Post-Quantum

Cryptography Conference

Transitioning National Security Systems to a Post Quantum Future

In this presentation, Dr. Morgan Stern, Senior Subject Matter Expert on Quantum-Resistant Cryptography within the National Security Agency (NSA)'s Cybersecurity Directorate, will discuss the NSA's approach to transitioning National Security Systems to a post-quantum future. Dr. Stern will highlight key strategies, challenges, and milestones in preparing for the quantum threat, ensuring secure and resilient systems for national defense.

Morgan Stern

Senior Quantum Resistant Cryptography Subject Matter Expert at National Security Agency (NSA)

SSL.com PQ SHIELD HID KEYFACTOR ENTRUST

January 15 and 16, 2025 - Austin, TX (US) | Online

PKI Consortium Inc. is registered as a 501(c)(6) non-profit entity (“business league”) under Utah law (10462204-0140) | pkic.org

PKI Consortium

NSA CYBERSECURITY

Transitioning to a Quantum Resistant Future

MORGAN STERN, PHD

JANUARY 15, 2025

What is a National Security System?

The Director of NSA serves as the National Manager for US National Security Systems, giving NSA the authority to set requirements for cryptography across this area. This is a key part of NSA's Cybersecurity mission.

Most systems run by the Department of Defense or Intelligence Community fall under this "National Security System" classification.

- Department of Defense has well over a million employees who need secured communications with minimal downtime, with many deployed to locations across the world.
    - NIPRNet, which has been up since the original ARPANET
- Classified networks
- Industrial control systems owned by Department of Defense
- GPS
- Weapon systems

A little history

- 2001: CNSSP-11 lays out that commercial-off-the-shelf products intended to protect National Security Systems must be validated using the FIPS and NIAP processes
- 2005: Suite B announced, laying out the use of commercial standards for public key to be used to protect National Security Systems
- 2016: CNSSP-15 updated to address the quantum threat, and introducing CNSA 1.0
- May 2022: National Security Memo 10 signed making it an aim of US to be off quantum vulnerable crypt by 2035
    - Calls out to several cybersecurity agencies across the US Government to work in their area of responsibility to ensure a timely transition: NIST, CISA, OMB, ONCD, NSA
    - Calls out NSA to make standards for NSS and give a timeline for deprecation of quantum vulnerable systems
- 2024: Finalization of CNSA 2.0 released laying out how to achieve quantum resistance in NSS

National Security Memo 10

Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

3 [T]he United States must prioritize the timely and equitable transition of cryptographic systems to quantum-resistant cryptography, with the goal of mitigating as much of the quantum risk as is feasible by 2035.

3.c.vii Within 90 days of the release of the first set of NIST standards for quantum-resistant cryptography… NIST, shall release a proposed timeline for the deprecation of quantum-vulnerable cryptography… with the goal of moving the maximum number of systems off… within a decade of the publication of the initial… standards.

3.c.ix Until the release of… of NIST standards… FCEB Agencies shall not procure any commercial quantum-resistant cryptographic solutions for use in IT systems supporting enterprise and mission operations.

3.c.x Within 1 year… the Director of NSA… shall provide guidance on quantum-resistant cryptography migration, implementation, and oversight for NSS.

With these goals in mind, NSA released the Commercial National Security Algorithm (CNSA) 2.0 Suite September 2022 (https://www.nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources/)

Commercial National Security Algorithm (CNSA) 2.0 Suite

Algorithm	Purpose	Relevant NIST standards
General purpose algorithms		
AES-256	Block Cipher	FIPS 197
SHA-384 or SHA-512	Cryptographic Hash	FIPS 180-4
ML-KEM-1024	Public Key Establishment	FIPS 203
ML-DSA-87	Digital Signature	FIPS 204
Specific use case algorithms		
LMS or XMSS (LMS 256-192 recommended)	Software/Firmware Signature	SP 800-208
SHA3-384 or SHA3-512	Hashing in internal hardware (e.g. secure boot)	FIPS 202

NSA updates Protection Profiles as industry develops appropriate standards because product lines may develop at different speeds. CNSA 1.0 algorithms will continue to be used until solutions can operate with CNSA 2.0.

We do not anticipate any major revisions to this list over the course of the quantum resistance transition

Broad goals with CNSA 2.0 selections

SECURITY

Data must be secured for a long time horizon against a robust set of threats

SIMPLICITY

It must be as easy as possible for our users to comply with our requirements

VALIDATIO N

It should be simple for our users to validate that their systems comply with NSA guidance

UNIVERSALITY

The requirements should cover the diverse set of use cases that make up the US National Security arena

EASE OF ACQUISITION

It should not be difficult to comply while staying within normal acquisition processes

Quantum resistance timeline

Specific product lines or technologies and applications will possibly have their own timeline, but barring such separate guidance, the current policy is:

- 2024: Algorithms finalized
- 2027: New NSS acquisitions expected to be capable of quantum resistant
- 2030: Baseline for NSS expected to be capable of quantum resistance
- 2031: Quantum resistance expected in NSS

Concrete steps today

- Ensure all new hardware can at least be upgraded to full QR
    - Likely requires a QR signature for the root of trust
- Update standards to support quantum resistance
    - Ensuring ML-KEM-1024 supported
    - CNSA supports ML-DSA-87, not HashML-DSA-87
- Set up quantum resistant Certificate Authorities
- Start acquisition process

Standards and hybrid

- The goal of NSA is to transition quickly and securely to a quantum resistant future
- The fastest standards to use are the ones we have today
- In some cases, such as IPsec, this means having both a quantum-vulnerable and a quantum-resistant key agreement (hybrid)
    - Protocol requires substantial structural changes to use a larger key agreement where presently quantum-vulnerable cryptography is used
- In most cases, adding hybrid agreements requires new standards and more validation
- Importantly, a hybrid agreement offers no quantum-resistant cryptographic security beyond what a pure quantum resistant option
- NSA expects CNSA-compliant profiles featuring (for example) TLS, to only use ML-KEM-1024
    - We recognize we may later define more protection profiles for interoperability

Coexistence, not hybrid

- All PKI transitions take time
- Any CA stood up today will likely still be valid when the first quantum resistant CA's arrive
- Just as today our devices can accept certificates signed with ECDSA and RSA, during the transition we expect certificates signed by ECDSA, RSA, and ML-DSA to exist in the same ecosystem
- In some circumstances, a given device may need both a quantum-vulnerable and a quantum-resistant identity
- Aiming to follow what we historically did as we moved to RSA 2048, and from SHA1 to SHA2
- We do not foresee a device needing a single certificate or identity that incorporates both at once
    - This added complexity increases attack surface and dramatically slows any transition

Takeaways

- The specifications for the quantum resistant future are here
- By the end of 2031 the expectation among commercial NSS will be quantum resistance
- Confidentiality is being quickly added to standards today and we expect fast deployment
- The PKI ecosystem is in a good place to evolve quickly if we work together

Questions?