Attested Intelligence

TECHNOLOGY BRIEF

Attested Intelligence builds the enforcement layer between AI policy and AI execution. Our patent-pending Attested Governance Artifacts (AGA) architecture creates sealed governance objects that actively control runtime behavior and generate tamper-evident proof of enforcement. Provider-agnostic: any model, any agent framework, any deployment environment, same cryptographic guarantees.

SEAL

Attest subject state. Compute sealed hash (SHA-256). Sign with Ed25519 over RFC 8785 canonical JSON. Immutable reference created before execution begins.

ENFORCE

Portal runtime boundary measures subject integrity continuously. Compares to sealed reference. Executes graduated enforcement on drift. Agent holds no keys.

PROVE

Evidence Bundles with Merkle inclusion proofs enable offline verification by any third party. No network callback. Standard cryptographic libraries only.

Key Differentiators

- Two-process key separation: agent holds zero cryptographic keys, cannot self-authorize
- 10 measurement embodiments including TEE attestation quote ingestion
- 7 graduated enforcement actions including phantom execution for forensic capture
- Offline-first: verification requires no network connectivity
- O(1) receipt generation and chain append per measurement cycle
- Privacy-preserving disclosure via automatic claim substitution

IP Portfolio

- **USPTO App. No. 19/433,835** Systems and Methods for Generating and Enforcing Attested Governance Artifacts (Patent Pending)
- **Trademark** ATTESTED INTELLIGENCE (Serial No. 99677085, Pending)
- **Reference Implementation** v1.0.0 with 112+ automated tests and independent cryptographic verifier
- **MCP Server** @attested-intelligence/aga-mcp-server on npm (AI tool integration)
- **Federal Record** Two NIST submissions: CAISI RFI (Docket NIST-2025-0035) and NCCoE AI Agent Identity

Deployment Scenarios

- Defense & Aerospace: air-gapped audit, DDIL operations, autonomous drone governance
- Critical Infrastructure: SCADA/ICS integrity enforcement, real-time OT compatibility
- Enterprise AI: multi-agent orchestration governance, model deployment gates, SOC evidence
- Regulated Industries: finance, healthcare, legal compliance with cryptographic proof

Standards Alignment

Architecture designed for alignment with NIST AI RMF 1.0, CISA Secure by Design, SLSA Level 3 supply chain requirements, CoSAI MCP Security, and EU AI Act transparency obligations.

Attested Intelligence is a research and intellectual property company. The AGA architecture is provided as a reference implementation for technical evaluation. All deployment scenarios describe architectural design intent.

Contact

admin@attestedintelligence.com

attestedintelligence.com