Compliance + Audit-Verifier Handbook

Regulatory posture, audit-chain architecture, and verifier walkthrough.

§1 Regulatory posture by jurisdiction

Framework	Sparcle's posture	Customer's path
HIPAA (US health)	Architecture designed for PHI residency. No PHI reaches Sparcle infrastructure because there is none in the data path. BAA available at deployment-services tier.	Customer's existing HIPAA boundary covers Sparcle as deployed software, not as a covered entity or business associate.
HITRUST CSF	Not held. ~12 months in self-attestation cycle if a customer sponsors.	Customer's HITRUST controls map to Sparcle's architecture (per-tenant CMK, audit chain, ACL pre-filter).
GDPR (EU)	Architecture aligned with Articles 6, 17 (erasure via crypto-shred), 25 (privacy-by-design), 32 (security), 44+ (no third-country transfers when EU-deployed).	Customer remains controller. Sparcle deploys inside customer's processing perimeter; no transfer event occurs.
DPDPA (India)	Architecture aligned. Per-tenant CMK supports localization.	Customer remains the data fiduciary.
CCPA / CPRA (California)	Architecture aligned. Right-to-delete supported via crypto-shred.	Customer's CCPA program covers Sparcle as on-premises tooling.
DORA (EU financial)	Architecture aligned. Sparcle is software, not an ICT third-party service provider, in the customer-deployed model.	Customer registers Sparcle under Article 28 if applicable, typically as non-critical.
NIS2 (EU)	Architecture aligned. Audit chain supports incident-report evidence requirements.	Customer's NIS2 program covers Sparcle as software dependency.
SEC Reg SCI	Architecture aligned. Tamper-evident audit chain supports Rule 1001(a) recordkeeping.	Customer's Reg SCI responsibilities supported by verifier-export workflow.
SOX (US public co.)	Architecture aligned. 4-axis ACL supports segregation-of-duties controls. Audit chain supports management-assertion evidence.	Customer's ICFR covers Sparcle as a deployed system.
GLBA (US financial)	Architecture aligned. Customer NPI residency supported by in-perimeter deployment.	Customer's Safeguards Rule program covers Sparcle.
PCI DSS	Not in scope. Sparcle is not in cardholder data flow.	Not applicable in normal deployment.
CMMC L1/L2/L3	Not held. Architecture maps to NIST 800-171; CMMC sponsor agency required for authorization path.	Customer's CMMC posture covers Sparcle as software dependency in CUI handling enclave.
FedRAMP	Not held. Architecture FedRAMP-Moderate-ready; ~12-18 months with sponsor agency.	Customer's existing ATO covers Sparcle as deployed software in the boundary.
ITAR / EAR	Architecture compatible. 4-axis ACL with `country` axis enforces nationality-based access.	Customer's export-control program covers Sparcle as deployed in CUI enclave.
FIPS 140-3	Not held — Sparcle does not ship its own crypto module. Operations route to customer-provided KMS / HSM.	Customer's FIPS-validated KMS / HSM covers Sparcle's cryptographic path.
ISO 27001 / 27017 / 27018	Not held. Architecture compatible with ISMS controls. ~18 months if sponsored.	Customer's existing ISMS covers Sparcle.

This posture is current as of the document version date. Compliance is a relationship, not a state — frameworks evolve and Sparcle's posture evolves with them. Refresh quarterly or on framework-change trigger. Last review: 2026-05.

§2 Audit-chain architecture

Every event Bolt + Aeira processes is sealed into a Merkle hash chain. Roots are signed by a KMS-held key every 10 seconds. The chain is cryptographically tamper-evident.

