SYMMETRIQ

Architecture & Deployment Guide

Decentralized identity for permissioned access to smart contracts on permissionless EVM networks.

PREPARED FOR

Chief Architects · CISOs · Platform Engineering · Security Architecture

Version 1.0 · Confidential under NDA

1. Executive summary

Identity for the chain, without changing the chain.

SymmetriQ provides a deployable identity and signing fabric that lets enterprises run regulated workloads on permissionless EVM networks. It bridges existing identity providers (Azure AD / Entra, Keycloak) to W3C DIDs, evaluates signing decisions through a deterministic policy engine, and produces every signature inside hardware key custody (HSM, TPM, secure enclave). All decisions are recorded in a tamper-evident, hash-chained audit store and exported to existing SIEM and SOAR estates.

This document is the reference for chief architects and CISOs evaluating SymmetriQ for enterprise deployment. It covers the logical and physical architecture, deployment topologies, network and trust boundaries, key management, threat model, compliance mapping, operational model, and a phased rollout plan.

At a glance

Deployment models	Private cloud (AKS/EKS/GKE), hybrid, on-prem, air-gapped enclave
Identity providers	Azure AD / Entra, Keycloak, any OIDC/SAML/LDAP IdP
Key custody	FIPS 140-2 Level 3 HSM (network or PCIe), TPM 2.0, AWS/Azure/GCP KMS, secure enclaves
Chain compatibility	Any EVM L1/L2; ERC-1271, ERC-4337, custom verifier libraries
Compliance posture	SOC 2 Type II controls, ISO 27001, NIS2, DORA-aligned audit trail
Crypto agility	secp256k1 today; Ed25519, BLS, NIST PQC (ML-DSA, SLH-DSA) ready
Footprint	Stateless services; ~6 vCPU / 12 GB per AZ baseline; horizontally scalable
SLO targets	Sign latency p95 < 120 ms (HSM-bound); 99.95% control plane availability

2. Reference architecture

SymmetriQ is composed of six logical services arranged across four security zones. Services are stateless and horizontally scalable; persistent state lives in PostgreSQL HA (DID Registry and Audit Store) and in hardware key stores (HSM/TPM). The reference architecture below shows the logical placement of every component, the direction of data flow, and the zones each component operates within.

