# The path to Quantum Safe and the impact on the Data Storage Industry Organizations

**Luis Freeman**

Supply Chain Engineering

IBM Infrastructure

the Future of Memory and Storage

# What is Quantum Safe Cryptography?

## New Cryptographic Algorithms will be required for classical computers to be Quantum Safe.

By 2033 is expected that the power of quantum computing will crack the public key cryptography used on classical computers.

Secure Authentication could be broken using Shor's algorithm.

Data encryption could be broken using Grover's algorithm.

## Your data and security are already at risk for Quantum attacks.

Harvest now, decrypt later
Malicious actors are collecting large volumes of encrypted data now with the intent to use quantum computers when powerful enough to decrypt it.

Implementation Cycle is long
Replacing cryptographic algorithms across the entire ecosystem will take several years.

# Quantum and Quantum Safe are different things

## Quantum Algorithms

Quantum algorithms will run on quantum computers

Used to solve complex problems with lots of variables interacting in complicated ways.

**Examples:**

- Shor's algorithm
- Grover's algorithm
- Monte Carlo Simulation Algorithm

## Quantum Safe Algorithms

Quantum Safe algorithms run on classical computer systems.

Cryptographic algorithms resistant to Quantum attacks.

**Examples:**

- ML-KEM (Previously CRYSTALS-Kyber)
- ML-DSA (Previously CRYSTALS-Dilithium)
- SLH-DSA (Previously SPHINCS+)

# Quantum Safe Algorithms

On September 2022, The National Security Agency (NSA) issued the CNSA 2.0 suite of Quantum-Resistant cryptographic algorithms required for National Security Systems.
CNSA 2.0 FAQ released December 2024 provides more details and clarifications.

**Data Encryption**

Use AES with 256-bit key.

