BUILD BEFORE Q-DAY • qorechain-diana (EVM 9800)

AegisQore

Post-Quantum AI Agent Firewall & Scoped EVM Policy Registry

Unified Apache-2.0 post-quantum security stack pairing NIST FIPS-204 ML-DSA-87 / FIPS-205 SLH-DSA cryptography, on-chain Scoped EVM Windows, 30-day owner-to-agent link leases, and a 6-tool MCP guard for QoreChain / QoreX.

62 / 62	0 H / 0 M	0x0A01	30 Days
AUTOMATED TESTS PASS	SLITHER 0.11.6 AUDIT	LIVE ON-CHAIN PQC VERIFY	MAX AGENT LINK LEASE

Why Autonomous AI Treasury Agents Need AegisQore

Threat 1: Quantum Key Recovery (Q-Day)

- Autonomous agents rely on classical secp256k1 / Ed25519 keys vulnerable to Shor's algorithm.
- Signing downgrade attacks strip post-quantum signatures back to classical-only payloads.
- Long-lived agent keys without mandatory TTL leases create permanent blast radius.

Threat 2: Prompt Injection & Unconstrained MCP

- Compromised LLM tool calls can invoke unlimited token approvals (`approve`, `setApprovalForAll`).
- No per-block window caps, no monotonic anti-replay nonces, and no calldata selector firewall.
- Accidental secret/mnemonic leakage into MCP tool arguments compromises treasury custody.

4-Layer Defense-in-Depth on QoreChain EVM 9800

1. MCP Firewall

6-tool `qoreguard-mcp` server with secret-input refusal (`SECRET_INPUT_REFUSED`) and side-effect-free policy quoting.

2. Hybrid PQC

`@qorechain/pqc` FIPS-204 ML-DSA-87 (2,592B pubkey / 4,627B sig) + SLH-DSA + secp256k1 anti-downgrade v2 envelopes.

3. Policy Engine

O(1) sliding daily caps, Scoped EVM Windows, 4-byte selector firewall, monotonic nonces, and SHAKE-256 audit bundles.

4. EVM 9800 Registry

`QoreGuardPolicyRegistry.sol` calling QoreChain precompiles `0x0A01`, `0x0A02`, `0x0B01`, and `0x0B02`.

1:1 Mapping to Official QoreChain Track Spec

TRACK REQUIREMENT	AEGISQORE IMPLEMENTATION	VERIFICATION
Scoped EVM Window	On-chain `openScopedEvmWindow(startBlock, endBlock, maxTxCount, maxTotalValue, targets)`	`Foundry 18/18 PASS`
30-Day Owner Link Lease	`MAX_LINK_TTL = 30 days`, `renewAgentLink()`, `relinkAgentKey()`, `revokeAgent()`	`Enforced On-Chain + TS`
Authenticated Messaging	`qorechain-msg-v1|<chainId>|<data>` hybrid secp256k1 + ML-DSA-87 verification	`Byte-for-Byte Parity`
Spend & Selector Firewall	Per-tx + O(1) 2-epoch daily caps; default-blocks `approve` & `setApprovalForAll`	`256-Run Fuzz PASS`
AI-Native Interface (MCP)	6-tool MCP server + 6-vector downgrade simulator + SHAKE-256 attested audit export	`InMemory MCP PASS`

Verified Live on qorechain-diana (EVM 9800)

Live Precompile & RPC Probe

- `npm run probe:testnet` verified live block **10,801,339** (consensus height 10,801,340).
- Generated fresh FIPS-204 **ML-DSA-87** keypair and signature via `@qorechain/pqc`.
- On-chain `IQorePQC.pqcVerify` (`0x...0A01`) returned **`verified: true`**.
- Confirmed `0x...0A02` (`pqcKeyStatus`) & `0x...0C01` (`rlConsensusParams`) live.

Registry Dry-Run & Security Audit

- **Solc 0.8.28 (paris)** creation bytecode: **15,896 bytes** (under 24KB EIP-170 limit).
- Live EVM 9800 gas estimate: **3,480,337 gas** (0.3915 QOR @ 112.5 gwei, block 10,802,524).
- **Slither 0.11.6** (102 detectors): **0 High / 0 Medium / 0 Optimization**.
- Zero hardcoded keys; turnkey env-var-driven broadcast scripts.

6-Vector Downgrade & Tamper Resistance

1. Strip PQC

Drops ML-DSA-87 signature to classical-only.

`QUANTUM_DOWNGRADE_CLASSICAL_ONLY`

2. Sign-Bytes v2→v1

Downgrades envelope framing version.

`QUANTUM_DOWNGRADE_SIGN_BYTES_V1`

3. Weak Algorithm

Substitutes ML-DSA-44 for ML-DSA-87.

`QUANTUM_DOWNGRADE_WEAK_ALGORITHM`

4. Amount Tamper

Mutates transfer value post-commitment.

`COMMITMENT_TAMPERED`

5. Signature Bit-Flip

Corrupts 1 byte of ML-DSA-87 signature.

`PQC_SIGNATURE_INVALID`

6. Nonce Replay

Re-submits an already consumed nonce.

`NONCE_REPLAY`

62 / 62 Automated Tests & Best AI-Native Build

18 / 18

Foundry Solidity Suite

Precompile `vm.etch` mocks, 256-run spend-cap fuzzing, 30d TTL renewal, Scoped EVM Windows, and `qorechain-msg-v1` tests.

36 / 36

Core SDK & MCP Vitest

Real FIPS-204/205 crypto, stateful velocity windows, InMemory MCP client/server round-trips, and secret-refusal checks.

8 / 8

Web Console Vitest

React 19 + Vite 6 interactive firewall console, Diana snapshot telemetry, 5-scenario lab, and SHA-256 receipt export.

Explore AegisQore Live

Live Endpoints

- **GitHub Repo:** `github.com/alphonshhhomenicmtu/aegisqore-qorechain`
- **Interactive Web Console:** `alphonshhhomenicmtu.github.io/aegisqore-qorechain/`
- **Pitch Deck PDF:** `.../aegisqore-qorechain/aegisqore-deck.pdf`

Demo & License

- **1080p Demo Video (108s):** `youtube.com/watch?v=La_8Dh7TA04`
- **Primary Track:** Post-Quantum AI Agents
- **Special Award:** Best AI-Native Build
- **License:** Apache-2.0 Open Source