Acquisition Brief (EN) - Attestability.com

Strategic domain for “trust by evidence” and remote attestation readiness

Asset offered

- Domain name: attestability.com (.com, exact-match)
- Nature: descriptive digital asset, reserved as a neutral, vendor-independent banner for the emerging category “Attestability”, i.e., the capability of systems to produce verifiable evidence about their origin, integrity, and state, so that third parties can rely on them in procurement, assurance, audit, and high-stakes operations.
- Not included:
  - no certification, no regulatory status, no accreditation, no official label,
  - no audit, consulting, legal, compliance, security, assurance, or procurement service,
  - no software, datasets, indices, proprietary methodology, or operational platform,
  - no claim of compliance, safety, security, performance, or “guaranteed trust”.

Contacts (suggested)

- Site: www.attestability.com
- Email: contact@attestability.com
- LinkedIn: www.linkedin.com/company/attestability (if applicable)

This document - who is it for, why

This brief is intended for a C-suite / Board decision committee:

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

• Procurement leadership (enterprise and public sector), internal control, audit & assurance leadership,

• Platform security, supply chain security, identity, cloud infrastructure, and risk governance teams,

• General Counsel / Compliance, Corporate Development, M&A, Partnerships, standards and industry initiatives.

Purpose: assess whether attestability.com should be secured as a category-grade banner for an institutional, vendor-neutral reference hub centered on Attestability: the capability to produce verifiable evidence that supports reliance decisions (procurement, auditability, underwriting, critical deployments) across confidential computing, software supply chain, machine/workload identity, and long-lived cryptographic evidence.

This document is informational only. It is not legal, compliance, audit, security, financial, technical, or investment advice.

Disclaimers (must remain identical across site and documents)

“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. Decision in one page

What it is

Attestability.com is a category-grade .com designed to name a foundational infrastructure property: the capability of a system to produce verifiable evidence about its origin and state so that relying parties can make defensible trust decisions. It frames “attestation” as an act and “attestability” as the underlying capability.

Category definition (short)

Attestability is the capability of a system to produce verifiable evidence about its origin and state, enabling third parties to verify and rely on that evidence in a defined context.

Key attributes (non-technical)

- Evidence-first: “trust by evidence” rather than trust by statement or policy alone.
- Procurement-ready: supports repeatable, defensible reliance decisions (what is claimed, what is evidenced, what is assumed).
- Architecture-native: maps cleanly to canonical remote attestation roles (Attester, Verifier, Relying Party).
- Cross-domain: spans confidential computing, software supply chain, workload identity, and long-lived cryptographic assurance.
- Longevity-aware: anticipates long retention horizons and cryptographic agility needs.

Why it matters now (signals, non-exhaustive)

- Procurement and assurance increasingly ask for attestations and evidence bundles (e.g., secure software development attestation practices).
- Confidential computing and “data-in-use” protections elevate attestation and measurement concepts into mainstream infrastructure governance.
- Long-lived evidence and identity require cryptographic agility, including post-quantum transition readiness for future-proof verification.

2. What it is / what it is not

2.1 Natural scope (examples)

- Confidential computing and “data-in-use” assurance where evidence of execution context matters.
- Software supply chain assurance and secure build/provenance evidence flows.
- Machine/workload identity where non-human actors must present verifiable state claims.
- High-stakes deployments where auditability and reliance must be defensible over time.

2.2 What it is not

- Not an audit firm, not a certification authority, not a regulator, not a standards body.
- Not a promise of compliance, safety, security, or performance.
- Not a commercial tool, platform, dataset, index, methodology, or service layer unless a future owner builds one independently.
- Not an endorsement of any vendor, lab, or institution.

3. Buyer set (who can rationally own it)

Cloud and infrastructure platforms

- Hyperscalers and infrastructure vendors standardising evidence-based trust across workloads, enclaves, and identity.

Cybersecurity and software supply chain leaders

- Security platforms and assurance ecosystems that productise evidence packs, provenance, and audit trails.

Assurance, audit, and risk governance

- Firms industrialising evidence review, auditability, and reliance decisions across enterprises and regulated sectors.

Insurance and reinsurance

- Underwriters, brokers, and reinsurers seeking standardised evidence structures to price and transfer cyber/tech risk.

Public sector, critical infrastructure, and standards initiatives

- Multi-stakeholder efforts needing a neutral banner to define vocabulary, architectures, and evidence expectations.

Typical sponsors

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

4. Deployment options (examples, non-prescriptive)

A. Reference hub (public, neutral)

Definitions, glossary, curated primary references, and clear explanations of attestability as a capability (not a certification).

B. Canonical architecture primer

A stable “minimal model” of remote attestation roles and evidence flows (attester/verifier/relying party), with procurement language.

C. Evidence and assurance library

Evidence quality concepts, retention horizons, chain-of-custody vocabulary, and evaluation patterns (without compliance claims).

D. Cross-domain mapping

Mappings across confidential computing, software supply chain evidence, identity, and cryptographic agility (including post-quantum readiness).

Related category assets (optional, seller portfolio signal)

- SignedResponse.com (signed evidence artifacts)
- ComputeIntegrity.com (integrity and evidence durability)
- AuditableTrust.com (auditability and reliance)
- AIDataControl.org (data governance and controls)
- ComputeSovereignty.com (strategic infrastructure framing)

5. Acquisition process (domain name only)

Typical institutional flow: NDA → strategic discussion → formal offer → escrow → domain transfer.

Unless explicitly agreed otherwise, the transaction covers only the attestability.com domain name as an intangible digital asset. No software, datasets, indices, consulting, lobbying, infrastructure, licence, or service layer is included.

Initial contact for serious enquiries: contact@attestability.com

Primary references (curated, non-exhaustive)

- Confidential Computing Consortium: common terminology for confidential computing (definitions and vocabulary)
- NIST: hardware-based confidential computing (reference framing)
- IETF RATS: remote attestation architecture (attester/verifier/relying party roles)
- CISA: secure software development attestation form (procurement evidence signal)
- EU AI Act resources: governance regimes increasing documentation and evidence expectations
- EU Cyber Resilience Act (CRA) summary: product security expectations and assurance pressure
- NIST post-quantum cryptography standards: cryptographic agility for long-lived evidence