autorités et responsabilités

Chaque événement critique du Passeport doit être attribuable à un acteur habilité : producteur, propriétaire, organisme de certification, administration, réparateur, douane ou autre autorité compétente. La gouvernance définit qui peut déclarer, confirmer, modifier, révoquer ou consulter chaque catégorie d'information.

8. Gouvernance des identités et des clés

Les identités des personnes, organisations, dispositifs et autorités doivent être gérées selon des niveaux d'assurance appropriés. Les clés cryptographiques critiques sont protégées, renouvelables et révocables ; dans les déploiements souverains, les autorités compétentes conservent la maîtrise des clés dont dépend la reconnaissance de leurs preuves.

9. Correction et révocation

Une erreur peut être corrigée sans effacer arbitrairement l'histoire. Corrections, révocations et remplacements restent traçables selon les règles applicables, afin de distinguer l'état courant de l'historique nécessaire à l'audit.

10. Portabilité, réversibilité et autonomie

Le Passeport Numérique Universel ne doit pas enfermer États ou organisations dans une dépendance technique irréversible. Standards documentés, API versionnées, formats exportables, migration et mécanismes de preuve vérifiables soutiennent l'autonomie stratégique.

11. Protection des données

Universalité ne signifie pas exposition universelle. Les données personnelles, commerciales, administratives ou souveraines sont soumises à finalité, minimisation, contrôle d'accès et

conservation proportionnée. Une vérification doit, lorsque possible, confirmer l'attribut nécessaire sans révéler les données sous-jacentes inutiles.

12. Audit et redevabilité

Les opérations sensibles doivent être auditables : accès, changement de statut, preuve utilisée, autorité, politique applicable, configuration et version. La souveraineté ne dispense pas de responsabilité ; elle exige une gouvernance démontrable.

13. Continuité transfrontalière

Lorsqu'un actif traverse une frontière, son Passeport Numérique Universel peut conserver son identité tout en changeant de contexte réglementaire. Le nœud destinataire peut vérifier une attestation du nœud d'origine sans obtenir toute la base source.

14. Non-ingérence

Les protocoles communs d'interopérabilité ne permettent pas à un participant de modifier les règles internes d'un autre pays. Reconnaissance, compatibilité, sécurité et traitement des incidents peuvent être communs ; les compétences souveraines restent nationales.

15. Principe institutionnel de référence

Une identité peut être universelle sans que ses données soient centralisées. Une preuve peut être interopérable sans que les souverainetés soient fusionnées. Une confiance peut être partagée sans devenir aveugle.

16. Architecture cible

Protocoles communs et services d'interopérabilité au niveau global → Corridors de Confiance entre juridictions → Nœuds Souverains Nationaux → systèmes nationaux, administrations, douanes, entreprises et infrastructures locales. La confiance circule ; la souveraineté reste distribuée.

17. Règle d'intégration dans le DMC

Cette mise à niveau doit être absorbée dans les chapitres correspondants du Volume VII lors de l' assemblage final. Elle complète la gouvernance existante sans reproduire le chapitre fondateur du Passeport Numérique Universel.

18. Conclusion

Dans le Volume VII, le Passeport Numérique Universel devient un instrument de confiance interinstitutionnelle gouvernée. Les Nœuds Souverains Nationaux protègent l'autonomie ; les Corridors de Confiance organisent les échanges ; les mécanismes cryptographiques protègent la preuve ; les autorités conservent leurs compétences. Deep Authenticity© peut ainsi rechercher une infrastructure universelle de vérité sans construire une autorité universelle de contrôle.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VIII — STRATÉGIE MONDIALE, IMPACT ET VISION 2040–2050

CHAPITRE 1 — DE L'INFRASTRUCTURE DE CONFIANCE À L'INFRASTRUCTURE UNIVERSELLE DE VÉRITÉ

VISION — 2040–2050 — PHYSIQUE — NUMÉRIQUE — ADMINISTRATIF — CONFIANCE — SOUVERAINETÉ — INTEROPÉRABILITÉ — TRANSFORMATION — CIVILISATION

1. Objet du chapitre

Ce chapitre ouvre le Volume VIII en définissant la trajectoire stratégique de Deep Authenticity© : passer d'une infrastructure de confiance interopérable à une infrastructure universelle de vérification capable de relier les domaines physique, numérique et administratif. L'objectif n'est pas de décréter une vérité mondiale, mais de rendre vérifiables l'origine, l'intégrité, le statut et l'historique des éléments critiques.

2. Vision 2040–2050

À l'horizon 2040–2050, la multiplication des objets connectés, contenus synthétiques, logiciels, identités numériques, documents et échanges automatisés renforcera le besoin de mécanismes de provenance et de vérification. Deep Authenticity© se positionne comme une couche transversale permettant aux systèmes existants d'échanger des preuves sans exiger leur centralisation.

3. Les trois domaines fondamentaux

Deep Authenticity© couvre trois domaines complémentaires : le physique, pour les objets, produits et actifs matériels ; le numérique, pour les logiciels, médias, contenus et propriété intellectuelle ; et l' administratif, pour les documents, identités, certificats et titres de propriété. Leur articulation constitue le cœur de l'infrastructure universelle de vérité.

4. Continuité entre le réel et le numérique

La valeur d'une preuve dépend de sa capacité à rester reliée à l'élément qu'elle décrit. Deep Authenticity© vise à maintenir cette continuité entre objet réel, représentation numérique, identité, événements et autorités compétentes. Les ruptures de liaison doivent être détectables, documentées et traitées selon le niveau de risque.

5. Authenticity Plus© comme fondation physique

Dans le domaine physique, l'architecture fondamentale d'Authenticity Plus© demeure centrale : trois QR codes fonctionnellement distincts pour le consommateur, le revendeur/professionnel et le contrôle/douanes. Les statuts restent VERT — original ; JAUNE — original mais déjà vérifié ou vendu ; ROUGE — contrefaçon ou code inexistant dans le système Authenticity Plus©. Les autres capacités complètent ce mécanisme sans le remplacer.

6. Vérité numérique vérifiable

Dans le domaine numérique, la vérification porte notamment sur la provenance, la signature, l'intégrité, l'auteur ou l'émetteur déclaré, les versions et les transformations significatives. Une signature cryptographique native ou une preuve équivalente peut permettre d'établir qu'un contenu correspond à une source identifiée, sans prétendre déterminer automatiquement la véracité de toutes ses affirmations.

7. Vérité administrative vérifiable

Dans le domaine administratif, Deep Authenticity© peut relier documents, identités, certificats, autorisations et titres à leurs autorités d'émission et à leurs statuts. La plateforme vérifie les éléments probants disponibles ; elle ne se substitue pas aux administrations, registres souverains, juridictions ou procédures légales qui déterminent leurs effets.

8. Identité et provenance

L'infrastructure universelle repose sur des identités suffisamment persistantes pour relier acteurs, objets, documents, contenus et événements. La provenance doit pouvoir être reconstruite sans supposer qu'un identifiant isolé constitue une preuve. L'autorité de l'émetteur, la signature, la chronologie et les règles applicables restent déterminantes.

9. Interopérabilité mondiale

Une infrastructure universelle ne peut dépendre d'un format, d'un fournisseur ou d'une juridiction unique. API documentées, formats structurés, signatures vérifiables, mécanismes de résolution et profils d'interopérabilité permettent à des systèmes hétérogènes de coopérer tout en conservant leurs architectures propres.

10. Souveraineté distribuée

L'universalité de la vérification n'implique pas une centralisation universelle des données. États, institutions, entreprises et individus peuvent conserver leurs informations dans les environnements autorisés et n'exposer que les preuves ou attributs nécessaires. Cette séparation entre donnée source et preuve vérifiable protège la souveraineté et la confidentialité.

11. Confiance vérifiable

Deep Authenticity© distingue la confiance déclarée de la confiance vérifiable. Une affirmation devient plus robuste lorsqu'elle peut être reliée à une identité, une autorité, une signature, une chronologie et des preuves contrôlables. Le niveau d'assurance doit rester explicite afin d'éviter qu'une preuve partielle soit interprétée comme une certitude absolue.

12. Transformation des échanges

À grande échelle, la vérification peut réduire certaines frictions entre producteurs, citoyens, entreprises et administrations : contrôles répétitifs, incertitudes sur l'origine, documents difficiles à

authentifier ou ruptures de traçabilité. Les gains attendus doivent toutefois être mesurés par secteur et ne doivent pas être présumés avant expérimentation.

13. Intelligence artificielle et preuve

L'intelligence artificielle peut contribuer à détecter anomalies, incohérences et risques, mais ses résultats restent distincts des preuves cryptographiques, administratives ou physiques. Deep Authenticity© doit conserver cette distinction : l'IA assiste l'analyse et la décision ; elle ne devient pas, à elle seule, l'autorité de vérité.

14. Jumeaux numériques et connaissance institutionnelle

Les jumeaux numériques nationaux, institutionnels ou sectoriels peuvent exploiter des données et preuves vérifiées afin d'améliorer simulation, anticipation et pilotage. Leur fiabilité dépend de la qualité, de la fraîcheur et de la représentativité des informations disponibles. Les résultats prospectifs doivent rester identifiés comme simulations et non comme faits futurs.

15. Économie de la confiance

Une infrastructure universelle de vérification peut créer de la valeur par la réduction de certains risques, la protection des chaînes de valeur, l'amélioration de la conformité et l'accélération de contrôles. Son modèle économique doit financer sécurité et innovation sans transformer l'accès à la vérité vérifiable en dépendance monopolistique.

16. Droits, confidentialité et proportionnalité

L'extension de la vérification doit rester compatible avec les droits fondamentaux, la protection des données, le secret légitime et la proportionnalité. Tous les acteurs n'ont pas besoin d'accéder aux mêmes informations. La divulgation sélective et la séparation des rôles constituent des protections structurelles.

17. Résilience civilisationnelle

Une infrastructure appelée à soutenir des fonctions critiques doit résister aux cyberattaques, défaillances, ruptures de connectivité, changements technologiques et tensions géopolitiques. Redondance, fédération, modes dégradés, migration cryptographique et réversibilité sont nécessaires pour éviter qu'une couche de confiance ne devienne un point unique de fragilité.

18. Limites et non-centralisation de la vérité

Deep Authenticity© ne doit pas être présenté comme une autorité capable de décider seule ce qui est vrai dans tous les domaines. Il fournit des mécanismes pour établir ce qui a été émis, signé, enregistré, transféré, certifié ou modifié, selon des preuves et des autorités identifiables. Les faits contestés, jugements de valeur et décisions souveraines conservent leurs procédures propres.

19. Deep Authenticity© et AP Ledger

Deep Authenticity© relie identités, objets, contenus, documents, autorités, droits et événements. AP Ledger peut ancrer les éléments critiques nécessaires à l'intégrité et à l'auditabilité : émissions, signatures, transferts, certifications, modifications, suspensions et révocations. Il constitue une couche probante, non un entrepôt universel de toutes les données.

20. Critères d'acceptation et conclusion

Une infrastructure universelle de vérification est acceptable si elle couvre les domaines physique, numérique et administratif sans confondre leurs règles ; si Authenticity Plus© demeure la fondation anti-contrefaçon du domaine physique ; si les preuves sont reliées à des autorités identifiables ; si l'interopérabilité évite la dépendance unique ; si la souveraineté et la confidentialité sont préservées ; si l'IA reste distincte de la preuve ; si la résilience et la réversibilité sont intégrées ; et si les limites de l'infrastructure sont explicitement reconnues.

Deep Authenticity© peut alors être envisagée comme une couche de vérité vérifiable au service de la société moderne : non pas un système qui impose ce que le monde doit croire, mais une infrastructure qui permet de déterminer plus rigoureusement ce qui peut être prouvé.

Cette ambition fonde la vision de Deep Authenticity© comme système d'exploitation de la civilisation moderne : une infrastructure reliant le physique, le numérique et l'administratif par des mécanismes communs de provenance, d'intégrité et de confiance vérifiable.

Le Chapitre 2 développera l'impact économique mondial potentiel de cette infrastructure et les mécanismes par lesquels la confiance vérifiable peut transformer les chaînes de valeur.

Note d'alignement international

La vision 2040–2050 présentée dans ce chapitre constitue une orientation prospective. Elle est conçue pour pouvoir s'articuler avec les standards et cadres internationaux applicables à l'identité numérique, à la traçabilité, à la cybersécurité, à la protection des données, à la signature électronique, à l'évaluation de conformité et à l'interopérabilité. Elle ne vaut ni prévision certaine, ni reconnaissance institutionnelle automatique.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VIII — STRATÉGIE MONDIALE, IMPACT ET VISION 2040–2050

CHAPITRE 2 — IMPACT ÉCONOMIQUE MONDIAL DE LA CONFIANCE VÉRIFIABLE

1. Objet du chapitre

Ce chapitre analyse les mécanismes par lesquels la confiance vérifiable peut produire un impact économique mondial. Deep Authenticity© ne crée pas de valeur par la seule accumulation de données : elle vise à réduire certaines asymétries d'information, améliorer la qualité des preuves, sécuriser les échanges et diminuer les coûts liés à l'incertitude, à la fraude et aux vérifications répétitives.

2. Le coût économique du déficit de confiance

Les économies modernes supportent des coûts lorsque l'origine, l'intégrité, la propriété ou le statut d' un actif sont difficiles à établir. Contrôles redondants, litiges, fraude, contrefaçon, rappels mal ciblés, documents falsifiés et ruptures de traçabilité mobilisent du capital et du temps. La confiance vérifiable cherche à réduire une partie de ces frictions sans prétendre supprimer l'ensemble des risques économiques.

3. Lutte contre la contrefaçon

Dans le domaine physique, Authenticity Plus© constitue la fondation anti-contrefaçon de Deep Authenticity©. Ses trois QR codes fonctionnellement distincts — consommateur, revendeur/professionnel et contrôle/douanes — permettent des vérifications adaptées aux rôles. Les statuts restent VERT — original ; JAUNE — original mais déjà vérifié ou vendu ; ROUGE — contrefaçon ou code inexistant dans le système Authenticity Plus©.

4. Protection des producteurs

Une identité de produit vérifiable peut aider les producteurs à protéger leur marque, leurs réseaux légitimes et leurs investissements. La traçabilité des événements significatifs facilite l'identification de certaines anomalies de distribution, de duplication ou de substitution. La valeur économique dépend toutefois de la qualité du déploiement, de l'adoption et de la capacité à agir sur les signaux détectés.

5. Protection des consommateurs

La réduction de l'incertitude sur l'authenticité peut améliorer la qualité de la décision d'achat. Un consommateur disposant d'un mécanisme simple de vérification peut mieux distinguer un produit connu du système d'un code inexistant ou déjà utilisé. Cette capacité ne remplace pas les garanties légales, contrôles de sécurité ou droits du consommateur.

6. Commerce et fluidité des échanges

Des preuves structurées et vérifiables peuvent réduire certaines vérifications manuelles ou duplications documentaires entre partenaires. Passeports numériques, certifications et événements

de traçabilité peuvent accompagner les flux lorsque les autorités et opérateurs concernés reconnaissent les mécanismes utilisés. Les gains doivent être mesurés par processus et par secteur.

7. Réduction des coûts de conformité

Une infrastructure interopérable peut permettre de réutiliser des preuves valides plutôt que de reconstruire plusieurs fois la même démonstration. Cette réutilisation doit respecter la portée, la date de validité et l'autorité de chaque preuve. La réduction des coûts de conformité ne doit jamais conduire à affaiblir les exigences réglementaires.

8. Productivité informationnelle

Une part croissante de l'activité économique consiste à rechercher, comparer et valider des informations. Deep Authenticity© peut améliorer cette productivité en reliant données, preuves, identités et statuts dans une structure vérifiable. Le bénéfice attendu réside moins dans la quantité d' information disponible que dans la réduction du temps nécessaire pour déterminer laquelle peut être raisonnablement utilisée.

9. Chaînes d'approvisionnement

Dans les chaînes d'approvisionnement complexes, la confiance vérifiable peut renforcer la continuité entre production, transformation, transport, distribution et vente. Les anomalies de lot, certification, provenance ou statut peuvent être détectées plus rapidement lorsque les événements sont correctement enregistrés. La plateforme complète les systèmes logistiques existants au lieu de les remplacer.

10. Marché de seconde main

Le marché de seconde main bénéficie particulièrement de la continuité d'identité et de propriété. Un passeport numérique peut permettre de vérifier certains événements antérieurs, transferts ou statuts autorisés et de réduire la réintroduction de produits frauduleux dans les circuits légitimes. La confidentialité des propriétaires successifs doit rester protégée.

11. Propriété intellectuelle et économie numérique

Dans le domaine numérique, la provenance et les signatures natives peuvent contribuer à mieux relier logiciels, médias, créations et contenus à leurs sources ou versions. Cette capacité peut soutenir la gestion de droits et la preuve d'antériorité ou d'intégrité lorsque les cadres applicables le permettent. Elle ne détermine pas automatiquement la titularité juridique d'un droit contesté.

12. Documents et économie administrative

La vérification des documents, certificats et autorisations peut réduire certaines fraudes et accélérer des procédures administratives ou commerciales. Une preuve d'émission et de statut peut éviter des vérifications répétitives auprès de l'autorité source. Les registres publics et procédures légales restent néanmoins les références lorsqu'ils possèdent une valeur juridique propre.

13. PME, artisans et producteurs indépendants

L'impact économique ne doit pas être réservé aux grands groupes. Des mécanismes accessibles peuvent permettre aux PME, artisans, agriculteurs, créateurs et producteurs indépendants de fournir des preuves de provenance ou d'authenticité comparables dans leur principe à celles de structures plus importantes. Les coûts et exigences doivent rester proportionnés au niveau de risque.

14. Investissement et confiance

Une meilleure qualité de preuve peut améliorer l'évaluation de certains actifs, opérations ou chaînes de valeur. Investisseurs, assureurs et partenaires peuvent disposer d'informations plus vérifiables sur des événements pertinents. Deep Authenticity© ne constitue cependant ni une notation financière, ni une garantie de rentabilité, ni un substitut à la diligence raisonnable.

15. Recettes publiques et souveraineté économique

La réduction de certaines formes de fraude, de commerce illicite ou de falsification peut contribuer à mieux protéger les recettes publiques et les marchés légitimes. Les administrations peuvent exploiter les preuves selon leurs compétences et règles nationales. Les effets fiscaux ou douaniers doivent être évalués empiriquement et ne peuvent être présumés à partir du seul déploiement technologique.

16. Données économiques et anticipation

Les événements vérifiés peuvent alimenter, sous des règles appropriées, des analyses agrégées sur flux, pénuries, anomalies, rappels ou dynamiques sectorielles. Ces informations peuvent améliorer les tableaux de bord et jumeaux numériques institutionnels. Les analyses doivent distinguer faits observés, estimations et simulations afin de ne pas transformer la prévision en certitude.

17. Modèle économique de Deep Authenticity©

La soutenabilité peut reposer sur plusieurs mécanismes : licences, services, abonnements, intégration, certification ou royalties contractuellement définies. Les hypothèses de revenus doivent être séparées des résultats constatés. Le modèle doit financer sécurité, maintenance et innovation tout en maintenant une accessibilité compatible avec l'ambition universelle.

18. Mesure de l'impact

L'impact économique doit être évalué à partir d'indicateurs vérifiables : fraude évitée ou détectée, délais de contrôle, coûts administratifs, incidents, taux d'adoption, récupération de valeur, efficacité des rappels et performance des chaînes de valeur. Les méthodologies, périodes de référence et limites doivent être publiées avec les résultats significatifs.

19. Scénarios d'adoption mondiale

Les scénarios internationaux peuvent modéliser différents niveaux d'adoption par secteur, région ou catégorie d'acteurs. Ils doivent présenter clairement les hypothèses de pénétration, tarification, coûts,

effets de réseau et incertitudes. Un scénario à 5 %, 10 % ou davantage du commerce mondial constitue une hypothèse prospective et non une prévision garantie.

20. Critères d'acceptation et conclusion

L'impact économique attribué à Deep Authenticity© est acceptable s'il repose sur des mécanismes identifiables ; si les économies annoncées sont mesurées plutôt que supposées ; si les scénarios distinguent hypothèses et résultats ; si Authenticity Plus© reste la fondation anti-contrefaçon du domaine physique ; si l'accessibilité aux petites structures est prise en compte ; si les droits et compétences réglementaires sont préservés ; et si la valeur créée est analysée au-delà des seuls revenus de la plateforme.

