TRACE CONTINUITY LABS, LLC

Technical Brief

Version 8 - capabilities, evidence, findings and limitations

Version 8 - 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. Summary

Trace checks, at the moment of action, whether an AI agent is still authorized to read, remember or act - and refuses when that cannot be established. Every decision produces evidence that can be verified offline from public keys.

Evidence status, 23 October 2026. Internal: 651/651 automated tests, 32/32 hosted acceptance checks, bypass scanner, build and type checks passed (17 October, staging). External: black-box evaluation of staging, 19-23 October - 14 PASS, 3 FAIL, 1 BLOCKED of 18 scenarios; 2 PASS, 1 NOT TESTED in the execution-boundary addendum; one Medium finding remediated. Production was not externally assessed.

2. Current capabilities

Capability	Status	External evaluation
Live authority on every call; no decision caching	VERIFIED, production + staging	Consistent: Scenario 15, JEB-01
Delegation containment; parent-suspension cascade	VERIFIED	Subchecks PASS (Scen. 14); overall FAIL on F-04
Irreversible revocation with key cascade	VERIFIED	PASS (Scen. 15, JEB-01)
Agent suspension; second-person reactivation	VERIFIED after fix	F-01 found, fixed, retest PASS (staging)
Tokenized memory; authorized detokenization	VERIFIED; exact return STAGING ONLY	PASS (Scen. 4, 5); F-02 open
Tenant isolation (object reads)	VERIFIED	PASS both ways (Scen. 8); F-03 open for lineage
Exact-action authorization, single use, replay/tamper refusal	VERIFIED	PASS (Scen. 10-13)
Consent-conditioned derived access; lineage retraction	VERIFIED	PASS (Scen. 16) - retraction does not itself revoke access
Signed evidence, checkpoints, offline verifier	VERIFIED	Restoration VERIFIED; Scen. 18 BLOCKED (1 withheld entry)
Alternate-route bypass resistance	Bypass scanner (internal)	NOT TESTED overall (JEB-03)

3. Supported API

REST/JSON over HTTPS under /api/public/v1/: memory/write, memory/read, conditions/report, conditions/history, provenance/declare, provenance/lineage, audit/list, actions/authorize, actions/redeem, actions/outcome, actions/evidence, GET evidence/keys, governance/persons/suspend; GET /api/public/health. Bearer API keys, one per authority, always expiring. Server-to-server only; browser cross-origin requests are blocked.

- **OPEN FINDING** Response contract: restricted and delegate detokenization currently return 200 with detokenized_payload:null; cross-tenant lineage returns 200 with null artifact/ancestry. Documentation says 403 / 404 / 409. Clients must check the body and must never treat HTTP 200 alone as a data-access or execution grant.

4. Integration requirements

- **VERIFIED** Trace provisions tenants, authorities, policies, agent keys and enforcement-point keys through governed administrative paths. No public provisioning API.
- **CUSTOMER INTEGRATION** Customer provides the orchestrator, boundary calls, and an enforcement-point adapter that executes only after redeem returns 200 and execute:true. Protected downstream credentials must live only behind that adapter. The evaluation's local synthetic executor is not evidence about any customer adapter.

5. Measured performance

Source	Measure	Result
Internal, production, 13 Oct, 12 agents / 3 tenants	Write / read / private read p50	1.95 s / 2.54 s / 3.03 s; 4.3 ops/s; 0 errors, 0 wrongful approvals
Internal, staging, 15 Oct, same workload	Write / read / private read p50	3.9 s / 4.8 s / 5.8 s; 2.3 ops/s; smallest database tier
External lab, staging, 57 samples	Mixed routes, network-inclusive	p50 1,080 ms; p95 2,455 ms; max 4,177 ms (low volume, 10 req/min cap)

- **LIMITATION** Seconds per governed call. No high-volume, soak, denial-of-service or race testing by anyone. No SLA.

6. Findings register

Finding	Severity	Status	What it means
F-01 Agent restoration lacked required second-person approval (Scenario 17)	Medium	REMEDIATED on staging; separate retest PASS	A privileged admin could lift an agent suspension without the required second approver. Fixed and retested for the tested paths. Original FAIL preserved.
F-02 Restricted detokenization returns HTTP 200 with null instead of documented 403 (Scenario 6)	Low	OPEN	No raw synthetic PII was disclosed; values stayed as tokens. The response code does not match the documentation.
F-03 Cross-tenant lineage returns HTTP 200 with null artifact/ancestry instead of 404/409 (Scenario 9)	Low	OPEN	No foreign lineage was disclosed. Response contract mismatch.
F-04 Delegate detokenization returns HTTP 200/null instead of 403 (Scenario 14)	Low	OPEN	Same behavior as F-02, likely same root cause. Delegation containment and restoration passed separately.

7. Limitations

- **LIMITATION** No certification, accredited assessment or third-party penetration test. The external evaluation was commissioned by Trace.
- **STAGING ONLY** Staging-only: single-call lookup, exact authorized disclosure, F-01 fix (production parity unconfirmed).
- **LIMITATION** Not tested externally: production, alternate routes and internal functions, customer adapters, interruption of running actions, concurrency races, tenant enumeration, person-level suspension, approval reuse.
- **LIMITATION** Vault keys in database (not KMS/HSM); signing keys not HSM-backed; database owner can alter data (detected, not prevented); pattern-based PII detection; shared multi-tenant hosting; no SDKs, SIEM connectors, gRPC or SSO for API callers; no uptime commitment or written RTO/RPO.

8. Recommended next technical steps

- **OPEN FINDING** Decide and implement the 403/404/409 contract for F-02/F-03/F-04, then have the lab re-verify separately (original FAILs stay on record).
- **NOT ESTABLISHED** Confirm the F-01 fix in production before claiming it there; keep dual-approval regression tests across named, generic and upsert paths.
- **OPEN FINDING** Provide a fully recomputable synthetic read-evidence example to resolve Scenario 18's withheld entry.