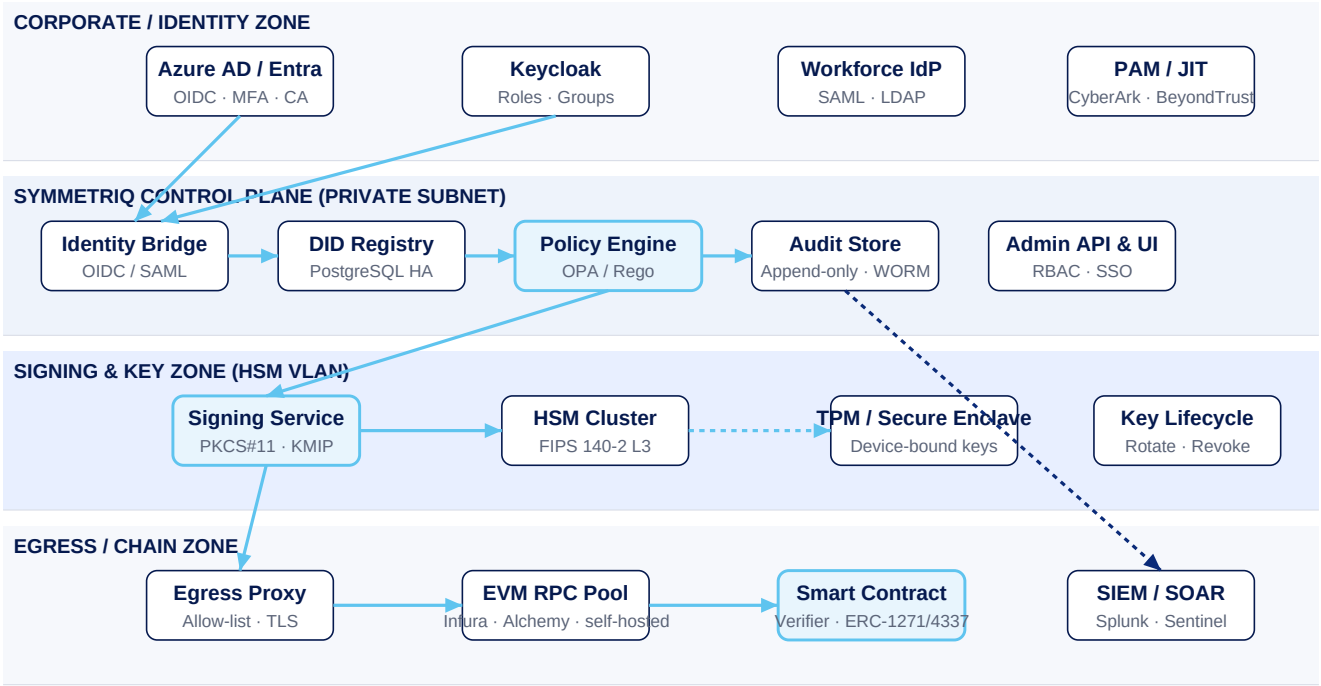

Figure 1 — Logical reference architecture across identity, control, signing and egress zones.

2.1 Component responsibilities

Component	Responsibility	Tech / interfaces
Identity Bridge	Federates with enterprise IdPs; validates tokens; resolves user, group, role claims.	OIDC, SAML 2.0, LDAP/SCIM
DID Registry	Issues, stores and lifecycles DIDs; maps corporate identity ↔ DID ↔ key handle.	W3C DID Core; PostgreSQL HA; gRPC
Policy Engine	Versioned policy-as-code; deterministic evaluation of every signing request.	OPA / Rego, JSON; GitOps-managed
Signing Service	Brokers signing to HSM/TPM/enclave; never sees plaintext key material.	PKCS#11, KMIP 2.x, platform attestation APIs
On-chain Verifier	Solidity library; rejects any transaction not signed by a valid SymmetriQ DID.	ERC-1271, ERC-4337, custom modifier
Audit Store	Append-only, hash-chained event log; exports to SIEM in near real-time.	PostgreSQL + WORM bucket; Kafka/HEC/Sentinel

3. Deployment topology

SymmetriQ is delivered as container images and Helm charts. The recommended production deployment is a multi-AZ Kubernetes cluster inside an enterprise-owned VPC, with the HSM cluster attached to a dedicated VLAN. Air-gapped deployments replace the cloud control plane with on-prem Kubernetes (OpenShift, Rancher, RKE2).