La confiance vérifiable peut devenir une infrastructure économique lorsqu'elle réduit le coût de l' incertitude sans créer une nouvelle dépendance opaque.

L'enjeu stratégique est de transformer la preuve en facteur de productivité, de protection et de fluidité économique, tout en conservant la possibilité de mesurer objectivement les résultats.

Le Chapitre 3 développera l'impact social et humain de Deep Authenticity©, notamment la protection des citoyens, l'accès équitable à la vérification et les nouvelles relations de confiance entre individus, entreprises et institutions.

Note d'alignement international

Les impacts économiques présentés dans ce chapitre constituent un cadre d'analyse et non une prévision financière garantie. Toute quantification future devra identifier ses sources, hypothèses, méthodes et marges d'incertitude. Les effets de Deep Authenticity© dépendront notamment du secteur, du niveau d'adoption, de l'intégration aux systèmes existants et des cadres réglementaires applicables.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VIII — STRATÉGIE MONDIALE, IMPACT ET VISION 2040–2050

CHAPITRE 3 — IMPACT SOCIAL ET HUMAIN DE DEEP AUTHENTICITY©

CITOYENS — CONFIANCE — PROTECTION — INCLUSION — DROITS — ACCESSIBILITÉ — IDENTITÉ — TRANSPARENCE — AUTONOMIE — COHÉSION

1. Objet du chapitre

Ce chapitre analyse l'impact social et humain potentiel de Deep Authenticity©. Une infrastructure de vérité vérifiable n'a de valeur collective que si elle renforce la capacité des citoyens à comprendre, vérifier et contester les informations qui les concernent, tout en protégeant leurs droits, leur autonomie, leur vie privée et leur accès équitable aux services.

2. La confiance comme bien social

La confiance facilite les relations entre citoyens, entreprises et institutions, mais elle devient fragile lorsque l'origine d'un produit, d'un document ou d'un contenu est difficile à établir. Deep Authenticity© vise à compléter la confiance déclarative par des preuves vérifiables. Cette capacité doit réduire l' incertitude sans instaurer une surveillance généralisée.

3. Protection du citoyen-consommateur

Dans le domaine physique, Authenticity Plus© permet au citoyen de vérifier un produit à travers le mécanisme consommateur de l'architecture à trois QR codes. Les statuts restent VERT — original ; JAUNE — original mais déjà vérifié ou vendu ; ROUGE — contrefaçon ou code inexistant dans le système Authenticity Plus©. Cette information complète, sans les remplacer, les droits et garanties du consommateur.

4. Accès équitable à la vérification

La capacité de vérifier ne doit pas être réservée aux administrations, grandes entreprises ou utilisateurs disposant d'équipements avancés. Les interfaces doivent rester simples, accessibles et compatibles avec différents niveaux de littératie numérique. Des solutions alternatives doivent être prévues lorsque la connectivité, le handicap ou l'absence d'équipement crée une barrière.

5. Inclusion numérique

Une infrastructure universelle doit être conçue pour éviter qu'une dépendance exclusive au numérique exclue certaines populations. Les mécanismes de vérification peuvent coexister avec des procédures assistées ou des canaux alternatifs lorsque le contexte l'exige. L'inclusion constitue une condition d' acceptabilité et non une fonction secondaire.

6. Identité et autonomie

L'identité numérique peut faciliter l'accès aux droits et services lorsqu'elle est gouvernée de manière proportionnée. Deep Authenticity© doit distinguer identification, authentification, autorisation et preuve afin d'éviter qu'une identité unique ne devienne un mécanisme de contrôle universel. L' utilisateur doit pouvoir comprendre les finalités des vérifications qui le concernent.

7. Vie privée et minimisation

La vérification d'une propriété ne nécessite pas toujours la révélation de l'ensemble des données sources. Deep Authenticity© privilégie la minimisation et, lorsque cela est approprié, la divulgation sélective. Un acteur doit recevoir les informations nécessaires à sa fonction, et non automatiquement l'historique complet d'une personne ou d'un actif.

8. Droit à l’explication et à la contestation

Lorsqu’un statut, une anomalie ou une décision affecte une personne, les éléments essentiels qui la fondent doivent pouvoir être compris selon les règles applicables. Une voie de contestation doit exister lorsque la décision produit des effets significatifs. La preuve technique doit soutenir la responsabilité, non rendre une décision incontestable.

9. Protection contre les erreurs

Aucun système de données n’est exempt d’erreurs, de données obsolètes ou d’associations incorrectes. Deep Authenticity© doit permettre correction, versionnement et traçabilité des rectifications sans effacer abusivement l’historique. Une anomalie algorithmique ou technique ne doit pas être automatiquement assimilée à une faute de l’utilisateur.

10. Relations citoyens–institutions

Des preuves vérifiables peuvent réduire certains échanges répétitifs entre citoyens et administrations lorsque des informations déjà établies peuvent être contrôlées de manière fiable. Cette simplification doit rester compatible avec le droit de fournir des éléments complémentaires, de corriger une information et d’accéder à un canal humain lorsque nécessaire.

11. Confiance dans les contenus numériques

La provenance et la signature native des contenus peuvent aider les citoyens à distinguer une source identifiée d’un contenu dont l’origine est inconnue ou altérée. Deep Authenticity© vérifie la provenance et l’intégrité lorsqu’elles sont démontrables ; elle ne doit pas devenir un mécanisme central déterminant quelles opinions ou interprétations sont autorisées.

12. Protection des créateurs

Artistes, auteurs, développeurs, journalistes, chercheurs et autres créateurs peuvent bénéficier de mécanismes reliant une œuvre ou un contenu à une origine et à un historique vérifiables. Ces preuves peuvent soutenir la reconnaissance et la gestion des droits sans se substituer aux règles juridiques de propriété intellectuelle.

13. Santé et continuité de l’information

Dans les usages de santé, une continuité d’information correctement gouvernée peut faciliter le suivi et réduire certaines ruptures documentaires. Les données de santé exigent toutefois des protections renforcées, des accès strictement contrôlés et des responsabilités explicites. Deep Authenticity© ne remplace ni le professionnel de santé ni la décision médicale.

14. Éducation et culture de la preuve

L’impact social dépend également de la capacité des citoyens à comprendre ce qu’une preuve démontre et ce qu’elle ne démontre pas. L’éducation à la provenance, aux signatures, aux statuts et

aux limites de l’intelligence artificielle peut contribuer à développer une culture de vérification plutôt qu’une confiance aveugle dans la technologie.

15. Équité entre acteurs

Une infrastructure de confiance ne doit pas donner systématiquement davantage de pouvoir aux acteurs qui possèdent déjà le plus de données ou de ressources. Les règles d’accès, de certification et de contestation doivent permettre aux petites structures et aux individus de participer dans des conditions proportionnées.

16. Prévention de la surveillance excessive

La traçabilité utile à l’authenticité d’un produit ou à la validité d’un document ne justifie pas la traçabilité permanente des personnes. Les architectures doivent séparer les finalités et limiter les corrélations non nécessaires. La confiance sociale dépend de la capacité à vérifier sans transformer l’ infrastructure en système de surveillance généralisée.

17. Cohésion et confiance institutionnelle

Lorsque les citoyens peuvent comprendre l’origine d’une information administrative, vérifier certaines preuves et identifier l’autorité responsable, la transparence opérationnelle peut soutenir la confiance institutionnelle. Cet effet dépend toutefois de la qualité de la gouvernance, de la possibilité de recours et du comportement réel des institutions.

18. Mesure de l’impact social

L’impact social doit être mesuré par des indicateurs tels que accessibilité, taux d’utilisation, erreurs corrigées, délais de service, satisfaction, recours, incidents de confidentialité et inclusion des populations vulnérables. Le nombre de vérifications ne suffit pas à démontrer une amélioration du bien-être ou de la confiance.

19. Deep Authenticity© comme infrastructure humaine

Deep Authenticity© relie objets, contenus et documents, mais son objectif ultime reste humain : permettre aux personnes d’interagir avec un environnement complexe en disposant de preuves plus compréhensibles et plus contrôlables. L’infrastructure doit donc être évaluée autant par la protection qu’elle apporte que par sa performance technique.

20. Critères d’acceptation et conclusion

L’impact social de Deep Authenticity© est acceptable si la vérification reste accessible ; si les personnes conservent leur autonomie ; si la vie privée et la minimisation sont intégrées ; si les erreurs peuvent être corrigées ; si les décisions significatives peuvent être contestées ; si les canaux non numériques restent disponibles lorsque nécessaires ; si la traçabilité ne devient pas une surveillance généralisée ; et si l’impact est mesuré par des résultats humains et non uniquement techniques.

La confiance vérifiable ne doit pas demander au citoyen de croire davantage à la technologie. Elle

doit lui permettre de dépendre moins de la confiance aveugle en donnant accès à des preuves, à leur provenance et aux responsabilités correspondantes.

Deep Authenticity© peut ainsi contribuer à une société dans laquelle la vérification renforce l' autonomie plutôt qu'elle ne la réduit.

Le Chapitre 4 développera la lutte mondiale contre la contrefaçon et la transformation des mécanismes de protection des produits, des chaînes de valeur et des marchés légitimes.

Note d'alignement international

L'approche sociale et humaine présentée dans ce chapitre s'inscrit dans une logique de conception centrée sur les personnes, d'inclusion, de protection des données, de sécurité et de responsabilité. Les bénéfices sociaux doivent être évalués dans chaque contexte de déploiement et mis en balance avec les risques d'exclusion, de surveillance, d'erreur ou de dépendance numérique.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VIII — STRATÉGIE MONDIALE, IMPACT ET VISION 2040–2050

CHAPITRE 4 — LUTTE MONDIALE CONTRE LA CONTREFAÇON ET PROTECTION DES MARCHÉS LÉGITIMES

CONTREFAÇON — AUTHENTIFICATION — TROIS QR — DOUANES — CONSOMMATEURS — PRODUCTEURS — TRAÇABILITÉ — COOPÉRATION — MARCHÉS — RÉSILIENCE

1. Objet du chapitre

Ce chapitre définit la contribution de Deep Authenticity© et d'Authenticity Plus© à une stratégie mondiale de lutte contre la contrefaçon. L'objectif est de renforcer la capacité des producteurs, consommateurs, revendeurs et autorités à distinguer les produits légitimes, détecter les anomalies et préserver la continuité de preuve tout au long des chaînes de valeur.

2. Dimension mondiale du phénomène

La contrefaçon constitue un risque transfrontalier qui exploite la complexité des chaînes d' approvisionnement, du commerce électronique et de la logistique moderne. Les estimations internationales doivent être utilisées avec leur méthodologie et leur année de référence ; elles décrivent un ordre de grandeur du commerce de faux et non la totalité des dommages économiques ou sociaux associés.

3. Architecture fondamentale d'Authenticity Plus©

La réponse physique repose sur l'architecture fondamentale des trois QR codes fonctionnellement distincts : consommateur, revendeur/professionnel et contrôle/douanes. Chaque accès répond à un rôle spécifique et contribue à la continuité d'authentification. Les couches d'IA, de traçabilité, de certification et d'analyse complètent ce mécanisme sans s'y substituer.

4. Interprétation universelle des statuts

L'interprétation utilisateur demeure constante : VERT signifie original ; JAUNE signifie original mais déjà vérifié ou vendu ; ROUGE signifie contrefaçon ou code inexistant dans le système Authenticity Plus©. Cette simplicité permet une lecture immédiate tout en laissant aux autorités et professionnels l'accès aux éléments supplémentaires correspondant à leur rôle.

5. Protection du consommateur

Le consommateur doit pouvoir effectuer une vérification simple avant ou après l'achat selon les règles du système. Le résultat l'aide à identifier un produit reconnu, un code déjà utilisé ou une situation nécessitant prudence et contrôle complémentaire. Cette fonction ne remplace pas les droits légaux du consommateur ni les contrôles réglementaires de sécurité.

6. Protection du producteur

Le producteur associe chaque unité protégée à une identité et à des éléments probants contrôlés. Cette architecture peut rendre plus difficile la simple reproduction visuelle d'un emballage ou d'un code et faciliter l'identification d'anomalies. L'efficacité dépend de la sécurité de l'émission, de l' intégration industrielle et du traitement opérationnel des alertes.

7. Rôle du revendeur professionnel

Le QR revendeur/professionnel permet d'intégrer la vérification aux opérations commerciales et de distribution. Il peut contribuer à confirmer la légitimité d'un produit avant sa remise en circulation, à enregistrer certains événements autorisés et à soutenir les fenêtres revendeur et seconde main de l' écosystème Authenticity Plus©.

8. Rôle des douanes et autorités de contrôle

Le QR contrôle/douanes constitue un canal distinct destiné aux acteurs habilités. Il peut donner accès aux éléments nécessaires à la vérification de l'identité, de l'origine, du statut ou de certains événements. La plateforme fournit des preuves et signaux ; la décision d'inspection, de retenue, de mainlevée ou de sanction demeure de la compétence de l'autorité concernée.

9. Traçabilité de la chaîne de valeur

La lutte contre la contrefaçon ne s'arrête pas au point de vente. Production, conditionnement, expédition, importation, distribution, vente, transfert et seconde main peuvent générer des événements pertinents. Une chronologie vérifiable aide à repérer les ruptures, doublons ou incohérences sans supposer qu'une anomalie constitue automatiquement une fraude.

10. Petits colis et commerce électronique

La fragmentation des expéditions et la croissance des petits colis compliquent les contrôles traditionnels. Une identité numérique vérifiable au niveau de l'unité peut compléter les méthodes de ciblage en permettant des vérifications plus rapides et sélectives. Son utilisation doit rester compatible avec les procédures douanières et les capacités opérationnelles réelles.

11. Localisation et assemblage des faux

Les réseaux de contrefaçon peuvent séparer composants, emballages et étapes d'assemblage afin de rapprocher la production frauduleuse des marchés de destination. Une stratégie efficace doit donc vérifier plusieurs points de la chaîne et ne pas dépendre exclusivement du pays d'expédition final ou d'un contrôle unique à la frontière.

12. Secteurs sensibles

La contrefaçon touche des catégories très diverses, depuis les biens de consommation jusqu'à des produits dont la non-conformité peut présenter des risques importants. Le niveau de contrôle, la profondeur des preuves et les procédures d'escalade doivent être adaptés au risque du secteur plutôt qu'appliqués uniformément.

13. Coopération avec les titulaires de droits

Les titulaires de marques, fabricants et détenteurs de droits peuvent fournir des informations nécessaires à l'identification des produits légitimes et à l'analyse des anomalies. Les mécanismes de partage doivent être gouvernés afin de protéger les secrets industriels, les données personnelles et les compétences des autorités.

14. Coopération internationale

Les chaînes de contrefaçon traversent plusieurs juridictions. Corridors de Confiance©, passeports numériques et preuves transfrontalières peuvent faciliter la coopération entre partenaires lorsque leurs règles de reconnaissance sont définies. La vérification technique d'une preuve étrangère n' emporte pas automatiquement reconnaissance juridique.

15. Intelligence artificielle et détection d'anomalies

L'intelligence artificielle peut analyser des volumes importants de scans, images, événements et comportements afin de détecter des configurations atypiques. Ces résultats constituent des signaux de risque et non des verdicts autonomes. Les décisions ayant des effets significatifs doivent rester gouvernées et appuyées par des preuves appropriées.

16. AP Shield, AP Ledger et couches complémentaires

AP Shield peut contribuer à la surveillance et à la détection de menaces, tandis qu'AP Ledger peut ancrer les événements probants nécessaires à l'auditabilité. Certification, IoT, cryptographie avancée

et analyses peuvent renforcer certains secteurs. Toutes ces capacités restent complémentaires à l' architecture des trois QR codes.

17. Seconde main et transfert de propriété

La continuité d'authenticité devient particulièrement importante lorsqu'un produit quitte son premier circuit de vente. Le transfert numérique sécurisé de propriété et la fenêtre seconde main peuvent aider à préserver l'identité du produit et à réduire la réintroduction de faux dans les marchés légitimes, sous réserve des règles de confidentialité.

18. Mesure de l'efficacité

L'efficacité doit être mesurée par des indicateurs tels que taux de vérification, anomalies qualifiées, faux détectés, délais de contrôle, incidents, faux positifs, adoption par les acteurs et évolution des risques sur les circuits couverts. Le nombre de scans, pris isolément, ne démontre pas une réduction de la contrefaçon.

19. Stratégie mondiale de protection

La stratégie mondiale combine prévention, authentification, traçabilité, coopération, ciblage des risques et capacité d'intervention. Deep Authenticity© fournit la couche de relation entre produits, preuves, acteurs et territoires ; Authenticity Plus© fournit le mécanisme anti-contrefaçon fondamental du domaine physique. L'objectif est de rendre les marchés légitimes plus vérifiables et plus difficiles à infiltrer.

20. Critères d'acceptation et conclusion

Une stratégie mondiale anti-contrefaçon fondée sur Authenticity Plus© et Deep Authenticity© est acceptable si les trois QR codes restent fonctionnellement distincts ; si les statuts VERT, JAUNE et ROUGE conservent leur signification ; si producteurs, consommateurs, revendeurs et contrôleurs disposent d'accès adaptés ; si les anomalies ne sont pas confondues avec des verdicts ; si les preuves transfrontalières respectent la souveraineté ; si les couches complémentaires ne remplacent pas le mécanisme central ; et si l'efficacité est mesurée sur le terrain.

La lutte contre la contrefaçon doit évoluer d'une logique principalement réactive vers une logique de vérification continue de l'identité et de la provenance des produits.

Authenticity Plus© fournit le point d'ancrage physique de cette transformation ; Deep Authenticity© l' étend à une infrastructure de confiance reliant les marchés, les institutions et les frontières.

Le Chapitre 5 développera le commerce éthique mondial et la manière dont la confiance vérifiable peut contribuer à rééquilibrer les relations entre producteurs, distributeurs, consommateurs et États.

Note d'alignement international

Les données internationales les plus récentes disponibles dans le rapport conjoint OCDE–EUIPO 2025 estiment à environ 467 milliards USD la valeur du commerce mondial de produits contrefaits en 2021,

soit jusqu'à 2,3 % des importations mondiales. Ces estimations reposent notamment sur des données de saisies douanières et comportent des limites méthodologiques ; elles ne doivent pas être assimilées à une mesure exhaustive de toutes les pertes liées à la contrefaçon.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VIII — STRATÉGIE MONDIALE, IMPACT ET VISION 2040–2050

CHAPITRE 5 — COMMERCE ÉTHIQUE MONDIAL ET RÉÉQUILIBRAGE DES RELATIONS ÉCONOMIQUES

ÉTHIQUE — COMMERCE — PRODUCTEURS — CONSOMMATEURS — PME — TRAÇABILITÉ — ÉQUITÉ — TRANSPARENCE — SOUVERAINETÉ — CONFIANCE

1. Objet du chapitre

Ce chapitre définit le commerce éthique mondial comme un environnement dans lequel l'origine, l' authenticité, certains engagements de conformité et les événements significatifs d'un produit peuvent être vérifiés par les acteurs habilités. Deep Authenticity© vise à réduire les asymétries d'information sans imposer un modèle économique unique ni se substituer aux autorités compétentes.

2. De la confiance déclarée à la confiance vérifiable

Le commerce repose sur de nombreuses déclarations : origine, composition, certification, propriété, conformité ou statut. La confiance vérifiable ajoute une couche probante permettant de relier ces affirmations à des émetteurs, des preuves et une chronologie. Elle ne garantit pas automatiquement qu'un produit est éthique dans toutes ses dimensions.

3. Authenticity Plus© comme fondation du produit légitime

Dans le domaine physique, Authenticity Plus© demeure le mécanisme fondamental de protection : trois QR codes fonctionnellement distincts pour le consommateur, le revendeur/professionnel et le contrôle/douanes. Les statuts restent VERT — original ; JAUNE — original mais déjà vérifié ou vendu ; ROUGE — contrefaçon ou code inexistant dans le système Authenticity Plus©.

4. Protection du producteur légitime

Une identité vérifiable peut aider un producteur à différencier ses produits des copies, à documenter leur provenance et à préserver la valeur de ses investissements. Cette capacité est particulièrement importante lorsque des intermédiaires multiples séparent le producteur du consommateur final.

5. Place des PME, artisans et producteurs indépendants

Le commerce éthique doit rester accessible aux petites structures. Les PME, artisans, agriculteurs, éleveurs, artistes et créateurs doivent pouvoir fournir des preuves proportionnées à leurs moyens et à leurs risques. Une infrastructure trop coûteuse ou complexe pourrait renforcer les acteurs dominants au lieu de rééquilibrer les marchés.