2.1 — The chain

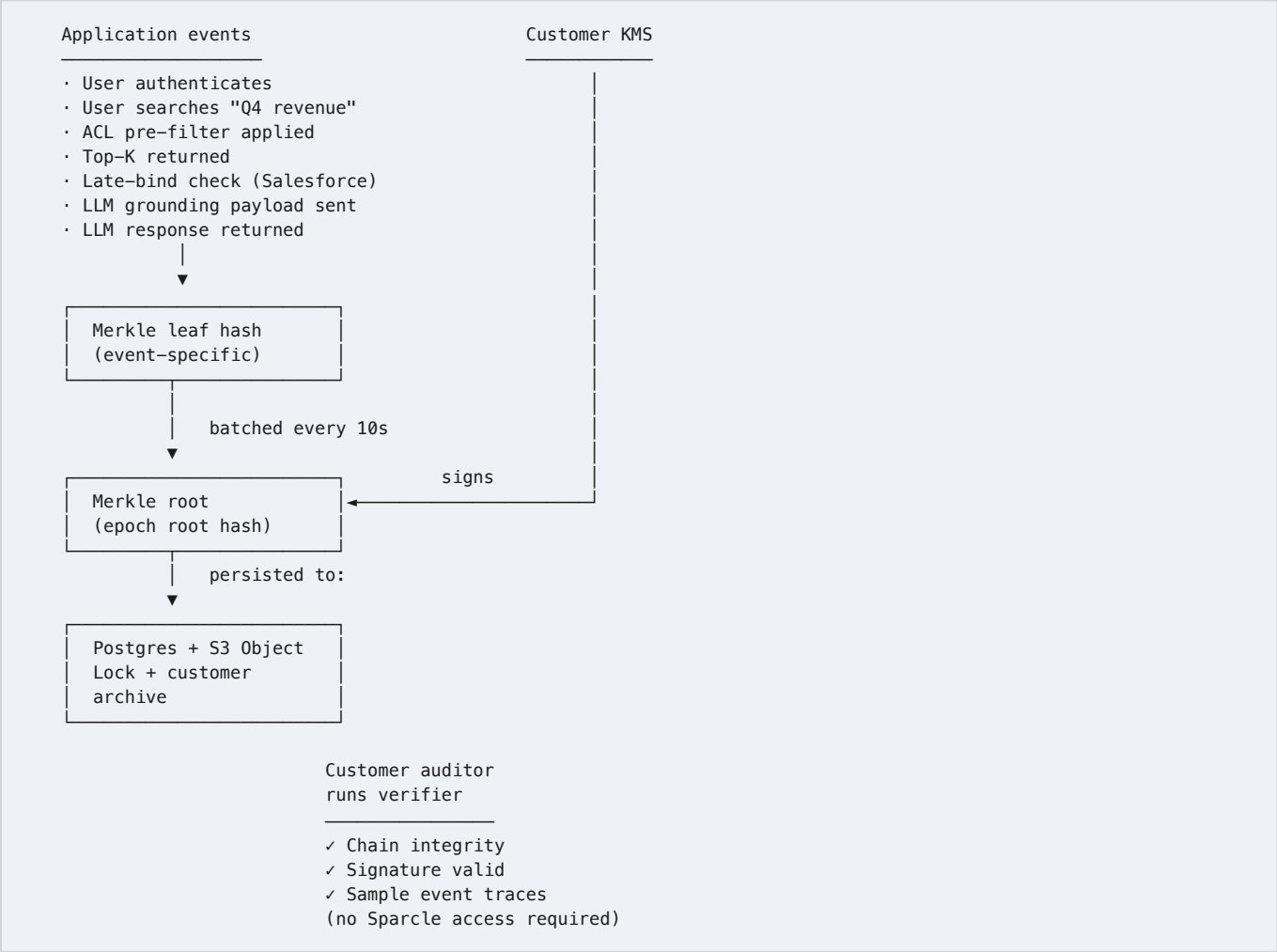
Every event — ingest, search, ACL decision, late-bind permission check, LLM grounding payload, administrative action — is sealed into a Merkle hash chain. Chain roots are signed by a KMS-held key on a 10-second cadence. The signed roots are persisted to the customer's database, to write-once storage if available (S3 Object Lock at Enhanced tier), and exportable to any customer-controlled archive. Modifying any historical event invalidates every subsequent Merkle root.

2.2 — Cross-product byte-compat

Bolt's session audit chain and Aeira's data-plane audit chain share an encoding format. A single chain export covers the full agent → substrate decision trail for a user session. This compatibility is enforced by the `aeira-traits-conformance` crate, which produces a byte-identical hash for the same logical event regardless of which product wrote it.

2.3 — KMS rotation

The signing key rotates on a customer-defined schedule (default: quarterly). Historical Merkle roots remain verifiable against the historical public key for the duration of the customer's retention policy. The verifier binary handles key rotation transparently: an audit export includes the per-epoch public key, and verification proceeds against the correct key for each Merkle root.



§3 Verifier walkthrough

How a customer auditor verifies Sparcle's audit chain. Without Sparcle's cooperation.

3.1 — Step-by-step

1. **Request a chain export.** The customer's Aeira administrator initiates `aeira-export-chain --tenant <id> --from <date> --to <date>` from the admin console or CLI. Output is a single `.aeira-chain` file containing the event log, Merkle roots, and KMS public-key bundle for the relevant epochs.
2. **Obtain the verifier.** The auditor obtains `aeira-audit-verify` from the customer or downloads from Sparcle's signed release page. The binary is statically linked, ~10 MB, runs on macOS / Linux / Windows. **No Sparcle services are contacted during verification.**
3. **Execute verification.** A single command. The verifier reads the chain, recomputes each Merkle root from leaf events, checks each KMS signature against the embedded public-key bundle, and outputs a pass/fail report.
4. **Inspect the report.** Chain integrity (PASS/FAIL), per-epoch signature validity, sample event traces with full payload and Merkle inclusion proofs, and tamper detection naming the affected epoch if any.
5. **Cross-verify.** If the customer archives chain roots to a separate write-once store, the auditor compares those roots to the chain export. A match confirms no rewriting occurred since the archive event.

