

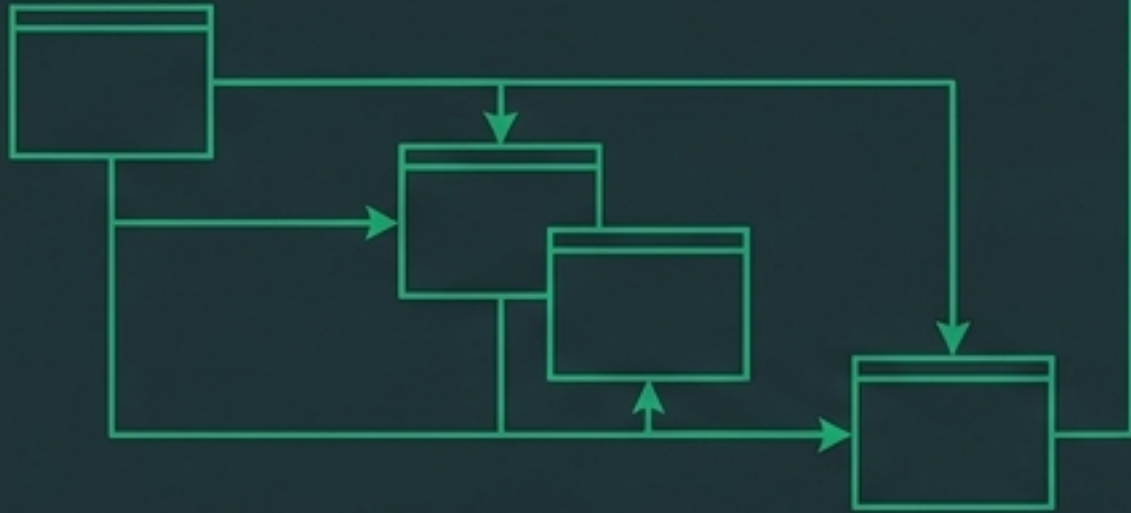


bulletproof-compliance-jobs

System Overview

bulletproof-compliance-jobs (FastAPI service)

- Unprivileged container (appuser, uid 10001)
- Port: 8087
- Local mutable state via SQLite



Reacts to events, enforces retention, cascades DSRs, produces tamper-evident reports.

Audit Trails & Governance Portals



Mounted strictly read-only (AUDIT_BUS_DBS)