6. Information du consommateur

Le consommateur peut bénéficier d'informations vérifiables sur l'authenticité et, selon le secteur, sur certains attributs de provenance ou de certification. L'interface doit distinguer clairement les faits démontrés, les déclarations du producteur et les certifications tierces afin d'éviter une apparence trompeuse de garantie universelle.

7. Traçabilité et chaînes de valeur

La traçabilité peut documenter les étapes pertinentes de production, transformation, transport, distribution et vente. Elle facilite l'identification de certaines ruptures ou incohérences et peut soutenir des exigences de durabilité ou de conformité. La granularité des données doit rester proportionnée aux finalités et aux obligations applicables.

8. Commerce durable et économie circulaire

Passeports numériques et preuves de cycle de vie peuvent soutenir réparation, réemploi, seconde main et recyclage en rendant disponibles des informations sur l'identité, la composition, l'historique ou le statut d'un produit. Ces mécanismes peuvent contribuer à une économie plus circulaire lorsque les données sont fiables et réellement utilisées.

9. Accès aux marchés internationaux

Des preuves de provenance, de conformité ou de durabilité peuvent aider des producteurs à répondre à certaines exigences de marchés étrangers. Deep Authenticity© peut faciliter la présentation et la vérification de ces preuves sans garantir l'accès réglementaire à un marché, qui demeure soumis aux règles de la juridiction concernée.

10. Réduction des asymétries d'information

Les acteurs disposant de peu de moyens ont souvent moins de capacité à démontrer la qualité ou la provenance de leurs produits. Une infrastructure commune de preuve peut réduire cette asymétrie si les règles sont ouvertes, proportionnées et interopérables. Elle ne doit pas créer une nouvelle barrière d'entrée fondée sur la maîtrise d'une technologie propriétaire.

11. Responsabilité des distributeurs

Distributeurs et revendeurs peuvent jouer un rôle dans la préservation de la continuité de preuve. Leurs opérations doivent respecter les statuts, droits et procédures définis par Authenticity Plus© et Deep Authenticity©. La traçabilité ne supprime pas leurs obligations contractuelles, réglementaires ou de vigilance.

12. Commerce électronique et plateformes

Dans le commerce électronique, l'acheteur ne peut pas toujours examiner physiquement le produit avant paiement. L'association d'une identité vérifiable, d'informations sur le vendeur et de preuves pertinentes peut réduire certaines incertitudes. Les plateformes conservent leurs responsabilités propres en matière de protection des consommateurs et de conformité.

13. Commerce transfrontalier

Les passeports numériques et Corridors de Confiance© peuvent faciliter la continuité des preuves entre territoires. Les partenaires définissent les catégories de preuves reconnues, les autorités habilitées et les procédures applicables. La circulation technique d'une preuve ne produit pas automatiquement les mêmes effets juridiques dans toutes les juridictions.

14. Concurrence et neutralité

Deep Authenticity© doit soutenir la concurrence plutôt que favoriser artificiellement un acteur. Les conditions d'accès, d'interopérabilité et de certification doivent être explicites. La gouvernance doit prévenir les situations dans lesquelles le contrôle de l'infrastructure de vérification pourrait devenir un moyen de verrouiller un marché.

15. Commerce éthique et droits sociaux

Certaines chaînes de valeur doivent démontrer des engagements sociaux ou environnementaux. Deep Authenticity© peut conserver ou référencer les preuves correspondantes lorsqu'elles proviennent d'autorités ou organismes compétents. La plateforme ne doit pas transformer une déclaration non auditée en certification implicite.

16. Inclusion des économies en développement

La transformation numérique du commerce peut créer de nouvelles opportunités mais aussi approfondir les écarts de capacité. Le déploiement doit intégrer formation, outils accessibles, infrastructures adaptées et renforcement des capacités locales. L'objectif est que la vérification facilite l'accès aux marchés plutôt qu'elle ne devienne une nouvelle condition impossible à satisfaire.

17. Souveraineté économique

Les États doivent pouvoir intégrer la confiance vérifiable à leurs politiques commerciales sans perdre le contrôle de leurs données, registres ou décisions réglementaires. Les architectures distribuées permettent de conserver localement les informations sensibles tout en échangeant les preuves nécessaires à certains flux.

18. Mesure de l'équité et de l'impact

Le succès d'un commerce plus éthique doit être évalué au-delà du volume de transactions : accès des petites entreprises, coûts de conformité, délais, litiges, fraude, capacité de vérification des

consommateurs et distribution de la valeur créée sont également pertinents. Les indicateurs doivent permettre d'identifier les effets indésirables.

19. Deep Authenticity© comme infrastructure de commerce éthique

Deep Authenticity© relie produits, producteurs, preuves, certifications, droits et événements ; Authenticity Plus© fournit la fondation d'authentification du produit physique. Ensemble, ils peuvent soutenir un commerce dans lequel les affirmations importantes deviennent plus vérifiables, sans remplacer les règles de concurrence, de travail, d'environnement ou de protection des consommateurs.

20. Critères d'acceptation et conclusion

Un modèle de commerce éthique fondé sur Deep Authenticity© est acceptable si l'authenticité reste vérifiable ; si les petites structures peuvent participer ; si les déclarations sont distinguées des certifications ; si la traçabilité reste proportionnée ; si la concurrence et l'interopérabilité sont préservées ; si les preuves transfrontalières respectent la souveraineté ; si les exigences de durabilité ne deviennent pas des barrières opaques ; et si l'impact est mesuré sur la distribution réelle des bénéfices et des coûts.

Le commerce éthique ne consiste pas à déclarer qu'une chaîne de valeur est vertueuse. Il consiste à rendre vérifiables les éléments sur lesquels cette qualification peut raisonnablement reposer. Deep Authenticity© peut ainsi contribuer à rééquilibrer les relations économiques en donnant aux producteurs légitimes, aux consommateurs et aux institutions un accès plus symétrique à la preuve.

Le Chapitre 6 développera les scénarios d'adoption internationale de Deep Authenticity© à l'horizon 2040–2050 et les trajectoires possibles de diffusion sectorielle, nationale et mondiale.

Note d'alignement international

Les principes de ce chapitre convergent avec les travaux internationaux qui associent commerce durable, inclusion, traçabilité, transparence et facilitation des échanges. Les exigences de diligence raisonnable et de durabilité peuvent toutefois imposer des coûts disproportionnés aux petits producteurs si elles ne sont pas accompagnées de capacités, d'interopérabilité et de dispositifs proportionnés. Toute mise en œuvre de Deep Authenticity© devra donc être adaptée aux règles commerciales et réglementaires applicables.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VIII — STRATÉGIE MONDIALE, IMPACT ET VISION 2040–2050

CHAPITRE 6 — SCÉNARIOS D'ADOPTION INTERNATIONALE DE DEEP AUTHENTICITY© À L'HORIZON 2040–2050

SCÉNARIOS — ADOPTION — 2040–2050 — SECTEURS — ÉTATS — CORRIDORS — INTEROPÉRABILITÉ — DIFFUSION — INCERTITUDE — MONDE

1. Objet du chapitre

Ce chapitre construit des scénarios d'adoption internationale de Deep Authenticity© à l'horizon 2040–2050. Il ne s'agit pas de prédictions, mais de trajectoires prospectives permettant d'examiner comment l'infrastructure pourrait évoluer selon l'adoption sectorielle, l'engagement des États, l'interopérabilité, les coûts, la réglementation, la confiance institutionnelle et les transformations du commerce mondial.

2. Principe de scénarisation

La prospective distingue les variables relativement maîtrisables des facteurs externes. Architecture, sécurité, gouvernance et qualité d'intégration peuvent être améliorées par conception ; géopolitique, réglementation, cycles économiques, standards concurrents et vitesse d'adoption restent plus incertains. Les scénarios doivent donc être révisables et accompagnés d'hypothèses explicites.

3. Point de départ 2026

Le contexte de départ est marqué par une numérisation croissante des échanges, des documents et des processus, mais par une interopérabilité internationale encore incomplète. Les politiques de commerce numérique progressent de manière hétérogène et les États conservent des exigences différentes en matière de données, d'identité, de cybersécurité et de reconnaissance.

4. Facteurs d'accélération

L'adoption peut être accélérée par une augmentation de la contrefaçon et de la fraude, des obligations de traçabilité, la généralisation des passeports numériques, la demande de provenance des contenus, l'automatisation des contrôles et la recherche de chaînes d'approvisionnement plus résilientes. Des pilotes démontrant une valeur mesurable peuvent également créer un effet d'entraînement.

5. Facteurs de ralentissement

Coûts d'intégration, fragmentation réglementaire, absence de standards communs, faible maturité numérique, méfiance institutionnelle, risques cyber, dépendance technologique ou bénéfices insuffisamment démontrés peuvent ralentir l'adoption. Une infrastructure trop centralisée ou difficile à quitter pourrait également provoquer une résistance légitime.

6. Scénario A — Adoption ciblée

Dans un scénario prudent, Deep Authenticity© reste principalement déployée dans des secteurs à forte valeur ou à risque élevé. Authenticity Plus© protège des catégories physiques prioritaires, tandis

que les fonctions numériques et administratives sont utilisées dans des projets limités. La croissance repose sur des résultats sectoriels plutôt que sur une diffusion universelle.

7. Scénario B — Fédération sectorielle

Dans un scénario intermédiaire, plusieurs secteurs adoptent des mécanismes compatibles de preuve et de passeport numérique. Des fédérations apparaissent entre chaînes de valeur, opérateurs et autorités. Deep Authenticity© devient une couche d'interopérabilité reconnue dans certains écosystèmes, sans constituer encore une infrastructure transversale nationale ou mondiale.

8. Scénario C — Adoption nationale

Des États peuvent intégrer progressivement Deep Authenticity© comme infrastructure de confiance reliant plusieurs secteurs. Les données souveraines restent distribuées, tandis que les preuves, identités et statuts deviennent interopérables. Les trois domaines — physique, numérique et administratif — commencent alors à fonctionner dans un cadre national cohérent.

9. Scénario D — Corridors internationaux

Plusieurs environnements nationaux matures peuvent établir des Corridors de Confiance©. Les partenaires définissent les preuves reconnues, les autorités habilitées et les procédures de contrôle. La croissance internationale se fait par relations bilatérales ou régionales démontrées plutôt que par adhésion immédiate à un système mondial.

10. Scénario E — Réseau fédéré mondial

Dans un scénario d'adoption élevée, des corridors et réseaux régionaux deviennent interopérables. Deep Authenticity© fonctionne comme une couche fédérée permettant de vérifier des preuves entre systèmes souverains. Cette portée mondiale n'exige ni base de données centrale unique ni reconnaissance juridique uniforme.

11. Authenticity Plus© dans tous les scénarios

Quel que soit le niveau d'adoption, le domaine physique conserve l'architecture fondamentale d' Authenticity Plus© : QR consommateur, QR revendeur/professionnel et QR contrôle/douanes. Les statuts restent VERT — original ; JAUNE — original mais déjà vérifié ou vendu ; ROUGE — contrefaçon ou code inexistant dans le système Authenticity Plus©.

12. Adoption du domaine numérique

La diffusion numérique dépendra notamment de la demande de provenance des contenus, de signatures natives, de vérification des logiciels et de gestion de propriété intellectuelle. La croissance de l'IA générative peut renforcer l'intérêt pour la provenance, mais les mécanismes devront rester interopérables et distinguer clairement origine, intégrité et véracité du contenu.

13. Adoption du domaine administratif

Dans l’administration, l’adoption peut progresser par certificats, documents, identités, titres et autorisations. Les gains potentiels résident dans la réutilisation de preuves et la réduction de vérifications répétitives. La vitesse de diffusion dépendra fortement du droit national, de l’identité numérique existante et de la capacité d’interopérabilité des services publics.

14. Adoption par les entreprises

Les grandes entreprises peuvent adopter plus rapidement lorsque la conformité, la traçabilité ou la protection de marque justifient l’investissement. Les PME nécessitent des outils plus simples et des coûts proportionnés. L’adoption mondiale ne sera réellement significative que si les petites structures peuvent participer sans infrastructure technique disproportionnée.

15. Adoption par les citoyens

L’adoption citoyenne dépendra de l’utilité concrète, de la simplicité, de la confiance, de la confidentialité et de la possibilité de contester les erreurs. Le volume de comptes ou de scans ne suffit pas à mesurer une adoption durable : il faut également observer la fréquence d’usage, la compréhension des statuts et la valeur réellement perçue.

16. Effets de réseau

La valeur d’une infrastructure interopérable peut augmenter avec le nombre d’acteurs compatibles, mais les effets de réseau peuvent aussi créer des risques de concentration. Standards ouverts, portabilité, fédération et réversibilité doivent empêcher que la croissance transforme une infrastructure de confiance en verrou technologique.

17. Indicateurs de trajectoire

Le suivi prospectif peut inclure secteurs couverts, États pilotes, corridors actifs, preuves transfrontalières, taux d’interopérabilité, adoption des PME, coûts d’intégration, incidents, disponibilité et utilisation dans les trois domaines. Ces indicateurs permettent de comparer la trajectoire réelle aux scénarios sans confondre objectifs et résultats.

18. Points de bascule

Certains événements peuvent accélérer une transition entre scénarios : reconnaissance réglementaire d’un mécanisme, adoption d’un standard interopérable, réussite d’un corridor, obligation sectorielle de passeport numérique ou démonstration d’une réduction significative des coûts. À l’inverse, un incident systémique ou une gouvernance défaillante peut ralentir ou inverser la trajectoire.

19. Horizon 2040–2050

À cet horizon, plusieurs trajectoires restent plausibles : infrastructure spécialisée, fédération de secteurs, réseaux nationaux interopérables ou couche mondiale de vérification. La stratégie doit donc préserver une architecture capable de produire de la valeur à chaque niveau, même si l’adoption universelle n’est jamais atteinte.

20. Critères d'acceptation et conclusion

Les scénarios d'adoption sont acceptables s'ils restent explicitement prospectifs ; si leurs hypothèses peuvent être révisées ; si les facteurs d'accélération et de ralentissement sont distingués ; si chaque niveau d'adoption peut produire une valeur autonome ; si la souveraineté et la réversibilité sont préservées ; si Authenticity Plus© conserve son architecture fondamentale ; et si les résultats réels sont comparés aux scénarios par des indicateurs mesurables.

L'ambition mondiale de Deep Authenticity© ne doit pas dépendre d'une seule prévision de croissance. Elle doit reposer sur une architecture capable de progresser par étapes et de rester utile dans plusieurs futurs possibles.

La prospective devient ainsi un outil de gouvernance : elle permet de préparer l'expansion sans transformer une vision 2040–2050 en certitude.

Le Chapitre 7 développera la transformation des relations entre producteurs, citoyens, entreprises et États dans un environnement où la confiance devient progressivement vérifiable.

Note d'alignement international

Les scénarios 2040–2050 sont prospectifs et ne constituent ni des prévisions garanties ni des engagements d'adoption. Les tendances actuelles du commerce numérique montrent simultanément une progression de la coopération internationale et une forte hétérogénéité réglementaire. Les travaux récents de l'OCDE soulignent également que l'interopérabilité technique et réglementaire demeure une condition majeure du passage à l'échelle des processus commerciaux numériques.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VIII — STRATÉGIE MONDIALE, IMPACT ET VISION 2040–2050

CHAPITRE 7 — TRANSFORMATION DES RELATIONS ENTRE PRODUCTEURS, CITOYENS, ENTREPRISES ET ÉTATS

PRODUCTEURS — CITOYENS — ENTREPRISES — ÉTATS — PREUVE — RESPONSABILITÉ — INTEROPÉRABILITÉ — AUTONOMIE — TRANSPARENCE — CONFIANCE

1. Objet du chapitre

Ce chapitre analyse la manière dont Deep Authenticity© peut transformer les relations entre producteurs, citoyens, entreprises et États lorsque la confiance déclarative est progressivement complétée par une confiance vérifiable. L'enjeu n'est pas de supprimer les relations humaines ou institutionnelles, mais de rendre les responsabilités, les preuves et les statuts plus contrôlables.

2. Du rapport de confiance au rapport de preuve

Dans de nombreux échanges, une partie dépend des déclarations de l'autre. Deep Authenticity© ajoute une capacité de vérification : identité de l'émetteur, intégrité d'un document, authenticité d'un produit, certification ou historique. La preuve réduit certaines asymétries sans éliminer la nécessité du jugement, du droit ou de la responsabilité.

3. Producteur et consommateur

Le producteur peut fournir au consommateur une identité de produit vérifiable plutôt qu'une simple affirmation commerciale. Authenticity Plus© conserve son architecture fondamentale : QR consommateur, QR revendeur/professionnel et QR contrôle/douanes, avec VERT — original ; JAUNE — original mais déjà vérifié ou vendu ; ROUGE — contrefaçon ou code inexistant dans le système.

4. Producteur et distributeur

La relation entre producteur et distributeur peut s'appuyer sur des événements de chaîne de valeur plus vérifiables : émission, réception, transfert, statut ou certification. Cette continuité peut réduire certains litiges et améliorer la détection d'anomalies, sans remplacer les contrats, obligations commerciales ou contrôles physiques nécessaires.

5. Entreprise et consommateur

L'entreprise peut rendre certaines affirmations plus vérifiables : provenance, statut, garantie, certification ou historique autorisé. L'interface doit distinguer clairement ce qui provient de l' entreprise, ce qui a été certifié par un tiers et ce qui est établi par une preuve technique afin d'éviter toute confusion.

6. Citoyen et administration

Un citoyen peut réutiliser certaines preuves administratives sans devoir reconstruire continuellement son dossier. L'administration peut vérifier l'émetteur, l'intégrité et le statut selon ses compétences. Le citoyen doit conserver des voies de correction, de recours et d'accès humain lorsqu'une donnée ou une décision produit un effet significatif.

7. Entreprises et administrations

Les entreprises peuvent transmettre des preuves structurées de conformité, d'autorisation ou de statut lorsque les autorités les acceptent. Cela peut réduire certaines duplications et accélérer des contrôles ciblés. La décision réglementaire reste du ressort de l'administration compétente et ne peut être déléguée implicitement à la plateforme.

8. Relations entre administrations

Des systèmes publics interopérables peuvent limiter la répétition de demandes d'informations déjà détenues par une autre autorité, sous réserve d'une base légitime et de règles d'accès. Deep

Authenticity© peut fournir une couche de preuve et de traçabilité permettant de comprendre quelle autorité a émis ou vérifié un élément.

9. États et entreprises

Les États peuvent exiger des preuves de conformité ou de traçabilité tout en laissant aux entreprises plusieurs moyens interopérables de les fournir. Deep Authenticity© doit éviter de devenir un canal commercial exclusif. La confiance vérifiable doit soutenir la régulation sans créer un monopole technique sur l'accès aux marchés.

10. États et citoyens

Une relation numérique de confiance exige davantage que l'identité technique. Les citoyens doivent savoir quelles données sont utilisées, pour quelle finalité et avec quelles voies de recours. Une infrastructure de preuve peut améliorer la transparence opérationnelle si elle est accompagnée de gouvernance, de proportionnalité et de garanties crédibles.

11. Producteurs et États

Les producteurs peuvent utiliser des passeports numériques et des preuves de traçabilité pour répondre à certaines exigences réglementaires ou douanières. Les États conservent le pouvoir de définir les preuves recevables, de demander des contrôles complémentaires et d'imposer les mesures prévues par leur droit.

12. Relations entre entreprises

Dans les relations B2B, une preuve réutilisable peut réduire certaines vérifications répétitives concernant identité, certification, statut ou origine. Les partenaires peuvent automatiser une partie des contrôles tout en conservant des procédures d'escalade lorsque les preuves sont absentes, expirées, contradictoires ou insuffisantes.

13. Transformation de la responsabilité

La traçabilité des émissions, validations et modifications rend plus visible la chaîne des responsabilités. Une erreur peut être reliée à l'étape où elle est apparue, sans présumer automatiquement d'une faute. Cette auditabilité peut encourager une meilleure discipline opérationnelle si les règles de responsabilité restent juridiquement définies.

14. Transparence proportionnée

La transformation des relations ne nécessite pas une transparence totale. Certaines informations doivent rester privées, confidentielles ou souveraines. Deep Authenticity© doit permettre de démontrer un attribut ou un statut sans révéler davantage que nécessaire lorsque l'architecture et le cadre juridique le permettent.