3.2 — Mock verifier output

```
$ aeira-audit-verify ./tenant-acme-chain-2026-q2.aeira-chain
aeira-audit-verify 1.0.0 (sparcle.app/audit-verify)

Loading chain ..................................... OK
  Loaded 412,841 events across 8 epochs (2026-04-01 → 2026-06-30)
  Tenant: acme-corp · Region: us-west-2

Verifying Merkle structure ........................ OK
  All 412,841 leaf hashes validated.
  All 8 epoch root hashes recomputed and matched.

Verifying KMS signatures .......................... OK
  Epoch 1 (2026-04-01..2026-04-30) — signed by key-id 9f12a3 — PASS
  Epoch 2 (2026-05-01..2026-05-31) — signed by key-id 9f12a3 — PASS
  Epoch 3 (2026-06-01..2026-06-30) — signed by key-id a4c918 — PASS
  ...

Sampling 10 events for trace inspection ........... OK
  Event 0a7b21 (2026-05-17T14:22:01Z) · user=u-7281 · query=...
  Event b1f3c8 (2026-05-22T09:11:33Z) · ACL decision=allow · ...
  ...

VERIFIER RESULT: PASS
Chain integrity confirmed. Signatures valid. No tampering detected.
```

3.3 — What the verifier does NOT do

- Does not assert Sparcle's behavior was "correct" — only that the recorded behavior was not altered after the fact.
- Does not validate the truth of LLM responses — only that the grounding payload and response were faithfully captured.
- Does not verify customer-side application logic — only the chain segment Sparcle produced.
- Does not provide a SOC 2 / ISO 27001 / HITRUST attestation.

> *The verifier provides cryptographic evidence; it does not provide legal compliance.* **Customer's auditor / regulator interprets the evidence.**

§4 Indemnity, sub-processor list, contractual addenda

4.1 — Sub-processors (by Bolt tier)

Bolt tier · deployment mode	Sparcle sub-processors
Bolt Absolute · customer self-hosted (docker-compose or Helm)	**None.** Customer chooses LLM endpoint, KMS, storage, Kubernetes provider. Each is a customer-side relationship; Sparcle does not contract with them on the customer's behalf.
Bolt Bundled · customer self-hosted + optional managed AI router	**None with BYO LLM (BYOK).** If customer opts into the managed AI router (10M-token pool), the upstream LLM provider becomes a Sparcle-contracted sub-processor for token routing only; customer can switch to BYO LLM to avoid this.
Bolt Complete · Sparcle-managed hosting	**Sparcle operates hosting** on customer's behalf — itself a contracted processor under GDPR Art. 28. Customer-isolated environments, customer-managed KMS (Vault / AWS KMS), customer-controlled signing keys. Underlying cloud (AWS / Azure / GCP) is a documented sub-processor. **For regulated workloads, Absolute or Bundled is the recommended tier.**
Trial sidecar (single binary, customer-laptop or dev VM)	None.

> **Compliance note.** *In Bolt Absolute and Bundled (BYO LLM), zero Sparcle-managed sub-processors — the key differentiator vs SaaS competitors (Glean, Hebbia, Harvey, Copilot), each of whom bring vendor-managed inference / storage / logging that become sub-processors under GDPR Art. 28, ICT third-party under DORA Art. 28, business associate under HIPAA. Bolt Complete is a contracted-processor model; not the recommended path for regulated buyers.*

4.2 — Indemnity posture

For deployment-services tier (pilot + ongoing support):

- Sparcle indemnifies customer against third-party claims arising from Sparcle's gross negligence or willful misconduct, up to fees paid in the preceding 12 months.
- No indemnity against customer misuse, customer-side configuration errors, choice of LLM endpoint, or claims arising from data ingested into the deployment.
- IP indemnity covers third-party claims that the software itself infringes a US-issued patent or copyright, subject to standard exclusions.

Caps and exclusions negotiated per pilot contract. Standard MSA template available on request.

4.3 — Customer contractual addenda

- **DPA:** Absolute / Bundled (BYO LLM) — Sparcle does not process personal data; DPA not strictly required, but Sparcle signs the customer's template as a courtesy. **Bolt Complete** — Sparcle is a processor under GDPR Art. 28; DPA required.
- **BAA (HIPAA):** offered at deployment-services tier under Absolute / Bundled (Sparcle is not a runtime business associate — no PHI flows through Sparcle infrastructure). Bolt Complete is not recommended for PHI; if used, full BAA required.
- **SCCs (EU):** not applicable in EU-deployed Absolute / Bundled (no third-country transfer). In non-EU Bolt Complete, SCCs apply.
- **Source-code escrow:** at pilot tier and above. Triggers: Sparcle bankruptcy / dissolution / sustained service termination. Customer-selected agent (Iron Mountain, NCC Group).

4.4 — Contact

For compliance-specific questions: **compliance@sparcle.app**
For pilot contract negotiations: **bolt@sparcle.app**