TECHNICAL BRIEF

Execution-Time Authority, Outcome Evidence and Coverage

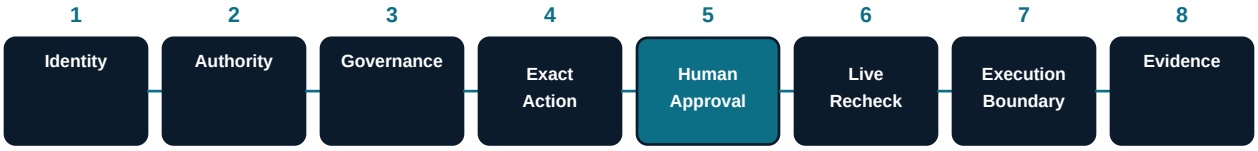
Current implementation, November security repairs, integration requirements, verification and stated limits.

Every Decision Begins With Authority.

Version 10 · 18 November 2026 · Trace Continuity Labs · tracecontinuity.com
Patent Pending — U.S. Provisional Patent Application No. 64/137,172. Not a certification.

1 · Positioning

Trace Continuity is an execution-time authority, governance and evidence layer for AI agents and enterprise systems. It answers three separate questions: who authorized the action, what actually happened, and whether the operation was inside the required enforcement coverage. It provides governed memory, exact-action enforcement and verifiable evidence without claiming visibility or control over systems that never pass through Trace.



Authority is re-checked live. Approval applies only when required.

Outcome and coverage remain separate evidence dimensions after the execution boundary.

2 · Capability inventory

Capability	Current implementation
Execution-time authority	Live credential, person, agent, authority, delegation, scope and execution-right checks
Governed memory	Policy/conditions, tokenization, encrypted vault handling, retrieval rechecks and reported lineage
Suspension and revocation	Reversible suspension stops the next governed request; permanent revocation cannot be undone
Exact-action enforcement	Canonical fingerprint, separate enforcement-point credential, live recheck and atomic single use
Outcome verification	Authorization, consumption, dispatch, reported outcome, target check and unknown states remain separate
Historical evidence	Saved single-statement captures reconstruct recorded knowledge at capture; arbitrary past wall-clock views are refused
Enforcement coverage	Declared routes compared with observed operations, credential mappings and registered bindings
Evidence and exports	Hash-chained evidence, signed packages, checkpoints, coverage JSON and report-generation audit entries
Governance over governance	Protection-reducing changes require a second administrator's approval of the exact change
Matter boundaries	Matters, ethical walls, legal holds and screened evidence reads fail closed

3 · Outcome-evidence model



Each state answers a different question. None is silently promoted to the next.

Dispatch ≠ target completion. Confirmation requires an explicit target-backed check.

Unknown or unavailable evidence remains unknown or unconfirmed.

State	What it establishes	What it does not establish
Authorization	Live authority and governance permitted one exact action	Execution, dispatch or target completion
Execution consumption	The bound enforcement point atomically redeemed the single-use permit	That the executor ran or the target changed
Dispatch	The request was sent or the executor returned	Successful completion of the intended effect
Reported outcome	The enforcement point reported confirmed, failed or unknown	Independent observation by Trace
Target confirmation	The bound enforcement point supplied a target receipt, read-back or reconciliation; optionally an Ed25519 receipt signed by the target system or a connector, verified by Trace against a governed registered key	Universal proof about arbitrary external systems
Unknown / unconfirmed	The necessary outcome or target evidence is absent, failed or unavailable	A hidden success or a hidden failure