15. Intelligence artificielle et relations institutionnelles

L'IA peut assister l'analyse de risques, l'orientation des contrôles et la détection d'anomalies. Elle ne doit pas devenir une autorité invisible entre citoyens, entreprises et États. Les décisions significatives nécessitent responsabilité, possibilité d'explication et supervision adaptées au contexte.

16. Autonomie et capacité de contestation

Une infrastructure de confiance devient socialement acceptable lorsque ses utilisateurs peuvent comprendre les preuves essentielles et contester les erreurs. La capacité de recours protège contre la transformation d'un statut technique en décision irrévocable. L'autonomie exige également des solutions de réversibilité et de portabilité.

17. Interopérabilité comme équilibre du pouvoir

L'interopérabilité permet aux acteurs de coopérer sans être enfermés dans un fournisseur unique. Standards, API, export des preuves et architectures fédérées peuvent réduire la dépendance. Cette capacité constitue un élément économique et institutionnel du rééquilibrage entre producteurs, entreprises, citoyens et États.

18. Mesure de la transformation

Les effets doivent être mesurés : délais de service, répétition des justificatifs, litiges, anomalies, satisfaction, adoption, recours, incidents de confidentialité et coûts de conformité. Une hausse du nombre de transactions numériques ne démontre pas, à elle seule, une amélioration de la confiance ou de l'équité.

19. Deep Authenticity© comme médiateur de preuve

Deep Authenticity© peut devenir une couche commune entre acteurs sans devenir leur arbitre universel. Elle relie les preuves, leurs émetteurs, leurs statuts et leur chronologie. Les producteurs continuent de produire, les entreprises d'échanger, les citoyens d'exercer leurs droits et les États de gouverner selon leurs compétences.

20. Critères d'acceptation et conclusion

La transformation des relations par Deep Authenticity© est acceptable si la preuve réduit les asymétries sans supprimer les responsabilités ; si les citoyens disposent de recours ; si les États conservent leurs compétences ; si les entreprises ne sont pas enfermées dans une infrastructure unique ; si la confidentialité est proportionnée ; si l'IA reste gouvernée ; si Authenticity Plus© conserve son architecture fondamentale ; et si l'amélioration des relations est mesurée par des résultats concrets.

La confiance vérifiable ne remplace pas la confiance humaine : elle lui fournit une base plus contrôlable lorsque les échanges deviennent complexes, numériques et transfrontaliers.

Deep Authenticity© peut ainsi transformer la relation économique et institutionnelle en faisant évoluer le modèle « croire l'affirmation » vers le modèle « vérifier la preuve, identifier la responsabilité, conserver le droit de contester ».

Le Chapitre 8 développera les risques géopolitiques, les rapports de puissance et les conditions de neutralité stratégique d'une infrastructure mondiale de vérité vérifiable.

Note d'alignement international

Les orientations de ce chapitre convergent avec les constats internationaux récents sur la transformation numérique : l'interopérabilité, la gouvernance des données, les services centrés sur les personnes, la transparence, les garanties et l'évaluation des résultats sont déterminants pour créer une confiance durable. Deep Authenticity© doit être évaluée selon ces principes sans revendiquer d' alignement ou de reconnaissance institutionnelle automatique.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VIII — STRATÉGIE MONDIALE, IMPACT ET VISION 2040–2050

CHAPITRE 8 — RISQUES GÉOPOLITIQUES, RAPPORTS DE PUISSANCE ET NEUTRALITÉ STRATÉGIQUE

GÉOPOLITIQUE — SOUVERAINETÉ — NEUTRALITÉ — PUISSANCE — DONNÉES — DÉPENDANCE — FÉDÉRATION — RÉSILIENCE — GOUVERNANCE — CONFIANCE

1. Objet du chapitre

Ce chapitre analyse les risques géopolitiques susceptibles d'apparaître lorsqu'une infrastructure de vérité vérifiable atteint une dimension internationale. Deep Authenticity© doit pouvoir relier des systèmes souverains sans devenir un instrument de domination technologique, économique ou politique. Sa crédibilité mondiale dépend donc autant de sa gouvernance que de sa performance technique.

2. La vérité vérifiable comme enjeu de puissance

Les infrastructures qui organisent l'identité, la provenance, la certification et les échanges de preuves peuvent acquérir une importance stratégique. Contrôler les standards, les interfaces ou les mécanismes de confiance peut influencer l'accès aux marchés et aux services. Deep Authenticity© doit anticiper ce risque afin que son expansion ne crée pas une nouvelle concentration de pouvoir.

3. Souveraineté des États

Chaque État conserve ses compétences sur ses registres, autorités, règles de reconnaissance, données souveraines et décisions réglementaires. L'interopérabilité internationale ne doit pas imposer un transfert général de souveraineté. Deep Authenticity© fournit des mécanismes de preuve et de coopération ; elle ne devient pas une autorité supranationale.

4. Neutralité stratégique

La neutralité stratégique signifie que l'infrastructure doit pouvoir être utilisée par des partenaires appartenant à des environnements politiques, économiques et technologiques différents, sous réserve des règles applicables. Cette neutralité repose sur des règles explicites, une gouvernance vérifiable, une séparation des responsabilités et l'absence de discrimination technique arbitraire.

5. Risque de dépendance technologique

Une dépendance excessive à un fournisseur, un cloud, une technologie cryptographique ou une infrastructure d'identité peut devenir un risque souverain. Portabilité, architectures fédérées, standards documentés, capacités de migration et diversité des opérateurs doivent permettre aux participants de maintenir leurs fonctions critiques en cas de changement de fournisseur ou de contexte.

6. Souveraineté des données

L'internationalisation de Deep Authenticity© ne suppose pas la création d'un entrepôt mondial unique. Les données sensibles peuvent rester dans les infrastructures nationales ou institutionnelles, tandis que les preuves ou attributs nécessaires sont échangés. Cette architecture limite l'exposition et facilite l'adaptation aux règles de localisation et de transfert.

7. Risque de fragmentation numérique

Des blocs technologiques incompatibles peuvent émerger lorsque standards, réglementations ou intérêts géopolitiques divergent. Deep Authenticity© doit privilégier des interfaces et mécanismes de traduction permettant une coopération minimale entre environnements différents, sans exiger l' uniformisation complète des systèmes ou des législations.

8. Risque de concentration économique

Si une infrastructure mondiale de vérification devient indispensable aux échanges, son contrôle économique pourrait conférer un pouvoir disproportionné. La séparation entre propriété intellectuelle, exploitation, certification, gouvernance et décision réglementaire contribue à limiter ce risque. Les conditions économiques doivent rester transparentes et réversibles.

9. Authenticity Plus© et souveraineté physique

Dans le domaine physique, l'architecture fondamentale d'Authenticity Plus© reste constituée de trois QR codes fonctionnellement distincts : consommateur, revendeur/professionnel et contrôle/douanes. Les statuts restent VERT — original ; JAUNE — original mais déjà vérifié ou vendu ; ROUGE — contrefaçon ou code inexistant dans le système. Les États conservent leurs pouvoirs de contrôle et de sanction.

10. Corridors de Confiance© et diplomatie

Les Corridors de Confiance© permettent une coopération limitée entre partenaires sans exiger une architecture mondiale préalable. Ils peuvent devenir des instruments de diplomatie économique lorsque leurs règles de reconnaissance, leurs responsabilités et leurs procédures de suspension sont explicites. Leur fédération doit rester volontaire et gouvernée.

11. Sanctions, restrictions et ruptures de coopération

Les relations internationales peuvent être affectées par des sanctions, restrictions commerciales ou ruptures diplomatiques. L'infrastructure doit pouvoir appliquer les obligations légales pertinentes, suspendre certaines relations et préserver les preuves historiques nécessaires à l'audit, sans transformer une mesure ciblée en panne générale du réseau.

12. Cybermenaces géopolitiques

Une infrastructure de confiance internationale peut devenir une cible de cyberespionnage, sabotage ou manipulation. La résilience exige segmentation, redondance, gestion cryptographique, surveillance, réponse aux incidents et exercices réguliers. La sécurité doit être organisée de manière à ce qu'une compromission locale ne produise pas automatiquement une compromission globale.

13. Désinformation et instrumentalisation

La provenance vérifiable peut aider à établir l'origine et l'intégrité de certains contenus, mais elle ne résout pas à elle seule la désinformation. Deep Authenticity© doit éviter d'être utilisée pour transformer une signature d'origine en validation automatique du contenu. La distinction entre provenance, authenticité et vérité factuelle reste fondamentale.

14. Standards et influence internationale

Les standards techniques peuvent devenir des instruments d'influence lorsqu'ils déterminent les conditions d'accès à des marchés ou réseaux. Deep Authenticity© doit rechercher l'interopérabilité avec les standards reconnus et contribuer à des processus ouverts lorsque cela est possible, sans présenter une compatibilité technique comme une reconnaissance institutionnelle.

15. Gouvernance multilatérale

À grande échelle, les décisions concernant référentiels communs, évolutions techniques ou mécanismes de reconnaissance doivent intégrer plusieurs catégories de participants. La gouvernance multilatérale doit empêcher qu'un État, une entreprise ou un groupe limité puisse modifier unilatéralement les règles critiques qui affectent l'ensemble du réseau.

16. Réversibilité géopolitique

Un participant doit pouvoir réduire, suspendre ou quitter certaines relations de confiance sans perdre la capacité de vérifier les preuves historiques nécessaires. Cette réversibilité protège la souveraineté et réduit la possibilité d'utiliser une dépendance technique comme moyen de pression politique ou économique.

17. Continuité en monde fragmenté

Deep Authenticity© doit pouvoir continuer à produire de la valeur même si l'environnement mondial devient plus fragmenté. Des réseaux régionaux, nationaux ou sectoriels peuvent fonctionner de manière autonome et se reconnecter lorsque les conditions le permettent. L'architecture mondiale doit être une fédération de capacités, non une dépendance à un centre unique.

18. Indicateurs de risque géopolitique

La gouvernance peut suivre concentration des fournisseurs, dépendances critiques, localisation des données, incidents transfrontaliers, suspensions de corridors, divergences de standards et obstacles réglementaires. Ces indicateurs permettent d'identifier les vulnérabilités avant qu'elles ne deviennent des crises systémiques.

19. Deep Authenticity© comme infrastructure de neutralité vérifiable

La neutralité ne peut reposer sur une déclaration du concepteur. Elle doit être démontrée par l' architecture : règles connues, auditabilité, séparation des pouvoirs, souveraineté des données, interopérabilité et capacité de sortie. AP Ledger peut ancrer les versions et décisions critiques afin de rendre l'évolution de la gouvernance elle-même vérifiable.

20. Critères d'acceptation et conclusion

La dimension géopolitique de Deep Authenticity© est acceptable si la souveraineté des États reste explicite ; si aucune base mondiale unique n'est obligatoire ; si les dépendances technologiques peuvent être réduites ; si la gouvernance limite la concentration de pouvoir ; si les corridors restent volontaires ; si les sanctions et crises peuvent être isolées ; si la provenance n'est pas confondue avec la vérité factuelle ; si les participants disposent d'une capacité de sortie ; et si la neutralité peut être auditée.

À l'échelle mondiale, la confiance ne peut être durable si l'infrastructure qui la porte devient elle-même un instrument de dépendance.

Deep Authenticity© doit donc viser une neutralité structurelle : permettre à des souverainetés différentes de vérifier des preuves communes sans leur demander de renoncer à leur autonomie stratégique.

Le Chapitre 9 développera la résilience mondiale de Deep Authenticity© face aux crises systémiques, aux ruptures technologiques et aux transformations de long terme.

Note d'alignement international

Les orientations de ce chapitre sont cohérentes avec les enjeux contemporains de souveraineté numérique, d'interopérabilité, de résilience et de réduction des dépendances critiques. L'OCDE souligne en 2026 que les infrastructures numériques publiques ne produisent pleinement leurs effets que lorsque gouvernance, interopérabilité, continuité et soutenabilité sont traitées conjointement.

Toute architecture internationale de Deep Authenticity© devra rester adaptable aux cadres juridiques et géopolitiques applicables.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VIII — STRATÉGIE MONDIALE, IMPACT ET VISION 2040–2050

CHAPITRE 9 — RÉSILIENCE MONDIALE FACE AUX CRISES SYSTÉMIQUES ET AUX RUPTURES TECHNOLOGIQUES

RÉSILIENCE — CONTINUITÉ — CRISES — CYBERSÉCURITÉ — REDONDANCE — INTEROPÉRABILITÉ — MIGRATION — SOUVERAINETÉ — RÉVERSIBILITÉ — ADAPTATION

1. Objet du chapitre

Ce chapitre définit les principes de résilience permettant à Deep Authenticity© de maintenir ses fonctions essentielles face aux crises systémiques, cyberincidents, ruptures de connectivité, défaillances de fournisseurs, transformations technologiques et changements géopolitiques. Une infrastructure de vérité vérifiable ne peut devenir critique sans intégrer la continuité dès sa conception.

2. Résilience comme propriété structurelle

La résilience ne se limite pas à la sauvegarde des données. Elle combine prévention, absorption des chocs, continuité en mode dégradé, récupération et adaptation. Chaque composant critique doit être analysé selon ses dépendances, ses conséquences de défaillance et les capacités nécessaires pour maintenir un niveau minimal de vérification.

3. Cartographie des dépendances

Services cloud, réseaux, identités, clés cryptographiques, registres, fournisseurs, systèmes nationaux et interfaces externes peuvent constituer des dépendances critiques. Deep Authenticity© doit maintenir une cartographie actualisée de ces dépendances afin d'identifier les concentrations, points uniques de défaillance et chaînes de dépendance indirectes.

4. Continuité de l'architecture physique

Dans le domaine physique, Authenticity Plus© doit préserver l'accès aux fonctions essentielles de ses trois QR codes — consommateur, revendeur/professionnel et contrôle/douanes — y compris dans des situations dégradées lorsque l'architecture le permet. Les statuts VERT, JAUNE et ROUGE conservent leur signification et ne doivent pas être artificiellement modifiés pour masquer une indisponibilité.

5. Modes dégradés et fonctionnement hors ligne

Certaines opérations peuvent nécessiter des mécanismes temporaires de vérification hors ligne ou à connectivité limitée. Ces modes doivent être explicitement bornés, utiliser des preuves préalablement sécurisées lorsque possible et prévoir une resynchronisation contrôlée. Une vérification hors ligne ne doit pas être présentée comme équivalente à une consultation complète en temps réel lorsque des informations peuvent avoir changé.

6. Redondance et segmentation

Les fonctions critiques doivent éviter les dépendances uniques lorsque le niveau de risque le justifie. Redondance géographique, segmentation des environnements, réplication contrôlée et séparation des privilèges peuvent limiter la propagation d'un incident. La redondance doit être testée régulièrement plutôt que supposée fonctionnelle.

7. Résilience cryptographique

Les algorithmes, tailles de clés et mécanismes de signature évoluent. Deep Authenticity© doit prévoir inventaire cryptographique, rotation des clés, révocation, migration et coexistence temporaire de mécanismes lorsque nécessaire. Les preuves historiques doivent rester interprétables et vérifiables après une transition technologique.

8. Préparation aux ruptures technologiques

Une technologie aujourd'hui dominante peut devenir obsolète, vulnérable ou incompatible avec de nouvelles exigences. Interfaces modulaires, formats exportables, standards documentés et découplage des composants permettent de remplacer une technologie sans reconstruire l'ensemble de l'infrastructure ni perdre l'historique probant.

9. Cyberincidents majeurs

Une attaque peut viser disponibilité, intégrité, confidentialité ou identité des acteurs. Les procédures doivent définir détection, confinement, communication, investigation, restauration et retour à la normale. Les preuves nécessaires à l'analyse doivent être préservées, et les responsabilités de décision doivent être connues avant l'incident.

10. Continuité des services souverains

Les États et institutions doivent pouvoir maintenir les fonctions relevant de leurs compétences même si un service externe ou une relation internationale devient indisponible. Les architectures nationales peuvent conserver des composants essentiels localement et se resynchroniser avec les réseaux fédérés lorsque les conditions sont rétablies.

11. Ruptures de connectivité

Pannes régionales, catastrophes ou incidents de télécommunication peuvent interrompre l'accès à certains services. Les procédures de continuité déterminent quelles fonctions peuvent être maintenues localement, lesquelles doivent être suspendues et comment les événements différés seront vérifiés lors du rétablissement.

12. Défaillance d’un fournisseur

La disparition, l’insolvabilité ou la rupture contractuelle d’un fournisseur critique ne doit pas rendre les preuves historiques inutilisables. Clauses de réversibilité, formats exportables, documentation, sauvegardes, compétences internes et solutions alternatives permettent d’organiser une transition sans dépendance irréversible.

13. Crises géopolitiques

Sanctions applicables, fermeture de frontières numériques, restrictions de transfert ou rupture de coopération peuvent affecter certains corridors. La fédération permet d’isoler les relations concernées tout en maintenant les autres. Les décisions de suspension doivent être traçables et ne doivent pas détruire les preuves historiques.

14. Crises sanitaires, naturelles et économiques

Des crises non technologiques peuvent provoquer des changements rapides de demande, de mobilité ou de disponibilité des ressources. Les tableaux de bord et jumeaux numériques peuvent contribuer à l’anticipation lorsqu’ils disposent de données fiables. Leurs simulations restent des outils d’aide à la décision et non des prédictions certaines.

15. Qualité et restauration des données

La restauration ne consiste pas seulement à récupérer des fichiers : il faut démontrer leur intégrité, leur version et leur cohérence avec les événements précédents. Des mécanismes de contrôle permettent d’identifier les divergences après restauration et d’éviter qu’une copie ancienne ne réintroduise silencieusement un état invalide.

16. Exercices et tests de résilience

Plans de continuité, sauvegardes et procédures d’urgence doivent être testés. Des exercices périodiques peuvent simuler indisponibilité, perte de fournisseur, compromission de clé ou rupture d’ interopérabilité. Les résultats servent à corriger les procédures, responsabilités et objectifs de récupération.

17. Gouvernance de crise

En situation de crise, les pouvoirs exceptionnels doivent rester définis, temporaires et auditables. Les rôles de décision, les seuils d’escalade, les communications et les conditions de retour au fonctionnement normal doivent être préétablis. L’urgence ne doit pas créer une concentration permanente de pouvoirs techniques.

18. Indicateurs de résilience

Le suivi peut inclure disponibilité, temps de détection, temps de récupération, fréquence des tests, dépendances uniques, réussite des restaurations, incidents de synchronisation et capacité de

migration. Les indicateurs doivent mesurer la continuité réelle et non uniquement l'existence de procédures documentées.

19. Deep Authenticity© et mémoire de crise

Deep Authenticity© peut conserver la chronologie des événements critiques, décisions, suspensions, restaurations et changements de version. AP Ledger peut ancrer certains événements probants afin de faciliter l'audit après crise. Cette mémoire permet de comprendre non seulement ce qui a échoué, mais comment l'infrastructure a réagi et évolué.

20. Critères d'acceptation et conclusion

La résilience mondiale de Deep Authenticity© est acceptable si les dépendances critiques sont identifiées ; si les fonctions essentielles disposent de plans de continuité ; si les modes dégradés sont clairement distingués du fonctionnement normal ; si la redondance est testée ; si la cryptographie peut migrer ; si les États peuvent maintenir leurs fonctions souveraines ; si les fournisseurs peuvent être remplacés ; si les crises peuvent être isolées ; si les pouvoirs d'urgence restent auditables ; et si les preuves historiques survivent aux transformations technologiques.

Une infrastructure mondiale de vérité ne peut être crédible si sa continuité dépend d'un monde sans crises.

Deep Authenticity© doit donc être conçue pour survivre au changement : absorber les ruptures, préserver la preuve, restaurer la confiance et évoluer sans perdre sa mémoire.

Le Chapitre 10 développera la vision civilisationnelle 2040–2050 et la place de Deep Authenticity© comme infrastructure transversale du physique, du numérique et de l'administratif.

