SymmetriQ

Decentralized Identity for the Enterprise Blockchain

Privileged, auditable access to smart contracts — bridging Azure AD, Keycloak and permissionless EVM networks.

Executive Briefing · Prepared for VDF · June 2026

THE QUESTION ON THE TABLE

Who is allowed to sign?

When a smart contract sits on a permissionless EVM network, anyone holding a private key can call it.

For an enterprise, that is not access control — it is the absence of it.

SymmetriQ turns a public blockchain into a private, governed surface — without changing the chain.

COMPANY

SymmetriQ

A digital identity company building the trust layer between enterprise IAM systems and decentralized ledgers.

Mission

Reconcile enterprise identity with decentralized execution. Compliance without centralization.

Focus

Regulated industries: energy, finance, telco. EVM-compatible chains. Hybrid IAM estates.

Differentiator

Native bridges to Azure AD and Keycloak. No custom chain. No fork. Drop-in for existing dApps.

PROBLEM

Two worlds that do not speak

Azure AD, Entra and Keycloak govern who your users are, what role they hold, and what they may do.

Smart contracts on a permissionless EVM care only about a private key — anonymous, ungoverned, irrevocable.

Bolting one onto the other usually means custodial wallets, off-chain whitelists, or a permissioned fork. Each breaks something important — control, auditability, or interoperability.

SOLUTION

SymmetriQ DID — the bridge

Every authorized VDF user receives a Decentralized Identifier (DID) cryptographically bound to their corporate identity in Azure AD and to their roles in Keycloak.

Result: the chain stays permissionless and open. Access to your contracts does not.

HOW IT WORKS

From login to on-chain call

1. User signs in to Azure AD / Entra with corporate SSO and MFA.
2. Keycloak resolves the user's roles, groups and entitlements.
3. SymmetriQ issues or unlocks a DID bound to that identity, scoped to the policy.
4. User initiates an action; SymmetriQ checks the policy and co-signs the transaction.
5. Transaction lands on the EVM contract; the contract verifies the DID signature on-chain.
6. Every step is logged with cryptographic integrity for audit and compliance.

CAPABILITIES

What SymmetriQ provides

Identity bridging

Native connectors for Azure AD / Entra ID and Keycloak. No replacement of your IAM.

Privileged access

Fine-grained mapping of corporate roles to on-chain actions and contract methods.

Policy enforcement

Approvals, quorum, rate limits and time windows enforced before signing.

Key custody

Keys generated and held in HSM / TPM / Secure Enclave. Never exported.

Revocation

Instant revocation of a user's on-chain authority without touching the contract.

Auditability

Tamper-evident log of every signature, decision and policy evaluation.

SECURITY & COMPLIANCE

Designed for regulated environments

Hardware-bound keys: HSM, TPM 2.0 or Secure Enclave. Private keys never leave silicon.

Strong authentication chain: Azure AD MFA Keycloak policy SymmetriQ signing policy.

Cryptographic audit trail of every decision, exportable for SOC 2, ISO 27001 and internal audit.

Quantum-safe roadmap: signature agility for NIST PQC algorithms when chains adopt them.

Zero custodial risk: VDF retains ownership of identity and keys at all times.

AGILITY

Built to bend, not break

Chain-agnostic across EVM networks (mainnet, L2s, private EVMs). Add a network without re-issuing identities.

Pluggable IAM: Azure AD and Keycloak today; OIDC / SAML / LDAP straightforward to extend.

Policy-as-code: signing rules versioned, reviewed and rolled out like any other software change.

Deploy where it makes sense: VDF private cloud, hybrid, or fully on-prem. No SaaS dependency required.

Coexists with existing dApps and wallets — no fork, no protocol change, no vendor lock-in at the chain layer.

VDF INTEGRATION

How SymmetriQ lands at VDF

Reuses what VDF already operates. Adds the missing identity layer between the corporate directory and the EVM smart contracts you intend to deploy.

Azure AD / Entra ID remains the source of truth for users and MFA.

Keycloak continues to own roles, groups and session policy.

SymmetriQ is deployed alongside, federating both — no migration, no rip-and-replace.

Smart contracts are written (or adapted) once to verify SymmetriQ-issued DID signatures.

Existing security operations gain a single, queryable audit trail across IAM and chain.

ENGAGEMENT

Suggested next steps with VDF

Phase 1	Phase 2	Phase 3
Discovery	**Pilot**	**Production**
2–3 weeks	6–8 weeks	Quarterly
Map target contracts, roles in Keycloak, identity flows in Azure AD. Define policy model.	Deploy SymmetriQ in a VDF environment. Integrate one business contract end-to-end.	Roll out additional contracts and user groups. Operationalize audit and revocation.

Permissionless chain.
Permissioned access.

SymmetriQ — the identity layer for VDF's smart contracts.

Contact · hello@symmetriq.io · symmetriq.io