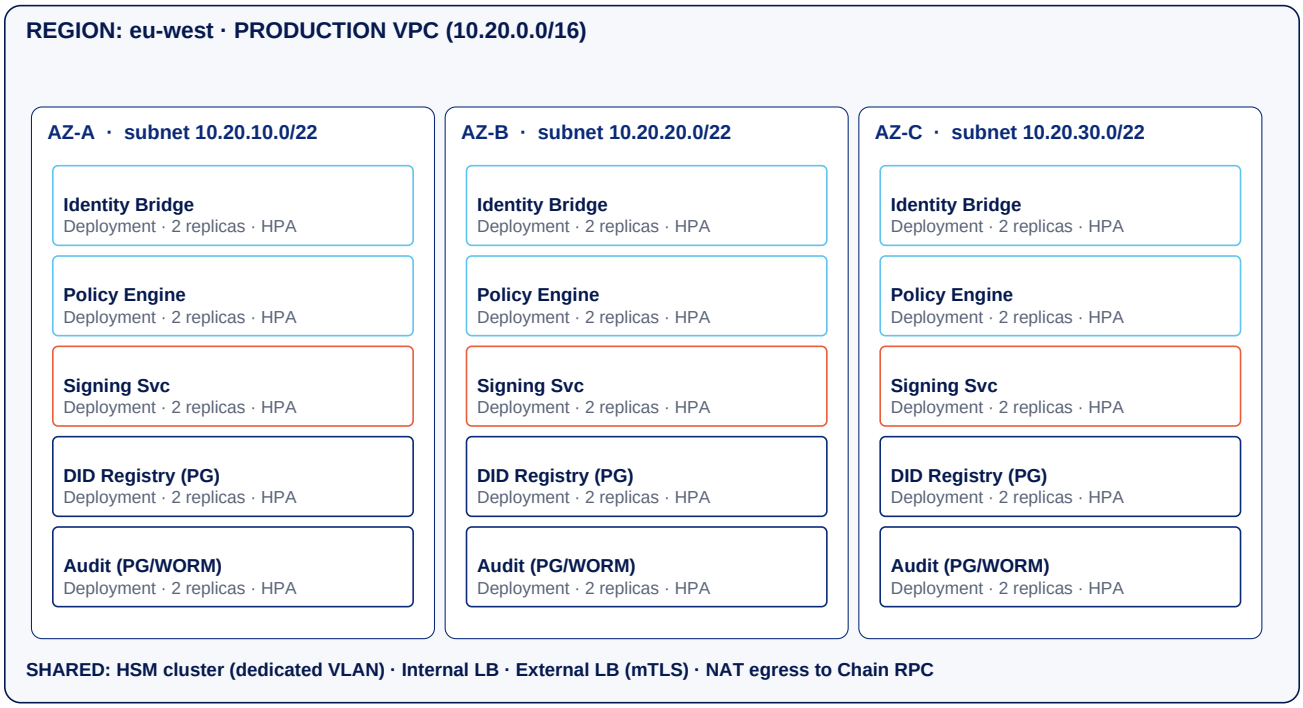

Figure 2 — Reference multi-AZ Kubernetes deployment. HSM cluster on dedicated VLAN, internal LB for east-west, external LB with mTLS for north-south.

3.1 Supported deployment models

Model	Use case	Control plane	Key custody
Private cloud	Default enterprise deployment	AKS / EKS / GKE in customer tenant	CloudHSM / KMS-backed HSM
Hybrid	Cloud control plane, on-prem keys	AKS/EKS + VPN/ExpressRoute	On-prem network HSM (Thales, Entrust, Utimaco)
On-prem	Regulated industries, data residency	OpenShift / RKE2 / Rancher	Rack-mount HSM cluster
Air-gapped	Defense, critical infrastructure	Isolated K8s, offline registry mirror	HSM in tamper-evident enclosure

3.2 Capacity & sizing

Per AZ baseline (production): 2 vCPU / 4 GB per stateless service replica × 5 services; PostgreSQL HA primary 4 vCPU / 16 GB / NVMe. Signing throughput is HSM-bound — a single Thales Luna 7 unit delivers ~5,000 secp256k1 signatures/sec; cluster two units for HA. For workloads exceeding 20k tx/min, scale HSM modules linearly.

4. Request lifecycle

Every signing request follows the same deterministic path. Deny is the default; allow is earned by an evaluated, versioned policy. Each step emits a structured audit event with a cryptographic hash chained to the previous event.