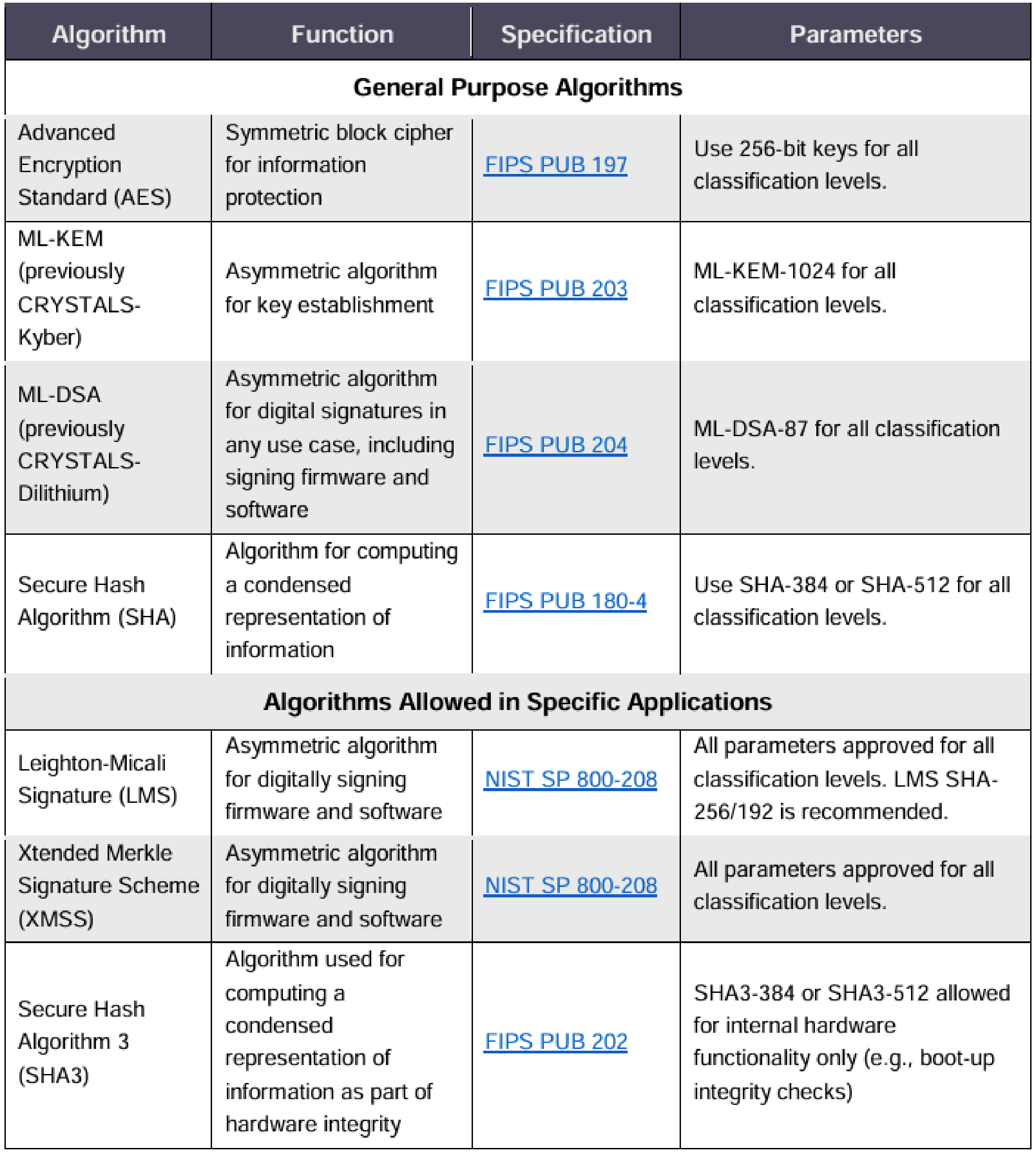
**Secure Authentication**

- Use ML-KEM-1024 for Key establishment
- Use ML-DSA-87 for Digital Signature for any case.
- LMS and XMSS can also be used for specific applications like signing firmware/software.
- Discontinue use of RSA, Diffie-Hellman (DH) and elliptic curve cryptography  (ECDH and ECDSA).

**NOTE that NIST and NSA are not aligned:**

Per CNSA 2.0 FAQ -  SLH-DSA (aka SPHINCS+) – FIPS PUB 205 is not part of CNSA 2.0 and is not approved for use.

*Table: Commercial National Security Algorithm Suite 2.0*



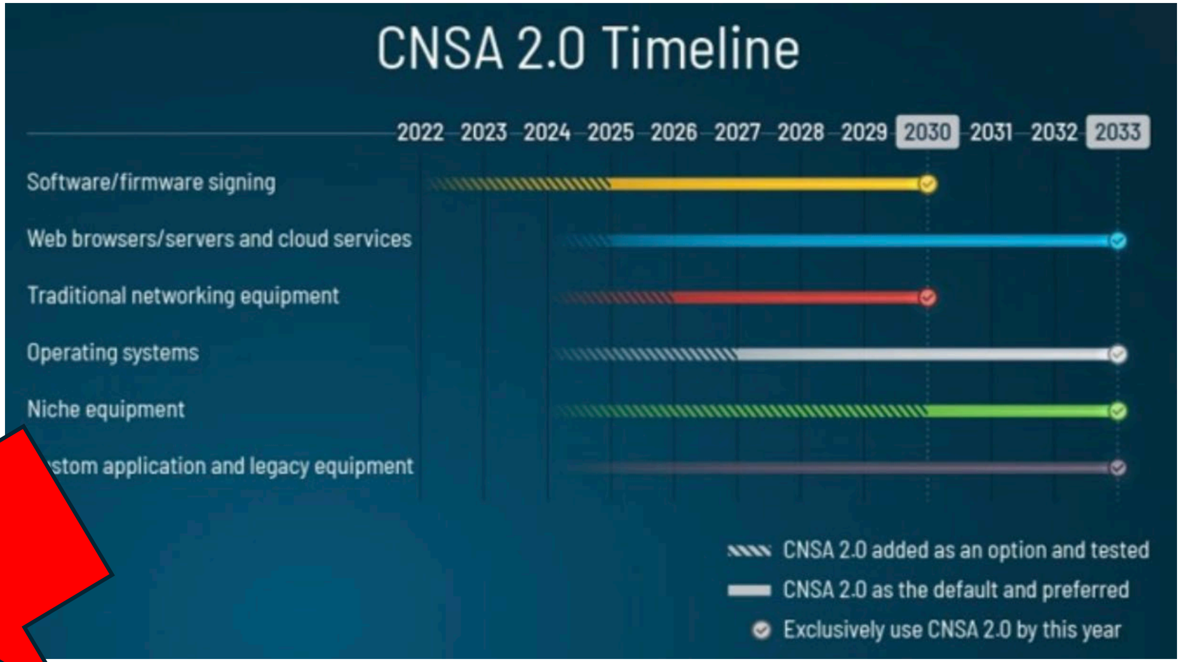
| Algorithm | Function | Specification | Parameters |
|---|---|---|---|
| **General Purpose Algorithms** | | | |
| Advanced Encryption Standard (AES) | Symmetric block cipher for information protection | FIPS PUB 197 | Use 256-bit keys for all classification levels. |
| ML-KEM (previously CRYSTALS-Kyber) | Asymmetric algorithm for key establishment | FIPS PUB 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 PUB 204 | ML-DSA-87 for all classification levels. |
| Secure Hash Algorithm (SHA) | Algorithm for computing a condensed representation of information | FIPS PUB 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 | NIST 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 | NIST 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 PUB 202 | SHA3-384 or SHA3-512 allowed for internal hardware functionality only (e.g., boot-up integrity checks) |