- The outcome endpoint accepts dispatched, legacy confirmed, failed and unknown reports. Executor-only reference-adapter calls record dispatched.
- Target confirmation requires a declared method, SHA-256 evidence hash and valid observation time. Entries are append-only and returned in deterministic audit order with a truncation flag.
- The reference adapter invokes its executor only after execute:true. If target evidence cannot be recorded, it reports unknown rather than upgrading to confirmed.
- Target checks run after execution and add no work to authorization or redemption. They remain attributed enforcement-point evidence unless a signed receipt is supplied.
- Signed receipts: Ed25519 signatures bound to tenant, authorization, action fingerprint, enforcement point, nonce, target and evidence hash. Forged, altered, replayed, wrong-action, unknown, revoked, expired or wrong-scope keys are refused, with no fallback to unsigned. New keys need second-administrator approval.
- Independent attestations: a separately registered third party may sign effect observed, effect not observed or could not establish. When signed records disagree, the state is TARGET_EFFECT_EVIDENCE_CONFLICTED with both records kept append-only; an independent denial is TARGET_EFFECT_EVIDENCE_DENIED, never flattened into unknown. Trace does not

observe the effect itself.

- Historical captures: POST actions/historical-evidence saves a single-statement MVCC view or reconstructs a saved snapshot under current evidence and matter authorization. Signed claim and audit writes are atomic. Intake-time key lifecycle is retained; arbitrary as_of requests and private detail exports are refused.

4 · Enforcement-coverage model

Input or signal	Meaning
Registered enforcement binding	A known enforcement-point identity can participate in the protocol; not proof of route completeness
Declared protected route	Customer-owned append-only declaration of operation, tool, target, environment, owner and credential boundary
Trace-observed operation	Authorization/consumption evidence actually recorded by Trace in the selected window
Customer-declared inventory	Systems, environments and completeness asserted by a named customer reviewer
Unregistered live key	Live Trace credential without a registered agent mapping; review signal, not proof of a bypass
Multiple credentials	More than one live key for an authority; potential alternate path requiring review
Unmapped observed operation	Observed action does not exactly match a current declared route
Verified observed coverage	Exact declared route matched observed governed evidence, with other risk fields still separate
Unknown / incomplete coverage	Missing, stale, ambiguous, out-of-scope or truncated information prevents a stronger conclusion

- Declarations and revisions are append-only. Cross-tenant enforcement-point references are refused; mutations use the configuration gate and evidence chain.
- Reports use bounded sources and expose truncation. Counts cover declared routes only; no enterprise-wide coverage percentage is produced.
- Each generated report writes a coverage/report_generated audit entry. JSON export is available; automatic email or paging alerts are not implemented.
- Coverage states include declared ungoverned, inactive enforcement point, registered unobserved and observed governed path. Credential and bypass-risk fields remain additional dimensions.

5 · November security repairs

Repair	Current behavior and test boundary
Offboarding authority binding	The presented credential's pinned authority is preserved; a restricted authority cannot fall back to another eligible authority
Protected evidence reads	Audit, condition, lineage and action evidence require live authority and applicable scope/right; read decisions are audited
Matter-wall failures	Matter, wall, access and preservation lookup errors deny distinctly; an error is not treated as no wall or no hold
Matter-screened evidence	Sensitive rows and target-check records are screened through their underlying action before return
Protected-memory reads	Direct ordinary-client SELECT is explicitly revoked and refused on a fresh isolated database
Atomic signed evidence intake	Each signed claim and its verification audit commit together; audit failure rolls back the claim
Historical privacy and key lifecycle	Clean captures remain exportable, private details stay withheld, and intake-time key facts survive later revocation
Expanded bypass scanning	Person-suspension, coverage-declaration and approval-detail records are included in scanner inventories

6 · Evidence integrity

- Per-action evidence is hash-chained and append-only against ordinary application code and database roles.
- Ed25519-signed packages verify offline against published public keys. Verification returns VERIFIED, FAILED or INCOMPLETE; withheld details are not silently verified.
- Tenant-wide checkpoints use database-assigned ordering and closed-transaction horizons. Trace re-verifies committed history before signing or extending a checkpoint chain and refuses on mismatch.
- Customers retain anchors outside Trace. Database-owner alteration is not prevented; committed-history alteration is detectable against retained evidence.

