Get Ready for Post Quantum Cryptography

Paul Suhler

Principal Engineer, SSD Standards, KIOXIA

Chair, IEEE Security in Storage Working Group

Post Quantum Cryptography (PQC)

- Cryptographically-relevant quantum computers will be able to run existing quantum algorithms that break classical encryption.
- Quantum-resilient algorithms (post-quantum cryptography – PQC) have been developed to protect against attacks using quantum computers.
- Encrypted data can be harvested now and attacked when quantum computers are available.
- Holders of data may be liable for future breaches.
- Systems must transition from classical algorithms to quantum-resilient algorithms.

The Transition to PQC Algorithms

- Commercial National Security Algorithm (CNSA) Suite 2.0 specifies PQC algorithms to use for national security systems.
- Vendors will want to meet those requirements for non-government customers.
- UK and EU timelines roughly align with CNSA 2.0 timelines.
- PQC algorithms are defined in other standards.

PQC Adoption Timeline

- Committee on National Security Systems Policy 15 (CNSSP 15):
  - By 1 January 2027, all new acquisitions must be CNSA 2.0 compliant.
  - By 31 December 2030, equipment & services not supporting CNSA 2.0 must be phased out.
  - By 31 December 2031, CNSA 2.0 algorithms must be used.
  - Transition to QR algorithms for NSS to be complete by 2035.

  Equipment pre-dating the required support date must be able to run new algorithms and to be updated to future algorithms (“cryptographic agility”).
- US government NSS and Defense Industrial Base (DIB) are required to follow the above.
- Guidance for other agencies will be issued by 1 December 2025.
- See Adoption Guidance in Supporting Material

Transitioning to Quantum-Resistant Algorithms

- PQC keys are large and must be integrated into certificates and protocols, for example:
  - Certificate signing
  - TLS key exchange
- How to allow PQC and non-PQC devices to interoperate during the transition period? Two schemes:
  - Deploy products that implement vulnerable algorithms, but which can be updated in the field to quantum-resistant algorithms.
  - Deploy products with hybrid algorithms (both vulnerable and resistant algorithms).

Standards

- NIST standards specify the required quantum-resistant algorithms and they can be certified as part of FIPS 140 compliance.
- Hybrid algorithms are not defined by NIST, and FIPS 140 compliance must be discussed with test labs.
- EU ENISA requirements may or may not specify NIST algorithms.

- See supporting material for standards and related references.
- See my data sanitization talk in session 201 for comments on legal requirements.

Hybrid Algorithms

- Hybrid algorithms are needed for TLS 1.3, Secure Shell (SSH), and X.509 certificates.
- Most work is being done by the Internet Engineering Task Force (IETF).
  - RFC 9180 Hybrid Public Key Encryption (HPKE) (2022)
  - Post-Quantum Cryptography Recommendations for TLS-based Applications
  - Hybrid key exchange in TLS 1.3
  - Enhancing Security in EAP-AKA' with Hybrid Post-Quantum Cryptography
  - Terminology for Post-Quantum Traditional Hybrid Schemes
  - Numerous others.
  - See also Luis Freeman’s discussion of IETF work on hybrid algorithms in his presentation in this session.

Summary

- A sufficient set of PQC algorithms has been standardized.
  - Work on future algorithms continues.
- The focus is on updating protocols to use PQC algorithms (TLS, SPDM, DICE, etc.)
  - Also: Secure Shell (SSH), Internet Protocol Security (IPsec), and Cryptographic Message Syntax (CMS).
- Libraries will be updated:
  - OpenSSL, BoringSSL, Libsodium, Java Cryptography Architecture (JCA), etc.

Supporting Material

Commercial National Security Algorithm (CNSA) Suite 2.0

- Includes algorithms resistant to attacks by cryptographically relevant quantum computers.
  - RSA, finite-field Diffie-Hellman (DH), and elliptic curve cryptography (ECDH and ECDSA) are deprecated.
  - FIPS 197 – Advanced Encryption Standard is constrained: 256-bit keys required (128-bit and 192-bit keys deprecated)
  - FIPS 202 - SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions: For hardware integrity checks only.
  - FIPS 203 – Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM).
  - FIPS 204 – Module-Lattice-Based Digital Signature Standard (ML-DSA).
  - FIPS 180-4 – Secure Hash Standard (SHS): SHA-384 and SHA-512 are allowed.
  - SP 800-208 - Layton-Micali Signature (LMS) and Xtended Merkel Signature Scheme (XMSS) for signing firmware and software. (HSS and XMSSMT are not allowed.)

Adoption Guidance

- NIST IR 8547 (Initial Public Draft) Transition to Post-Quantum Cryptography Standards , Nov. 2024
- The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ, Dec. 2024, Ver. 2.1.
- UK: Timelines for migration to post-quantum cryptography
- EU: Roadmap for the Transition to Post-Quantum Cryptography

Other Standards

- DMTF (formerly the Distributed Management Task Force)
  - Security Protocols and Data Models (SPDM) 1.4.0 (DSP0274) includes:
    - FIPS 203 ML-KEM
    - FIPS 204 ML-DSA
    - FIPS205 Stateless Hash-Based Digital Signature Standard (SLH-DSA; not part of CNSA 2.0)
- Trusted Computing Group (TCG)
  - Device Identifier Composition Engine (DICE)
  - Core architecture
  - Opal family of standards
  - Enterprise SSC
  - Key Per I/O

Thank you!