

ARCHITECTURE BRIEF

From Identity to Evidence

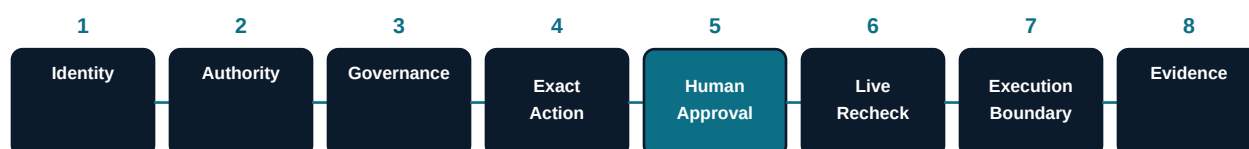
How Trace sits between actors and consequential systems, and where the trust boundaries are.

Every Decision Begins With Authority.

Version 1 · October 2026 · Trace Continuity Labs · tracecontinuity.com
Patent Pending — U.S. Provisional Patent Application No. 64/137,172. Not a certification.

1 · The execution path

Trace Continuity is an execution-time authority, governance and evidence layer for AI agents and enterprise systems. It determines whether an actor is authorized to perform a specific action at the moment of execution, enforces that decision at the execution boundary, and produces verifiable evidence of what was authorized and what occurred.

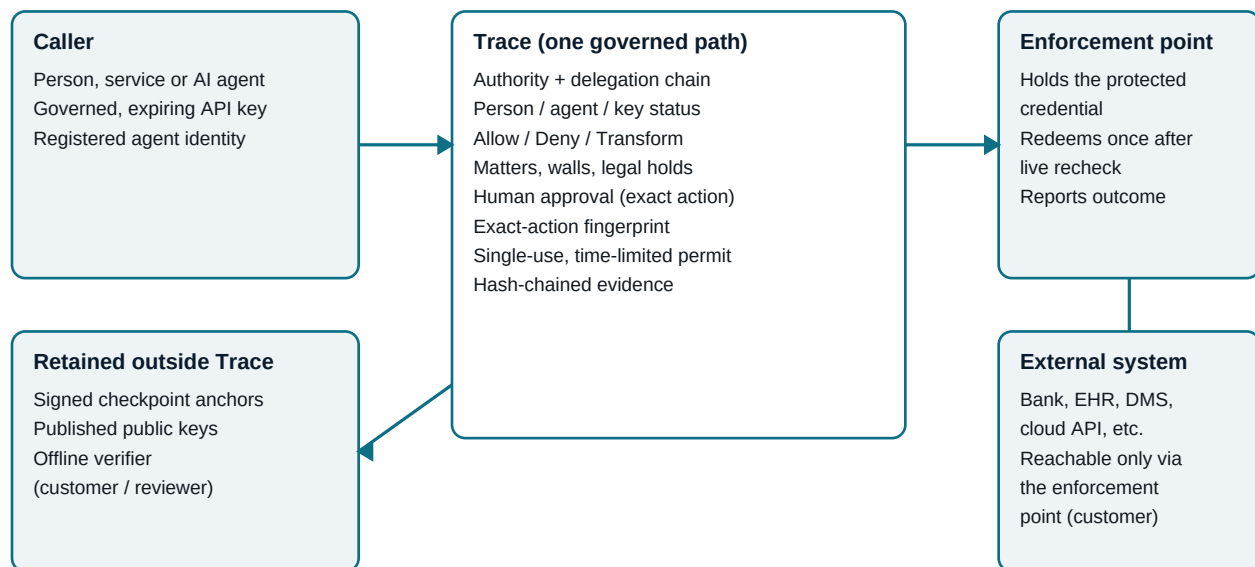


Human approval applies when the action requires it. Authority is re-checked live at the boundary.

Evidence is recorded at every step and signed; tenant-wide checkpoints can be retained outside Trace.

