Post-Quantum Cryptography (PQC)

NAESB WEQ Cybersecurity Subcommittee

Paul van Brouwershaven - June 5, 2025

Cryptography is **Critical** to Cybersecurity

- Essential for protecting sensitive data, ensuring integrity, authenticity, non-repudiation, and preventing unauthorized access.
- Weak cryptography can lead to severe consequences such as data breaches, espionage, and systemic vulnerabilities.

Quantum Computing Threatens Current Cryptography

- Most current cryptographic systems are vulnerable to future quantum attacks.
- Quantum computers may break today's widely used algorithms within 10 to 20 years.

Impact to Cryptography

	Symmetric	Asymmetric
Encryption	Authenticated Encryption, Block Cipher + Mode, Stream Cipher	Public-key Encryption
Authentication / Integrity	Authenticated Encryption, Message Authentication Code	Digital Signature
Key Generation / Distribution	(Pseudo) Random Number Generator	Key Exchange, Key Encapsulation

- For **symmetric-key primitives**, quantum computers pose a moderate threat. Grover's algorithm offers a quadratic speed-up, effectively halving the security level.
- In contrast, **asymmetric-key cryptography** faces a much more severe threat. Shor's algorithm can completely break widely used public-key schemes such as RSA, ECDSA, ECDH, and EdDSA.

Why Act Now?

- **Store-Now-Decrypt-Later:** Encrypted data intercepted today may be decrypted in the future by quantum computers.
- **Long-Lived Systems:** Critical infrastructure deployed today may not be upgradable to PQC later.
- **Migration Complexity:** Replacing cryptographic infrastructure is slow and resource-intensive.
- **No-Regret:** Early steps (like inventorying cryptographic assets and risks) provide value beyond PQC.

Industrial IoT Migration Risks

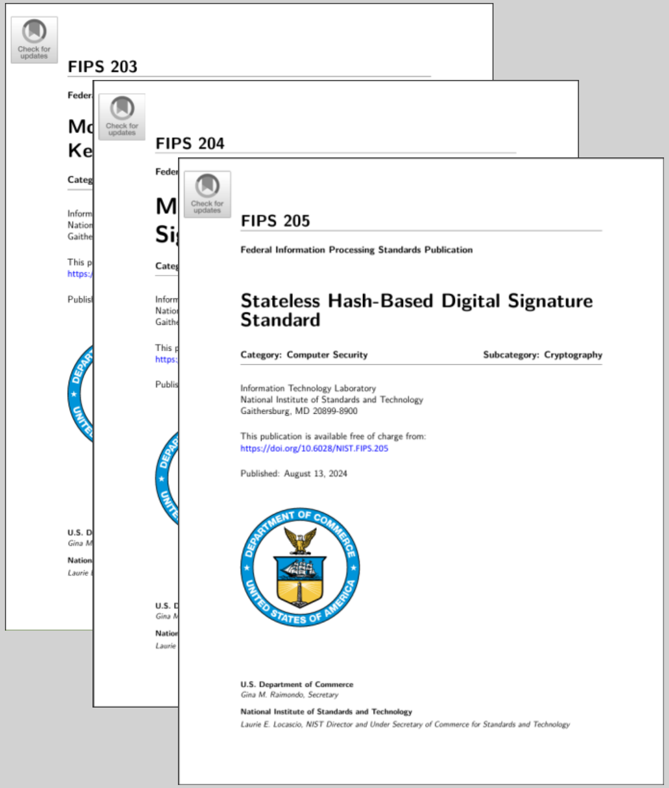
- Deployments
  - Often involve large volumes of field devices
  - Devices may be spread across vast geographic areas, including remote or harsh environments
- Devices may be
  - Be resource-constrained and not crypto-agile
  - Be non-upgradeable, or not remotely upgradable
  - Be embedded, hard to service, or not designed for replacement
  - Use proprietary or PQC-incompatible protocols
  - Be internet-connected, posing elevated cybersecurity risks

PQC Migration Has Begun

- NIST has published the initial PQC standards
- Governments are setting policies, deadlines and provide guidance
- Vendors start to release products that are quantum safe or ready