Note d'alignement international

Les principes de résilience présentés dans ce chapitre convergent avec les constats de l'OCDE sur les infrastructures numériques : la résilience et la soutenabilité dépendent de choix de gouvernance, d' investissements durables, de responsabilités claires, d'interopérabilité et de capacités de maintenance et d'adaptation. L'existence d'une infrastructure ne suffit pas ; sa continuité et son utilisation effective doivent être démontrées dans le temps.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VIII — STRATÉGIE MONDIALE, IMPACT ET VISION 2040–2050

CHAPITRE 10 — VISION CIVILISATIONNELLE 2040–2050 : DEEP AUTHENTICITY© COMME INFRASTRUCTURE TRANSVERSALE

1. Objet du chapitre

Ce chapitre formule la vision civilisationnelle de Deep Authenticity© à l'horizon 2040–2050. Il examine comment une infrastructure commune de provenance, d'intégrité, de statut et d'historique pourrait relier les domaines physique, numérique et administratif sans devenir une autorité universelle déterminant ce que les sociétés doivent considérer comme vrai.

2. Une civilisation de plus en plus médiée par le numérique

Les activités économiques, administratives, culturelles et sociales reposent progressivement sur des systèmes numériques interconnectés. Dans cet environnement, distinguer une source identifiable, une preuve valide, un objet authentique ou un document émis par une autorité devient une fonction d' infrastructure plutôt qu'un simple service spécialisé.

3. Les trois espaces de la vérité vérifiable

Deep Authenticity© articule trois espaces fondamentaux : le physique, comprenant objets et produits ; le numérique, comprenant logiciels, médias, contenus et propriété intellectuelle ; et l'administratif, comprenant documents, identités et titres. L'infrastructure recherchée rend leurs relations vérifiables tout en respectant les règles propres à chaque domaine.

4. Le physique : identité des objets

Dans le monde physique, la confiance commence par la capacité à relier un objet à une identité numérique protégée. Authenticity Plus© demeure le mécanisme fondamental anti-contrefaçon avec trois QR codes fonctionnellement distincts : consommateur, revendeur/professionnel et contrôle/douanes.

5. Les statuts fondamentaux d'Authenticity Plus©

L'interprétation des trois QR conserve une sémantique simple : VERT signifie original ; JAUNE signifie original mais déjà vérifié ou vendu ; ROUGE signifie contrefaçon ou code inexistant dans le système Authenticity Plus©. Cette simplicité constitue l'interface humaine d'une architecture de preuve plus profonde.

6. Le numérique : provenance à l'ère de l'IA

À mesure que les contenus synthétiques deviennent plus courants, l'origine et l'historique d'un contenu peuvent devenir aussi importants que son apparence. Signatures cryptographiques natives, preuves de provenance et versionnement peuvent aider à établir qui a émis ou modifié un élément. Ils ne déterminent pas automatiquement la vérité de son message.

7. L'administratif : continuité institutionnelle

Documents, identités, certificats et titres peuvent être reliés à leurs autorités d'émission et à leurs statuts. Deep Authenticity© peut faciliter la vérification entre administrations et territoires sans remplacer les registres souverains ni les procédures qui déterminent la valeur juridique de ces éléments.

8. Le passeport numérique universel

Le passeport numérique peut devenir le point de continuité d'un produit, actif ou élément vérifiable à travers son cycle de vie. Il peut agréger des références vers identité, provenance, certifications, événements et droits selon des accès différenciés. Son universalité signifie interopérabilité, non accumulation universelle de données.

9. Une couche commune entre systèmes

La vision 2040–2050 n'exige pas le remplacement des ERP, registres publics, plateformes sectorielles ou systèmes nationaux. Deep Authenticity© se positionne comme une couche de relation entre ces infrastructures, permettant d'échanger des preuves et d'interpréter leurs statuts selon des règles connues.

10. Souveraineté dans un monde interconnecté

Plus les systèmes deviennent interconnectés, plus la souveraineté doit être explicitement protégée. États et institutions doivent pouvoir conserver leurs données sensibles, leurs autorités et leurs règles tout en participant à des mécanismes communs de vérification. L'interopérabilité doit relier les souverainetés plutôt que les dissoudre.

11. De la donnée à la preuve

L'abondance de données ne produit pas automatiquement de la confiance. Une donnée devient plus utile lorsqu'elle peut être reliée à une source, une signature, un contexte, une date et une autorité identifiable. Deep Authenticity© vise cette transformation : passer d'un monde saturé d'informations à un monde capable de distinguer plus rigoureusement les éléments probants.

12. Citoyen et autonomie informationnelle

Dans cette vision, le citoyen n'est pas seulement un sujet vérifié par les institutions. Il doit également pouvoir vérifier les produits, documents et contenus qui influencent ses décisions, comprendre l' origine des preuves et contester les erreurs. La confiance vérifiable doit augmenter l'autonomie plutôt que créer une surveillance permanente.

13. Entreprises et responsabilité vérifiable

Les entreprises peuvent rendre plus contrôlables l'origine de leurs produits, certains engagements, certifications et événements de chaîne de valeur. Cette auditabilité peut transformer la responsabilité économique : les déclarations importantes deviennent progressivement accompagnées de preuves dont la portée et l'émetteur sont identifiables.

14. États et capacité d’anticipation

Les États peuvent exploiter des données vérifiées et agrégées pour améliorer tableaux de bord, détection de pénuries, rappels, analyses de flux et jumeaux numériques. La Simulation Institutionnelle Profonde peut soutenir l’évaluation de scénarios avant décision, tout en distinguant strictement observation, estimation, simulation et décision politique.

15. Intelligence artificielle au service de la vérité vérifiable

L’IA peut détecter des anomalies, analyser des relations complexes et aider à interpréter de grands volumes d’événements. Elle reste une couche d’assistance. La vision civilisationnelle de Deep Authenticity© repose sur la combinaison entre preuve, gouvernance et analyse, non sur la délégation de la vérité à un modèle algorithmique.

16. Infrastructure et droits fondamentaux

Une infrastructure transversale doit intégrer protection des données, proportionnalité, sécurité, accessibilité, non-discrimination et recours. La capacité technique de relier davantage d’informations ne constitue pas une justification suffisante pour le faire. Les finalités et pouvoirs doivent rester bornés par des règles légitimes.

17. Résilience de long terme

Une infrastructure conçue pour plusieurs décennies doit survivre aux changements de technologies, fournisseurs, standards et rapports géopolitiques. Modularité, fédération, migration cryptographique, réversibilité et conservation des preuves historiques permettent de maintenir la continuité sans figer l’architecture dans les choix techniques de 2026.

18. Le système d’exploitation de la civilisation moderne

Au niveau conceptuel le plus élevé, Deep Authenticity© peut être décrite comme « le système d’exploitation de la civilisation moderne » : non parce qu’elle commanderait la société, mais parce qu’elle fournirait une couche commune permettant aux objets, contenus, documents, droits, institutions et acteurs d’établir des relations vérifiables entre leurs mondes respectifs.

19. Limites de l’ambition universelle

L’universalité doit rester une ambition d’interopérabilité et non de pouvoir. Deep Authenticity© ne peut déterminer seule la vérité scientifique, politique, historique, juridique ou morale. Elle peut démontrer qu’un élément a été émis, signé, enregistré, transféré ou certifié par une source identifiable, puis préserver la chronologie de cette preuve.

20. Critères d’acceptation et conclusion

La vision civilisationnelle de Deep Authenticity© est acceptable si les trois domaines restent clairement distingués ; si Authenticity Plus© demeure la fondation du domaine physique ; si l’universalité signifie interopérabilité plutôt que centralisation ; si les États conservent leur

souveraineté ; si les citoyens conservent leurs droits et recours ; si l'IA reste distincte de la preuve ; si l'infrastructure peut évoluer sur plusieurs décennies ; et si ses limites sont explicitement reconnues.

À l'horizon 2040–2050, la question centrale pourrait ne plus être seulement : « disposons-nous de l'information ? », mais : « pouvons-nous établir d'où elle vient, ce qui lui est arrivé, qui en répond et quelles preuves permettent de lui faire confiance ? »

Deep Authenticity© propose une réponse architecturale à cette question en reliant le physique, le numérique et l'administratif par une infrastructure commune de vérité vérifiable.

Le Chapitre 11 développera les principes d'une gouvernance civilisationnelle de long terme, afin que l'expansion de cette infrastructure demeure compatible avec la liberté, la souveraineté, la pluralité et la responsabilité.

Note d'alignement international

La vision 2040–2050 présentée dans ce chapitre est prospective. Elle décrit une architecture possible de confiance vérifiable et non une prévision certaine de l'évolution des sociétés. Toute mise en œuvre devra rester compatible avec les droits fondamentaux, les cadres souverains, les standards applicables, les mécanismes démocratiques de responsabilité et l'évolution des technologies.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VIII — STRATÉGIE MONDIALE, IMPACT ET VISION 2040–2050

CHAPITRE 11 — GOUVERNANCE CIVILISATIONNELLE DE LONG TERME : LIBERTÉ, SOUVERAINETÉ, PLURALITÉ ET RESPONSABILITÉ

GOUVERNANCE — LIBERTÉ — SOUVERAINETÉ — PLURALITÉ — RESPONSABILITÉ — DROITS — CONTRE-POUVOIRS — AUDIT — RÉVERSIBILITÉ — LONG TERME

1. Objet du chapitre

Ce chapitre définit les principes de gouvernance nécessaires si Deep Authenticity© devient, à long terme, une infrastructure transversale reliant les domaines physique, numérique et administratif. Plus une infrastructure devient importante pour la société, plus ses pouvoirs, responsabilités, limites et mécanismes de contrôle doivent être explicitement organisés.

2. Gouverner l'infrastructure sans gouverner la société

Deep Authenticity© doit gouverner ses protocoles, preuves, interfaces et règles opérationnelles sans devenir une autorité générale sur les personnes, les institutions ou les opinions. La distinction entre

gouvernance de l'infrastructure et gouvernement de la société constitue une protection fondamentale contre l'extension indéfinie de son mandat.

3. Primauté de la liberté

La vérification doit augmenter la capacité d'agir des personnes plutôt que conditionner chaque activité à une autorisation numérique. Les citoyens doivent conserver des espaces d'autonomie, des possibilités de recours et, lorsque le contexte le permet, des alternatives aux mécanismes automatisés. L'efficacité technique ne justifie pas la suppression de libertés fondamentales.

4. Souveraineté des États

Les États conservent leurs compétences constitutionnelles, administratives, judiciaires et réglementaires. Deep Authenticity© peut faciliter l'échange et la vérification de preuves, mais ne peut créer par elle-même une autorité juridique supérieure. Les règles de reconnaissance internationale doivent résulter de cadres légitimes et explicitement acceptés.

5. Pluralité institutionnelle

Une infrastructure universelle doit pouvoir coexister avec plusieurs systèmes juridiques, cultures administratives, standards et modèles économiques. L'interopérabilité vise à créer des points de compréhension commune sans imposer l'uniformité. La pluralité devient ainsi une propriété de conception et non un obstacle à éliminer.

6. Séparation des pouvoirs techniques

Émission des identités, exploitation des infrastructures, certification, audit, gouvernance des standards et décisions réglementaires ne doivent pas être automatiquement concentrés entre les mêmes mains. Une séparation adaptée des rôles limite les conflits d'intérêts et réduit le risque qu'un opérateur technique devienne juge de sa propre conformité.

7. Gouvernance d'Authenticity Plus©

Dans le domaine physique, la gouvernance doit protéger l'architecture fondamentale d'Authenticity Plus© : trois QR codes fonctionnellement distincts — consommateur, revendeur/professionnel et contrôle/douanes — et les statuts VERT — original ; JAUNE — original mais déjà vérifié ou vendu ; ROUGE — contrefaçon ou code inexistant dans le système Authenticity Plus©.

8. Gouvernance des évolutions

Les protocoles et référentiels évolueront avec les technologies et les risques. Les changements importants doivent être versionnés, documentés, testés et soumis à une procédure de décision proportionnée à leur impact. Les participants doivent disposer d'un délai et d'informations suffisantes pour préparer les migrations significatives.

9. Auditabilité de la gouvernance

La gouvernance elle-même doit produire des preuves. Décisions critiques, modifications de référentiels, suspensions, habilitations et changements de version peuvent être enregistrés de manière vérifiable. AP Ledger peut contribuer à préserver cette chronologie afin que l'infrastructure puisse être auditée non seulement techniquement, mais institutionnellement.

10. Contre-pouvoirs et supervision

Une infrastructure à forte portée doit accepter la supervision. Audits indépendants, comités spécialisés, autorités compétentes, mécanismes de recours et publication d'indicateurs peuvent constituer des contre-pouvoirs adaptés. Leur composition et leurs pouvoirs doivent éviter une supervision purement symbolique.

11. Protection contre la capture

Une infrastructure mondiale peut être exposée à la capture par un État, un groupe économique, un fournisseur ou une coalition d'intérêts. Diversité de représentation, règles de conflits d'intérêts, transparence des décisions et capacité de sortie réduisent ce risque. Aucun participant ne doit pouvoir modifier seul les règles critiques communes.

12. Gouvernance des données

La gouvernance doit distinguer propriété, responsabilité, accès, conservation, partage et suppression des données. La participation à Deep Authenticity© ne doit pas transférer automatiquement la maîtrise des données sources à l'opérateur de l'infrastructure. La minimisation et la souveraineté restent des principes structurants.

13. Gouvernance de l'intelligence artificielle

Les modèles d'IA utilisés pour détecter des anomalies, produire des analyses ou assister les décisions doivent être gouvernés selon leur niveau de risque. Provenance des données, performance, limites, supervision et procédures de contestation doivent être documentées lorsque leurs résultats peuvent affecter significativement un acteur.

14. Droit à la contestation

Une infrastructure de vérité vérifiable doitreconnaître qu'une donnée, une association ou un statut peut être erroné. Les personnes et organisations concernées doivent disposer de procédures permettant de signaler une erreur, fournir des preuves et obtenir une révision lorsque les règles applicables le prévoient.

15. Réversibilité et droit de sortie

La capacité de quitter un fournisseur, un service ou certaines relations de confiance constitue un mécanisme de gouvernance. Les preuves nécessaires, formats documentés et historiques doivent pouvoir être conservés ou transférés selon les droits applicables. La dépendance irréversible est incompatible avec une infrastructure fondée sur la souveraineté.

16. Gouvernance intergénérationnelle

Une infrastructure conçue pour plusieurs décennies doit éviter de lier les générations futures aux décisions techniques ou économiques de sa création. Standards évolutifs, clauses de réexamen, migrations et évaluations périodiques permettent de remettre en question les choix devenus inadaptés.

17. Légitimité par les résultats

La légitimité ne peut reposer uniquement sur la sophistication technologique. Elle doit être soutenue par des résultats : réduction d'erreurs ou de fraudes, amélioration de l'accès à la preuve, protection des droits, résilience et satisfaction des acteurs. Les effets indésirables doivent être publiés et corrigés.

18. Gouvernance en situation exceptionnelle

Crises, cyberattaques ou ruptures majeures peuvent nécessiter des décisions rapides. Les pouvoirs d' urgence doivent être prédéfinis, temporaires, proportionnés et auditables. Leur expiration et le retour aux procédures normales doivent être organisés afin d'éviter qu'une exception ne devienne un mode permanent.

19. Pacte civilisationnel de confiance

À maturité, la gouvernance de Deep Authenticity© peut être comprise comme un pacte de confiance : aucune autorité unique ne possède la vérité ; les preuves ont une provenance identifiable ; les pouvoirs sont bornés ; les souverainetés peuvent coopérer ; les citoyens conservent leurs droits ; et l' infrastructure reste contestable, auditable et réversible.

20. Critères d'acceptation et conclusion

La gouvernance civilisationnelle de Deep Authenticity© est acceptable si l'infrastructure ne se confond pas avec le gouvernement de la société ; si les libertés et souverainetés sont préservées ; si la pluralité institutionnelle est possible ; si les pouvoirs techniques sont séparés ; si les évolutions sont auditables ; si des contre-pouvoirs existent ; si la capture peut être combattue ; si les erreurs peuvent être contestées ; si la sortie reste possible ; et si les générations futures peuvent réviser les choix hérités.

Une infrastructure de vérité ne mérite la confiance que si ceux qui la gouvernent peuvent eux-mêmes être contrôlés.

La vision de Deep Authenticity© comme système d'exploitation de la civilisation moderne exige donc une architecture de responsabilité aussi ambitieuse que son architecture technique.

Le Chapitre 12 développera l'héritage stratégique 2050 et au-delà : transmission, évolution et pérennité de Deep Authenticity© à travers les générations.

Note d'alignement international

Cette gouvernance de long terme est formulée comme un cadre prospectif. Sa mise en œuvre devra s' adapter aux systèmes constitutionnels, aux droits fondamentaux, aux règles de protection des données, aux régimes de responsabilité et aux mécanismes de supervision applicables dans chaque juridiction. L'interopérabilité institutionnelle ne vaut jamais transfert automatique de compétence.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VIII — STRATÉGIE MONDIALE, IMPACT ET VISION 2040–2050

CHAPITRE 12 — HÉRITAGE STRATÉGIQUE 2050 ET AU-DELÀ : TRANSMISSION, ÉVOLUTION ET PÉRENNITÉ

HÉRITAGE — 2050+ — TRANSMISSION — PÉRENNITÉ — ÉVOLUTION — MÉMOIRE — STANDARDS — GÉNÉRATIONS — SOUVERAINETÉ — CONTINUITÉ

1. Objet du chapitre

Ce chapitre examine la pérennité de Deep Authenticity© au-delà de l'horizon 2050. Une infrastructure conçue pour soutenir durablement la vérité vérifiable doit pouvoir être transmise, maintenue, transformée et, si nécessaire, remplacée partiellement sans perdre les preuves, les droits, les responsabilités et la mémoire accumulés au fil du temps.

2. De la création à l'héritage

La réussite de long terme ne se mesure pas uniquement à l'adoption initiale. Elle dépend de la capacité de l'infrastructure à continuer de produire de la valeur lorsque ses fondateurs, technologies, opérateurs et environnements réglementaires auront changé. L'héritage stratégique commence donc par la préparation consciente de la succession.

3. Préserver les principes, faire évoluer les technologies

Les technologies utilisées en 2026 ne doivent pas devenir des contraintes permanentes. Deep Authenticity© doit préserver ses principes structurants — provenance, intégrité, traçabilité, souveraineté, interopérabilité, auditabilité et réversibilité — tout en permettant le remplacement progressif des composants devenus obsolètes.

4. Pérennité d'Authenticity Plus©

Dans le domaine physique, l'évolution doit préserver la fonction fondamentale de l'architecture d' Authenticity Plus© : trois QR codes fonctionnellement distincts pour le consommateur, le revendeur/professionnel et le contrôle/douanes. Toute évolution technologique doit maintenir la séparation fonctionnelle et le niveau de protection recherché.

5. Continuité des statuts

Les statuts fondamentaux doivent conserver une interprétation stable pour les utilisateurs : VERT signifie original ; JAUNE signifie original mais déjà vérifié ou vendu ; ROUGE signifie contrefaçon ou code inexistant dans le système Authenticity Plus©. Les interfaces futures peuvent évoluer sans rendre ambiguë cette sémantique centrale.

6. Mémoire numérique de long terme

Les preuves historiques doivent rester interprétables malgré l'évolution des formats, logiciels et infrastructures. Archivage, métadonnées, documentation des versions, mécanismes de migration et vérification d'intégrité sont nécessaires pour éviter qu'un événement ancien devienne techniquement illisible ou institutionnellement incompréhensible.

7. Migration cryptographique

Les mécanismes cryptographiques devront évoluer face aux nouvelles capacités de calcul et aux découvertes scientifiques. L'infrastructure doit prévoir inventaire des algorithmes, périodes de transition, renouvellement des clés, re-signature lorsque nécessaire et conservation de la preuve du contexte cryptographique applicable au moment de l'événement.

8. Transmission institutionnelle

Les connaissances nécessaires à l'exploitation ne doivent pas dépendre d'un nombre limité de personnes. Documentation, procédures, formation, gouvernance des compétences et mécanismes de succession doivent permettre aux institutions futures de comprendre les choix réalisés et d'exercer leurs responsabilités de manière autonome.

9. Transmission du savoir-faire

L'héritage comprend l'architecture, mais aussi les méthodes : analyse des risques, intégration, certification, réponse aux incidents, gouvernance des preuves et coopération internationale. Ces connaissances doivent être organisées de façon à pouvoir être enseignées, auditées et améliorées par de nouvelles générations de professionnels.

10. Standards et interopérabilité dans le temps

Les standards évoluent et certains disparaissent. Deep Authenticity© doit éviter de confondre interopérabilité avec fidélité éternelle à un format. Des couches d'adaptation, mécanismes de conversion et profils versionnés doivent permettre aux preuves anciennes et nouvelles de coexister pendant les périodes de transition.