Step	Decision	Fails closed when
1 Identity	Who or what is calling: person, service or registered agent, via a governed, expiring key	Key unknown, expired, revoked or agent suspended
2 Authority	Whether the actor's authority, and every link of its delegation chain, permits this	Any link missing, suspended, revoked, expired, cross-tenant or exceeding its grantor; person suspended
3 Governance	Allow / Deny / Transform; conditions, matters, ethical walls, legal holds, lineage	Required state missing or stale
4 Exact action	Canonical fingerprint of the precise action	Action differs from what was authorized
5 Human approval	When required, a different person approves the exact action	Self/dependent approver; approval reused or changed
6 Live recheck	Authority and governance re-evaluated immediately before execution	Anything changed since issuance
7 Execution boundary	Registered enforcement point redeems a single-use, time-limited permission	Wrong enforcement point, expired or already used
8 Evidence	Hash-chained record, signed packages, tenant checkpoints	Committed history no longer matches (Trace refuses to sign)

2 · Trust boundaries



Customer deployment boundary: the external credential must sit behind the enforcement point.

Trace is the decision and evidence layer. The enforcement point is the component that holds the protected credential and only acts on a valid, live-rechecked Trace permission. The customer's deployment decides whether the external credential is reachable only through it — that is what makes enforcement non-bypassable for that action.

3 · Evidence retention and independent verification

- Trace publishes its Ed25519 public keys, including retired and compromised ones, at a public endpoint. Reviewers keep a copy from a trusted channel.
- Signed evidence packages verify offline with the public verifier; no call to Trace is needed.
- Checkpoint anchors are small files the customer retains outside Trace. A later chain export must contain each retained checkpoint exactly.
- Trace itself refuses to sign new packages or extend the chain when committed history has changed, and records the refusal.

4 · What a privileged database owner can and cannot do

Action by a database owner	Result
Rewrite or delete committed evidence, or backdate entries	Detected by Trace on its next check (refuses to sign) and against retained anchors
Delete the checkpoint chain	Trace fails closed and will not restart the chain; retained anchors also show it
Substitute a public key in Trace's registry	Trace confirms keys against its own custody and refuses
Alter activity after the latest retained checkpoint	Not detectable until a later checkpoint is retained
Erase every Trace-held record of earlier checkpoints	Detectable only with checkpoints retained outside Trace

Action by a database owner	Result
Use the platform's signing secret	Outside the database; protected by platform secret storage (not an HSM today)

5 • Deployment responsibilities

Area	Belongs to
HSM / KMS-backed signing keys	Deployment architecture
Dedicated tenancy; staging/production separation	Deployment architecture
SSO and SCIM / identity-provider offboarding	Customer IdP, calling Trace's person-suspension endpoint
Rate limiting, WAF, network edge	Deployment / network
Monitoring and SIEM forwarding	Customer security operations
Backups and point-in-time recovery procedures	Deployment operations
Write-once retention of checkpoint anchors	Customer storage or escrow
Placing external credentials behind the enforcement point	Customer integration

6 • Validation and limits

October 10, 2026: the database-owner validation run passed 567 tests across 35 files with zero failed and zero skipped, on an isolated PostgreSQL cluster built from all 55 migrations. The ordinary run passed 427 tests with 140 special-environment skips. The build-blocking bypass scanner reported no bypass, and the production build succeeded. These results validate application and database rules; they are not a certification, a formal penetration test or customer acceptance testing.

- Signed checkpoints do not prevent a database owner from changing data. They make later alteration or deletion of committed history detectable against checkpoints retained outside Trace. Activity after the most recent retained checkpoint is covered only once a later checkpoint is retained.
- If a database owner erased every Trace-held record of earlier checkpoints, only checkpoints retained outside Trace would reveal it. Retaining anchors is part of the control.
- External-action enforcement is non-bypassable when the protected credential or action is placed behind the Trace enforcement point. A credential left outside it can be used without Trace; Trace can only show that no Trace authorization exists for that use.
- Signing keys are held in platform secret storage today, not an HSM or KMS. There is no independent timestamping or transparency log.
- Reviewers must obtain Trace's public keys through a channel they trust; an old copy of the key list will not show a later key compromise.
- Trace evaluates the state reported to it. It does not discover changes in outside systems that nobody reported.

- No SOC 2, HIPAA or other certification, and no third-party penetration-test certification, is claimed.