Post-Quantum

Cryptography Conference

Overcoming Challenges in Post-Quantum Cryptography Adoption

Frank Michaud

Principal Enginer Tech Lead for Cisco Crypo Services at Cisco

October 28 - 30, 2025 - Kuala Lumpur, Malaysia

Overcoming Challenges in Post-Quantum Cryptography Adoption

Adoption Timelines and Product-Dependent Challenges

Post-Quantum Cryptography Conference – PKI Consortium

Kula Lumpur October 28 - 30, 2025

Frank Michaud, Principal Engineer

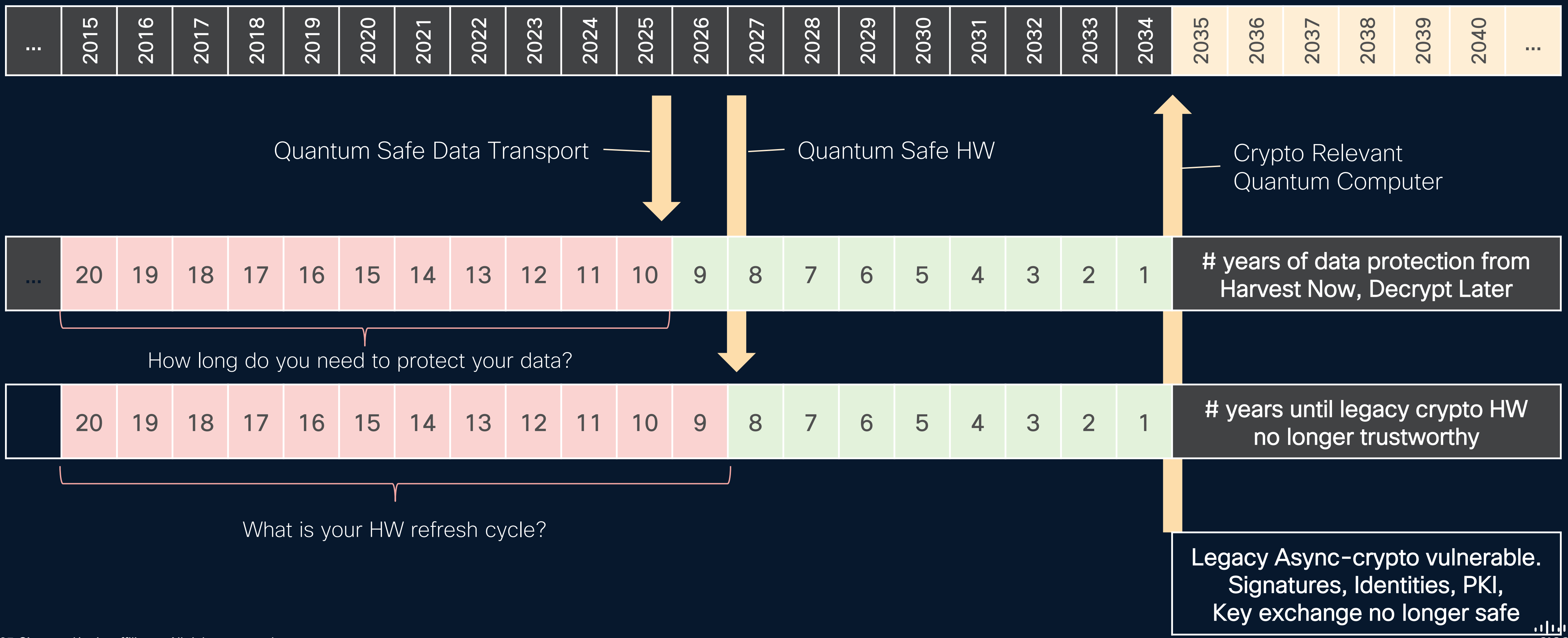
2025-10-13

Quantum Threat & PQC Shift

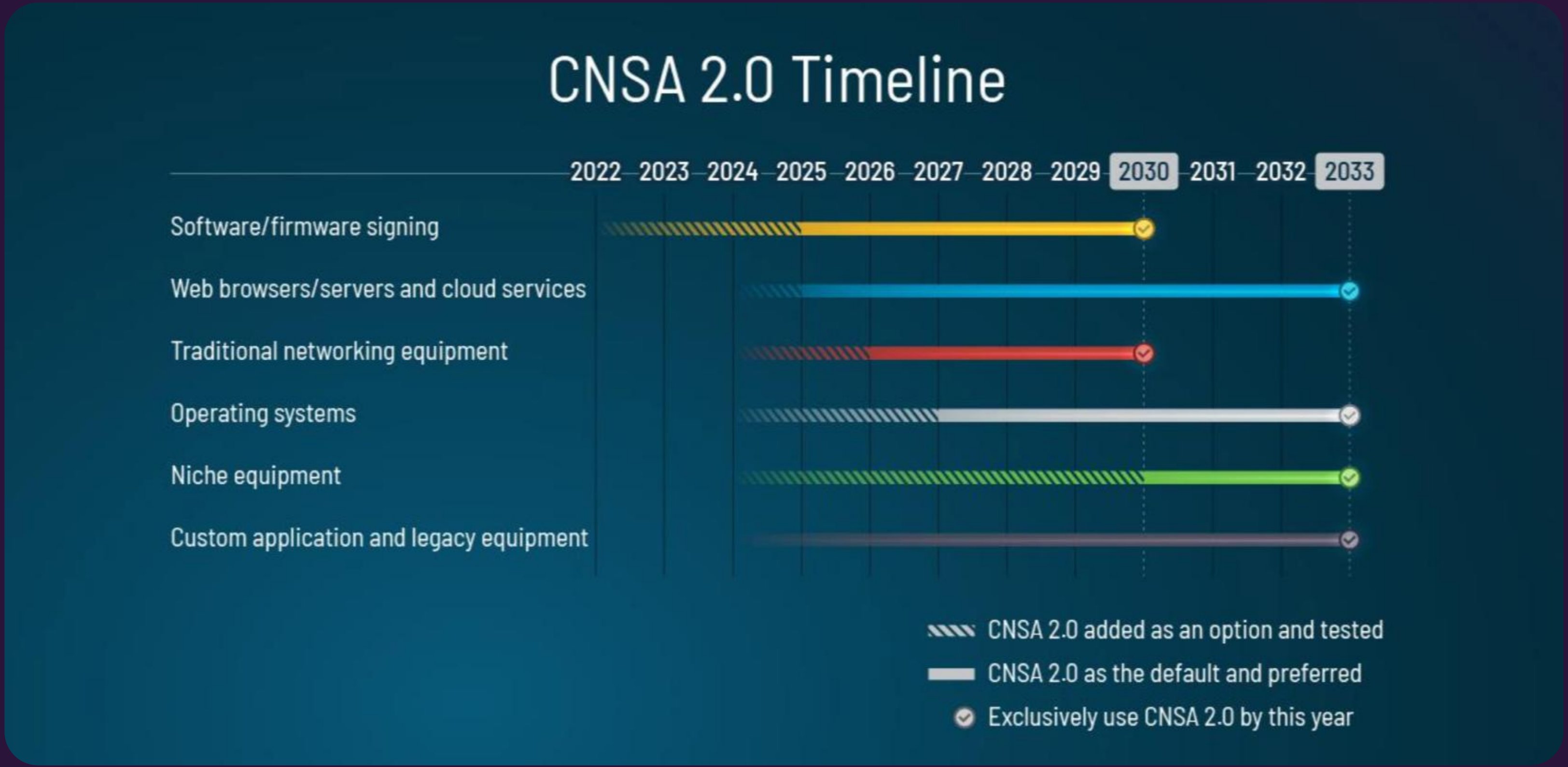
- Quantum computing risk
  - RSA/ECC/DH vulnerable
- Shift in approach
  - No silver bullet, domain-specific solutions
- PQC standards in place
  - But not all standards are in place yet

Why worry today, when QC is not yet available?