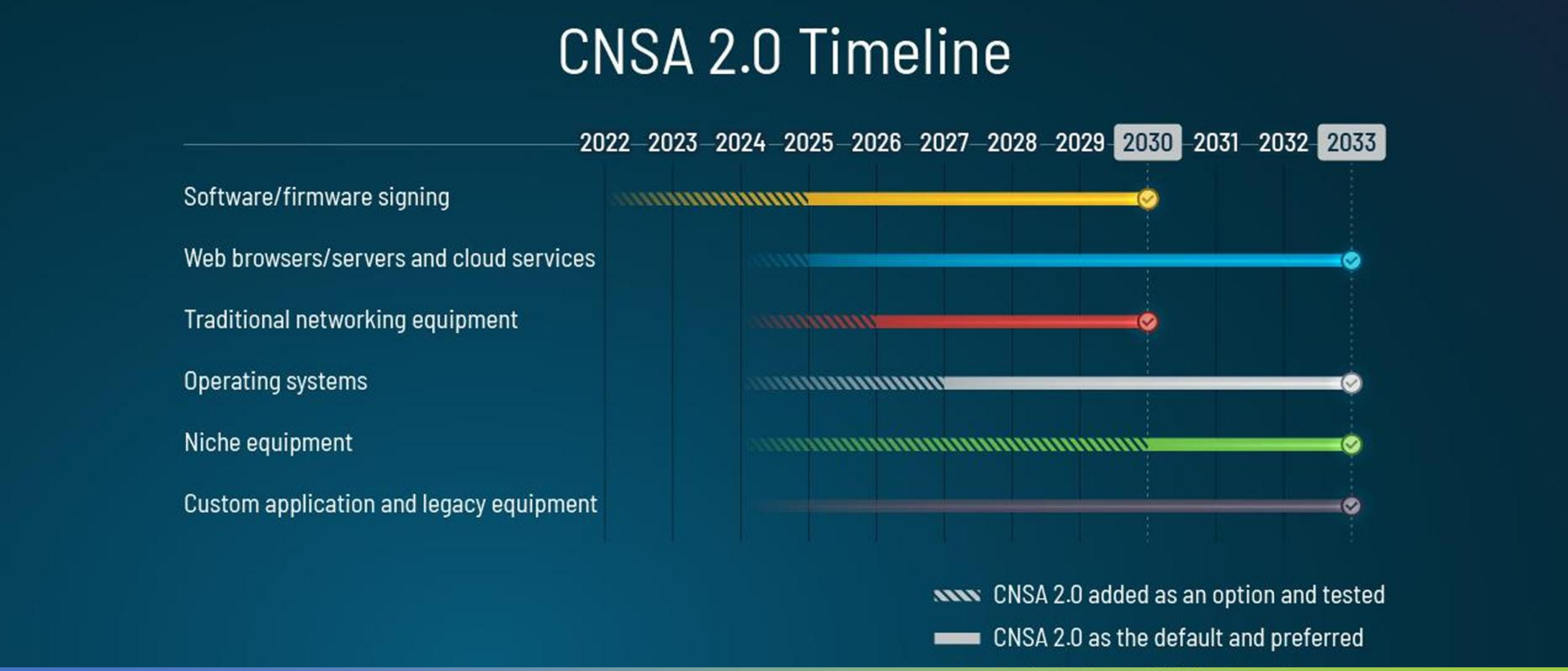
PQC Standards Published by NIST

- **FIPS 203 – ML-KEM**
  Based on CRYSTALS-Kyber (Key Encapsulation Mechanism)
- **FIPS 204 – ML-DSA**
  Based on CRYSTALS-Dilithium (Digital Signatures)
- **FIPS 205 – SLH-DSA**
  Based on SPHINCS+ (Stateless Hash-Based Signatures)



CNSA Suite 2.0

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher for information protection	FIPS 197	Use 256-bit keys for all classification levels.
ML-KEM (previously CRYSTALS Kyber)	Asymmetric algorithm for key establishment	FIPS 203	ML-KEM-1024 for all classification levels.
ML-DSA (previously CRYSTALS Dilithium)	Asymmetric algorithm for digital signatures in any use case, including signing firmware and software	FIPS 204	ML-DSA-87 for all classification levels.
Secure Hash Algorithm (SHA)	Algorithm for computing a condensed representation of information	FIPS 180-4	Use SHA-384 or SHA-512 for all classification levels.
Algorithms Allowed in Specific Applications			
Leighton-Micali Signature (LMS)	Asymmetric algorithm for digitally signing firmware and software	FIPS SP 800-208	All parameters approved for all classification levels. LMS SHA 256/192 is recommended.
Xtended Merkle Signature Scheme (XMSS)	Asymmetric algorithm for digitally signing firmware and software	FIPS SP 800-208	All parameters approved for all classification levels.
Secure Hash Algorithm 3 (SHA3)	Algorithm used for computing a condensed representation of information as part of hardware integrity	FIPS SP 202	SHA3-384 or SHA3-512 allowed for internal hardware functionality only (e.g., boot-up integrity checks)



Commercial National Security Algorithm (CNSA) Suite 2.0

NIST Internal Report 8547 (Draft)

- NIST IR 8547 is setting a **2030** deadline **to deprecate** RSA-2048 and ECC-256 algorithms and **banning RSA and ECC entirely by 2035**.