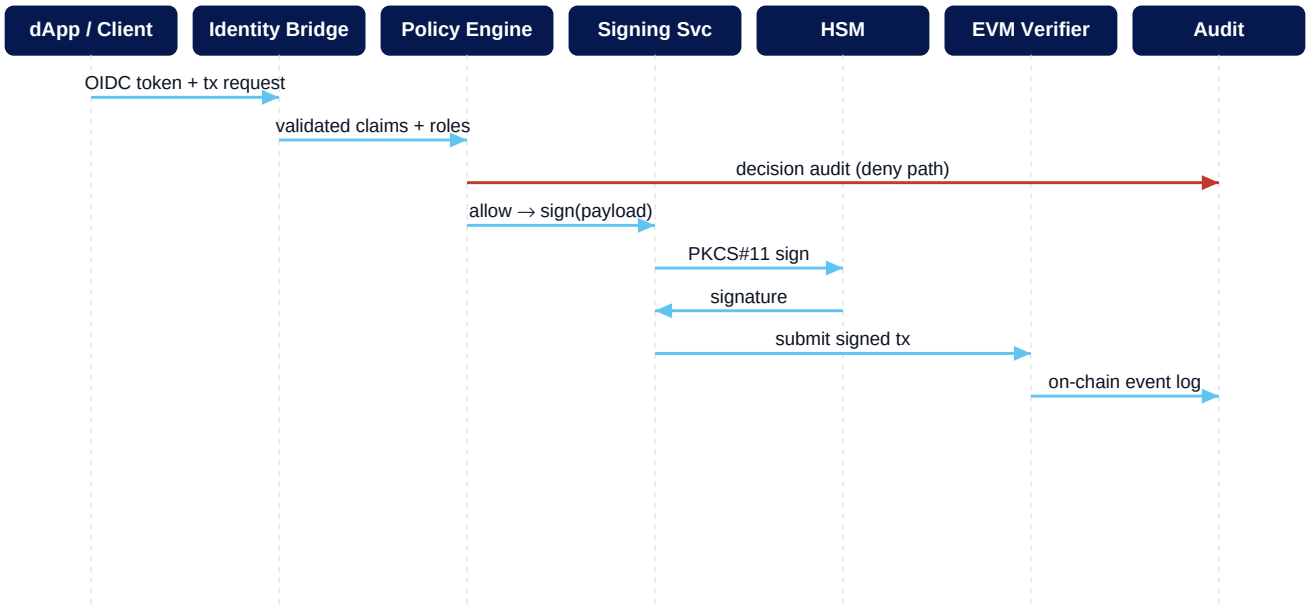

Figure 3 — Sequence of a signing request from client to on-chain verification.

4.1 Decision pseudocode

```
1. validate OIDC token (Azure AD) → claims
2. resolve roles + groups (Keycloak) → principal
3. resolve DID + key handle (DID Registry) → did:symq:<id>
4. load policy bundle (Policy Engine, current revision) → policy
5. evaluate policy(principal, did, tx, context)
   ■■■ deny → audit(deny, reason) → 403
   ■■■ allow → signing_service.sign(payload, key_handle)
       ■■■ HSM PKCS#11 C_Sign
       ■■■ submit tx via egress proxy → EVM RPC
       ■■■ verifier contract checks DID signature
       ■■■ audit(allow, tx_hash, block) → 200
```

5. Network & segmentation

SymmetriQ is deployed inside customer-owned network boundaries. The recommended segmentation isolates the HSM VLAN from all internet egress and restricts the Signing Service to a single, auditable path into key custody. All east-west traffic is mTLS via a service mesh (Istio, Linkerd, or Consul Connect) using SPIFFE/SPIRE workload identity.

