SymmetriQ

Technical Briefing

Decentralized Identity for permissioned access to smart contracts on permissionless EVM networks. Integration with Azure AD / Entra ID and Keycloak.

Confidential — Prepared for VDF · June 2026 · v1.0

1. Executive Summary

SymmetriQ is a digital identity layer that lets enterprises grant fine-grained, role-based access to smart contracts deployed on permissionless EVM-compatible blockchains. It bridges existing corporate identity systems — Azure AD / Entra ID for authentication, Keycloak for authorization — to on-chain execution, without requiring a private fork of the chain or custodial wallets for users.

For VDF, this means employees, contractors and service identities can interact with blockchain-deployed smart contracts under the same governance, MFA and audit rules already enforced for the rest of the IT estate. The chain remains open and interoperable; access to VDF's contracts is not.

2. Capabilities at a Glance

Identity bridging	Native federation with Azure AD / Entra ID and Keycloak; OIDC and SAML supported.
DID issuance	W3C-style DIDs cryptographically bound to a corporate identity and a key in HSM/TPM.
Policy engine	Role, attribute, quorum, time-window and rate-limit rules evaluated before any signature.
Signing service	Hardware-backed signing (HSM, TPM 2.0, Secure Enclave); private keys never leave silicon.
On-chain verification	Lightweight Solidity verifier or ERC-1271/4337 hooks for DID signature checks.
Revocation	Real-time revocation of a user's on-chain authority without modifying the contract.
Audit & forensics	Tamper-evident log of every identity, policy and signing event; SIEM-ready exports.
Crypto-agility	Pluggable signature suites; PQC-ready signing roadmap as chains adopt new algorithms.

3. Architecture

SymmetriQ sits between VDF's identity providers and the target EVM network. It is composed of four logical services, each independently scalable and deployable in VDF's own infrastructure.

3.1 Components

Identity Bridge	Federates with Azure AD (OIDC) and Keycloak; resolves user, group, role claims.
DID Registry	Issues, stores and lifecycles DIDs; maps corporate identity DID key handle.

Policy Engine	Versioned, policy-as-code rules (Rego/JSON); deterministic and auditable evaluation.
Signing Service	Talks to HSM / TPM / Secure Enclave via PKCS#11 / KMIP / platform APIs.
On-chain Verifier	Solidity library or ERC-1271/4337 module used by VDF contracts to verify signatures.
Audit Store	Append-only, hash-chained event log; exports to Splunk, Sentinel, Elastic.

3.2 Topology (logical)

```
Azure AD / Entra ■ Keycloak (roles) ■ SymmetriQ (DID + sign) → EVM contract
■ ■ ■ ■
SSO / MFA policies HSM / TPM on-chain verification
```

4. User Flow

From the end-user perspective the experience is a single corporate sign-in followed by a normal transaction approval. The on-chain mechanics are not exposed to the user.

Authenticate. User signs in to Azure AD / Entra ID via the existing SSO, including MFA.

Authorize. Keycloak resolves the user's groups, roles and entitlements and issues a token.

Bind. SymmetriQ Identity Bridge validates the token and resolves the user's DID and signing policy.

Request. User initiates a contract action from a VDF portal, internal app or wallet.

Evaluate. Policy Engine checks role, scope, quorum, time-window and rate limits.

Sign. Signing Service produces a DID signature inside the HSM/TPM; private key never leaves.

Submit. The signed transaction is broadcast to the EVM network through standard infrastructure.

Verify. The smart contract calls the SymmetriQ verifier and either executes or reverts.

Audit. Every step is appended to the tamper-evident log and replicated to VDF's SIEM.

5. Business Flow

At the business layer, SymmetriQ makes contract access an extension of standard joiner-mover-leaver processes, not a parallel governance regime.

Onboarding. A new employee added to Azure AD inherits a DID automatically the first time their role grants on-chain capability. No separate provisioning.

Role change. A role update in Keycloak immediately changes which contracts and methods the user can invoke. No re-issuance, no manual key rotation.

Offboarding. Disabling the corporate account revokes the DID's on-chain authority in real time across all contracts that trust the SymmetriQ verifier.

Approvals. High-value actions trigger N-of-M quorum signatures, mapped to existing approval chains and recorded for audit.

Reporting. Compliance and audit teams query a single source of truth across IAM events and on-chain decisions.

6. Logic Flow (signing decision)

```
request → validate token (Azure AD)
        → resolve roles (Keycloak)
        → resolve DID + policy (SymmetriQ)
        → evaluate policy
          → deny  → audit + return error
          → allow → HSM/TPM signs
                    → submit tx to EVM
                    → contract verifier
                          → revert / execute
                    → audit event
```

7. Capabilities in Detail

7.1 Identity integration

Azure AD / Entra ID via OIDC; supports conditional access, MFA, device compliance signals.

Keycloak as the authorization model: realms, roles, groups, client scopes mapped 1:1 into policies.

Service identities (workload identity, managed identity) treated as first-class principals.

Optional federation with additional OIDC/SAML/LDAP sources as VDF estate evolves.

