Brief d’acquisition (FR) - Attestability.com

Domaine stratégique pour “trust by evidence” et la readiness d’attestation

Actif proposé

• Nom de domaine : attestability.com (.com, exact-match)

• Nature : actif numérique descriptif, réservé comme bannière neutre et indépendante pour la catégorie émergente “Attestability”, c’est-à-dire la capacité d’un système à produire des preuves vérifiables sur son origine, son intégrité et son état, afin que des tiers puissent s’y fier (achats, assurance, audit, opérations à enjeux élevés).

• Ne sont pas inclus :

o aucune certification, aucun statut réglementaire, aucune accréditation, aucun label officiel,

o aucun service d’audit, de conseil, juridique, conformité, sécurité, assurance ou achats,

o aucun logiciel, base de données, index, méthodologie propriétaire, ni plateforme opérationnelle,

o aucun engagement de conformité, de sûreté, de sécurité, de performance ou de “trust garanti”.

Contacts (suggestion)

• Site : www.attestability.com

• Email : contact@attestability.com

• LinkedIn : www.linkedin.com/company/attestability (si applicable)

Ce document - pour qui, pourquoi

Ce brief est destiné à un comité de décision C-suite / Board :

• CEO, CFO, COO, CRO, CAE (Chief Audit Executive), CISO, CTO, CIO,

• directions Achats (enterprise et public), contrôle interne, Audit & Assurance (interne et indépendant),

• équipes sécurité plateforme, supply chain security, identity, cloud infrastructure, gouvernance du risque,

• Juridique/Compliance, Corporate Development, M&A, Partenariats, initiatives de normalisation.

Objet : évaluer si attestability.com doit être sécurisé comme bannière category-grade pour un hub de référence institutionnel, vendor-neutral, centré sur l'Attestability : la capacité à produire des preuves vérifiables permettant des décisions de reliance défendables (procurement, auditabilité, souscription assureur, déploiements critiques) à travers le confidential computing, la supply chain logicielle, l'identité machine/workload, et la durabilité cryptographique des preuves.

Ce document est informatif. Il ne constitue ni un avis juridique, ni un avis de conformité, ni un avis d'audit, ni un avis de sécurité, ni une recommandation financière ou d'investissement.

Disclaimers (à conserver identiques partout)

"Attestability.com is an independent, informational resource. It is not affiliated with any government entity, standards body, certification authority, or commercial provider."

"Nothing on this site constitutes legal, compliance, audit, or security advice. Consult qualified professionals and primary sources."

"The domain Attestability.com may be available for institutional partnership or acquisition by qualified entities."

1. Décision en une page

Ce que c’est

Attestability.com est un .com category-grade conçu pour nommer une propriété d’infrastructure : la capacité d’un système à produire des preuves vérifiables sur son origine et son état, afin que des relying parties puissent prendre des décisions de confiance défendables. Il distingue clairement “attestation” (l’acte) et “attestability” (la capacité).

Définition de catégorie (court)

L’attestability est la capacité d’un système à produire des preuves vérifiables sur son origine et son état, permettant à des tiers de vérifier et d’utiliser ces preuves dans un contexte défini.

Attributs clés (non techniques)

• Evidence-first : “trust by evidence” plutôt que confiance par déclaration.

• Procurement-ready : décisions de reliance répétables et défendables (ce qui est affirmé, prouvé, supposé).

• Architecture-native : s’aligne sur les rôles canoniques de l’attestation (Attester, Verifier, Relying Party).

• Transverse : confidential computing, supply chain logicielle, identité workload/machine, assurance long terme.

• Pensé long terme : horizons de conservation et besoins d’agilité cryptographique (y compris transition post-quantique).

Pourquoi c’est stratégique maintenant (signaux, sans surpromesse)

• Les organisations et les achats exigent de plus en plus des attestations et “evidence bundles” (notamment autour des pratiques de développement logiciel sécurisé).