# Timeline for adoption

CNSS Policy 15 Released March 4, 2025 and the CNSA 2.0 FAQ released December 2024 define the following timeframe for adoption which supersedes CNSA 2.0 timeline:

- **CNSA 1.0** algorithms are **acceptable** in all products through **12/31/2025**.
- **CNSA 2.0** algorithms will be **required** starting **01/01/2027** in all new products and services providing cryptographic protection unless otherwise excepted or waived.
- Equipment and services that cannot or will not be updated to CNSA 2.0 algorithms must be phased out and replaced by **12/31/2030**.
- **CNSA 2.0** algorithms are mandated for all protocol use by **12/31/2031**, unless excepted or waived.

Original Timeline in CNSA 2.0 Superseded by CNSS Policy 15



US Executive Order 14306 released in June 2025 removes agencies other than National Security Systems (NSS) and Defense Industrial Base (DIB) from requirement to immediately start procuring Quantum Safe equipment.

Guidelines for other agencies to be issued 12/1/2025, with implementation target no later than 1/2/2030.

# Quantum Safe Algorithms are needed everywhere in the System Infrastructure

Firmware is everywhere in the System Platform and requires to be signed for authentication.

Data is stored in different parts of the System Platform and requires encryption

Data transmitted internally on the System Platform requires encryption and authentication.

Data transmitted externally across networks requires encryption and authentication.

| Device | Contains Firmware | Stores Data | Transmits Data |
|---|---|---|---|
| SSD / HDD | X | X | X |
| DDIMM/Memory | X | X | X |
| Power Supply & PDUs | X | | |
| Optics | X | X | X |
| Tape Drive | X | X | X |
| CPU | X | X | X |
| Switch | X | | X |
| Crypto Module | X | X | X |
| NIC Adapter Cards | X | X | X |
| Glue Logic | X | | |
| Drawers | X | X | X |
| BMC | X | ? | ? |
| Fans | X | | |

# Challenges of replacing discontinued algorithms

Let’s use RSA as example

## Where is being used?

RSA as such is rarely used directly. It’s embedded in software and firmware to:

- Encrypt session keys
- Sign certificates

Finding where it’s used means you must go over source code to locate the direct and indirect usages (e.g TLS, 3rd party libraries, device firmware, etc).

## What to replace it with?

There is no single drop-in replacement solution.

Two new algorithms are needed:

- One for Key Encryption
- One for Signatures

Options for Signature vary in performance, key size and cyphertext sizes. Important factors to consider if legacy infrastructure has size constraints.

## Is replacement secure?

There is no proven record that the new algorithms will stand the test of time.

