CISO

- What risk does Secrets Platform reduce?
  - Eliminates secret sprawl, enforces purpose-bound access via PDP, and provides non-leaky auditing (HMAC resource_ref) across all use via Kafka → Analytics.
- How do we ensure least privilege?
  - Policy decisions (PDP) with obligations (ttl, max_uses) + optional OAuth scopes at the API surface; tenant/mount guards prevent cross-tenant access.
- How is misuse or exfiltration detected?
  - Structured audits with subject, purpose, effect, correlation/trace IDs; dashboards and alerts via Analytics/Prometheus/Grafana.
- What's our vendor lock-in risk?
  - Providers are pluggable (OpenBao/HashiCorp KVv2, YAML dev); Canonical URIs and policy stay stable across providers.
- Compliance reporting?
  - Kafka audit topics feed Analytics and ClickHouse for retention, filtering by subject/resource_ref/purpose; export to your GRC tool.

See: `services/crud-service/secrets/05-security-model` , `services/crud-service/secrets/12-auditing-logging` .

Security Architect

- How do PEP and PDP integrate?
  - PEP in `VaultService` calls PDP with subject, tenant, canonical URI, purpose, and context; enforces obligations and sender binding before provider access.
- What bindings are supported?
  - DPoP/mTLS preferred; audience checks as fallback; anti-replay with JTI.
- How are Canonical URIs structured?
  - `provider[+engine]://<mount>/<path>#<fragment>[?version=N]` ; used for policy attributes and safe audits (HMAC ref).
- How do we segment tenants/mounts?
  - `TENANT_ALLOWED_MOUNTS` guard pre-authorizes, blocking cross-tenant access by construction.
- Where do we see decisions and obligations?
  - PDP decision payloads and PEP enforcement are traceable via OTel and auditable via Kafka topics.

See: `services/crud-service/secrets/03-canonical-uris-and-policy`, `services/crud-service/secrets/11-authorization-model-authzen`, `services/crud-service/secrets/SECRETS_PDP_ENRICHMENT`.

DevOps / SRE

- How do I deploy and observe Secrets?
  - Use provided Docker/K8s configs; metrics on `/metrics`, traces via OTLP, logs to stdout/Loki; health/readiness endpoints per service.
- Where do audits and errors go?
  - Kafka topics (e.g., `crud.secrets`, `crud.secrets.audit`, `crud.errors`), ingested by Analytics.
- How do I configure providers and HA?
  - Set `VAULT_URL`, credentials, timeouts/pools; for OpenBao/HashiCorp HA, see HA guide and load-balancing recommendations.
- What knobs gate API hardening?
  - `SECRETS_API_REQUIRE_AUTH`, `SECRETS_ENFORCE_SCOPES`, `SECRETS_AUDIENCE`.
- How do I validate end-to-end?
  - Run sample reads/writes, verify audits/metrics/traces, and confirm PDP decisions/obligations in logs.

See: `services/crud-service/secrets/06-observability`, `services/crud-service/secrets/SECRETS_DEVOPS_GUIDE`, `services/crud-service/secrets/SECRETS_HA_OPENBAO`.

QA / Test

- How do I test without a live vault?
  - Use YAML provider or record/replay; writes/deletes are blocked outside dev/test.
- What edge cases should I cover?
  - Missing metadata, soft-deleted keys, 404 vs 403 mapping, version-pin reads, obligation expiry and max_uses exhaustion.
- How do I correlate failures?
  - Use `correlation_id` and trace IDs; inspect Kafka `crud.errors` and `crud.operations` where `success=false`.
- How do I simulate multi-provider behavior?
  - Canonical URIs select strategies; switch schemes to validate parity.

See: `services/crud-service/secrets/04-providers`, `services/crud-service/secrets/10-troubleshooting-runbooks`.

Sales / Field

- When do we win?
  - Per-use PDP authorization, programmatic auditing, and workflow/automation integration; strong for cloud/dev secrets and platform teams.
- How do we compare to PAM and workflow tools?
  - We don’t broker human sessions; we secure programmatic use and integrate with CRUD workflows and PDP decisions.
- What’s the executive pitch?
  - Reduce risk and blast radius with purpose-bound grants, full observability, and provider choice—without breaking developer velocity.
- What’s the proof plan?
  - Demo canonical URIs, PDP decisions with obligations, audits flowing to Analytics, and a simple rotation workflow.

See: `personas/sales`, `services/crud-service/secrets/01-executive-overview`.