Harvest Now- Decrypt Later (HNDL) vulnerability



NSA | Commercial National Security Algorithm Suite 2.0



CNSA FAQ update December 2024 version 2.1:

Required-by date accelerated to **January 2027.**

Only PQC allowed in NSS after **December 2031.**

Source: National Security Agency, *Commercial National Security Algorithm Suite 2.0*

Adoption Timelines & Key Dependencies

- Dependency readiness
  - HSM, SDKs, TLS stacks, OS/toolchains
- Performance tuning
  - MTU, bandwidth, storage, latency budgets
- Protocol/profile work
  - Cert formats, hybrid modes, interop tests
- Compliance
  - FIPS, Common Criteria, CNSA 2.0, audits
- Risk controls
  - Rollback, hybrid, observability, SLOs
- Guidance
  - Multi-year embedded; weeks-months cloud hybrid

NIST Postquantum Algorithms

ML-KEM (FIPS 203)

- Based on CRYSTALS-Kyber
- Lattice-based
- Secures the exchange of keys over untrusted medium

ML-KEM Use Cases

- Securing web connections
- VPN session key establishment

ML-DSA (FIPS 204)

- Based on CRYSTALS-Dilithium
- Lattice-based
- Digital signature scheme for authenticity and integrity of data

ML-DSA Use Cases

- Signing software and updates
- Communcation Authentication
- Authenticating digital docs

SLH-DSA (FIPS 205)

- Based on SPHINCS+
- Stateless hash-based
- Digital signature scheme for authenticity and integrity of data

SLH-DSA Use Cases

- Long-term code and firmware signing
- Validating certificates
- Authenticating archival documents

FN-DSA (FIPS 206) Draft

- Based on FALCON
- Lattice-based
- Very compact digital signature scheme for authenticity and integrity of data

FN-DSA Use Cases

- TLS handshakes
- Securing IoT/Embedded Devices
- Authenticate sessions for high performance systems (Ex., VPNS, Load Balancers)

HQC (Draft)

- Serves as a backup for ML-KEM to diversify outside lattices
- Code-based (decoding random linear codes problem)

HQC Use cases

- General Key Exchange (TLS, VPN, Messaging)
- Backup crypto-system

LMS/XMSS (NIST SP 208)

- Stateful hash-based signatures

LMS/XMSS Use Cases

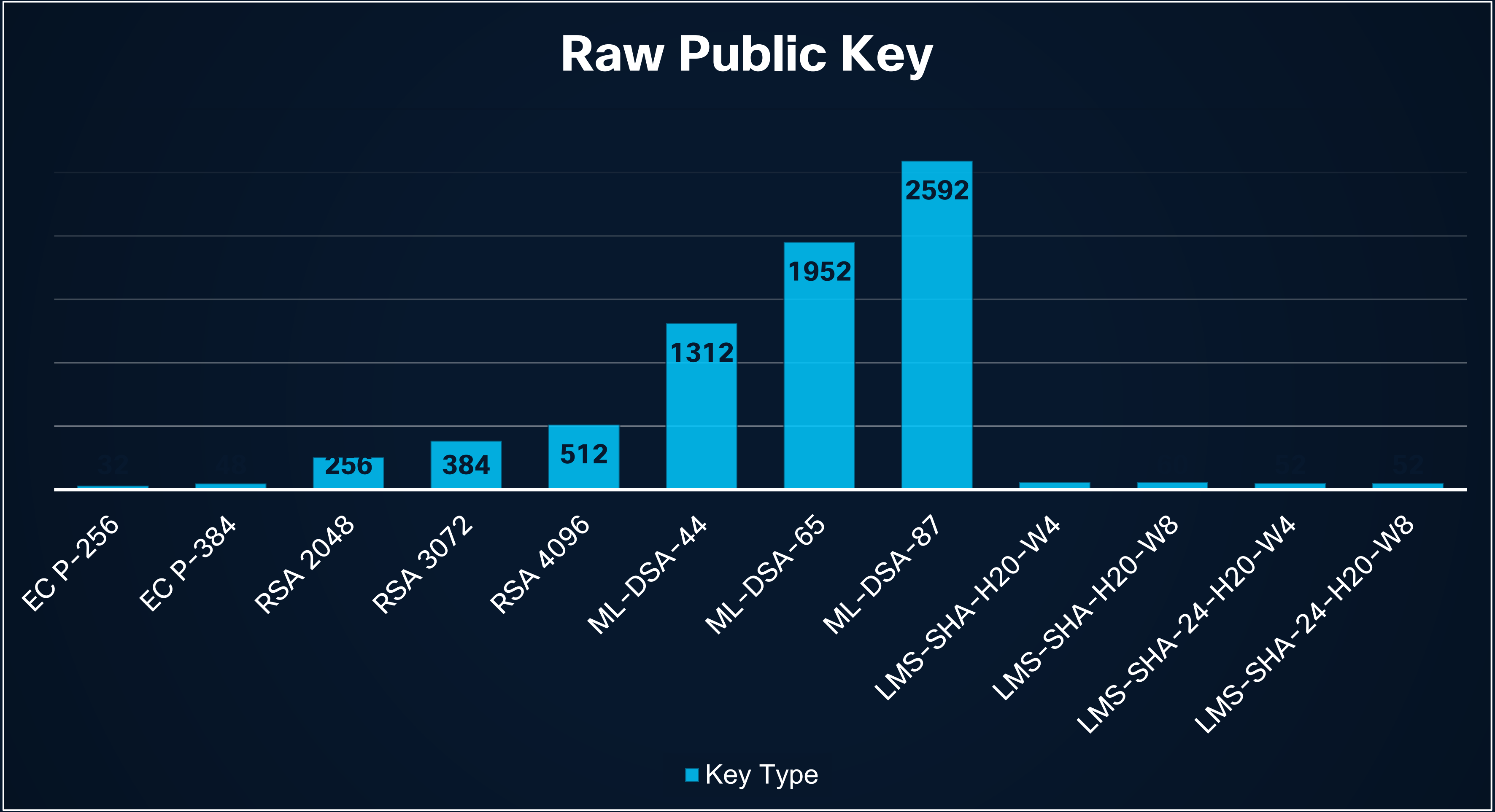
- Firmware / software signing
- Bootloader / OS image signing
- Code updates
- Hardware root of trust

