Authorization Infrastructure for Autonomous and Agentic Systems

A dual-use framework for machine-readable authorization evidence in high-consequence AI environments

THE PROBLEM

Autonomous and agentic systems are increasingly deployed across planning, analysis, logistics, cybersecurity, data management, and decision-support functions.

Existing governance approaches emphasize identity, authentication, access control, provenance, logging, and auditability. These capabilities establish who an entity is, what actions occurred, and where information originated.

A separate challenge exists around authorization evidence. Organizations increasingly need to demonstrate:

- Who authorized an action
- What authority was granted
- Under what conditions authority was granted
- Whether authorization remained valid at execution time
- Whether authorization can be independently verified after execution

This challenge grows in significance as autonomous systems perform higher-consequence actions with reduced direct human intervention.

CAPABILITY

CreatorGuard is developing a patent-pending authorization infrastructure framework that generates machine-readable, cryptographically verifiable authorization records for autonomous and agentic systems.

The framework produces authorization artifacts demonstrating:

- Authorizing principal and verified identity
- Scope and conditions of authority granted
- Timestamp of authorization issuance
- Authorization validity status at execution time
- Offline-verifiable boolean authorization state

Records are cryptographically bound using Ed25519 signatures and SHA-256 asset fingerprinting, built on W3C Verifiable Credential and Decentralized Identifier standards. Each record remains independently verifiable without network connectivity.

DEFENSE APPLICATIONS

- Autonomous mission planning and execution systems
- Human-in-the-loop accountability environments
- Multi-agent coordination and tasking systems
- Supply chain authorization and chain-of-custody
- Cybersecurity operations and agentic workflows
- Zero Trust architecture implementation
- Cross-organizational data access governance
- Contested and disconnected environment operations

DEFENSE PRIORITY ALIGNMENT

- DoD Trustworthy AI and Responsible Autonomous Systems
- DoD Zero Trust Strategy (FY2027 mandate)
- Human accountability in autonomous pipelines
- June 2, 2026 Executive Order on AI agent authorization
- NIST AI Agent Identity and Authorization Standards Initiative
- Multi-domain operations and agent accountability

COMMERCIAL APPLICATIONS

Dual-use commercial deployment spans enterprise AI platforms, identity and access management, financial systems, healthcare workflows, media platforms, and critical infrastructure.

COMPANY INFORMATION

CreatorGuard Technology LLC

- SAM.gov UEI: QPGEMXLRHSK5
- DUNS: 14-464-9875
- Patent-pending: USPTO Docket 85498 (Jan 28, 2026)
- Reference implementation: CreatorGuard.tech
- Standards: W3C VC, W3C DID, C2PA ecosystem

Eddie Evans, Founder

Contact@CreatorGuard.tech | CreatorGuard.tech