Etch Trust Report

Compliance evidence for etch.systems. Generated 2026-09-14 UTC.

> **Report scope.** Compliance posture, framework mapping, cryptographic primitives, and external anchor detail for the Etch hosted service. Reflects the shipped-today product state. Signed monthly statements + adversarial-suite results + full dogfooding report live at `https://etch.systems/evals`.

Compliance posture

Data Processing Agreement (DPA) available on request: `security@etch.systems`.

Framework mapping

Every Article and control ID cited below is addressed by a specific mechanism in the shipped product today. The "covered by" column names the mechanism so a compliance officer can trace every claim to code.

ARTICLE / CONTROL	REQUIREMENT	COVERED BY
EU AI Act		
`Art. 12`	Automatic recording of logs ("logs")	Signed tamper-evident event log + Merkle epoch closes
`Art. 13`	Transparency + provision of information	Offline reference verifier + public key fingerprints
`Art. 14`	Human oversight	pin_annotation MCP tool signs human notes into the chain
`Art. 15`	Accuracy, robustness, cybersecurity	Hybrid Ed25519 + SLH-DSA-SHA2-128f (FIPS 205) signing
SOC 2		
`CC6.6`	Logical + physical access boundaries	Per-project keys + scoped API tokens + admin scopes
`CC7.2`	System monitoring	Scheduled offline verifier + attestation history
`CC7.3`	Incident evaluation	Attestation verdicts + drill-into stack trace
ISO 27001		
`A.12.4`	Logging + monitoring	Signed audit chain + attestation cadence enforcement

ARTICLE / CONTROL	REQUIREMENT	COVERED BY
A.14.2	Secure system engineering	OSS + offline verifier + reproducible builds (roadmap)

Cryptographic primitives

- **SHA-256** (FIPS 180-4). Event hash. Every event canonicalized to JSON, then hashed. Chain is a linked list of these hashes.
- **Ed25519** (FIPS 186-5). Classical epoch signature. Signs the epoch envelope. Verifiable with pinned public keys.
- **SLH-DSA-SHA2-128f** (FIPS 205). Post-quantum epoch signature. Hash-based scheme. Hybrid with Ed25519 so verification survives a hypothetical break of classical elliptic-curve cryptography.
- **RFC 6962 Merkle tree**. Certificate-Transparency-shaped tree with 0x00 leaf and 0x01 node domain separators.
- **ECDSA-P256**. External anchor signature. Per-project key used only for Sigstore Rekor and Bitcoin OpenTimestamps submissions. Separate from the audit-chain hybrid.

External anchors

Every closed epoch is anchored to two independent public logs. Neither log is operated by Etch. Rewriting a signed epoch would require the log operator to publish evidence of the rewrite, which immediately breaks the anchor comparison.

- **Sigstore Rekor**. Public append-only log run by the Linux Foundation. Confirmation within hours. Look up any entry: `https://rekor.sigstore.dev/api/v1/log/entries/<uuid>`.
- **Bitcoin OpenTimestamps**. Public timestamping protocol using Bitcoin block headers. Confirmation within 6 to 12 hours. Auditors verify offline with `ots verify <proof>`.

Independent verification

Etch's guarantees are verifiable without operator cooperation. Any auditor can independently:

- Pin the project's public keys via the open endpoint `/projects/<project_id>/audit-log/public-keys`.
- Download the signed audit-log dump manifest via `/projects/<project_id>/audit-log/dump`.
- Run the reference verifier: `pip install etch-verify && etch-verify <manifest>`.
- Recompute chain integrity in a browser via the "Run chain-integrity check" widget on the auditor preview URL.

Report a security issue. security@etch.systems. Written responses within one business day.
Verify this report. The HTML source at `https://etch.systems/evals` renders the same content from

`src/etch/kpis_board.framework_matrix_with_articles`. Both are updated in the same commit if either changes.

ETCH TRUST