7.2 DID and key custody

DIDs follow W3C DID Core; resolvable through a SymmetriQ DID method or did:web alias.

Keys generated inside HSM (PKCS#11 / KMIP), TPM 2.0 or Secure Enclave; non-exportable.

Key rotation and re-binding without changing the DID identifier; consumers stay valid.

Recovery and continuity via M-of-N admin custodianship; no single-vendor escrow.

7.3 On-chain integration

Verifier exposed as a Solidity library and as ERC-1271 / ERC-4337 compatible module.

Works with new contracts (recommended) or via a thin proxy in front of legacy contracts.

Chain-agnostic across EVM L1s, L2s and private EVMs; multi-chain deployments supported.

No protocol change to the underlying chain; nothing to lobby, fork or wait for.

8. Agility and Flexibility

Policy-as-code. Signing rules are versioned, reviewed and deployed like software, not configured in a UI a single admin can change unobserved.

Pluggable cryptography. Signature suites (secp256k1 today, Ed25519, BLS, and post-quantum schemes when chains support them) are abstracted behind the Signing Service.

Pluggable identity. Today Azure AD and Keycloak; tomorrow any OIDC- or SAML-speaking provider.

Deployment modes. VDF private cloud, hybrid, fully on-prem, or air-gapped enclave for the most sensitive operations.

No vendor lock-in at the chain layer. Existing wallets, dApps and tooling continue to work; SymmetriQ only adds the access decision.

Incremental adoption. Start with one contract and one user group; expand without re-architecture.

9. Security Model

9.1 Threats addressed

Lost or stolen private keys (keys never leave hardware).

Insider misuse (policy + quorum + audit + revocation).

Compromised endpoint (MFA, device compliance signals, signing happens server-side).

Rogue contract calls (on-chain verifier rejects non-DID-signed transactions).

Repudiation (cryptographic, tamper-evident audit trail).

Stale access after offboarding (real-time revocation propagated to all consumers).

9.2 Controls and standards

FIPS 140-2/3 validated HSMs; TPM 2.0 and Secure Enclave for endpoint-bound identities.

OIDC / SAML / OAuth 2.0 for federation; W3C DID Core for identifiers.

Designed to support SOC 2, ISO 27001, NIST 800-53 control mappings.

Crypto-agility path toward NIST PQC (ML-DSA, SLH-DSA) for long-lived signatures.

Separation of duties between identity admins, policy authors and key custodians.

9.3 Data and key handling

No custody of user credentials. Authentication remains at Azure AD; passwords never reach SymmetriQ.

Private keys remain inside hardware boundaries. SymmetriQ holds key handles, not key material.

Audit data encrypted at rest and in transit; hash-chained to detect tampering.

Optional on-prem deployment for environments where data cannot leave VDF infrastructure.

10. Integration with VDF

Connect SymmetriQ Identity Bridge to VDF's Azure AD tenant via an OIDC application registration.

Map Keycloak realms and roles to SymmetriQ policies; one-to-one for the initial pilot.

Deploy the Signing Service against VDF's existing HSM estate, or provide a managed appliance.

Adapt or write the target smart contracts to use the SymmetriQ verifier (or ERC-1271 hook).

Wire SymmetriQ audit events into VDF's SIEM (Sentinel, Splunk, Elastic) using standard syslog/HTTP.

No changes required to the underlying blockchain network, node operators or wallet vendors.

11. Operational Considerations

HA and DR. All services are stateless except the DID Registry and Audit Store, both deployable in active-active with PostgreSQL HA or equivalent.

Performance. Signing latency dominated by HSM round-trip; typically sub-100ms per signature.

Scaling. Horizontal across all services; throughput limited by HSM capacity, scalable by adding modules.

Observability. OpenTelemetry traces, metrics and logs; pre-built dashboards for Grafana.

Upgrades. Rolling upgrades; policy changes versioned and reversible without service interruption.

12. Engagement Roadmap

Discovery · 2–3 weeks	Target contracts identified; identity and role model mapped; success criteria agreed.
Pilot · 6–8 weeks	SymmetriQ deployed in VDF environment; one business contract end-to-end; pilot user group live.
Production · Quarterly	Additional contracts and groups onboarded; full audit, revocation and quorum flows in operation.

13. Glossary

DID	Decentralized Identifier (W3C); a globally unique, cryptographically verifiable identifier.
EVM	Ethereum Virtual Machine; the execution environment used by Ethereum and compatible chains.
Permissionless chain	A blockchain anyone can read from, write to, and run a node on.

Azure AD / Entra ID	Microsoft's enterprise identity provider.
Keycloak	Open-source identity and access management server.
HSM	Hardware Security Module; tamper-resistant device that protects cryptographic keys.
TPM 2.0	Trusted Platform Module; hardware root of trust embedded in modern devices.
ERC-1271	Standard for on-chain signature verification by smart contracts.
Quorum signing	N-of-M signature scheme requiring multiple parties to authorize an action.

Contact · hello@symmetriq.io · symmetriq.io