TRACE CONTINUITY LABS, LLC

Architecture Brief

Version 5 - with October 2026
external evaluation evidence

Version 5 - 23 October 2026
Public release - 24 October 2026
Not a certification or guarantee of security.

Patent Pending - U.S. Provisional Patent Application No. 64/137,172

1. What Trace is

Trace is a hosted, execution-time authority, governance and evidence layer for AI agents and enterprise systems. It separates an agent's request from the decision to permit a governed memory operation or external action, enforces that decision at a supported boundary, and records signed evidence of what was authorized and what happened.

> Evidence labels: VERIFIED = current source and Trace's internal tests. EXTERNALLY OBSERVED = recorded by the October 2026 external black-box evaluation on staging (commissioned by Trace; not a certification). STAGING ONLY / PRODUCTION = where it runs.

2. Trust boundaries

Layer	Responsibility	Evidence status
Agent / application	Holds one expiring, authority-bound key; requests memory or action authorization	VERIFIED; distinct agent and enforcement-point roles EXTERNALLY OBSERVED
Trace governance API	Identity, live authority, policy, conditions, matter boundary, lineage, tokenization	VERIFIED; selected checks EXTERNALLY OBSERVED (Scenarios 1-17)
Authorization artifact	Exact-action fingerprint (SHA-256 of canonical JSON, 17-field envelope), nonce, expiry, principal and EP bindings	Fingerprint independently recomputed - EXTERNALLY OBSERVED
Enforcement point	Redeems the exact grant; runs the protected action only on execute:true; reports outcome	Reference adapter VERIFIED; customer adapters CUSTOMER INTEGRATION
Evidence	Hash-chained audit, Ed25519-signed packages and checkpoints, offline verifier	VERIFIED; restoration package and checkpoint inclusion EXTERNALLY OBSERVED

3. Enforcement flow

> identity -> live authority (delegation chain, suspension, revocation, expiry, person, agent) -> policy -> material conditions -> matter boundary -> lineage -> pre-execution evidence -> execution -> final evidence

- **VERIFIED** Order is fixed and callers cannot change it. Anything that cannot be established refuses; 'could not establish' stays distinct from 'absent'. Protected-value reads re-check authority before decryption and at the final boundary.
- **VERIFIED** External actions: authorize -> enforcement point recomputes fingerprint -> redeem with its own key -> execute only on 200 + execute:true -> outcome. Authorization alone is not permission. Single use is one conditional database update.
- **EXTERNALLY OBSERVED** Exact replay 409; wrong redeemer 403; altered action/hash 403; malformed fingerprint 400; expired 410; executor never ran on refusal (Scenarios 10-13).

4. Authority, delegation, suspension and revocation

- **VERIFIED** Authorities: one tenant, one person, scopes, execution rights, expiry, reversible suspension, irreversible revocation (database trigger). Delegates cannot exceed grantors - enforced at configuration, by database trigger, and by live chain walk.

- **EXTERNALLY OBSERVED** Parent suspension denied the delegate's key; approved restoration restored it (Scenario 14). Revocation cascade turned four working calls into 401 (Scenario 15). A grant valid when issued was refused after revocation, before expiry (JEB-01). Suspended agent's held work refused at redemption (JEB-02).
- **LIMITATION** Not shown: interrupting an already-running operation; native/third-party queue cancellation; enforcement of uncascaded authority with an otherwise active key.
- **REMEDIATED** Second-person approval for protection-reducing changes. The October evaluation found agent reactivation bypassed it (F-01, Medium); fixed and retested on staging. Production parity to be confirmed.

5. Governed memory and private data

- **VERIFIED** Detection and tokenization at write; AES-256-GCM per-tenant vault; detokenization needs the detokenize right plus fresh rechecks.
- **EXTERNALLY OBSERVED** Ordinary reads returned tokens; authorized identity recovered exact values; cross-company reads 404 both ways (Scenarios 4, 5, 8).
- **OPEN FINDING** Restricted and delegate detokenization return 200 with detokenized_payload:null instead of documented 403 (F-02, F-04). No raw values disclosed.
- **STAGING ONLY** Production masks private values after authorized decryption; exact authorized disclosure and the single-call authority lookup run on staging only.

6. Lineage and derived data

- **VERIFIED** Append-only, hash-chained per-tenant edges; retraction entries, never edits; bounded walks refuse rather than truncate; provenance-required mode optional.
- **EXTERNALLY OBSERVED** Consent false/true/false -> derived read 200/403/200. Retraction removed active ancestry and preserved history; the report remained readable after retraction. Three chain links recomputed; nine altered copies rejected (Scenario 16).
- **OPEN FINDING** Cross-tenant lineage returns 200 with null fields rather than 404/409 (F-03); no foreign lineage disclosed.

7. Evidence

- **VERIFIED** Ed25519-signed per-tenant checkpoints over database-assigned transaction horizons; history re-verified before every signing; a sealed tenant cannot restart at checkpoint 1.
- **EXTERNALLY OBSERVED** Restoration package 18/18 entries VERIFIED; 12 checkpoints (2,731 entries) verified; 18 restoration leaves found in checkpoint 11; 54 altered preimages rejected. A separate read package: 25/26 entries recomputable; Scenario 18 BLOCKED.
- **LIMITATION** Database owner can alter data; Trace detects, does not prevent. Signing keys are managed secrets, not HSM. Vault keys not in KMS.

8. Production versus staging

Item	Production (tracecontinuity.com)	Staging (staging.tracecontinuity.com)
Database, keys, signing keys	Own	Separate, own; staging keys refused by production
Authority lookup	Parallel reads	Single-call lookup (identical decisions)

Item	Production (tracecontinuity.com)	Staging (staging.tracecontinuity.com)
Authorized private-value return	Masked after decryption	Exact authorized spans returned
F-01 fix	Not externally tested - confirm	Retested PASS
External evaluation	Excluded	Tested 19-23 Oct 2026
Data	Shared multi-tenant	Synthetic only; invite-only pages