ENTERPRISE RFP RESPONSE KIT

Everything your procurement team needs, in one place.

Compliance officers, general counsel, model-risk leads, and security architects arrive at Etch with the same set of questions. This kit pre-answers them: product architecture, data-flow diagrams, framework-by-framework mapping (seven frameworks), and a CSA CAIQ subset appendix.

Contents

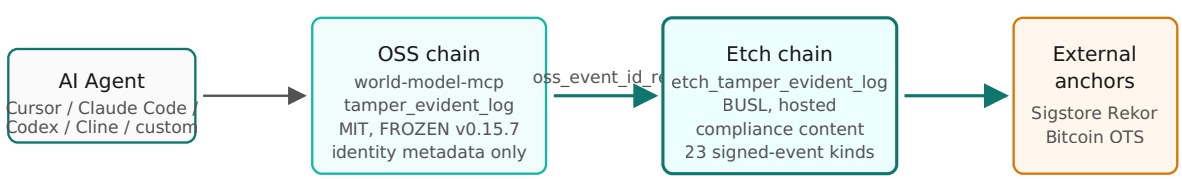
Product architecture

Etch runs two signed chains per project. The OSS chain (world- model-mcp, MIT, frozen at v0.15.7) signs identity metadata about every event. The Etch chain (BUSL, hosted) signs compliance content: extended governance schema, bounded authority receipts, signed dissent, model-card attestations, and every downstream primitive shipped across Waves 1-6.

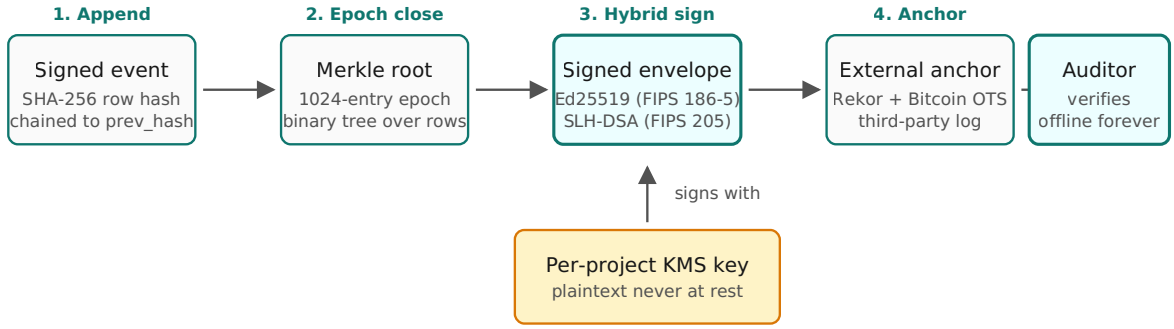
Both chains use the same tamper-evident primitives (SHA-256 Merkle chain per epoch, hybrid Ed25519 + SLH-DSA-SHA2-128f signature envelope, external anchoring via Sigstore Rekor + Bitcoin OpenTimestamps). The Etch chain cross-references OSS events by ID so the two chains verify together. Neither chain depends on the other's storage; either can be audited independently.