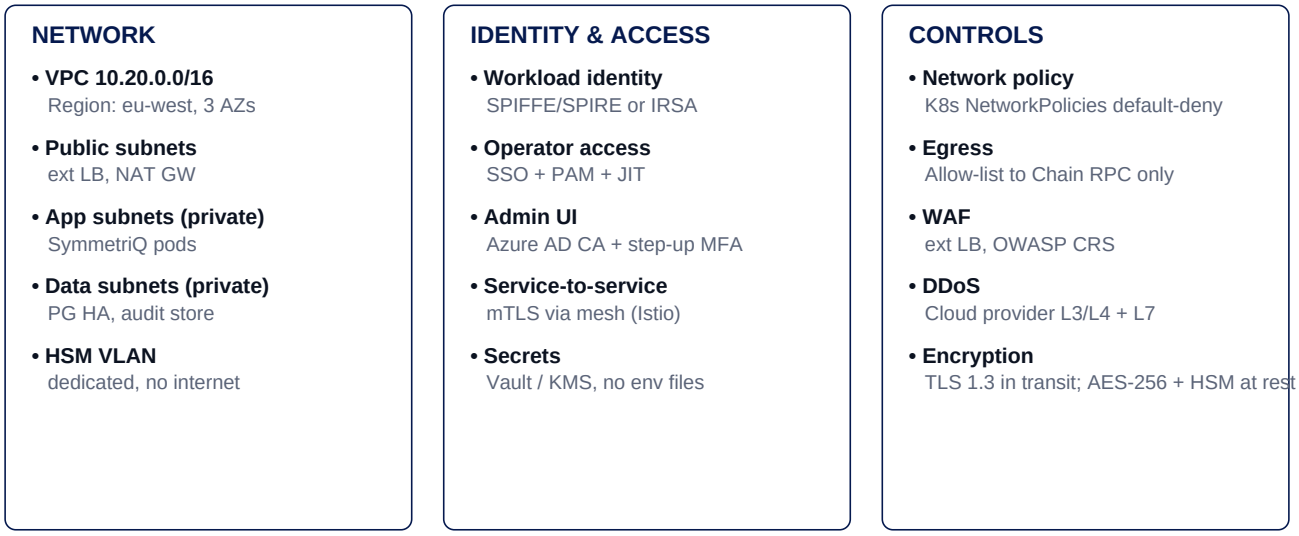

Figure 4 — Network, identity and control surfaces.

5.1 Ingress, egress and DNS

- Ingress is restricted to the Admin UI and a single dApp-facing API endpoint, both behind a WAF and external LB with mTLS.
- Egress is allow-listed to the configured EVM RPC endpoints (self-hosted, Infura, Alchemy, Quicknode) and the corporate IdP only.
- Outbound DNS is restricted to an internal resolver; no recursive resolution to the public internet from any SymmetriQ pod.
- All inter-service calls require mTLS with SPIFFE-issued workload identities; certificates rotate every 24h.
- Kubernetes NetworkPolicies enforce default-deny; only declared service-to-service flows are permitted.

5.2 Required ports

Source	Destination	Port / protocol	Purpose
dApp / API client	External LB	443/TCP (mTLS)	Signing API
Identity Bridge	Azure AD / Keycloak	443/TCP	OIDC / SAML
Signing Service	HSM cluster	1792/TCP (PKCS#11) or KMIP 5696/TCP	Sign / verify
All pods	Internal CA / mesh	8443/TCP	mTLS certs
Audit Store	SIEM (Splunk HEC / Sentinel)	8088/TCP, 443/TCP	Event forwarding
Egress proxy	EVM RPC	443/TCP	Tx submission

6. Identity, key management & cryptography

6.1 Identity model

Corporate identity remains the source of truth. SymmetriQ never stores passwords or long-lived credentials. Each authenticated principal is mapped to one or more DIDs (e.g. `did:symq:<tenant>:<uuid>`), and each DID is bound to a non-exportable key handle inside the HSM. Group membership and roles flow from the IdP into the Policy Engine on every request — there is no cached role state to go stale.

6.2 Key lifecycle

Stage	Operation	Control
Generate	C_GenerateKeyPair inside HSM; key marked non-extractable.	Quorum (M-of-N) of key custodians; logged.
Activate	DID issued and bound to key handle in DID Registry.	Signed by SymmetriQ root; audit event.
Use	Signing request → policy → HSM C_Sign.	Policy decision + signed audit event.
Rotate	New keypair generated; DID updated; old key set inactive.	Scheduled or on-demand; zero downtime.
Revoke	DID marked revoked; on-chain verifier rejects.	Real-time propagation; SIEM event.
Destroy	Key handle deleted via PKCS#11 C_DestroyObject.	Quorum approval; certificate of destruction.

6.3 Cryptographic agility

SymmetriQ separates the signing algorithm from the policy decision. Today's chain support drives secp256k1; the signing abstraction additionally supports Ed25519 and BLS12-381 (for ERC-4337 aggregation), and is being prepared for NIST PQC standards (ML-DSA / FIPS 204, SLH-DSA / FIPS 205) as soon as chains adopt verifier opcodes. Hybrid signatures (classical + PQC) are supported in audit-only mode today for evidence of forward secrecy.