• Le confidential computing et la protection “data-in-use” rendent l’attestation centrale dans la gouvernance infra.

• Les preuves et identités long terme imposent une crypto-agilité, incluant la préparation à la transition post-quantique.

2. Ce que c’est / ce que ce n’est pas

2.1 Périmètre naturel (exemples)

• Confidential computing et assurance “data-in-use” où la preuve de contexte d’exécution compte.

• Supply chain logicielle : provenance, builds, et preuves structurées.

• Identité machine/workload : acteurs non-humains qui doivent présenter des preuves de state.

• Déploiements à enjeux élevés : auditabilité et reliance défendables dans le temps.

2.2 Ce que ce n’est pas

• Ni cabinet d’audit, ni autorité de certification, ni régulateur, ni organisme de normalisation.

• Ni promesse de conformité, de sûreté, de sécurité ou de performance.

• Ni outil commercial, plateforme, base de données, index, méthodologie propriétaire ou service, sauf développement autonome par l’acquéreur.

• Aucune affiliation revendiquée avec des acteurs publics, standards, labs ou vendors.

3. Acheteurs naturels (logique d’acquisition)

Cloud et plateformes d’infrastructure

• Acteurs standardisant la confiance par preuves pour workloads, enclaves et identity.

Cybersécurité et supply chain logicielle

• Plateformes structurant evidence packs, provenance, et trails d’audit.

Audit, assurance, gouvernance du risque

• Acteurs industrialisant la revue de preuves, l’auditabilité, et la reliance défendable.

Assureurs / réassureurs

• Souscripteurs, brokers, réassureurs cherchant des preuves standardisées pour tarifer et transférer le risque.

Secteur public, infrastructures critiques, initiatives multi-acteurs

• Coalitions cherchant une bannière neutre pour vocabulaire, architectures, et attentes de preuves.

Sponsors typiques

CISO, CAE, CRO, CTO, Head of Platform Security, Head of Supply Chain Security, Juridique/Compliance, Corporate Development.

4. Déploiements possibles (exemples, non prescriptifs)

A. Hub de référence (public, neutre)

Définitions, glossaire, références primaires, explications claires de l'attestability comme capacité (pas une certification).

B. Primer d'architecture canonique

Modèle minimal des rôles et flux de preuves (attester/verifier/relying party), avec langage procurement.

C. Bibliothèque preuve et assurance

Vocabulaire qualité de preuve, horizons de conservation, chaîne de possession, patterns d'évaluation (sans claims de conformité).

D. Cartographie transverse

Confidential computing, supply chain evidence, identité, agilité cryptographique (incluant readiness post-quantique).

Mise en avant autres actifs (option, signal portefeuille)

• SignedResponse.com (artefacts de preuves signées)

• ComputeIntegrity.com (intégrité et durabilité des preuves)

• AuditableTrust.com (auditabilité et reliance)

• AIDataControl.org (data governance et contrôles)

• ComputeSovereignty.com (cadre stratégique infrastructure)

5. Process d’acquisition (nom de domaine uniquement)

Process type : NDA → échanges stratégiques → offre formelle → escrow → transfert du domaine.

Sauf accord explicite contraire, la transaction porte uniquement sur le nom de domaine attestability.com en tant qu’actif numérique incorporel. Aucun logiciel, base de données, index, conseil, lobbying, infrastructure, licence ou service n’est inclus.

Contact initial pour échanges sérieux : contact@attestability.com

Références primaires (curation, non exhaustif)

• Confidential Computing Consortium : terminologie de référence (vocabulaire et définitions)

• NIST : confidential computing (cadre de référence)

• IETF RATS : architecture d’attestation (rôles attester/verifier/relying party)

• CISA : secure software development attestation form (signal procurement)

• Ressources UE AI Act : pression croissante sur la documentation et l’évidence

• Cyber Resilience Act (CRA) : attentes sécurité produit et pression d’assurance

• NIST post-quantum cryptography : crypto-agilité pour preuves long terme