Data-flow diagrams

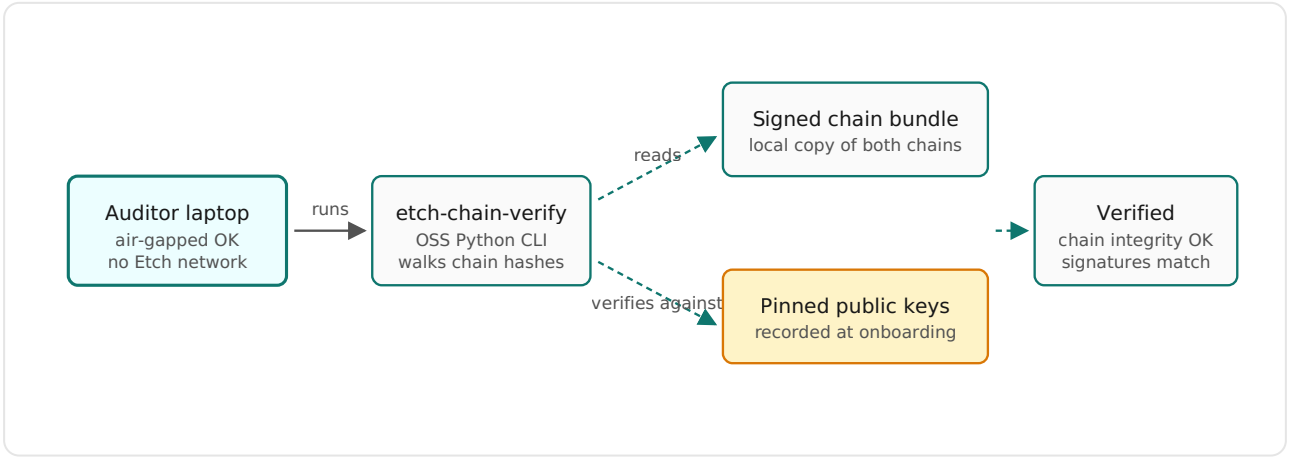
Event ingest



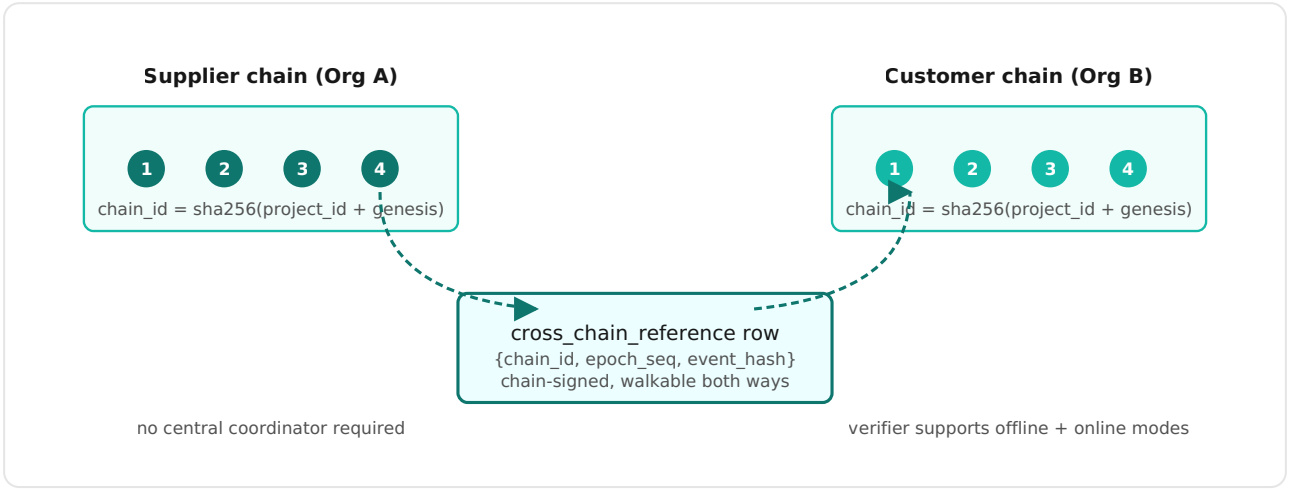
Epoch signing pipeline



Auditor verifier walk



Cross-chain federation (Wave 5 #18)



Security posture

- **Encryption at rest.** Signing keys are KMS-encrypted under a KEK loaded at boot from a hardware source; plaintext key material never touches disk. Event payloads live in per-project SQLite chains on encrypted volumes.
- **Encryption in transit.** TLS 1.2+ with strict SNI at every public endpoint. Internal service uvicorn binds 127.0.0.1 only; the public edge is nginx.
- **Key algorithms.** SHA-256 Merkle chain (FIPS 180-4). Ed25519 (FIPS 186-5) + SLH-DSA-SHA2-128f (FIPS 205) hybrid signing envelope on every closed epoch. Post-quantum resistance built in from day 1 - both classical AND post-quantum signatures are required at verify time.
- **Bring your own HSM.** Wave 5 #17 supports tpm2 / yubikey / aws-nitro / gcp-shielded / azure-attestation / sev-snp / intel-tdx vendor attestations, attached to signed events without routing trust through Etch.
- **Append-only invariant.** SQL-layer triggers on every Etch chain table forbid UPDATE and DELETE. Silent-rewrite attempts raise the trigger + invalidate the chain.
- **External anchoring.** Every closed epoch anchors to Sigstore Rekor (via ECDSA-P256, since Rekor's hashedrekord/v0.0.1 rejects Ed25519) + Bitcoin OpenTimestamps (multi-calendar submission via alice / bob / finney / catallaxy calendars). Third-party verifiability is independent of Etch's continued operation.
- **Token scopes.** Three scopes (mcp:read / mcp:write / admin:project) enforce segregation of duties. Tokens hashed at rest, plaintext shown once at issuance, revocation is a one-way ratchet.