11. Gouvernance intergénérationnelle

Les générations futures doivent pouvoir réviser les choix qui ne correspondent plus à leurs besoins, tout en préservant les droits et preuves légitimement acquis. Des cycles de réexamen, évaluations

indépendantes et procédures de modification constitutionnelle de la gouvernance peuvent empêcher la fossilisation de l'infrastructure.

12. Préservation de la souveraineté

La transmission internationale ne doit pas conduire à une dilution progressive des souverainetés. Les États et institutions doivent conserver la possibilité d'adapter leurs composants, de migrer leurs données et de redéfinir certaines relations de confiance selon les règles applicables, sans perdre l' accès à leur propre histoire probante.

13. Pérennité économique

Une infrastructure de plusieurs décennies nécessite un modèle économique capable de financer sécurité, maintenance, migrations, support, recherche et gouvernance. Les revenus doivent être suffisamment diversifiés pour éviter qu'une crise d'un seul secteur ou partenaire ne compromette les fonctions essentielles.

14. Recherche et innovation continue

La pérennité dépend d'une capacité permanente d'apprentissage. Cryptographie, intelligence artificielle, identité, réseaux, matériels sécurisés et sciences de la donnée continueront d'évoluer. La recherche doit tester les innovations avant leur adoption et distinguer progrès réel, effet de mode et risque de dépendance.

15. Préservation des droits dans le temps

Un droit, une propriété ou une certification peut survivre à plusieurs générations de systèmes informatiques. Les migrations doivent préserver la possibilité d'établir la chaîne des preuves et les changements de statut. La modernisation technique ne doit pas effacer silencieusement des droits ou responsabilités historiques.

16. Scénarios de succession technologique

Deep Authenticity© doit envisager plusieurs futurs : évolution progressive de la plateforme, fédération avec de nouvelles infrastructures, remplacement de composants majeurs ou transfert de certaines fonctions vers des standards devenus universels. La réussite peut donc inclure la capacité à transmettre une fonction au-delà de la technologie qui l'a initialement portée.

17. Préparation aux ruptures civilisationnelles

Des transformations majeures — nouvelles formes d'identité, informatique post-quantique, autonomisation des agents numériques ou changements profonds du commerce — peuvent modifier les besoins de preuve. L'architecture doit pouvoir absorber ces ruptures sans abandonner ses principes de responsabilité, provenance et contrôle.

18. Indicateurs de pérennité

La pérennité peut être suivie par la capacité de migration, la lisibilité des preuves anciennes, la diversité des compétences, la dépendance aux fournisseurs, la fréquence des réexamens, la soutenabilité financière et le succès des exercices de succession. Ces indicateurs mesurent la capacité à durer, non simplement l'âge de l'infrastructure.

19. Héritage civilisationnel de Deep Authenticity©

L'héritage le plus durable ne serait pas nécessairement une plateforme ou une marque, mais un principe devenu normal : toute affirmation critique concernant un objet, un contenu ou un document devrait pouvoir être reliée à une provenance, une responsabilité et des preuves vérifiables. Deep Authenticity© aurait alors contribué à installer une culture durable de la preuve.

20. Critères d'acceptation et conclusion

L'héritage stratégique de Deep Authenticity© est acceptable si les technologies peuvent évoluer sans perdre les principes ; si les preuves historiques restent vérifiables ; si Authenticity Plus© conserve son architecture fondamentale dans le domaine physique ; si les compétences peuvent être transmises ; si les générations futures peuvent réviser la gouvernance ; si la souveraineté et les droits survivent aux migrations ; si le modèle économique finance la maintenance de long terme ; et si l'infrastructure peut transmettre ses fonctions même au-delà de ses technologies initiales.

La pérennité ne consiste pas à empêcher le changement. Elle consiste à permettre au changement de se produire sans perdre la mémoire, la preuve et la responsabilité.

À l'horizon 2050 et au-delà, la réussite de Deep Authenticity© pourra donc se mesurer à sa capacité à devenir transmissible : une infrastructure capable d'évoluer avec la civilisation plutôt que de chercher à la figer.

Le Chapitre 13 développera la stratégie d'impact mondial à long terme et les indicateurs permettant d'évaluer, sur plusieurs décennies, la contribution réelle de Deep Authenticity© à la confiance, à la sécurité et à la prospérité.

Note d'alignement international

La perspective 2050 et au-delà est volontairement prospective. Elle ne suppose ni permanence des technologies actuelles ni adoption universelle de Deep Authenticity©. Elle établit des principes de transmission, de réversibilité, de migration et de préservation des preuves destinés à maintenir la valeur de l'infrastructure dans plusieurs futurs possibles.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VIII — STRATÉGIE MONDIALE, IMPACT ET VISION 2040–2050

CHAPITRE 13 — STRATÉGIE D'IMPACT MONDIAL À LONG TERME ET INDICATEURS DE CONTRIBUTION

IMPACT — CONFIANCE — SÉCURITÉ — PROSPÉRITÉ — INDICATEURS — MESURE — ATTRIBUTION — TRANSPARENCE — ÉVALUATION — LONG TERME

1. Objet du chapitre

Ce chapitre établit un cadre permettant de mesurer, sur plusieurs décennies, la contribution réelle de Deep Authenticity© à la confiance, à la sécurité et à la prospérité. Une ambition mondiale ne peut être évaluée par le seul nombre d'utilisateurs, de scans ou de territoires couverts : elle doit être reliée à des résultats observables, comparables et auditables.

2. De l'ambition à l'impact démontré

La stratégie d'impact distingue les intentions, les activités, les résultats immédiats et les effets de long terme. Déployer une infrastructure ne prouve pas qu'elle a réduit la fraude, amélioré la confiance ou créé de la prospérité. Chaque affirmation d'impact significative doit être accompagnée d' indicateurs, d'une période de référence et d'une méthode d'évaluation.

3. Trois dimensions fondamentales

Le cadre retient trois dimensions transversales : confiance, sécurité et prospérité. La confiance mesure la capacité à établir des preuves compréhensibles et utilisables ; la sécurité mesure la réduction des risques et la résilience ; la prospérité mesure la valeur économique et sociale créée ou protégée sans négliger sa distribution.

4. Indicateurs de confiance

Les indicateurs peuvent inclure taux de vérification aboutie, compréhension des statuts, réutilisation de preuves, délais de vérification, erreurs corrigées, recours, satisfaction et confiance déclarée. Les mesures perceptives doivent être distinguées des preuves comportementales et des résultats opérationnels.

5. Indicateurs de sécurité

La sécurité peut être suivie par anomalies qualifiées, incidents, contrefaçons détectées, compromissions, temps de détection, temps de récupération, faux positifs, disponibilité et réussite des exercices de continuité. L'objectif est de mesurer la capacité à prévenir, détecter, contenir et récupérer.

6. Indicateurs de prospérité

La contribution économique peut être évaluée par coûts de contrôle évités, délais réduits, valeur protégée, accès aux marchés, efficacité des rappels, réduction de certains litiges, productivité administrative et participation des petites structures. Les bénéfices doivent être comparés aux coûts d'intégration, d'exploitation et de conformité.

7. Authenticity Plus© et impact du domaine physique

Dans le domaine physique, l'évaluation doit partir de l'architecture fondamentale d'Authenticity Plus© : QR consommateur, QR revendeur/professionnel et QR contrôle/douanes. Les statuts restent VERT — original ; JAUNE — original mais déjà vérifié ou vendu ; ROUGE — contrefaçon ou code inexistant dans le système Authenticity Plus©.

8. Mesure de la lutte anti-contrefaçon

L'impact anti-contrefaçon doit distinguer détection, prévention, déplacement du risque et réduction effective. Le nombre de codes rouges ou d'anomalies ne suffit pas : il faut examiner les faux confirmés, les circuits affectés, les récidives, les délais d'intervention et l'évolution du risque dans les périmètres couverts.

9. Impact du domaine numérique

Dans le numérique, les indicateurs peuvent mesurer contenus signés, provenance vérifiable, altérations détectées, versions correctement reliées et délais d'établissement de l'origine. Ils ne doivent pas présenter la provenance comme une mesure automatique de vérité factuelle ou de qualité du contenu.

10. Impact du domaine administratif

Dans l'administratif, l'évaluation peut porter sur justificatifs réutilisés, délais de traitement, documents falsifiés détectés, erreurs corrigées, taux d'interopérabilité et satisfaction des usagers. Les gains de rapidité doivent être mis en balance avec accessibilité, recours, protection des données et qualité des décisions.

11. Inclusion et distribution des bénéfices

Un impact mondial positif suppose que la valeur ne soit pas concentrée uniquement chez les grandes organisations. Les tableaux de bord doivent distinguer adoption et bénéfices pour PME, artisans, producteurs indépendants, citoyens et territoires à capacités numériques différentes. L'inclusion est une dimension de l'impact, non un indicateur périphérique.

12. Souveraineté et impact institutionnel

La contribution institutionnelle peut être mesurée par capacité à conserver les données localement, réduction des dépendances uniques, nombre de systèmes interopérables et réussite des migrations ou sorties. Une infrastructure mondiale ne doit pas considérer l'augmentation de la centralisation comme un indicateur positif par défaut.

13. Corridors de Confiance©

Les corridors peuvent être évalués par volumes couverts, preuves reconnues, temps de contrôle, incidents, litiges, disponibilité, adoption des opérateurs et extension à de nouveaux cas d'usage. Leur

réussite doit être démontrée bilatéralement ou régionalement avant d'être extrapolée à une performance mondiale.

14. Méthodes d'attribution

Les changements économiques et sociaux résultent rarement d'une seule intervention. Les évaluations doivent distinguer contribution et causalité. Comparaisons avant/après, groupes de référence lorsque possibles, analyses sectorielles et documentation des facteurs externes permettent d'éviter d'attribuer automatiquement à Deep Authenticity© toute amélioration observée.

15. Qualité des données d'impact

Les indicateurs ne sont crédibles que si les données sources sont suffisamment complètes, cohérentes et documentées. Définitions, périodes, périmètres, méthodes de calcul et changements de version doivent être conservés. AP Ledger peut ancrer les versions critiques de certains référentiels et résultats afin d'améliorer leur auditabilité.

16. Transparence des résultats

Les résultats favorables et défavorables doivent être traités avec la même rigueur. Incidents, limites, effets inattendus et objectifs non atteints constituent des informations nécessaires à l'amélioration. Une stratégie d'impact crédible évite de transformer le tableau de bord en instrument de communication sélective.

17. Tableaux de bord multi-échelles

Les indicateurs peuvent être organisés aux niveaux produit, entreprise, secteur, territoire, État, corridor et réseau international. Chaque niveau doit disposer de métriques adaptées et de règles d'agrégation. Les comparaisons internationales doivent tenir compte des différences de périmètre, de maturité et de réglementation.

18. Horizon décennal et révision

Des évaluations annuelles peuvent suivre l'exploitation, tandis que des revues pluriannuelles examinent les effets structurels. Les objectifs 2030, 2040, 2050 et au-delà doivent pouvoir être révisés lorsque les hypothèses changent. La stratégie de mesure doit survivre aux évolutions technologiques sans figer des indicateurs devenus obsolètes.

19. Tableau de contribution civilisationnelle

À très long terme, un tableau de contribution peut synthétiser plusieurs dimensions : authenticité des échanges, qualité de la provenance numérique, fiabilité administrative, autonomie des citoyens, résilience institutionnelle, inclusion économique et interopérabilité souveraine. Il doit rester un outil d' évaluation et non un classement absolu des sociétés.

20. Critères d'acceptation et conclusion

La stratégie d'impact mondial de Deep Authenticity© est acceptable si elle distingue activité et résultat ; si confiance, sécurité et prospérité sont mesurées séparément ; si les coûts et effets indésirables sont inclus ; si l'attribution reste prudente ; si les petites structures et citoyens sont visibles dans les indicateurs ; si Authenticity Plus© conserve son architecture fondamentale ; si les données d'impact sont auditables ; et si les objectifs de long terme peuvent être révisés.

Une infrastructure mondiale ne devient pas importante parce qu'elle affirme transformer le monde, mais parce qu'elle peut démontrer où, comment et dans quelles limites elle améliore réellement la confiance, la sécurité et la prospérité.

Deep Authenticity© doit ainsi faire de la mesure de son propre impact une composante de sa responsabilité institutionnelle.

Le Chapitre 14 développera la doctrine mondiale de confiance vérifiable et les principes susceptibles de guider l'adoption de Deep Authenticity© par des sociétés, institutions et économies différentes.

Note d'alignement international

Le cadre d'impact présenté dans ce chapitre privilégie la mesure, la transparence méthodologique et la prudence d'attribution. Les indicateurs proposés devront être adaptés à chaque secteur et juridiction. Les scénarios économiques ou civilisationnels ne doivent pas être présentés comme des résultats constatés avant l'existence de données empiriques suffisantes.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VIII — STRATÉGIE MONDIALE, IMPACT ET VISION 2040–2050

CHAPITRE 14 — DOCTRINE MONDIALE DE CONFIANCE VÉRIFIABLE : PRINCIPES UNIVERSELS D'ADOPTION

DOCTRINE — CONFIANCE — PREUVE — UNIVERSALITÉ — SOUVERAINETÉ — PROPORTIONNALITÉ — INTEROPÉRABILITÉ — DROITS — RESPONSABILITÉ — ADOPTION

1. Objet du chapitre

Ce chapitre formule une doctrine mondiale de confiance vérifiable destinée à guider l'adoption de Deep Authenticity© dans des sociétés, économies et institutions différentes. Cette doctrine ne cherche pas à uniformiser les systèmes juridiques ou culturels : elle définit un noyau de principes permettant à des acteurs hétérogènes de partager des preuves compréhensibles et contrôlables.

2. Principe de vérifiabilité

Une affirmation critique doit, lorsque cela est possible et proportionné, pouvoir être reliée à une provenance, un émetteur, une date, un statut et des éléments probants. La vérifiabilité ne signifie pas que toute réalité peut être réduite à une donnée technique ; elle signifie que la portée exacte de ce qui est démontré doit pouvoir être comprise.

3. Principe de séparation entre preuve et jugement

Deep Authenticity© établit ou transporte des preuves ; elle ne remplace pas le jugement humain, scientifique, administratif ou judiciaire. Une signature peut démontrer l'origine d'un document sans démontrer la vérité de toutes ses affirmations. Cette séparation protège l'infrastructure contre une extension abusive de sa fonction.

4. Principe de souveraineté

Chaque État et institution conserve ses compétences, registres, autorités et règles de reconnaissance. L'adoption de Deep Authenticity© doit pouvoir s'effectuer sans transfert automatique de souveraineté. Les preuves transfrontalières ne produisent des effets que dans les conditions reconnues par les cadres applicables.

5. Principe d'interopérabilité

L'universalité recherchée repose sur la capacité de systèmes différents à comprendre et vérifier des éléments communs. API, formats structurés, identités, signatures et profils de reconnaissance doivent limiter l'enfermement technologique. L'interopérabilité ne requiert ni base mondiale unique ni uniformité totale des infrastructures.

6. Principe de proportionnalité

Le niveau d'identification, de traçabilité, de conservation et de contrôle doit correspondre au risque et à la finalité. Un produit courant, un médicament, un titre de propriété ou une identité administrative ne nécessitent pas nécessairement les mêmes garanties. La doctrine rejette l'application indifférenciée du niveau maximal de contrôle.

7. Principe fondamental d'Authenticity Plus©

Dans le domaine physique, la doctrine conserve l'architecture fondamentale d'Authenticity Plus© : trois QR codes fonctionnellement distincts — consommateur, revendeur/professionnel et contrôle/douanes. Les technologies complémentaires peuvent renforcer ce mécanisme, mais ne doivent pas en effacer la logique centrale.

8. Principe universel des statuts

L'interprétation utilisateur demeure stable : VERT signifie original ; JAUNE signifie original mais déjà vérifié ou vendu ; ROUGE signifie contrefaçon ou code inexistant dans le système Authenticity Plus©. Une sémantique stable réduit l'ambiguïté et permet une compréhension commune à travers les secteurs et territoires.

9. Principe de minimisation des données

La preuve nécessaire doit être distinguée de la totalité des données disponibles. Lorsqu'un attribut suffit, l'infrastructure ne doit pas exiger automatiquement l'accès à l'ensemble du dossier. La minimisation réduit les risques de surveillance, de fuite, de détournement de finalité et de dépendance informationnelle.

10. Principe de responsabilité identifiable

Une preuve utile doit permettre de comprendre qui a émis, certifié, modifié ou validé l'élément pertinent selon les règles applicables. L'auditabilité ne signifie pas culpabilité automatique : elle rend la chaîne de responsabilité plus visible et permet aux procédures compétentes d'examiner les faits.

11. Principe de contestabilité

Aucun statut technique ne doit devenir incontestable lorsqu'il peut produire des effets significatifs. Les mécanismes doivent permettre de signaler une erreur, présenter des éléments probants et obtenir une révision selon les droits applicables. La contestabilité constitue une condition de légitimité de la confiance vérifiable.

12. Principe de transparence des niveaux d'assurance

Toutes les preuves n'offrent pas le même niveau d'assurance. Une déclaration d'entreprise, une certification tierce, une signature cryptographique et une décision administrative doivent être distinguées. L'interface et les API doivent permettre de comprendre la source, la portée, la validité et les limites du niveau présenté.

13. Principe de neutralité technologique

La doctrine doit survivre aux technologies qui la mettent en œuvre. QR codes, NFC, capteurs, registres distribués, cryptographie ou nouvelles interfaces peuvent évoluer. Les choix techniques doivent être évalués selon sécurité, accessibilité, interopérabilité, coût, réversibilité et adéquation au risque.

14. Principe de résilience

Une infrastructure de confiance doit continuer à produire des preuves utiles en présence de pannes, cyberattaques, ruptures de connectivité ou changements de fournisseurs. Modes dégradés, redondance, migration cryptographique, sauvegardes et fédération doivent être prévus selon la criticité des fonctions.

15. Principe d'inclusion

La confiance vérifiable ne doit pas devenir un privilège réservé aux grandes entreprises, administrations ou populations fortement numérisées. PME, artisans, producteurs indépendants et citoyens doivent disposer de modalités proportionnées et accessibles. L'inclusion doit être mesurée comme une composante de la performance.

16. Principe de non-surveillance

La capacité de tracer un objet ou de vérifier un document ne justifie pas la surveillance permanente d'une personne. Les finalités doivent être séparées et les corrélations limitées. La doctrine établit que l'infrastructure doit permettre de vérifier davantage de preuves sans exiger de suivre davantage les individus.

17. Principe de réversibilité

Un acteur doit pouvoir changer de fournisseur, migrer ses composants ou suspendre certaines relations sans perdre la capacité d'interpréter ses preuves historiques. Portabilité, formats documentés et procédures de sortie réduisent la dépendance et renforcent la souveraineté opérationnelle.

18. Principe d'évaluation continue

L'adoption doit être accompagnée d'indicateurs de sécurité, confiance, inclusion, coût, résilience et impact. Les résultats défavorables doivent pouvoir conduire à des corrections ou à l'arrêt d'un mécanisme. La doctrine privilégie une expansion démontrée par étapes plutôt qu'une généralisation fondée uniquement sur l'ambition.

19. Les douze engagements de confiance vérifiable

La doctrine peut être résumée en douze engagements : vérifier sans centraliser ; prouver sans imposer ; identifier sans surveiller ; tracer sans exposer inutilement ; interopérer sans uniformiser ; automatiser sans déresponsabiliser ; sécuriser sans enfermer ; certifier sans confondre les niveaux d'assurance ; coopérer sans abandonner la souveraineté ; mesurer sans manipuler ; évoluer sans perdre la mémoire ; et étendre l'infrastructure sans supprimer le droit de contestation.

20. Critères d'acceptation et conclusion

La doctrine mondiale de confiance vérifiable est acceptable si elle distingue preuve et jugement ; protège la souveraineté ; impose la proportionnalité ; préserve l'architecture fondamentale d'Authenticity Plus© ; maintient les statuts VERT, JAUNE et ROUGE ; minimise les données ; rend les responsabilités identifiables ; garantit la contestabilité ; distingue les niveaux d'assurance ; favorise l'interopérabilité et la réversibilité ; prévient la surveillance excessive ; et soumet l'expansion à une évaluation continue.

Une doctrine universelle ne doit pas demander au monde d'adopter une seule manière de gouverner, de produire ou de penser. Elle doit définir les conditions minimales permettant à des systèmes différents de partager une confiance vérifiable.