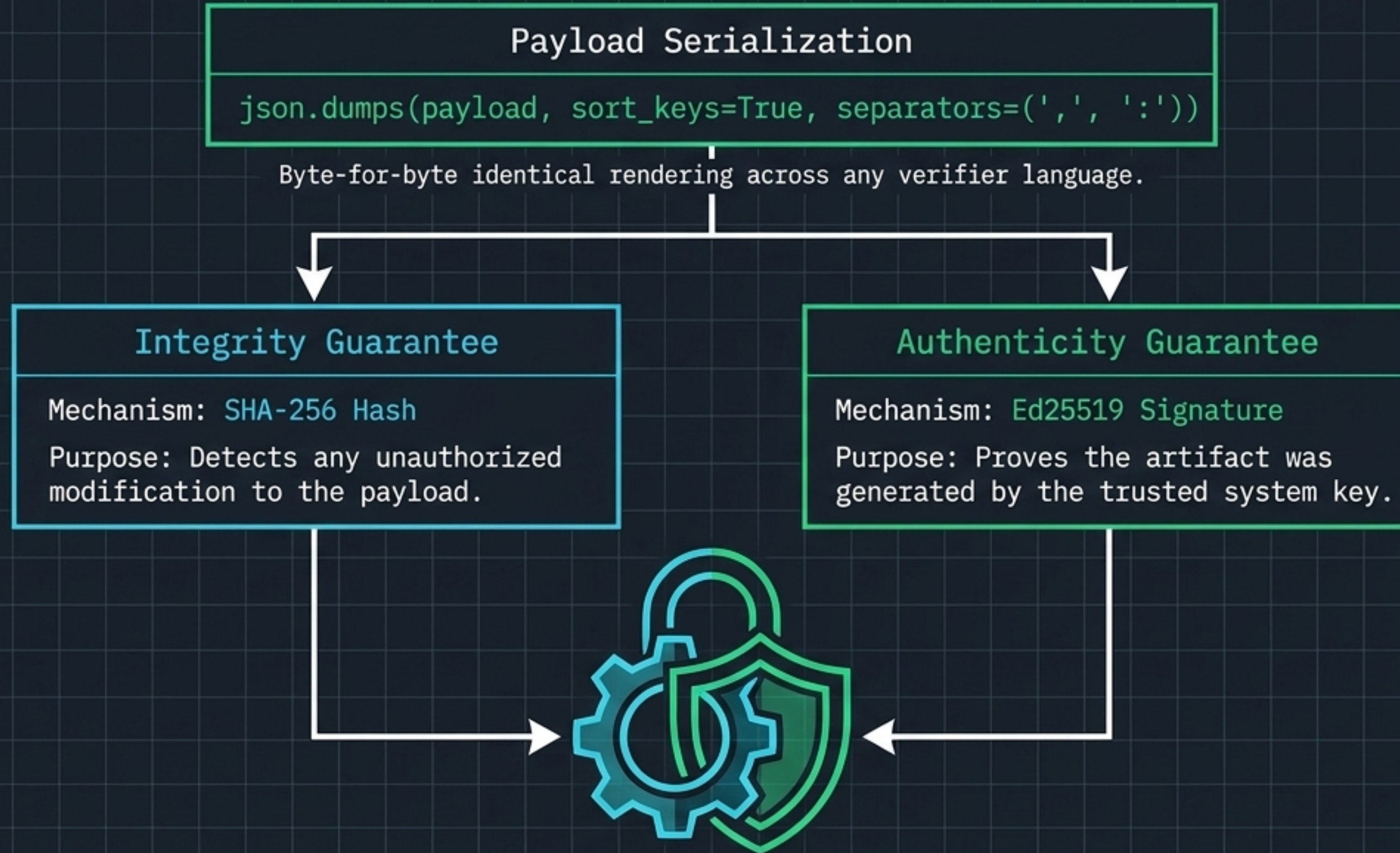


The system consumes these; it never hosts, exposes, or mutates the source-of-truth audit trail.

Capability Matrix

Job	Backing Code	Cadence	Primary Action
Merkle Publisher	app/merkle.py (_merkle_loop)	MERKLE_INTERVAL_MINUTES=60	Hashes/chains prior hour's events -> writes root
Retention Enforcer	app/retention.py (_retention_loop)	RETENTION_INTERVAL_HOURS=24	Archives past-horizon records -> deletes from source (if RW)
Annual Report Scheduler	app/reports.py (_annual_report_loop)	ANNUAL_CHECK_HOURS=1	Evaluates due-ness for SOX, NY DFS, EU AI Act
NAIC Listener	app/main.py (_naic_adverse_action_loop)	NAIC_POLL_SECONDS=300	Polls for adverse actions -> generates artifact per new event

Tamper-Evidence Model





The Chain Mechanism

- Reads audit events across AUDIT_BUS_DBs for the prior hour.
- Hashes each event into a leaf.
- Generates a root hash and signs it.
- Optionally POSTs to MERKLE_PUBLISH_URL via MERKLE_PUBLISH_TOKEN

Verification

```
Response:
{
  total_roots: N,
  breaks: [...],
  intact: true|false
}
```

A non-empty break array requires immediate investigation.

Erasure Cascade

Trigger: DSR Request Received
subject_id / user_id / data_subject_id (erasure, access, rectification, etc.)

Step 1: The Purge
Outbound call to QDRANT_URL to purge vector points matching the subject.

Step 2: File Deletion
System deletes all subject-tagged evidence files.

Step 3: Audit Counting
Audit trail is immutable. References are counted but strictly NOT deleted.
The deletion event itself is recorded.