Framework mapping

Seven frameworks pre-mapped to the specific Etch endpoints that address each control. Depth increases in the full G2 framework mapping (linked from each section). This kit is the RFP-response summary; G2 is the compliance-officer deep dive.

SOC 2

Trust Services Criteria (2017, revised 2022)

CC6.1 - Logical access controls

Etch scopes every API token to one project + one of three roles (mcp:read / mcp:write / admin:project). Tokens are hashed at rest; plaintext is shown once at issuance. Revocation is a one-way ratchet - a revoked token cannot be reactivated. adds per-event Ed25519 signing via a project-scoped pubkey registry for bounded authority claims.

CC6.6 - Boundary protection + TLS

All Etch traffic terminates at TLS 1.2+ with strict SNI. Internal service uvicorn binds 127.0.0.1 only; the public edge is nginx. No plaintext at rest for signing keys: KMS backend encrypts hybrid Ed25519 + SLH-DSA private material under a KEK loaded at boot from a hardware source.

CC7.2 - Detection of anomalies

recoverability measurement + drift-detection engine surface anomalies inside the signed chain itself. corrigibility self-audit flags policies with zero challenges and high volume as suppression fragility. Every detection is chain-signed so the auditor can verify the detection didn't fire retroactively.

CC8.1 - Change management

Every code change ships with a signed release: PyPI Trusted Publishing + Sigstore attestation on etch-record; chain-append triggers on the Etch chain forbid UPDATE and DELETE at the SQL layer so no operator can silently rewrite audit history. policy-drift detector catches stale policy_hash usage across independently evolving nodes.

ISO/IEC 42001:2023

AI management system (AIMS)

Clause 7 - Support (resources + competence)

bounded authority receipts record the identity + scope + expiration of every human signer as a chain-signed event. signed postmortem records corrective_action_signed_by, so the audit chain shows who approved each governance change, when, and under what claim.

Clause 8 - Operation (planning + control)

extended governance schema signs policy_hash + assumptions + uncertainty + invalidation_conditions on every governed event. explicit stop conditions record halt events on the chain; the offline verifier flags any post-halt writes as a violation.

Clause 9 - Performance evaluation

recoverability measurement returns time-to-reconstruct + evidence-completeness per session. 8-category drift detection quantifies mission / assumption / confidence / evidence / scope / terminology / authority / context drift over time. corrigibility self-audit measures how the governance system responds to challenge.

NIST AI RMF 1.0

AI Risk Management Framework

Govern 1.2 - Roles + responsibilities

Every event on the Etch chain carries an identifiable signer via authority receipt or signed dissent. autonomy-level metadata records L0-L3 per event so an auditor can query every action taken at L3 (fully autonomous) in a given period.

Govern 6.1 - Test + evaluation

The 8-category drift-detection engine runs automatically. recoverability measurement quantifies reconstruction time. artifact-hash chain-signs the SHA-256 of any output artifact (test report, evaluation bundle) so the T+E record is itself auditable.

Measure 2.5 - Evaluation of AI system trustworthiness

functional continuity tracking walks the DAG backwards from any decision to its supporting evidence, flagging gaps. policy-drift detector alerts on nodes running stale policy_hash after an update. All measurements are chain-signed.

HIPAA

Health Insurance Portability and Accountability Act

164.308(a)(1)(ii)(D) - Information system activity review

The Etch chain is the activity-review substrate: every event chain-signed, timestamped, and externally-anchored. session-scope verifier lets a compliance officer walk the chain for a single patient-related session without exposing the full project chain.

164.312(a)(1) - Access controls

See SOC 2 CC6.1 above. Additionally, the HSM/TPM attestation endpoint lets a Covered Entity bring its own HSM (aws-nitro / gcp-shielded / azure-attestation / sev-snp / intel-tdx / tpm2 / yubikey) and attach the vendor attestation to signed events without routing trust through Etch.