✗ RSA
✗ ECDSA
✗ EdDSA
✗ DH
✗ ECDH

National Cyber Security Centre (NCSC) - UK

2028

Define migration goals, conduct a full discovery exercise (assess cryptographic dependencies), and build an initial migration plan.

2031

Carry out early, high-priority PQC migration activities and refine the plan.

2035

Complete migration to PQC for all systems, services, and products

Australian Signals Directorate (ASD)

- Phase out **all weak encryption algorithms** for High Assurance Cryptographic Equipment (HACE) **by 2030**, including those based on RSA, ECDH, ECDSA, and SHA-256.
- The **development** and **procurement** of new cryptographic equipment and software **ensures support** for the use of ML-DSA-87, ML-KEM-1024, SHA-384, SHA-512 and AES-256 by **no later than 2030**.

How Organizations can Prepare

1. **Establish a Quantum-Readiness Roadmap**
   - Project management team to plan and scope the migration to PQC
2. **Prepare an Inventory of Cryptography and Assets**
   - Identity protocols/applications/devices that use vulnerable cryptography
   - Identify high-value data requiring long-term secrecy
3. **Discuss Quantum Safe Roadmaps with Technology Vendors**
   - Include Quantum-Readiness in RFPs and Tenders
   - Determine Supply Chain Quantum-Readiness
4. **Develop a Migration Strategy**
   - Prioritize high-impact systems, and those requiring long-term secrecy
   - Integrate with technology modernization/refresh efforts
   - Prepare to rearchitect, rebuild, or replace legacy applications/systems
5. **Validate and Test Systems**
   - Check the Interoperability of Systems
6. **Educate and Train Staff**

PQC Capabilities Matrix (PQCCM)

https://pkic.org/pqccm

Vendor	Product	Category	Last updated	X.509 Hybrid certificates	LMS	XMSS	ML-KEM/FIPS-203	ML-DSA/FIPS-204	SLH-DSA/FIPS-205
ANKATech	ANKASecure	REST API & SaaS	2025-05-30	✗	✓	✓	✓	✓	✓
AppViewX	AVX ONE PKIaaS	PKI	2025-04-21	✓	🕒	🕒	✗	✓	✓
Botan	Botan	Software library	2025-02-27	✗	✓	✓	✓	✓	✓
Bouncy Castle	BC	Software library	2025-02-27	✓	✓	✓	✓	✓	✓
Crypto4A	QxEDGE	HSP	2025-02-27	N/A	✓	✓	✓	✓	✓
Crypto4A	QxHSM	HSM	2025-02-27	N/A	✓	✓	✓	✓	✓
Entrust	nShield	HSM	2025-03-01	N/A	✗	✗	✓	✓	✗
essendi it GmbH	essendi xc	CLM	2025-05-21	✗	✗	✗	🕒	✓	🕒
EVERTRUST	STREAM/HORIZON	PKI	2025-03-03	✓	✗	✗	🕒	✓	🕒
Eviden	IDnomic PKI	PKI	2025-03-05	✗	✗	✗	✓	✓	✗
Eviden	Trustway Proteccio™ NetHSM	HSM	2024-12-09	N/A	✗	✗	✓	✓	✓
ExeQuantum	ExeQuantum	REST API & SaaS	2025-04-29	✗	✗	✗	✓	✓	✓
Fortanix	DSM	HSM	2025-02-27	N/A	✓	✓	✓	✓	✓
I4P	Trident	HSM	2025-04-16	N/A	✗	✓	✓	✓	✓
InfoSec Global	AgileSec Analytics	Software	2025-02-27	✗	✓	✓	✓	✓	✓
Keyfactor	SignServer	Signing	2025-02-27	✗	✓	✗	✗	✓	✓

PKI Consortium

Post-Quantum Cryptography Conference

October 28 - 30, 2025 - Kuala Lumpur, Malaysia | Online | https://pkic.org/pqcc

- **One day of hands-on workshops** (technical deep dives and training)
- **Two days of expert talks** (keynotes, panels, breakout sessions) in two parallel tracks:
  - Strategic sessions targeting business leaders.
  - Technical sessions targeting engineers.
- Speakers are selected on the quality of their abstracts and are not permitted to promote products or services.
- Workshops may focus on a specific product or solution but must have an educational intend.

PKI Consortium

https://pkic.org/**register**

Thank you

Paul van Brouwershaven
Director of Technology
SSL.com

paulvb@ssl.com