7 · API and application surfaces

Surface	Current capability
POST memory/write, memory/read	Governed tokenized storage and retrieval with fresh checks
POST conditions/report, conditions/history	Material-state assertions and screened append-only history
POST provenance/declare, provenance/lineage	Reported derivation and bounded, matter-screened lineage
POST audit/list	Live-authorized, matter-screened tenant evidence listing
POST actions/authorize, redeem, outcome	Exact-action issuance, live atomic redemption and reported outcome
POST actions/target-confirmation	Append-only target-backed check from the bound enforcement point
POST actions/independent-attestation	Signed third-party effect statement; no Trace credential is presented
POST actions/historical-evidence	Capture current evidence or reconstruct a saved historical view
POST actions/evidence	Live-authorized action/outcome/target evidence
Governance → Coverage	Authenticated application reporting and JSON export; not a new public REST surface
GET evidence/keys	Public verification-key registry without private material

8 · Verification

Reverified 18 November 2026: 633 ordinary tests passed with 208 environment-dependent tests skipped; 838 isolated-database tests passed with three port-gated affiliate tests skipped, and those three passed separately. Twenty-nine named historical-evidence checks passed, including atomic rollback, privacy, concurrency, replay, tamper and later-key-revocation cases. Live production synthetic memory write/read, cross-tenant refusal and revoked-key refusal passed. The full hosted signed external-action flow remains unestablished because no external-action authority or action records are provisioned. These are not certification results.

The separate 4 November internal staging benchmark remains a staging result: approximately 1.5 seconds per complete authorize → redeem → outcome → evidence workflow, approximately 3.17 workflows/second, concurrency 10, 25 and 50, and 160/160 successful workflows. Replay, cross-tenant and mid-action suspension attempts were refused; that run reported 714/714 security tests. It was not rerun for this brief and does not establish production capacity, sustained throughput or support for 1,000+ agents.

9 · Deployment responsibilities

Area	Owner / requirement
Exclusive downstream credential custody	Customer IAM, secrets manager and workload identity
Complete execution routing	Customer APIs, integrations, jobs, SDKs, MCP servers and manual paths
Network egress and alternate-route closure	Customer infrastructure
Exact-action construction and fail-closed adapter	Customer enforcement point
Target receipt, read-back or reconciliation	Customer integration where actual effect matters
Coverage inventory ownership and review	Named customer owner; review before due date
Checkpoint anchor retention	Customer storage or escrow outside Trace
KMS/HSM, SSO/SCIM, SIEM, residency and formal service objectives	Separate deployment work; not claimed current

10 · Stated limits

- Trace cannot detect or prevent an action occurring entirely outside its integration and network visibility. Customers must control credentials, IAM, network egress, jobs, alternate APIs and manual paths.
- A registered enforcement point or an observed governed request does not prove that all customer routes are governed. Inventory completeness and exclusive credential custody remain customer declarations until independently established.
- Target confirmation is attributed to the bound enforcement point. An unsigned target-evidence hash fingerprints reported content only. A signed receipt is verified by Trace against a registered key and labeled target-system-signed or connector-signed; it cannot prove the signer's key was never stolen.
- Signed checkpoints do not stop a database owner from changing data. Externally retained anchors make later alteration or deletion of committed history detectable; later activity is covered once a subsequent checkpoint is retained.
- Signing keys are held in managed secret storage, not an HSM. Tenant vault keys remain in the application database. No independent timestamping or public-ledger anchoring is claimed.
- Trace evaluates reported state and reported lineage. It does not discover hidden derivations, terminate arbitrary external processes or recall data/actions already released.
- Historical reconstruction requires a previously saved capture. Append-only rows, alleged event dates or an arbitrary as_of time cannot establish what was visible in the past. Signed statements attribute claims; they do not prove physical effects or external wall-clock time.
- Sensitive-data recognition is pattern/context-based and not exhaustive identification of arbitrary prose. No compliance certification or universal security guarantee is claimed.