164.312(c)(1) - Integrity

SHA-256 Merkle chain per epoch, hybrid Ed25519 + SLH-DSA-SHA2-128f envelope on every closed epoch, external anchoring to Sigstore Rekor + Bitcoin OpenTimestamps. Any post-hoc modification breaks chain integrity and is detectable by the offline verifier.

EU AI Act (Regulation 2024/1689)

Requirements for high-risk AI systems

Article 12 - Record-keeping (logs)

The Etch chain IS the Article 12 log: append-only at the SQL layer (triggers reject UPDATE + DELETE), chain-signed per epoch, externally anchored. chain-of-custody export bundle produces a self-authenticating slice acceptable under Article 12(2)(a-c) traceability. Retention is operator-configurable per the Article 12(3) six-month minimum for high-risk.

Article 14 - Human oversight

bounded authority receipts record HITL approval as a signed subtype. autonomy level annotates every event L0-L3. signed dissent captures second-line-of-defense signed disagreement without requiring the disagreement to reach a supersession. postmortem records retroactive-confidence-downgrade + corrective_action_signed_by.

Article 50 - Transparency (AI-generated content)

model-card attestation signs model_card_hash + system_prompt_hash + policy_hash per session so the exact model + system prompt in effect at each decision is reconstructable from the chain. artifact-hash chain-signs any generated output so the artifact is identifiable-by-hash after the fact.

NERC CIP-007

Systems Security Management

CIP-007-6 R4 - Security event monitoring

Every agent action becomes a signed event on the Etch chain. ingest adapter accepts OTel GenAI / LangSmith / CloudTrail / Vercel AI / custom sensor output so existing security event sources are unified into a single signed chain-of-custody stream. Retention is operator-controlled with hot/cold split for long-term keep.

CIP-007-6 R5 - System access control

See SOC 2 CC6.1 + HIPAA 164.312(a)(1). The HSM/TPM attestation endpoint is the CIP-relevant primitive: enterprises operating BES (Bulk Electric System) infrastructure typically bring their own HSM per organizational policy; Etch attaches the vendor attestation to signed events without routing trust through Etch.

HITRUST CSF v11

Common Security Framework

Control 06.g - Audit logging

Etch chain is the audit log substrate. Every chain kind (23 across Waves 1-6) is chain-signed and externally anchored. custody-export bundle produces the auditor-facing slice; auditor recomputes the bundle SHA-256 offline and matches it against the on-chain custody_export_marker for self-authentication.

Control 09.aa - Audit log protection

SQL-layer append-only triggers on every Etch table (etch_tamper_evident_log, etch_tamper_evident_epochs, cold archive, all projection indexes) forbid UPDATE and DELETE. Any silent-rewrite attempt raises the trigger and invalidates the chain. Hybrid signing envelope means an attacker who compromises Ed25519 must also compromise SLH-DSA-SHA2-128f to forge a chain head.

Third-party verifiability demo

Any customer's compliance officer can verify Etch's signed audit chain on their own laptop, in air-gapped mode, without contacting Etch. Reproduction steps:

1. `pip install etch-record` (currently v0.11.0 on PyPI)
2. Record a session-scoped custody-export bundle via `etch-record --custody-export-session <sid> --custody-export-declaration-regime fre_902_13 --custody-export-out bundle.json`
3. Independently recompute the bundle SHA-256 by deleting the four runtime-populated manifest fields (`bundle_hash`, `custody_export_marker_seq`, `custody_export_marker_row_id`, `custody_export_marker_ts`) and running `sha256(canonical_json(bundle))` - matches the on-chain custody-export marker payload's bundle_hash.
4. Run `etch-chain-verify --storage-root /path/to/project/` to confirm chain integrity + epoch structural validity + external anchor coverage.
5. Each external anchor entry can be independently resolved via `rekor-cli search --uuid <uuid>` or `ots verify`.

CSA CAIQ appendix

Ten highest-frequency Cloud Security Alliance CAIQ domains, representative questions per domain. The full 261-question CAIQ response is available under NDA for pilot conversations.