https://csrc.nist.gov/projects/post-quantum-cryptography/selected-algorithms

PQC Performance vs RSA/ECC

- Larger keys and signatures than RSA/ECC
  - Higher storage and transport costs
- Different computational profile
  - Impact on HSM throughput and latency
- Operational implications
  - Ecosystem/library maturity still evolving

Comparison of Public Key Sizes In Bytes



Comparison of Signature Sizes In Bytes

LMS Stateful PKI Backend Challenges

- No OTS reuse in LMS
  - Strict state tracking
- Concurrency control
  - Prevent state conflicts
- Durable state for offline signing
  - Support long workflows
- Disaster recovery
  - Restore without state duplication
- Audit processes
  - Track exhaustion, rollover, root hash integrity
- NIST SP 800-208

Path to post-quantum cryptography

NIST PQC Algorithms

LMS – RFC8554 – approved

XMSS – RFC8391 – approved

NIST SP.800-208 – approved (implementation requirements for LMS & XMSS)

CRYSTALS Kyber: FIPS 203 – ML-KEM - approved
- Module-Lattice-Based Key-Encapsulation Mechanism Standard

CRYSTALS Dilithium: FIPS 204 – ML-DSA - approved
- Module-Lattice-Based Digital Signature Standard

SPHINCS+: FIPS 205 – SLH-DSA - approved
- Stateless Hash-Based Digital Signature Standard

Final standards for FIPS 206 TBD

Falcon DSA (FIPS 206) – stated expectation date passed
HQC – draft pending – expected 2027

Protocol standards (the most urgent set)

IKEv2:

RFC 9370 – Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2) – approved
RFC 9242 – Intermediate Exchange in the Internet Key Exchange Protocol Version 2 (IKEv2) – approved
Post-quantum Hybrid Key Exchange with ML-KEM in the Internet Key Exchange Protocol Version 2 (IKEv2) – draft

TLS:

Hybrid key exchange in TLS 1.3 – draft

SSH:

Post-quantum Hybrid Key Exchange in SSH – draft

PKI:

Composite Signatures For Use In Internet PKI – draft
Internet X.509 Public Key Infrastructure: Algorithm Identifiers for ML-DSA – draft
Internet X.509 Public Key Infrastructure – Algorithm Identifiers for Kyber – draft

PQC Strategy: Key Takeaways & Actions

- Planning
  - Decade long transition – need to survive throughout all hurdles
  - Dependency list can be longer than expected
  - Think of the lifetime of your products/services to evaluate the risk

- PQC algorithm
  - No silver bullet found, yet ...
  - New algos might have an impact on your design and operations

- Standards
  - You can start already
  - TLS and IKE are on the way

Thank you