Deep Authenticity© peut ainsi proposer non seulement une architecture technologique, mais une doctrine de coopération fondée sur la preuve, la souveraineté, la responsabilité et la liberté.

Le Chapitre 15 développera la projection stratégique finale 2050 : les scénarios de transformation mondiale et la place possible de Deep Authenticity© dans l'architecture future des échanges et des institutions.

Note d’alignement international

La doctrine proposée constitue un cadre conceptuel de Deep Authenticity© et non une norme internationale officiellement adoptée. Sa mise en œuvre doit être adaptée aux droits fondamentaux, cadres constitutionnels, règles commerciales, exigences de cybersécurité, protection des données et mécanismes de reconnaissance applicables dans chaque juridiction.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VIII — STRATÉGIE MONDIALE, IMPACT ET VISION 2040–2050

CHAPITRE 15 — PROJECTION STRATÉGIQUE FINALE 2050 : SCÉNARIOS DE TRANSFORMATION MONDIALE

2050 — PROJECTION — TRANSFORMATION — MONDE — ÉCHANGES — INSTITUTIONS — CONFIANCE — SOUVERAINETÉ — FÉDÉRATION — CIVILISATION

1. Objet du chapitre

Ce chapitre projette la place possible de Deep Authenticity© dans l’architecture mondiale des échanges et des institutions à l’horizon 2050. Il ne présente pas un futur unique, mais plusieurs configurations plausibles dans lesquelles la provenance, l’intégrité, l’identité et la continuité des preuves deviennent progressivement des fonctions ordinaires de l’économie et de l’administration.

2. Horizon 2050 : un monde de preuves numériques

À mesure que les objets, contenus, identités, transactions et décisions deviennent plus numériques, la question de leur origine et de leur intégrité gagne en importance. L’horizon 2050 peut être caractérisé par une multiplication d’agents automatisés et d’interactions machine-à-machine, rendant nécessaires des mécanismes de confiance lisibles aussi bien par les humains que par les systèmes.

3. Scénario 1 — Infrastructure spécialisée

Dans un scénario prudent, Deep Authenticity© demeure une infrastructure spécialisée utilisée dans des secteurs à risque élevé, des chaînes de valeur sensibles et certains services administratifs. Sa valeur réside alors dans une expertise profonde et des mécanismes de preuve ciblés plutôt que dans une couverture universelle.

4. Scénario 2 — Infrastructure multi-sectorielle

Dans un scénario intermédiaire, plusieurs secteurs adoptent les mêmes mécanismes de provenance, de passeport numérique et de vérification. Deep Authenticity© relie des écosystèmes économiques

distincts tout en laissant leurs systèmes opérationnels autonomes. Les effets de réseau augmentent sans nécessiter une architecture mondiale unique.

5. Scénario 3 — Infrastructure nationale de confiance

Certains États peuvent utiliser Deep Authenticity© comme couche d'interopérabilité entre produits, contenus, documents, identités et services publics. Les registres et données restent souverains, tandis que les preuves circulent selon des règles nationales. L'infrastructure devient alors un élément du socle numérique national sans se substituer aux institutions.

6. Scénario 4 — Fédération internationale

Des États, secteurs et organisations peuvent relier leurs infrastructures par des Corridors de Confiance© puis des fédérations. Les preuves deviennent vérifiables entre environnements différents selon des accords explicites. La fédération mondiale repose sur la compatibilité et la reconnaissance contrôlée plutôt que sur une centralisation universelle.

7. Scénario 5 — Couche civilisationnelle de vérité vérifiable

Dans le scénario le plus ambitieux, les mécanismes de Deep Authenticity© deviennent une couche transversale reliant le physique, le numérique et l'administratif. L'infrastructure ne gouverne pas le monde : elle fournit un langage commun permettant d'établir la provenance, l'intégrité, le statut et l' histoire des éléments critiques.

8. Authenticity Plus© dans l'architecture 2050

Quelle que soit l'évolution des interfaces, le domaine physique conserve le principe fondamental d' Authenticity Plus© : trois fonctions de vérification distinctes pour le consommateur, le revendeur/professionnel et le contrôle/douanes. Les supports techniques pourront évoluer au-delà du QR tout en préservant cette séparation fonctionnelle et ses garanties.

9. Continuité des statuts de confiance

La sémantique VERT — original ; JAUNE — original mais déjà vérifié ou vendu ; ROUGE — contrefaçon ou code inexistant dans le système Authenticity Plus© doit rester immédiatement compréhensible. Les technologies futures peuvent enrichir l'information, mais ne doivent pas rendre ambiguë cette lecture fondamentale.

10. Transformation des échanges mondiaux

Les échanges pourraient évoluer vers des flux dans lesquels produits, documents et autorisations transportent leurs preuves vérifiables. Certains contrôles pourraient devenir plus automatisés et ciblés, tandis que les anomalies déclencheraient des examens approfondis. La fluidité dépendrait alors de la qualité et de la reconnaissance des preuves.

11. Transformation des institutions

Les institutions pourraient passer d'une logique de collecte répétitive de justificatifs à une logique de vérification de preuves émises par des sources reconnues. Cette transformation peut réduire certaines frictions administratives tout en exigeant de nouvelles compétences en gouvernance des identités, des accès, des algorithmes et des responsabilités.

12. Agents autonomes et économie machine-à-machine

À l'horizon 2050, des agents logiciels pourraient négocier, acheter, contrôler ou exécuter des processus avec une autonomie accrue. Deep Authenticity© peut leur fournir des éléments permettant de vérifier l'identitéd'un actif, l'autorité d'un document ou le statut d'une contrepartie avant d'agir, selon des politiques déterminées par les acteurs responsables.

13. Intelligence artificielle et infrastructure de preuve

L'IA peut devenir omniprésente dans l'analyse et l'automatisation, mais la nécessité d'une couche de preuve indépendante devient alors plus importante. Deep Authenticity© doit permettre de distinguer ce qu'un modèle infère de ce qu'une source identifiable a réellement signé, enregistré, certifié ou transféré.

14. Souveraineté dans l'architecture mondiale

Une architecture 2050 crédible doit permettre aux États et institutions de participer à des réseaux mondiaux tout en conservant leurs données sensibles, leurs règles et leur capacité de sortie. La fédération et la localisation des données constituent des mécanismes permettant d'associer coopération internationale et autonomie stratégique.

15. Nouveaux risques

L'expansion peut créer de nouveaux risques : concentration du pouvoir, exclusion numérique, erreurs à grande échelle, attaques contre les infrastructures de confiance, dépendance à certains standards ou utilisation abusive de la traçabilité. La projection stratégique doit intégrer ces risques au même niveau que les bénéfices attendus.

16. Conditions du scénario mondial

Une portée véritablement mondiale suppose des résultats démontrés, une sécurité durable, une gouvernance légitime, une interopérabilité réelle, des coûts accessibles et une capacité à fonctionner dans plusieurs cadres juridiques. L'adoption ne peut être durable si elle dépend uniquement d'un avantage technologique temporaire.

17. Indicateurs de bascule vers 2050

Les signes d'une transition vers une infrastructure mondiale peuvent inclure reconnaissance de preuves entre plusieurs juridictions, adoption par des secteurs différents, interopérabilité entre infrastructures souveraines, participation significative des PME, baisse mesurée de certaines fraudes et utilisation régulière des passeports numériques.

18. Deep Authenticity© comme système d'exploitation de la civilisation moderne

Dans son expression conceptuelle la plus élevée, Deep Authenticity© peut être qualifiée de « système d'exploitation de la civilisation moderne » : une couche commune permettant aux systèmes humains et numériques de vérifier leurs relations avec les objets, contenus, documents et droits. Cette expression décrit une fonction d'infrastructure, non un pouvoir de gouvernement.

19. La réussite au-delà de la plateforme

Le succès ultime ne dépend pas nécessairement de la permanence de chaque technologie ou module. Si les principes de provenance, d'intégrité, de responsabilité et de preuve deviennent des exigences ordinaires des échanges mondiaux, l'héritage de Deep Authenticity© peut dépasser la plateforme elle-même et contribuer à une nouvelle culture institutionnelle de la confiance.

20. Critères d'acceptation et conclusion

La projection stratégique 2050 est acceptable si elle présente plusieurs scénarios plutôt qu'une prédiction unique ; si chaque scénario peut produire une valeur autonome ; si Authenticity Plus© conserve son architecture fonctionnelle fondamentale ; si l'IA reste distincte de la preuve ; si les souverainetés peuvent coopérer sans disparaître ; si les nouveaux risques sont explicitement intégrés ; si les conditions de passage à l'échelle sont mesurables ; et si la vision civilisationnelle reste une fonction d'infrastructure plutôt qu'une prétention au gouvernement.

L'horizon 2050 ne doit pas être compris comme la date d'achèvement de Deep Authenticity©, mais comme un point de projection permettant d'évaluer la direction de son évolution.

La question stratégique n'est pas de savoir si une seule plateforme contrôlera la vérité mondiale. Elle est de savoir si la civilisation disposera de mécanismes suffisamment ouverts, souverains et vérifiables pour distinguer plus rigoureusement l'origine, l'intégrité et la responsabilité dans un monde profondément automatisé.

Le Chapitre 16 développera la feuille de route finale 2026–2050 : jalons, priorités et séquencement stratégique permettant de relier la vision du Livre Blanc à une trajectoire de réalisation progressive.

Note d'alignement international

La projection 2050 présentée dans ce chapitre est un exercice prospectif. Les scénarios ne constituent ni des prévisions garanties ni des engagements institutionnels. Ils servent à tester la robustesse de la vision Deep Authenticity© face à plusieurs futurs possibles et à identifier les conditions nécessaires à une expansion responsable.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VIII — STRATÉGIE MONDIALE, IMPACT ET VISION 2040–2050

CHAPITRE 16 — FEUILLE DE ROUTE FINALE 2026–2050 : JALONS, PRIORITÉS ET SÉQUENCEMENT STRATÉGIQUE

FEUILLE DE ROUTE — 2026–2050 — JALONS — DÉPLOIEMENT — PILOTES — ÉTATS — CORRIDORS — INTEROPÉRABILITÉ — ÉVALUATION — PASSAGE À L'ÉCHELLE

1. Objet du chapitre

Ce chapitre transforme la vision stratégique de Deep Authenticity© en une trajectoire progressive 2026–2050. La feuille de route n'est pas un calendrier rigide : elle organise les dépendances, les priorités et les critères de passage entre phases afin que l'expansion repose sur des résultats démontrés plutôt que sur la seule ambition.

2. Principe de séquencement

Le déploiement doit suivre une logique : sécuriser le noyau, démontrer la valeur, standardiser les interfaces, fédérer les acteurs, ouvrir les corridors, puis étendre les fonctions. Chaque phase doit produire une valeur autonome et pouvoir être corrigée avant que ses choix ne deviennent des dépendances à grande échelle.

3. Phase I — 2026–2027 : consolidation du socle

La priorité initiale est de consolider architecture, sécurité, gouvernance, modèles de données, procédures d'intégration et documentation. Les domaines physique, numérique et administratif doivent disposer de frontières fonctionnelles claires, tandis que les composants transversaux — identité, preuve, audit et interopérabilité — sont stabilisés.

4. Authenticity Plus© comme priorité fondatrice

Dans le domaine physique, le déploiement conserve comme fondation l'architecture des trois QR codes : consommateur, revendeur/professionnel et contrôle/douanes. Les statuts restent VERT — original ; JAUNE — original mais déjà vérifié ou vendu ; ROUGE — contrefaçon ou code inexistant dans le système Authenticity Plus©.

5. Phase I — pilotes sectoriels

Les premiers pilotes doivent cibler des cas où la contrefaçon, la traçabilité ou la preuve de provenance créent un besoin identifiable. Les pilotes doivent mesurer sécurité, ergonomie, coûts, faux positifs, temps de vérification, adoption et capacité d'intégration afin de produire des références empiriques.

6. Phase II — 2028–2030 : industrialisation

Après validation des pilotes, l'objectif devient l'industrialisation : automatisation du déploiement, supervision, support, outils pour producteurs et revendeurs, API, tableaux de bord et mécanismes de certification. La capacité à intégrer des PME sans infrastructure disproportionnée constitue un critère essentiel.

7. Passeport numérique et cycle de vie

La période 2028–2030 doit renforcer le passeport numérique des produits et actifs : provenance, événements, certifications, transferts et statuts autorisés. La conception doit respecter la minimisation des données et permettre une continuité de preuve entre production, distribution, vente, seconde main et fin de vie.

8. Phase III — 2030–2033 : intégration institutionnelle

Cette phase vise des intégrations avec administrations, organismes de contrôle, douanes et systèmes sectoriels lorsque les cadres juridiques le permettent. Les projets institutionnels doivent conserver la souveraineté des registres et distinguer clairement preuve technique, reconnaissance réglementaire et décision administrative.

9. Domaine numérique et provenance des contenus

En parallèle, Deep Authenticity© doit développer la vérification des contenus, logiciels, médias et propriété intellectuelle autour de signatures cryptographiques natives, provenance et versionnement. L'objectif est d'établir l'origine et l'intégrité sans présenter la provenance comme une validation automatique de la vérité factuelle.

10. Domaine administratif

Les pilotes administratifs peuvent concerner documents, certificats, identités ou titres lorsque les autorités compétentes définissent les règles d'émission et de vérification. La priorité est de réduire les falsifications et les vérifications répétitives tout en garantissant recours, protection des données et accessibilité.

11. Phase IV — 2033–2036 : Corridors de Confiance©

Une fois plusieurs environnements nationaux ou sectoriels suffisamment matures, des Corridors de Confiance© peuvent relier des partenaires volontaires. Chaque corridor définit preuves reconnues, autorités habilitées, niveaux d'assurance, procédures d'incident, conditions de suspension et règles de réversibilité.

12. Phase V — 2036–2040 : fédération régionale

Des corridors compatibles peuvent progressivement former des fédérations régionales ou sectorielles. L'objectif n'est pas de centraliser les données, mais de permettre la vérification entre systèmes souverains. Des tests réguliers d'interopérabilité et de continuité doivent précéder tout élargissement significatif.

13. Phase VI — 2040–2045 : convergence des trois domaines

À maturité, les domaines physique, numérique et administratif peuvent partager davantage de primitives communes : identité, signature, provenance, droits, chronologie et preuve. Cette convergence doit rester fonctionnelle : elle ne justifie pas la fusion de toutes les données dans un profil universel.

14. Jumeaux numériques et Simulation Institutionnelle Profonde

Les tableaux de bord, jumeaux numériques nationaux et la Simulation Institutionnelle Profonde peuvent être développés à mesure que la qualité des données devient suffisante. Ils servent à détecter tendances, simuler scénarios et éclairer les décisions. Les résultats doivent distinguer observation, estimation, simulation et décision.

15. Phase VII — 2045–2050 : réseau mondial fédéré

Dans le scénario de passage à l'échelle le plus avancé, plusieurs fédérations peuvent devenir interopérables à l'échelle mondiale. Deep Authenticity© agit alors comme couche de confiance entre systèmes autonomes. L'expansion reste conditionnée à la souveraineté, la sécurité, la gouvernance et la capacité de sortie.

16. Priorités permanentes 2026–2050

Certaines priorités ne sont pas attachées à une phase : cybersécurité, migration cryptographique, protection des données, accessibilité, résilience, audit indépendant, documentation, formation et lutte contre les dépendances uniques. Elles doivent évoluer avec l'infrastructure et être financées durablement.

17. Gouvernance des jalons

Le passage d'une phase à la suivante doit dépendre de critères mesurables : sécurité démontrée, stabilité opérationnelle, adoption utile, coûts maîtrisés, interopérabilité testée, gouvernance fonctionnelle et absence d'effets indésirables majeurs non traités. Une date cible ne doit jamais remplacer un critère d'acceptation.

18. Indicateurs de trajectoire

La feuille de route peut suivre secteurs déployés, producteurs intégrés, PME participantes, preuves vérifiées, anomalies qualifiées, incidents, temps de récupération, administrations connectées, corridors actifs, systèmes interopérables et résultats d'impact. Ces indicateurs doivent être comparés aux coûts et aux risques.

19. Cap stratégique 2050

Le cap 2050 est une infrastructure capable de relier, sans les centraliser, les preuves du monde physique, numérique et administratif. Deep Authenticity© peut alors remplir sa fonction conceptuelle

de « système d'exploitation de la civilisation moderne » : une couche de relations vérifiables, et non une autorité gouvernant la civilisation.

20. Critères d'acceptation et conclusion

La feuille de route 2026–2050 est acceptable si elle consolide le socle avant l'expansion ; si Authenticity Plus© et ses trois QR restent la fondation du domaine physique ; si les pilotes précèdent l'industrialisation ; si les États conservent leurs compétences ; si les Corridors de Confiance© précèdent la fédération mondiale ; si la convergence des trois domaines n'entraîne pas une centralisation universelle ; si les jalons reposent sur des critères mesurables ; et si la trajectoire peut être révisée.

La vision mondiale de Deep Authenticity© devient ainsi une succession de preuves de faisabilité, de valeur et de confiance.

Entre 2026 et 2050, l'enjeu n'est pas de déployer le plus vite possible, mais de construire dans le bon ordre : protéger le noyau, démontrer, interopérer, fédérer, mesurer et transmettre.

Cette feuille de route clôt la projection stratégique du Volume VIII et prépare la conclusion générale du Livre Blanc 2026 : la synthèse de l'architecture, de la doctrine et de la vision de Deep Authenticity©.

Note d'alignement international

Cette feuille de route est prospective et révisable. Les périodes indiquent un séquencement stratégique et non des engagements calendaires garantis. Chaque passage à l'échelle doit dépendre de résultats empiriques, de la maturité technologique, des cadres juridiques applicables, de la sécurité et de l'acceptation des acteurs concernés.

LIVRE BLANC 2026

AUTHENTICITY PLUS© / DEEP AUTHENTICITY©

VOLUME VIII — STRATÉGIE MONDIALE, IMPACT ET VISION 2040–2050

CONCLUSION GÉNÉRALE DU VOLUME VIII — DE LA VISION MONDIALE À L'INFRASTRUCTURE DE VÉRITÉ

SYNTHÈSE — VÉRITÉ VÉRIFIABLE — PHYSIQUE — NUMÉRIQUE — ADMINISTRATIF — SOUVERAINETÉ — CONFIANCE — RÉSILIENCE — 2050 — CIVILISATION

1. Une vision devenue architecture

Le Volume VIII a porté Deep Authenticity© jusqu'à son horizon le plus large : celui d'une infrastructure mondiale de vérité vérifiable. Cette ambition ne repose pas sur la création d'une autorité universelle

de la vérité, mais sur la capacité à relier les affirmations critiques à une provenance, une intégrité, un statut, une chronologie et une responsabilité identifiables.

2. Les trois domaines fondamentaux

Deep Authenticity© se définit comme une infrastructure transversale couvrant trois domaines : le physique — objets et produits ; le numérique — logiciels, médias, contenus et propriété intellectuelle ; et l'administratif — documents, identités et titres de propriété. Ces domaines restent distincts tout en partageant des mécanismes communs de preuve et d'interopérabilité.

3. Authenticity Plus©, fondation du domaine physique

Dans le monde physique, Authenticity Plus© demeure la fondation anti-contrefaçon. Son architecture centrale repose sur trois QR codes fonctionnellement distincts : consommateur, revendeur/professionnel et contrôle/douanes. Les technologies complémentaires — IA, IoT, cryptographie, AP Ledger, analyse et certification — renforcent cette architecture sans s'y substituer.

4. Une sémantique universelle et immédiate

Les statuts de vérification conservent leur interprétation fondamentale : VERT signifie original ; JAUNE signifie original mais déjà vérifié ou vendu ; ROUGE signifie contrefaçon ou code inexistant dans le système Authenticity Plus©. Cette simplicité d'usage traduit, à l'interface humaine, une infrastructure de preuve beaucoup plus profonde.

5. Du produit à l'écosystème

Le Volume VIII montre que l'authentification d'un produit peut devenir le point d'entrée d'un écosystème plus vaste : traçabilité, propriété, seconde main, contrôle, certification, rappels, tableaux de bord, commerce éthique et coopération institutionnelle. La valeur provient de la continuité de la preuve à travers le cycle de vie.