7. Threat model & trust boundaries

The architecture explicitly enumerates trust zones and the threats addressed at each boundary. Every cross-boundary call traverses an enforced control: mTLS for east-west, WAF + mTLS for north-south, HSM session for the Restricted boundary.

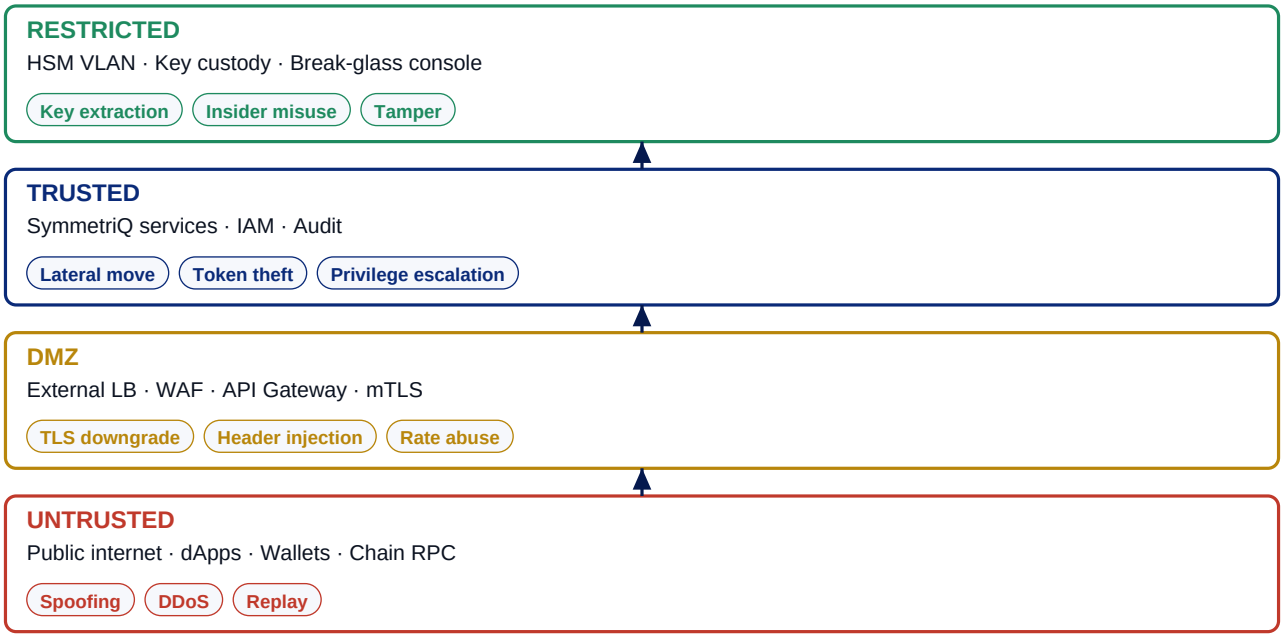

Figure 5 — Trust boundaries and representative STRIDE-class threats per zone.

7.1 Threats addressed

Threat	STRIDE	Mitigation
Lost / stolen private keys	Tampering / Info disclosure	Non-extractable HSM keys; no export path.
Insider misuse	Elevation of privilege	Policy quorum, separation of duties, audit, JIT access.
Compromised admin endpoint	Spoofing	Azure AD CA + step-up MFA + device compliance signal.
Rogue contract call	Tampering	On-chain verifier rejects non-DID signatures.
Replay of signed transaction	Tampering	Nonce + chain id + expiry in payload; verifier enforces.
Policy bypass	Elevation of privilege	Signed, versioned policy bundles; deny-by-default.
Repudiation	Repudiation	Hash-chained, signed audit log; exported to SIEM.
Stale access after offboarding	Elevation of privilege	Real-time IdP de-provisioning → DID revoked.
Supply chain compromise	Tampering	Signed images (cosign), SBOM, reproducible builds, SLSA L3.
Side-channel key extraction	Info disclosure	FIPS 140-2 L3 HSM; tamper-evident enclosure; physical access controls.