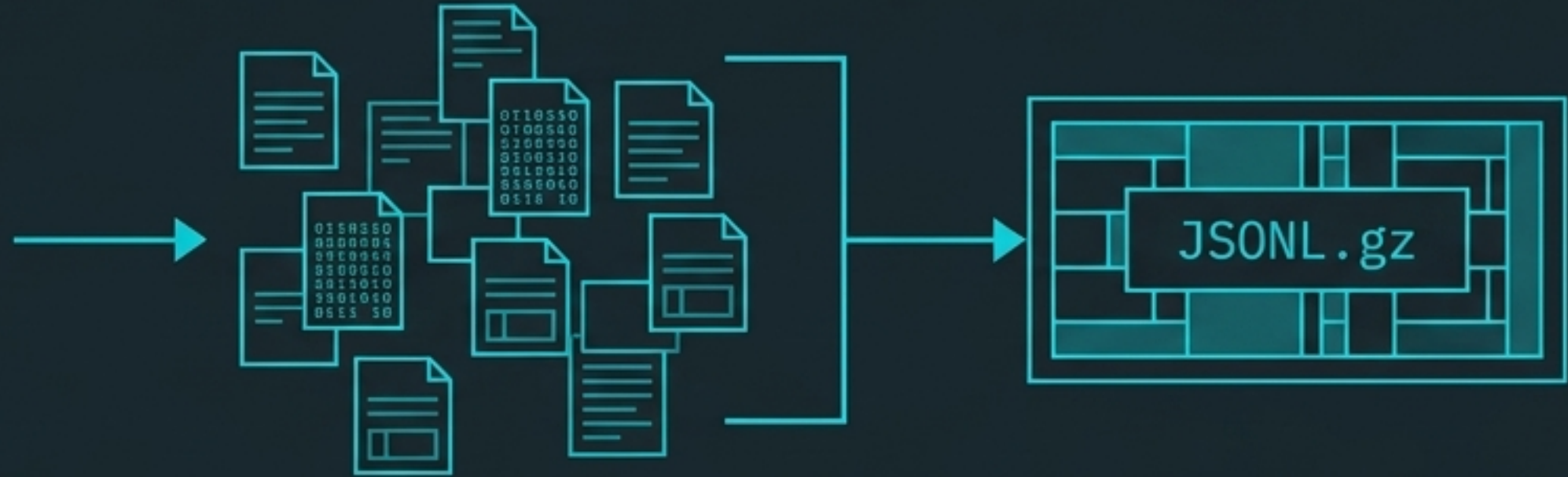


Artifact Output
Signed deletion-confirmation artifact written to DSR_DELETION_CONFIRMATION_DIR

Standard Automated Sweep

Driven by
`AUDIT_RETENTION_YEARS` and
`EVIDENCE_RETENTION_YEARS`
(default 7)

Action: Records past the horizon are
bundled and compressed.