6. La confiance vérifiable comme doctrine

La doctrine développée dans ce volume repose sur une idée simple : remplacer, lorsque cela est pertinent, la confiance purement déclarative par une confiance appuyée sur des preuves vérifiables. Cette évolution ne supprime ni le jugement humain ni le droit ; elle rend plus explicites la provenance, la responsabilité et les limites de ce qui est démontré.

7. Souveraineté et fédération

Une infrastructure mondiale ne doit pas exiger une base mondiale unique. Deep Authenticity© privilégie une architecture fédérée dans laquelle États, institutions et entreprises peuvent conserver leurs données et leurs compétences tout en échangeant les preuves nécessaires. L'interopérabilité relie les souverainetés sans les dissoudre.

8. Corridors de Confiance©

Les Corridors de Confiance© constituent une méthode progressive de coopération transfrontalière. Ils permettent à des partenaires volontaires de définir les preuves reconnues, les niveaux d'assurance, les autorités habilitées et les procédures d'incident avant toute fédération plus large. La mondialisation de la confiance devient ainsi graduelle et vérifiable.

9. Une infrastructure centrée sur les droits

La puissance technique doit rester bornée par la liberté, la proportionnalité, la minimisation des données, la contestabilité et la réversibilité. Une preuve peut être forte sans nécessiter une surveillance permanente. Une infrastructure de confiance ne devient légitime que si les personnes et institutions conservent des droits face à elle.

10. Intelligence artificielle et preuve

L'intelligence artificielle peut détecter des anomalies, analyser des flux et assister la décision, mais elle ne constitue pas la source ultime de vérité. Deep Authenticity© distingue l'inférence algorithmique de la preuve émise, signée, enregistrée ou certifiée par une source identifiable. Cette séparation devient essentielle dans un monde saturé de contenus synthétiques.

11. Résilience et continuité

La crédibilité de long terme exige une infrastructure capable de survivre aux pannes, cyberattaques, ruptures géopolitiques et transformations technologiques. Redondance, fédération, modes dégradés, migration cryptographique, réversibilité des fournisseurs et conservation de la mémoire probante sont des propriétés fondamentales de cette résilience.

12. Gouvernance et contre-pouvoirs

Plus Deep Authenticity© devient importante, plus sa gouvernance doit pouvoir être auditée. Séparation des rôles, supervision, gestion des conflits d'intérêts, droit de contestation et capacité de sortie empêchent l'infrastructure de devenir un pouvoir incontrôlé. Gouverner l'infrastructure ne signifie jamais gouverner la société.

13. Commerce éthique et prospérité

La confiance vérifiable peut soutenir un commerce plus équitable en réduisant certaines asymétries d'information, en protégeant les producteurs légitimes et en améliorant l'accès à la provenance et à la certification. Son impact doit cependant être mesuré en intégrant les coûts, l'inclusion des PME et la distribution réelle des bénéfices.

14. Transformation institutionnelle

Dans le domaine administratif, la réutilisation de preuves vérifiables peut réduire certaines vérifications répétitives et améliorer la continuité entre services. Les registres souverains, autorités compétentes et voies de recours restent indispensables. Deep Authenticity© agit comme infrastructure de relation et non comme administration universelle.

15. Simulation et anticipation

Les tableaux de bord, jumeaux numériques et la Simulation Institutionnelle Profonde peuvent transformer des données vérifiées en capacité d'anticipation. Ils peuvent aider à explorer pénuries, flux, risques et effets possibles de décisions. La simulation reste distincte de la décision politique et doit exposer ses hypothèses et incertitudes.

16. Une trajectoire 2026–2050

La feuille de route finale privilégie un développement par étapes : consolidation, pilotes, industrialisation, intégration institutionnelle, Corridors de Confiance©, fédérations régionales, convergence des trois domaines puis éventuel réseau mondial. Chaque étape doit être justifiée par des résultats avant le passage à l'échelle.

17. Mesurer avant d'affirmer

L'impact mondial ne peut être déduit du nombre de scans ou de comptes. Confiance, sécurité, prospérité, inclusion, résilience et souveraineté doivent disposer d'indicateurs auditables. Deep Authenticity© doit accepter de mesurer ses limites et ses effets indésirables avec la même rigueur que ses réussites.

18. Le système d'exploitation de la civilisation moderne

Dans sa formulation conceptuelle la plus élevée, Deep Authenticity© est « le système d'exploitation de la civilisation moderne ». Cette expression désigne une couche commune de relations vérifiables entre objets, contenus, documents, droits, acteurs et institutions. Elle ne signifie ni gouvernement mondial, ni centralisation universelle de la vérité.

19. L'héritage au-delà de la technologie

À long terme, l'héritage de Deep Authenticity© pourrait dépasser ses technologies initiales. Si provenance, intégrité, responsabilité et preuve deviennent des exigences ordinaires du monde physique, numérique et administratif, l'infrastructure aura contribué à installer une culture durable de la vérité vérifiable.

20. Conclusion finale du Volume VIII

Le Volume VIII referme la trajectoire prospective du Livre Blanc en reliant architecture, doctrine, souveraineté, géopolitique, résilience, gouvernance, impact et horizon 2050.

Deep Authenticity© propose une ambition précise : permettre à la civilisation numérique de disposer d'une infrastructure capable de répondre plus rigoureusement à quatre questions fondamentales — d'où vient cet élément ? est-il authentique et intègre ? quel est son statut ? qui porte la responsabilité de la preuve ?

Dans le physique, cette ambition commence concrètement avec Authenticity Plus© et ses trois QR codes. Dans le numérique, elle se prolonge par la provenance et les signatures natives. Dans l'

administratif, elle s'étend aux documents, identités et titres. À l'échelle mondiale, elle repose sur l' interopérabilité, la fédération et le respect des souverainetés.

La finalité n'est donc pas de construire un monde où une plateforme décide de la vérité, mais un monde où les éléments critiques peuvent être accompagnés de preuves suffisamment robustes pour être vérifiés, contestés, transmis et compris.

Ainsi s'achève le Volume VIII : non comme la fermeture d'une vision, mais comme son point de convergence. Deep Authenticity© devient le projet d'une infrastructure universelle de vérité vérifiable, conçue pour relier le physique, le numérique et l'administratif tout en préservant la liberté, la souveraineté et la responsabilité.

Note d'alignement international

Cette conclusion synthétise la vision prospective du Volume VIII du Livre Blanc 2026. Les horizons 2040–2050, scénarios d'adoption et effets civilisationnels présentés dans le volume constituent des cadres stratégiques et non des prévisions garanties. Leur réalisation dépendra de validations techniques, institutionnelles, juridiques, économiques et sociétales successives.

1. Le Passeport Numérique Universel dans la vision mondiale

À l'échelle du Volume VIII, le Passeport Numérique Universel dépasse la fonction d'identification d'un produit. Il devient un principe d'infrastructure : permettre à un objet, contenu, document, titre ou actif vérifiable de conserver une identité numérique persistante, évolutive et vérifiable à travers le temps, les organisations et, lorsque le cadre le permet, les frontières.

2. De l'authentification à la continuité civilisationnelle

Une civilisation numérique ne peut reposer uniquement sur des vérifications ponctuelles. Elle doit pouvoir relier l'origine, l'état, les transformations et les transmissions d'un élément. Le Passeport Numérique Universel apporte cette continuité : il transforme une preuve d'instant en histoire vérifiable.

3. La Trilogie de la Vérité comme fondation

Cette universalité repose sur trois mécanismes natifs adaptés aux trois domaines de Deep Authenticity© : les trois QR Codes dans le domaine physique, l'Empreinte Cryptographique Native dans le domaine numérique et le QR Code Dynamique dans le domaine administratif. Le Passeport Numérique Universel relie ensuite la preuve native au cycle de vie.

4. Le domaine physique

Dans le physique, les trois QR Codes demeurent le mécanisme anti-contrefaçon fondateur. La première activation légitime du QR consommateur protégé par le film à gratter déclenche le Passeport Numérique Universel et permet son rattachement au premier propriétaire. À partir de cet événement, l'objet entre dans une continuité numérique de propriété et de cycle de vie.

5. Le domaine numérique

Dans le numérique, l'Empreinte Cryptographique Native agit comme le sésame de l'identité des logiciels, médias, contenus et actifs de propriété intellectuelle. Le Passeport Numérique Universel peut prolonger cette empreinte par la provenance, les versions, les droits et les événements autorisés.

6. Le domaine administratif

Dans l'administratif, le QR Code Dynamique documentaire relie la copie présentée à l'état vivant reconnu par l'autorité compétente. Le Passeport Numérique Universel peut organiser la continuité du document, du titre ou du droit : émission, statut, modification, révocation, remplacement et autres événements autorisés.

7. Un langage commun de confiance

Le Passeport Numérique Universel fournit un langage commun : identité persistante, provenance, statut, événements, autorité, niveau d'assurance et droits d'accès. Les secteurs peuvent conserver leurs propres modèles tout en partageant un noyau de compréhension commun.

8. Commerce mondial

Dans le commerce international, un actif vérifiable peut traverser producteurs, distributeurs, douanes, revendeurs, propriétaires et marchés de seconde main sans perdre son identité de référence. Cette continuité peut réduire les ruptures d'information et renforcer la capacité de vérification entre acteurs.

9. Économie circulaire mondiale

Réemploi, réparation, reconditionnement, transfert, recyclage et fin de vie peuvent être intégrés au cycle du passeport. La valeur d'un produit n'est alors plus seulement liée à sa fabrication initiale, mais également à la qualité vérifiable de son histoire.

10. États et Nœuds Souverains Nationaux

L'universalité du Passeport Numérique Universel n'exige pas une base mondiale unique. Les Nœuds Souverains Nationaux permettent aux États de conserver la maîtrise des données, clés, registres et politiques relevant de leur souveraineté tout en participant à des mécanismes communs de vérification.

11. Corridors de Confiance internationaux

Les Corridors de Confiance permettent à plusieurs juridictions ou organisations d'échanger les preuves minimales nécessaires. Le Passeport Numérique Universel peut ainsi rester continu à l' échelle internationale tout en respectant les frontières juridiques, institutionnelles et informationnelles.

12. Une infrastructure de vérité sans autorité mondiale unique

Deep Authenticity© vise l'interopérabilité de la preuve, non la concentration universelle du pouvoir. Les autorités compétentes continuent d'émettre, reconnaître, révoquer et gouverner les éléments relevant de leurs compétences. L'infrastructure rend ces décisions vérifiables et interopérables selon des protocoles communs.

13. Du Passeport à l'intelligence collective

Les événements autorisés et agrégés issus des passeports peuvent alimenter tableaux de bord, systèmes d'alerte, analyses, jumeaux numériques et simulations. La continuité individuelle devient ainsi, sous gouvernance, une source de connaissance collective sans abolir la confidentialité.

14. Résilience mondiale

Une infrastructure de passeports distribuée et fédérée peut contribuer à la résilience en conservant la provenance des actifs, en facilitant les rappels, en identifiant les ruptures de chaînes et en permettant la reprise après incident. La résilience dépend toutefois de l'architecture, des procédures et des capacités souveraines de continuité.

15. Interopérabilité générationnelle

Le Passeport Numérique Universel doit être conçu pour survivre aux évolutions technologiques. Formats versionnés, standards, migration, réversibilité et agilité cryptographique sont nécessaires afin que l'identité d'un actif puisse rester vérifiable au-delà d'une technologie ou d'un fournisseur particulier.

16. Droit à la continuité et droit à la protection

La continuité de l'identité d'un actif ne doit pas entraîner une exposition permanente de la personne qui le possède. Le paradigme doit concilier persistance de l'identité de l'actif, protection des données personnelles, minimisation et contrôle des accès.

17. Une mémoire vérifiable de la valeur

Le Passeport Numérique Universel peut devenir la mémoire vérifiable de la création, de la transmission et de la transformation de la valeur : fabrication, création intellectuelle, certification, propriété, entretien, transfert et fin de vie. Il relie la valeur économique à une histoire de preuve.

18. Deep Authenticity© comme système d'exploitation de la civilisation moderne

Dans sa formulation la plus large, Deep Authenticity© peut être présenté comme le système d' exploitation de la civilisation moderne : non parce qu'il remplacerait les États, marchés ou institutions, mais parce qu'il fournit une couche commune de vérité vérifiable entre le physique, le numérique et l' administratif. Le Passeport Numérique Universel en constitue l'un des mécanismes de continuité fondamentaux.

19. Formule civilisationnelle

Les mécanismes natifs établissent la vérité. Le Passeport Numérique Universel donne une identité durable à cette vérité. AP Core orchestre sa continuité. Les Nœuds Souverains préservent les souverainetés. Les Corridors de Confiance permettent la coopération. Les Jumeaux Numériques représentent le réel. La Simulation Institutionnelle Profonde explore les futurs possibles.

20. Conclusion générale du principe

Le Passeport Numérique Universel donne au paradigme Authenticity Plus© / Deep Authenticity© une dimension qui dépasse l'anti-contrefaçon. Il crée la continuité entre origine, authenticité, propriété, transformation, circulation et mémoire. Dans le physique, le numérique et l'administratif, les mécanismes de vérité sont différents, mais la finalité converge : qu'un élément vérifiable puisse conserver une identité digne de confiance dans le temps. C'est cette continuité qui permet à Deep Authenticity© de passer d'un système de vérification à une infrastructure universelle de vérité.

RÈGLE DE CONSOLIDATION DANS LE DMC

Lors de l'assemblage du Document Maître Définitif, ces développements doivent être absorbés dans les sections mondiales, prospectives et civilisationnelles correspondantes du Volume VIII. Le Passeport Numérique Universel y apparaît comme mécanisme de continuité ; les mécanismes natifs de la Trilogie de la Vérité restent les mécanismes d'établissement de la preuve.

FORMULE FINALE DU VOLUME VIII

Les mécanismes natifs établissent la vérité. Le Passeport Numérique Universel lui donne une continuité durable. AP Core orchestre. Les Nœuds Souverains Nationaux préservent les souverainetés. Les Corridors de Confiance organisent la coopération. Les Jumeaux Numériques représentent le réel. La Simulation Institutionnelle Profonde explore les futurs possibles. Deep Authenticity© relie ces couches dans une infrastructure universelle de vérité, de provenance et de continuité.

LIVRE BLANC 2026 — DEEP AUTHENTICITY©

CONCLUSION GÉNÉRALE

DE L'AUTHENTIFICATION À LA CONTINUITÉ UNIVERSELLE DE LA VÉRITÉ

Le Passeport Numérique Universel au cœur du paradigme

1. Une infrastructure universelle de vérité

Deep Authenticity© se définit comme une infrastructure universelle de vérité couvrant trois domaines fondamentaux : le physique — objets et produits ; le numérique — logiciels, médias, contenus et propriété intellectuelle ; l'administratif — documents, identités, titres et droits. Sa finalité n'est pas seulement de produire davantage de données, mais de permettre de savoir quelles informations peuvent être reliées à une identité, une origine, une autorité et une histoire vérifiables.

2. La Trilogie de la Vérité

La cohérence du paradigme repose sur trois mécanismes natifs distincts. Dans le domaine physique, les trois QR Codes — consommateur, revendeur/professionnel et contrôle/douanes — constituent le mécanisme anti-contrefaçon fondateur. Dans le domaine numérique, l'Empreinte Cryptographique Native constitue le sésame de l'identité et de la provenance des logiciels, médias et contenus. Dans le domaine administratif, le QR Code Dynamique relie le document présenté à son état vivant et à l'autorité compétente.

3. Le Passeport Numérique Universel : le chaînon de continuité

À ces mécanismes de vérité s'ajoute un élément qui donne au paradigme toute sa profondeur temporelle : le Passeport Numérique Universel. Il ne remplace aucun des mécanismes natifs. Il prolonge leur preuve dans le temps. L'authenticité répond à la question de la vérité au moment de la vérification ; le Passeport Numérique Universel maintient l'identité, l'état et l'histoire autorisée de l'élément vérifié.

4. Le geste fondateur du produit physique

Dans le domaine physique, la première activation légitime du QR Code consommateur protégé par le film à gratter constitue un événement majeur. Elle déclenche le Passeport Numérique Universel du produit et permet son rattachement initial à son premier propriétaire. Le produit authentifié entre alors dans une continuité numérique : origine, propriété, événements de cycle de vie, maintenance, rappels, transferts, seconde main et fin de vie peuvent être conservés ou référencés selon les droits applicables.

5. De la propriété à la seconde main

Le transfert numérique sécurisé de propriété prolonge cette continuité. Le propriétaire peut changer sans que l'identité du produit soit recréée. La seconde main devient ainsi une nouvelle étape du même cycle de vie vérifiable. Authenticity Plus© ne protège plus seulement la première transaction : il permet de préserver la continuité de l'actif au fil de ses transmissions.

6. AP Core et l'architecture de continuité

AP Core orchestre identités, preuves, statuts, événements et droits. AP Ledger peut ancrer les événements exigeant une preuve renforcée ; AP Cloud ou les infrastructures souveraines assurent disponibilité et distribution ; AP Shield protège les opérations et accès. API, ERP, IoT et NFC peuvent enrichir cette continuité sans remplacer les mécanismes fondateurs.

7. De la vérité individuelle à l'intelligence systémique

Les événements vérifiables issus des Passeports Numériques Universels peuvent, lorsqu'ils sont autorisés, minimisés et agrégés, contribuer aux statistiques, Watch Systems, alertes, tableaux de bord et analyses. Une discipline essentielle demeure : un fait observé, une donnée agrégée, une prédiction et une simulation doivent toujours rester distingués.

8. Passeport, Jumeau Numérique et Simulation Institutionnelle Profonde

Le Passeport Numérique Universel documente la continuité du réel. Le Jumeau Numérique en construit une représentation structurée. La Simulation Institutionnelle Profonde explore des futurs possibles. Le monitoring continu compare ensuite le scénario anticipé à la réalité exécutée. Cette chaîne permet à Deep Authenticity© de relier preuve, observation, compréhension, anticipation et apprentissage.

9. Souveraineté et Nœuds Souverains Nationaux

L'universalité ne doit pas être confondue avec la centralisation. Les Nœuds Souverains Nationaux permettent aux États de conserver la maîtrise de leurs données, clés, registres et politiques. Les Corridors de Confiance permettent d'échanger les preuves minimales nécessaires entre environnements souverains. Une identité peut être universellement vérifiable sans que toutes ses données soient universellement accessibles.

10. Une infrastructure au service des acteurs

Producteurs, artisans, agriculteurs, créateurs, commerçants, consommateurs, institutions et États peuvent participer à la même infrastructure de confiance tout en conservant leurs rôles propres. La force du paradigme réside précisément dans cette capacité à relier des acteurs hétérogènes autour d' identités et de preuves interopérables.

11. La portée civilisationnelle

À son niveau conceptuel le plus élevé, Deep Authenticity© peut être présenté comme le système d'exploitation de la civilisation moderne : non comme un substitut aux États, aux institutions ou aux marchés, mais comme une couche commune de vérité vérifiable reliant le physique, le numérique et l'administratif. Le Passeport Numérique Universel constitue l'un des mécanismes essentiels qui donnent à cette vérité une mémoire et une continuité.

12. Formule doctrinale finale

Les mécanismes natifs établissent la vérité. Le Passeport Numérique Universel donne à cette vérité une identité durable. AP Core orchestre sa continuité. La traçabilité construit son histoire. Le transfert sécurisé prolonge la propriété. Les Nœuds Souverains préservent les souverainetés. Les Corridors de Confiance rendent possible la coopération. Les Jumeaux Numériques représentent le réel. La Simulation Institutionnelle Profonde explore les futurs possibles.

13. Conclusion

Le passage de Authenticity Plus© à Deep Authenticity© exprime une extension de portée : de la lutte contre la contrefaçon vers une infrastructure universelle de vérité. Mais cette extension ne doit jamais faire oublier le socle. Pour le produit physique, les trois QR Codes restent la fondation anti-contrefaçon. Le Passeport Numérique Universel transforme ensuite cette preuve en continuité de vie. Dans le numérique et l'administratif, les mécanismes natifs changent, mais le principe demeure : établir une identité vérifiable et permettre à cette vérité de traverser le temps.

Ainsi, Deep Authenticity© ne cherche pas seulement à répondre : « Est-ce authentique ? ». Il cherche également à rendre possible une question plus profonde : « Quelle est l'identité vérifiable de cet élément, d'où vient-il, quel est son état et quelle est son histoire ? ».

C'est dans cette continuité — de la preuve à la mémoire, de la mémoire à la confiance, et de la confiance à la décision — que se situe l'ambition du Livre Blanc 2026.