8. Compliance & assurance

SymmetriQ is engineered to slot into a SOC 2 Type II / ISO 27001 control environment and to satisfy DORA and NIS2 obligations for ICT risk management and incident reporting. The audit log is the primary evidence source: every decision (allow, deny, key event, policy change, admin action) is captured with cryptographic integrity and exportable in CSV, JSON and CEF formats.

8.1 Control mapping (illustrative)

Domain	Control	Where evidenced in SymmetriQ
Access control	Least privilege, MFA, JIT, revocation	IdP + DID Registry + audit events; quarterly access review export.
Change management	Versioned, reviewed deployments	Policy bundles via GitOps; signed Helm releases; rollback log.
Cryptography	Approved algorithms, key custody, rotation	FIPS 140-2 L3 HSM; key lifecycle events; rotation schedule.
Logging & monitoring	Tamper-evident logs, SIEM integration	Hash-chained audit store; HEC / Sentinel / Elastic exporters.
Incident response	Detection, containment, evidence preservation	SIEM detections, DID revoke API, immutable WORM bucket.
Vendor / supply chain	SBOM, signed artifacts, vulnerability mgmt	Cosign-signed images, monthly SBOM, patched base images.
Resilience (DORA)	RTO/RPO, exercises, third-party concentration	Multi-AZ HA, quarterly DR drill, multi-RPC provider abstraction.

8.2 Reports & evidence packs

- Pre-built SOC 2 evidence pack: access reviews, change tickets, key events, incident timelines.
- ISO 27001 Annex A control map exported as CSV for inclusion in the SoA.
- DORA-aligned incident report template generated from audit trail in under 2 hours.
- Pen-test scope template covering external LB, Admin UI, Signing API, Policy bundle pipeline.

9. Operational model

9.1 Roles and separation of duties

Role	Owns	Cannot do
Identity administrator	IdP user/group lifecycle, DID issuance request	Cannot author policy or access keys.
Policy author	Authoring and reviewing policy bundles	Cannot deploy policy without quorum approval; cannot access keys.
Key custodian	Quorum member for key lifecycle operations	Cannot bypass policy; cannot author policy.
Platform operator	Cluster, observability, patching	Cannot read audit log payloads in clear; cannot extract keys.
Auditor / security	Read-only audit, SIEM, incident response	Cannot mutate state.

9.2 SLOs and runbooks

- Signing API availability: 99.95% monthly. Error budget consumed → freeze deploys.
- Sign latency p95 < 120 ms (HSM-bound). p99 < 250 ms.
- Policy deploy time: < 5 min from merge to active in all regions.
- DID revoke propagation: < 30 s end-to-end (IdP → Registry → Verifier cache).
- RPO 0 for audit store (synchronous WORM mirror). RTO 15 min (multi-AZ active-active).

9.3 Observability

OpenTelemetry traces, metrics, and logs are emitted from every service. Pre-built Grafana dashboards cover request volume, decision outcomes, HSM saturation, policy evaluation time, audit pipeline lag, and on-chain submission outcomes. Pre-built detections ship for Splunk ES, Microsoft Sentinel and Elastic Security: anomalous deny rate, policy bypass attempt, off-hours key event, signing throughput spike.

9.4 Backup, DR, and chaos exercises

- PostgreSQL HA with synchronous replication intra-AZ, async cross-AZ; PITR for 35 days.
- Audit store mirrored to WORM bucket with object lock; quarterly restore drill.
- HSM keys backed up via vendor-encrypted backup token under quorum; tested annually.
- Quarterly game days: AZ failure, HSM failover, policy rollback, IdP outage.