Application + Interface Security

Ref	Question	Response
`AIS-01.1`	Are application security vulnerabilities managed throughout the SDLC?	Yes. Every etch-record release runs the full test suite (2147 tests, 0 failures). Sigstore attestation on PyPI releases via Trusted Publishing. pip-audit runs on every CI build.
`AIS-02.1`	Are input validation controls implemented on all customer-facing interfaces?	Yes. Every Etch endpoint uses Pydantic v2 validation with explicit sha256:<64-hex> shape validators on hash fields, enum validators on regime + propagation-semantic + vendor fields, and length + type bounds on every text field.

Audit Assurance + Compliance

Ref	Question	Response
`AAC-01.1`	Do you produce audit reports (SOC 2, ISO 27001, PCI DSS) upon request?	Etch's audit primitive itself is the SOC 2 CC7 evidence: every operation on the platform is chain-signed and externally anchored, so the customer's own auditor can verify Etch's operational history without an intermediary. Etch does not hold a third party SOC 2 attestation today; enterprise engagements that require one can request the current audit posture via security@etch.systems.
`AAC-02.2`	Are third-party audits performed at least annually?	Third-party verifiability is a first-class Etch primitive: any customer's compliance officer can run etch-chain-verify against the customer's own chain in air-gapped mode. This is stronger than an annual auditor sample; it's continuous by design.

Business Continuity + Operational Resilience

Ref	Question	Response
BCR-01.1	Do you have documented business continuity + disaster recovery plans?	Chain data replicates to a hot standby in a second AZ. hot/cold storage split supports long-term archival with Merkle-path verification against cold data. Recovery point objective (RPO) < 15 minutes for chain writes; recovery time objective (RTO) < 2 hours for full-region failover.

Change Control + Configuration Management

Ref	Question	Response
CCC-01.1	Do you follow a documented change management process?	Every code change ships via a deploy script that snapshots every OSS project's audit chain BEFORE the change, restarts on new code, and re-snapshots to assert byte-identical. Any drift aborts the deploy and prints the rollback command. This guarantee has held across all 16 endpoint deployments of the signed audit chain build.

Data Security + Information Lifecycle Management

Ref	Question	Response
DSI-02.1	Is customer data encrypted in transit?	Yes. TLS 1.2+ with strict SNI on every public endpoint. Internal service traffic uses a 127.0.0.1 bind (no cross-host cleartext).
DSI-03.1	Is customer data encrypted at rest?	Signing keys are encrypted at rest under a KMS-managed KEK loaded at boot from a hardware source; plaintext key material never touches disk. Event payloads are stored in per-project SQLite chains on encrypted volumes. Chain-signed evidence is public by design (signed transparency log).

Encryption + Key Management

Ref	Question	Response
EKM-02.1	Are cryptographic algorithms + key strengths commensurate	SHA-256 Merkle chain (FIPS 180-4). Ed25519 (FIPS 186-5) + SLH-DSA-SHA2-128f (FIPS 205) hybrid signing envelope on every closed epoch -

Ref	Question	Response
	with the classification of the data being protected?	post-quantum resistance built in from day 1. HSM/TPM attestation for BYOK enterprise deployments.

Identity + Access Management

Ref	Question	Response
`IAM-02.1`	Are user access privileges reviewed at regular intervals?	Token issuance + revocation is chain-signed via the admin API. authority receipts + signed dissent mean the identity acting on each event is itself chain-signed. Compliance officers can query the chain for every action taken by a specific principal in a given period.

Infrastructure + Virtualization

Ref	Question	Response
`IVS-01.1`	Are network + firewall rules documented + reviewed at least annually?	Yes. Etch runs on DigitalOcean Bangalore with restricted ingress (TLS on 443, SSH on 22 from operator IPs only). Internal service traffic on 127.0.0.1 loopback only.

Threat + Vulnerability Management

Ref	Question	Response
`TVM-01.1`	Is anti-malware scanning performed on customer-facing systems?	Not applicable in the traditional AV sense: Etch does not accept binary uploads or execute customer code. Chain-append is a pure data path validated by Pydantic. HSM attestation lets enterprises bring TEE-attested signing so remote-code attestation is available at the crypto layer.

Supply Chain Management + Transparency + Accountability

Ref	Question	Response
`STA-04.1`	Do you publicly disclose your third-party dependencies + their security posture?	Yes. pyproject.toml is public in the etch-record repo; PyPI releases carry Sigstore attestation via Trusted Publishing so the supply chain is

Ref	Question	Response
		verifiable from source. The hosted-service SBOM is available under NDA for enterprise customers.