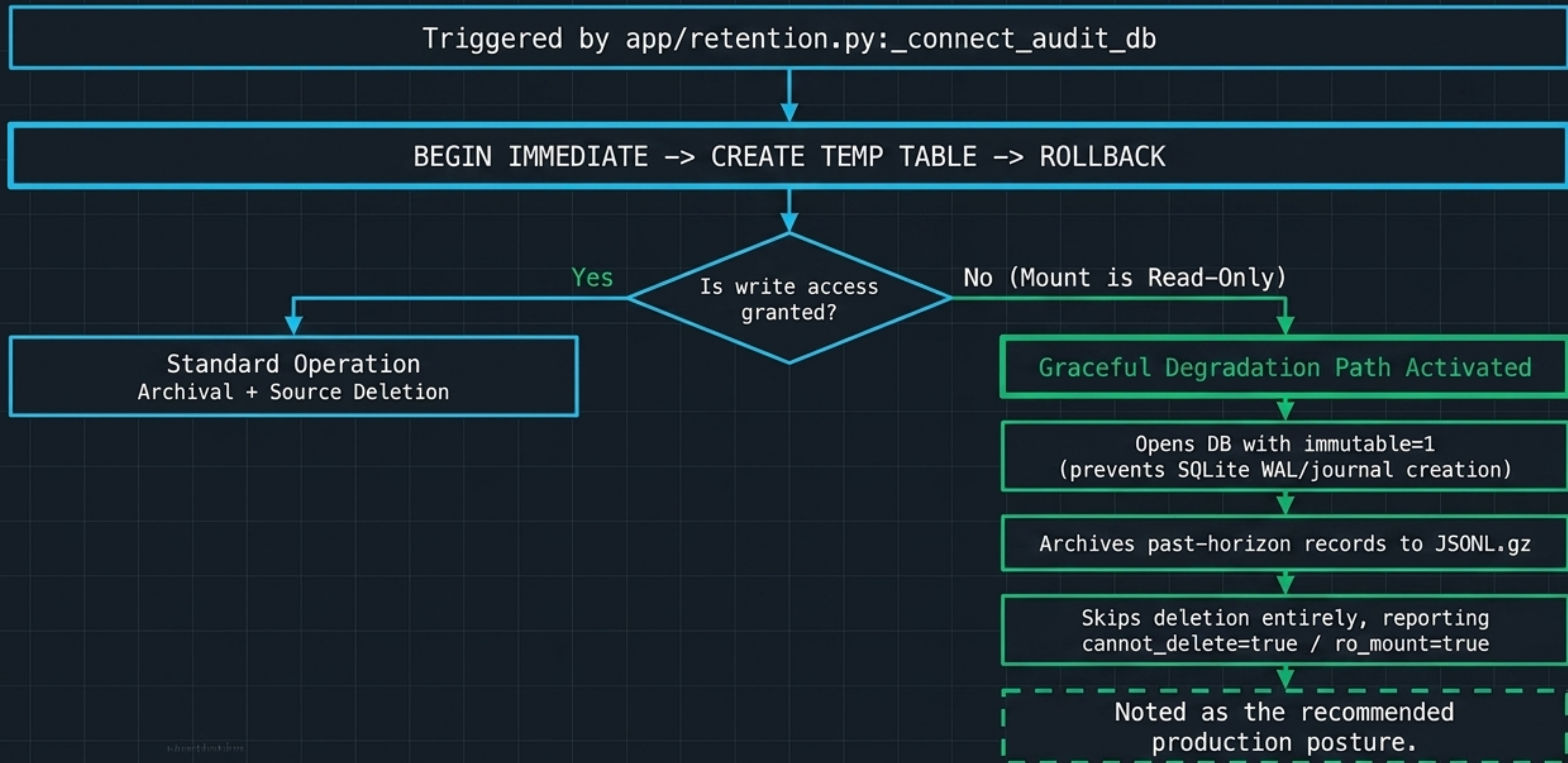


Legal Hold Override

Active hold pauses deletion for
a specific session ID, stored
in `LEGAL_HOLD_DIR`



Read-Only Graceful Degradation



Regulatory Reports



Trigger: Manual run-now (accepts year 1970-2200) or auto-fires annually.

Types: sox_attestation, nydfs_part500, eu_ai_act, naic_adverse_action_consolidated.

Output: Signed JSON evidence packages saved to **REPORTS_DIR** with embedded signature, **artifact_path**, and **artifact_sha256** using **REPORT_OPERATOR_ID**.

NAIC Adverse Actions



Logic: Scans for policy denials, threat detections, and high/critical guardian actions.

Safety: Idempotent execution. Re-running skips processed events (**skipped_already_tracked**).

State Volume: Cryptographic State Store

Volume: /state

Warning: Losing this volume loses signing keys and Merkle history

/compliance_jobs.sqlite	Local operational state DB (SQLITE_PATH)
/merkle-roots/	Immutable JSON files per Merkle root (MERKLE_ROOTS_DIR)
/archive/	Compressed JSONL.gz retention archives (ARCHIVE_DIR)
/dsr-confirmations/	Signed DSR deletion proofs (DSR_DELETION_CONFIRMATION_DIR)
/regulatory-reports/	Signed regulatory report artifacts (REPORTS_DIR)
/signing-keys/	Ed25519 key material (SIGNING_KEY_DIR)

Database: `app/db.py`

Applies additive migrations automatically on start via PRAGMA `table_info` introspection.

	merkle_roots
	Sequence-numbered, chained, signed hourly roots.

	legal_holds
	Active/released holds that pause deletion.

	regulatory_runs
	Generated report metadata + signing key id.

	retention_runs
	History of retention sweeps and per-class counts.

	dsrcascades
	Request log with per-subsystem deletion counts.

	naic_actions
	Idempotent tracking of adverse-action events.