10. Engagement & rollout

A typical enterprise deployment runs in six phases over eight to twelve weeks to first production traffic. SymmetriQ engineering pairs with customer platform, security and identity teams throughout. Below is the reference timeline; phases compress for greenfield estates and extend where contract refactoring is required.

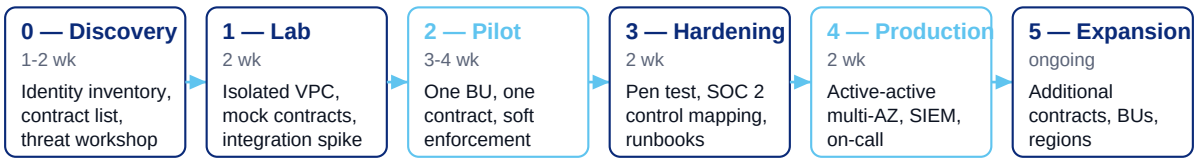

Figure 6 — Reference rollout timeline.

10.1 Acceptance criteria for go-live

- End-to-end signing flow demonstrated against the production HSM cluster.
- Multi-AZ failover test passed (loss of one AZ; zero data loss; < 60 s recovery).
- External penetration test report delivered with no unresolved high or critical findings.
- SIEM detections live; on-call rota staffed; runbooks signed off by security and platform.
- Policy bundle GitOps pipeline reviewed; quorum approval enforced on the protected branch.
- DR drill passed: full restore of audit store and DID Registry into a clean environment.

10.2 What SymmetriQ delivers

- Reference Helm chart, Terraform modules (AKS/EKS/GKE), and air-gap manifests.
- Pre-built policy library (treasury, RBAC, quorum, rate-limiting, geofence).
- Integration adapters for Azure AD, Keycloak, Okta, Ping, AD FS.
- Solidity verifier library and ERC-4337 paymaster reference.
- Operator runbooks, training, and a named SRE during the pilot.

Appendix A — Bill of materials (reference)

Layer	Component	Reference selection
Compute	Kubernetes	AKS 1.29 / EKS 1.29 / GKE 1.29 / OpenShift 4.15 / RKE2
Service mesh	mTLS east-west	Istio 1.22 or Linkerd 2.15 (with SPIRE)
Identity	Workload identity	SPIFFE/SPIRE, IRSA on EKS, Workload Identity on AKS/GKE
Database	DID + Audit	PostgreSQL 16 HA (Patroni) or managed equivalent
Object store	WORM audit	S3 Object Lock, Azure Blob immutable, MinIO with object lock
HSM	Key custody	Thales Luna 7 / Entrust nShield 5c / Utimaco SecurityServer / CloudHSM
Secrets	Bootstrap & ops	HashiCorp Vault / cloud KMS
Observability	Metrics, traces	Prometheus + Grafana + Tempo + Loki, or Datadog
SIEM	Audit forwarding	Splunk ES / Microsoft Sentinel / Elastic Security
Supply chain	Image signing	Cosign + Sigstore; SBOM via Syft; vulnerability scan via Grype/Trivy

Appendix B — Glossary

DID	Decentralized Identifier. W3C-standard identifier resolved to a key handle, not a person.
HSM	Hardware Security Module. Tamper-resistant device that performs cryptographic operations without exposing key material.
KMIP	Key Management Interoperability Protocol. Standard for talking to key stores.
PKCS#11	Cryptoki API for HSMs and tokens.
OPA / Rego	Open Policy Agent and its declarative policy language.
SPIFFE / SPIRE	Workload identity framework providing short-lived mTLS certs.
ERC-1271	Standard for contract-based signature validation.
ERC-4337	Account abstraction standard enabling smart-contract wallets.
WORM	Write Once Read Many storage with object lock.
DORA / NIS2	EU regulations for digital operational resilience and cybersecurity.

Appendix C — Contact

For a tailored architecture review against your estate, contact the SymmetriQ team via **symmetriq.io/contact**. A scoped briefing typically runs two to three weeks and produces a deployment blueprint specific to your identity providers, target EVM networks, and regulatory perimeter.