ATARC Zero Trust Lab Phase 3 – Quantum Track

Final Use Cases

Introduction

The ATARC Zero Trust Lab Phase 3 – Quantum Track is designed to operationalize the transition toward post-quantum cryptography (PQC) by providing a hands-on environment where industry partners can demonstrate real, interoperable solutions. This phase reflects the operational urgency of the PQC transition, highlighted in NIST and GSA briefings, which emphasize that *"current cryptographic infrastructure has an expiration date and requires immediate migration planning"*.

Building on the applied research efforts of NIST's National Cybersecurity Center of Excellence (NCCoE)—including Automated Cryptographic Discovery and Inventory (ACDI), interoperability testing, and crypto-agility demonstrations—this phase moves beyond theoretical planning. It enables agencies to observe how PQC can be integrated into complex architectures without disrupting mission operations. As NIST notes in the MIGRATION TO POST-QUANTUM CRYPTOGRAPHY (PQC), organizations must *"maintain connectivity and interoperability… during the transition from quantum-vulnerable algorithms to quantum-resistant algorithms"* .

The Quantum Track focuses on three pillars essential to federal PQC readiness:

- **Automated Cryptographic Discovery**
- **Hybrid Classical–PQC Implementation**
- **Orchestrated Cryptographic Agility**

These demonstrations reinforce that PQC migration is not a one-time replacement effort but a sustained, iterative modernization aligned with Zero Trust principles and other federal mandates.

Scenario 1: Cryptographic Discovery and Inventory (CDI)

This scenario reflects the NCCoE's Discovery Workstream, which highlights that organizations are often unaware of the *"breadth and scope of application and function dependencies on public-key cryptography"*. The goal is to establish an understanding of how cryptography operates across entire systems, including hidden cryptographic dependencies, in order to provide agencies with an actionable baseline for PQC migration.

Automated Cryptographic Discovery and Inventory (ACDI)

Vendors will demonstrate automated tools capable of detecting quantum-vulnerable cryptography across endpoints, networks, firmware, code repositories, and operational systems. This aligns with NIST SP 1800-38B, which showcases *"automated cryptographic discovery and inventory (Endpoint and Network)"* .

Cryptographic Bill of Materials (C-BOM)

Tools should generate a normalized inventory of cryptographic components—including RSA, Diffie-Hellman, ECC, and other algorithms identified as vulnerable to quantum attacks. NIST's MIGRATION TO POST-QUANTUM CRYPTOGRAPHY paper emphasizes the need to identify *"instances of quantum-vulnerable public-key algorithm use, where they are used in dependent systems, and for what purposes"* .

Risk-Based Prioritization

Demonstrations should show how discovery outputs feed into a risk-analysis engine. Prioritization should consider Harvest-Now-Decrypt-Later risks, system criticality, and mission impact.

Cryptographic Baseline & Anomaly Detection

Vendors should illustrate how establishing a cryptographic baseline enables detection of unexpected algorithm use or regressions after updates—mirroring the NCCoE's emphasis on normalization, correlation, and continuous monitoring within a data-centric crypto-risk framework.

Scenario 2: Hybrid Implementation and Protocol Interoperability

This scenario evaluates how classical and PQC algorithms can coexist during the transition period—an approach emphasized repeatedly in the NIST interoperability workstream.

Protocol Resilience and Latency Management

Solutions will be tested for their ability to handle PQC's larger key sizes and signatures without degrading performance or breaking legacy systems. NIST's MIGRATION TO POST-QUANTUM CRYPTOGRAPHY paper notes that PQC algorithms may differ in *"key size, signature size, error handling properties, [and] number of operations"* and that maintaining interoperability during migration is a *"truly significant challenge"* .

Web Cipher Translation and PQC-Ready TLS

Vendors will demonstrate upgrading insecure or deprecated TLS configurations to PQC-ready cipher suites while maintaining secure symmetric encryption. This aligns with NCCoE's interoperability testing across *"TLS, QUIC, SSH, code signing, public key certificates, hardware security modules, PKI systems, [and] smart cards"*.

Scenario 3: Orchestrated Cryptographic Agility

This scenario reflects the NCCoE's emphasis on crypto-agility as a long-term operational requirement, not a one-time migration task. As the NIST Cybersecurity White Paper NIST CSWP 39-upd1 states, *"Cryptographic (crypto) agility refers to the capabilities needed to replace and adapt cryptographic algorithms in protocols, applications, software, hardware, firmware, and infrastructures while preserving security and ongoing operations."*

Modular Architecture Decoupling

Vendors will demonstrate architectures where cryptographic functions are abstracted behind standardized APIs, enabling rapid algorithm replacement without modifying application logic. This mirrors the NCCoE's crypto-agility guidance and the GSA message that PQC must be integrated into supply-chain and acquisition processes.

"Zero-Touch" Automated Updates

Demonstrations should show automated key rotations, certificate issuance, and algorithm swaps within CI/CD pipelines—reflecting the NCCoE's focus on automation across *"code development pipelines, operational systems, and applications"* - CSWP 48, Mappings of Migration to PQC Project Capabilities to NIST Cybersecurity Framework 2.0 and to Security and Privacy Controls for Information Systems and Organizations | CSRC.

Platform Independence

Solutions must support multiple cryptographic libraries and hardware platforms to avoid vendor lock-in. This aligns with the federal requirement to maintain interoperability across diverse systems and the NCCoE's multi-vendor collaboration model.

Appendix:

- https://buy.gsa.gov/find-samples-templates-tips?page=1&keyword=Post+quantum+cryptography
- Publications (FIPS)
- Migration to Post-Quantum Cryptography NIST SP 1800-38 Practice Guide Preliminary Draft | NCCoE
- Post-Quantum Cryptography | CSRC
- Frequently Asked Questions about Post-Quantum Cryptography
- Post Quantum Cryptography Buyer's Guide (GSA 2025)
- NATIONAL CYBERSECURITY CENTER OF EXCELLENCE MIGRATION TO POST-QUANTUM CRYPTOGRAPHY PROJECT