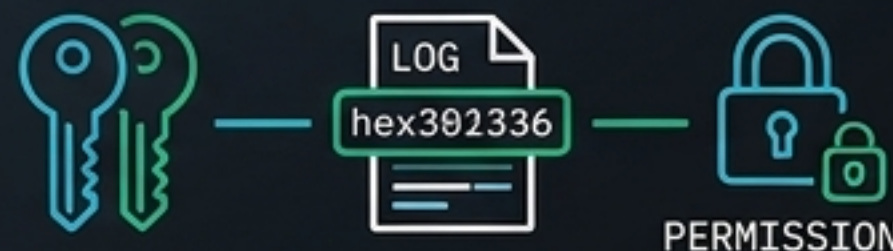
Rotation Mechanism

Top-level files are moved into `signing-keys/archive/<key_id>/`.
System restart mints a new keypair.



Genesis

Keypair generated on first start.
The `key_id` (16-hex prefix of public key) is logged exactly once.
The private key (with `0600` permissions) is NEVER logged.



Resilience

Public key files automatically self-heal if deleted while the private key remains on disk.

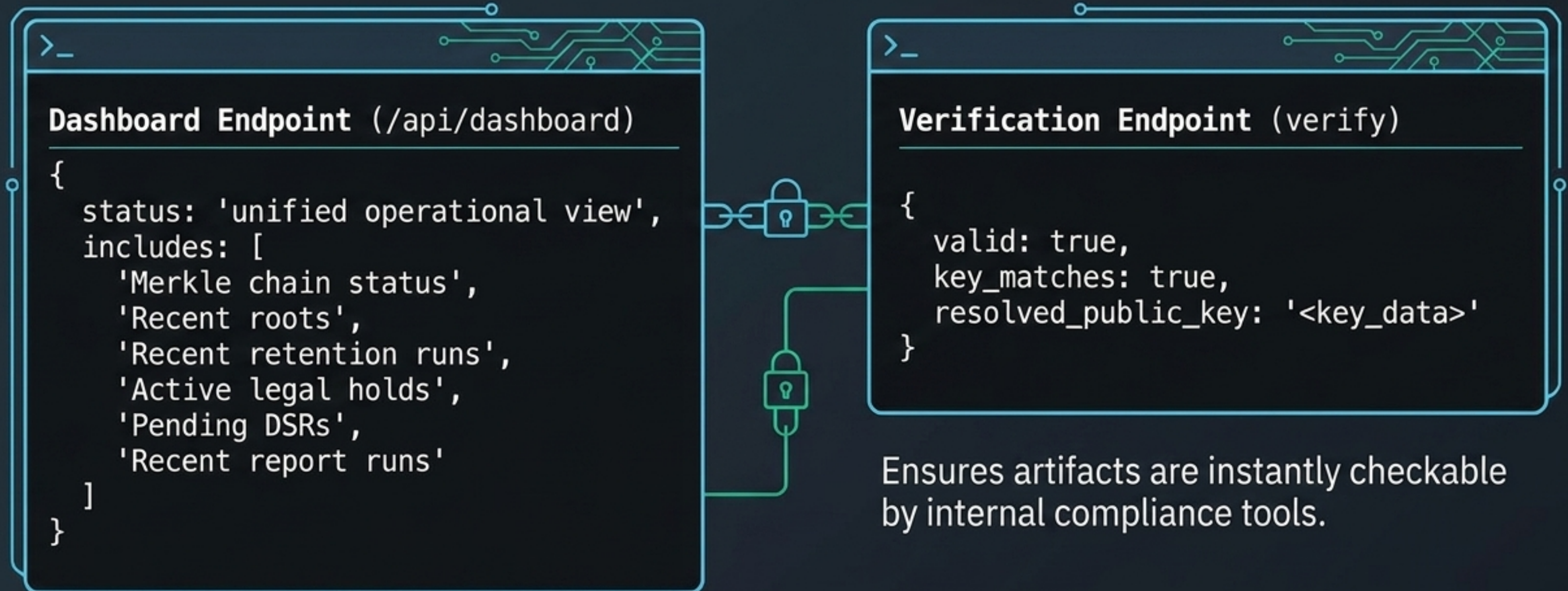


