



AEGISQ TECHNOLOGIES INC.

TECHNICAL OVERVIEW DOCUMENT (WEBSITE VERSION)

Title:

Post-Quantum Security Infrastructure for Enterprise Systems

---

Executive Summary

AegisQ Technologies Inc. is developing a three-layer enterprise platform designed to enable organizations to transition from classical cryptographic systems to post-quantum security infrastructure.

The platform addresses a critical global challenge: existing encryption systems will be broken by quantum computing, and organizations must migrate to new standards within defined regulatory timelines.

AegisQ provides a complete system to:

- discover cryptographic exposure
- implement post-quantum security
- orchestrate enterprise-wide migration
- maintain continuous compliance

---

The Problem

Current global digital infrastructure relies on cryptographic systems such as RSA and ECC. These systems are vulnerable to quantum computing attacks.

Risks include:

- exposure of encrypted data
- compromised identity systems

- long-term data breaches (harvest-now-decrypt-later)
- regulatory non-compliance

This is not theoretical. It is a mandated transition.

---

## Regulatory Environment

Global standards have been finalized:

- NIST FIPS 203, 204, 205 (August 2024)
- NSA CNSA 2.0 migration requirements
- OMB quantum readiness mandates
- EU DORA compliance requirements

Migration deadlines range from 2030 to 2035.

---

## Platform Architecture

AegisQ operates a three-layer architecture:

Layer 1: AegisDiscover — Cryptographic Visibility

- maps all cryptographic assets
- identifies vulnerabilities
- prioritizes migration

Layer 2: AegisCore — Cryptographic Trust

- implements post-quantum standards
- manages key lifecycle
- supports hybrid cryptography

Layer 3: AegisNet — Migration Orchestration

- coordinates enterprise migration
- ensures operational continuity
- validates compliance

---

### Continuous Compliance Model

The platform operates as a loop:

Discover → Secure → Orchestrate → Validate → Repeat

This ensures ongoing compliance as systems evolve.

---

### Deployment Model

AegisQ is software-only:

- no hardware required
- deploys on existing infrastructure
- integrates with current systems

---

### Conclusion

AegisQ is building foundational infrastructure for the post-quantum transition.

This is not a product category. It is a new layer of cybersecurity required for the next generation of computing.