The Envelope: Cryptographic Containment Architecture for AI Agents

exact.works, Inc. | Technical Whitepaper | March 2026

Abstract. The Envelope is exact.works' cryptographic containment infrastructure that physically constrains AI agent execution. It enforces network containment (allowedEgressUrls), budget circuit breakers (maxCostCents), temporal boundaries (timelineDays), and credential isolation — making the legal contract and the execution environment the same object.

1. Network Containment. The Envelope operates as a TLS-intercepting proxy. Every egress connection from an Agent is validated against the allowedEgressUrls array compiled into the Paper's Execution Manifest. Connections to undeclared domains are terminated with a 403 response and logged as egress violations in the AuditLog. The Agent cannot bypass this restriction because the Envelope IS the network path — there is no alternative route.

2. Budget Enforcement. Token-level cost metering tracks every API call the Agent makes. When accumulated cost approaches the maxCostCents ceiling, the Envelope terminates execution before the ceiling is breached. This is a circuit breaker, not a soft limit.

3. Temporal Boundaries. The timelineDays field in the Execution Manifest sets a hard deadline. The Envelope enforces expiration at the PostgreSQL UTC timestamp corresponding to compilation time + timelineDays. No extension without a formal Amendment.

4. Credential Isolation. Buyer-provided credentials (API keys, access tokens) are injected into the Agent's environment by the Envelope without exposure to Agent Logic. The Developer's instructions.md never sees raw credentials. Credentials are rotated per the schedule specified in the applicable Industry Schedule.

5. Sandboxed Execution Environment. Agents execute in an isolated sandboxed execution environment with no persistent state between sessions, no access to other Agents' data, and no ability to modify the Envelope configuration.

6. Audit Trail. Every Envelope event is recorded in the INSERT-ONLY AuditLog: egress attempts (allowed and blocked), cost metering checkpoints, credential injections, state machine transitions, and termination events. This audit trail is the evidentiary backbone for dispute resolution under SAISA Article 7.

The Envelope is what makes the SAISA enforceable. The legal contract defines the constraints. The Envelope enforces them. The gap between agreement and execution is zero.

exact.works, Inc. | Delaware | https://exact.works/trust