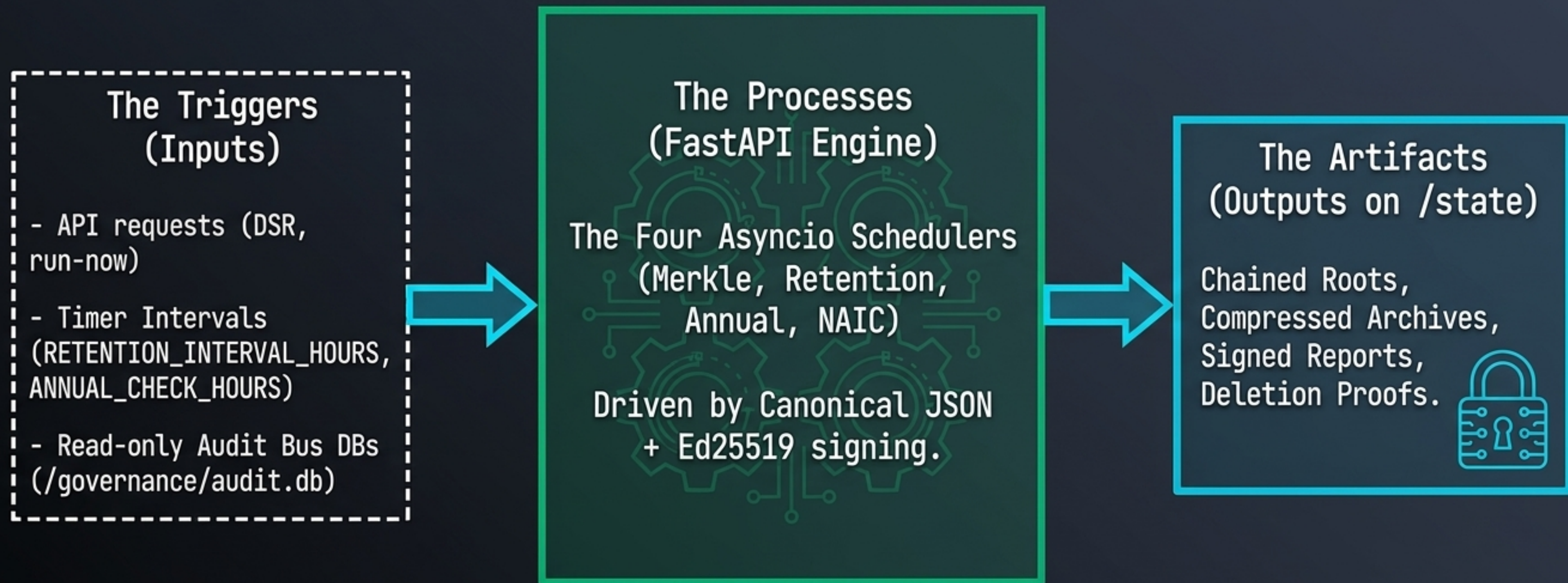
Seamless Backwards Compatibility:

``POST /signing/verify`` resolves both current and archived keys by ``key_id`` to maintain historical verifiability.

API Visibility Layer

No built-in authentication (relies on network policy).
Tests (tests/) are hermetic and require no external services.





bulletproof-compliance-jobs translates chaotic operational data into pristine, cryptographically verifiable compliance evidence—automatically, immutably, and transparently.