



Post-Quantum Cryptography Migration

Course: Cryptographic Inventory, Crypto-Agility and Hybrid TLS



Post-Quantum Cryptography Migration Course: Cryptographic Inventory, Crypto-Agility and Hybrid TLS

Introduction:

Post-quantum cryptography migration, covering cryptographic inventory, crypto-agility and hybrid TLS, is a 1-week course for security architecture, PKI and cryptography engineering units that ends with a Post-Quantum Migration Plan for a case organisation. Encrypted traffic and archives captured today can be decrypted once large quantum computers exist, yet most organisations cannot say where RSA and elliptic curve keys sit in their systems or which suppliers can ship replacements. Nominees already configure servers, certificates or security tooling and learn through lab work with discovery scanners, test handshakes and inventory templates. CoreConcept Training Center delivers this post-quantum cryptography migration course.

Course Objectives:

- Score the quantum exposure of each business service using data shelf-life, migration effort and the Mosca inequality
- Select ML-KEM, ML-DSA or SLH-DSA parameter sets for each protection need and justify hybrid use
- Build a cryptographic bill of materials from network, code and certificate discovery results
- Design crypto-agile interfaces and algorithm policies so that primitives can be replaced without application rewrites
- Test hybrid TLS and SSH key exchange for latency, message size and legacy client interoperability
- Produce a Post-Quantum Migration Plan with migration waves, a vendor readiness register and progress indicators

Target Audience:

- Security architecture units that define encryption, key exchange and signature requirements for new and existing systems
 - PKI and certificate operations units that run issuing hierarchies, HSMs and certificate renewal
 - Cryptography and application security engineering units that review libraries, code and protocol settings
 - Infrastructure and network units that operate load balancers, VPN gateways, SSH estates and TLS termination
 - IT risk and technology supplier management units that track cryptographic dependencies in purchased products
-

Course Outline:

Day 1: Quantum Threat Exposure and Cryptographic Estate Baseline

- Shor's Algorithm Impact on RSA and Elliptic Curve Keys
- Grover's Algorithm and Symmetric Key Length Adjustments
- Harvest Now Decrypt Later Exposure for Long-Lived Data
- Mosca Inequality Scoring of Data Shelf-Life and Migration Effort
- Current-State Cryptographic Dependency Baseline by Business Service

Day 2: Post-Quantum Standards and Hybrid Protocol Architecture

- FIPS 203 ML-KEM Parameter Sets and Key Encapsulation Flow
- FIPS 204 ML-DSA Signature Sizes and Verification Costs
- FIPS 205 SLH-DSA Hash-Based Signatures for Firmware Signing
- Hybrid Key Exchange Design Combining Classical and Lattice Schemes
- Falcon and HQC Candidates in Algorithm Selection Planning

Day 3: Cryptographic Bill of Materials and Crypto-Agility Engineering

- Passive Network Scanning for TLS and SSH Cipher Suites
- Source Code and Binary Analysis for Cryptographic Library Calls
- Cryptographic Bill of Materials Records for Algorithms and Keys
- Crypto-Agility Abstraction Layers and Configurable Algorithm Policies
- Risk-Based Prioritisation Matrix for Quantum-Vulnerable Systems

Day 4: Hybrid TLS, PKI, HSM and Supplier Readiness Problem Cases

- Hybrid TLS Handshake Testing for Latency and Packet Size
- Middlebox and Legacy Client Interoperability Failure Diagnosis
- Hybrid and Composite Certificate Options for Issuing Hierarchies
- HSM Firmware Upgrade Paths for Post-Quantum Key Generation
- Supplier Readiness Questionnaire and Crypto-Agility Contract Clauses

Day 5: Lab Work on the Post-Quantum Migration Plan

- Case Organisation Brief Covering Payments, Archives and E-Services
 - CBOM Extract Build From Case Discovery Scan Outputs
 - Migration Wave Sequencing by Exposure Score and Dependency
 - Vendor Readiness Register and Remediation Tracking Sheet
 - Post-Quantum Migration Plan Completion and Peer Challenge
-

Skills You Will Gain:

- Quantum Exposure Scoring
- Post-Quantum Algorithm Selection
- Cryptographic Discovery and CBOM Building
- Crypto-Agile Architecture Design
- Hybrid Handshake Testing
- HSM and Supplier Readiness Assessment
- Migration Wave Planning

Why Attend This Course:

- Deliver a Post-Quantum Migration Plan with a CBOM extract and migration waves to the chief information security officer and the architecture board
- Decide which services move first to hybrid key exchange, which certificates need new signature algorithms and which can wait
- Avoid late, rushed algorithm replacement, failed handshakes with legacy clients and HSM purchases that cannot support post-quantum keys
- Coach infrastructure, application and supplier management colleagues on discovery scanning, CBOM upkeep and readiness questionnaires

Conclusion:

Back at work, the participant gives the chief information security officer and the architecture board a Post-Quantum Migration Plan that links each quantum-vulnerable system to an exposure score, a migration wave, a target algorithm and an accountable owner. The board uses it to approve funding, supplier requirements and the order in which TLS endpoints, certificates, HSMs and applications move. After the first migration wave, the unit should rescan the estate, refresh the CBOM, record handshake and performance results and adjust later waves and supplier deadlines.

Frequently Asked Questions FAQ:

What should participants know before a post-quantum cryptography migration course?

Participants should already work with TLS certificates, SSH, key management or security architecture and understand public-key and symmetric encryption at a working level. No advanced mathematics is needed; lattice and hash-based schemes are explained through their parameters, sizes and deployment effects.

How does post-quantum cryptography migration differ from a quantum computing overview or a PKI operations course?

This course is hands-on migration engineering: discovery scanning, CBOM building, hybrid handshake testing, HSM and supplier readiness and wave planning. A quantum computing overview stays at business and use-case level, and a PKI operations course runs certificate authorities day to day.

Why does post-quantum cryptography migration start with a cryptographic inventory?

Organisations cannot replace algorithms they cannot find. An inventory shows where RSA and elliptic curve keys, protocols and libraries sit, which data they protect and how long that data must stay secret, so the migration can be ordered by real exposure.

What do participants take back from the post-quantum cryptography migration course?

Each participant takes back a Post-Quantum Migration Plan for a case organisation, with a CBOM extract, exposure scores, migration waves, a vendor readiness register and progress indicators that can be adapted to their own systems and suppliers.