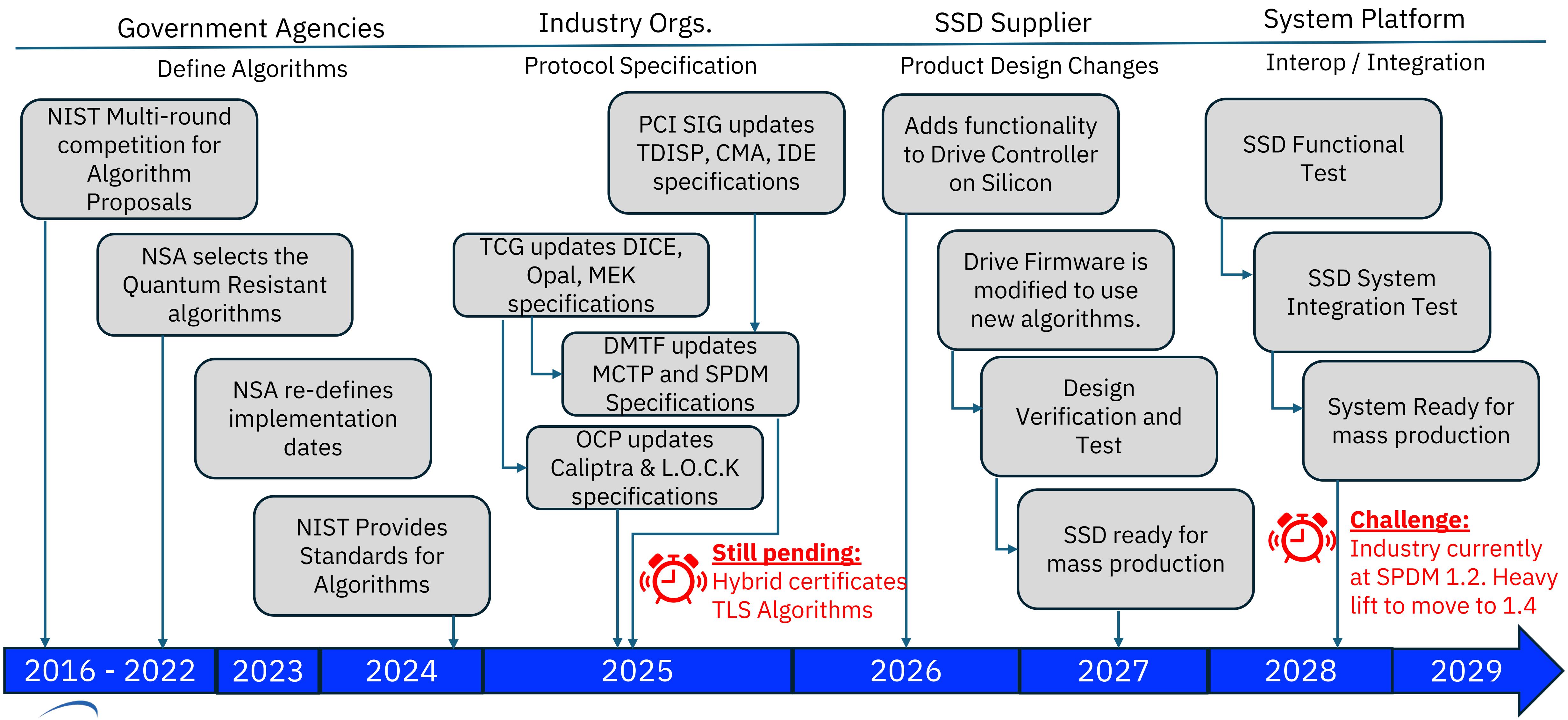
During NIST evaluation process, some of the candidate algorithms were broken using classical computers.

Some recommend to use a hybrid approach of Traditional and Post Quantum algorithms (Hybrid T/PQ).

Note that NSA does not require the use of Hybrids because it adds complexity and NSA is confident on CNSA 2.0 Algorithms.

# Why Quantum Safe Implementation takes so long?

Let's use an SSD as example. On an ideal world....



Government Agencies

Define Algorithms

NIST Multi-round competition for Algorithm Proposals

NSA selects the Quantum Resistant algorithms

NSA re-defines implementation dates

NIST Provides Standards for Algorithms

Industry Orgs.

Protocol Specification

PCI SIG updates TDISP, CMA, IDE specifications

TCG updates DICE, Opal, MEK specifications

DMTF updates MCTP and SPDM Specifications

OCP updates Caliptra & L.O.C.K specifications

SSD Supplier

Product Design Changes

Adds functionality to Drive Controller on Silicon

Drive Firmware is modified to use new algorithms.

Design Verification and Test

SSD ready for mass production

System Platform

Interop / Integration

SSD Functional Test

SSD System Integration Test

System Ready for mass production

2016 - 2022 | 2023 | 2024 | 2025 | 2026 | 2027 | 2028 | 2029

**Still pending:**
Hybrid certificates
TLS Algorithms

**Challenge:**
Industry currently at SPDM 1.2. Heavy lift to move to 1.4

# The status of the Industry Standards Organizations

# DMTF

**Distributed Management Task Force**

## MCTP

The Management Component Transport Protocol (MCTP) is a media independent protocol designed for communication between intelligent devices within a computer system platform

**Version 2.0 Released 04/17/25 Introduces major improvements. Some to enable Quantum Safe on SPDM.**

**Changes:**

- Adds support for 64K endpoints up from 255
- Two levels of segmentation and reassembly with ACK/NACK Protocol for reliability.
- Enablement for SPDM
  - Support of Secured messages
  - Secure message agnostic MCTP bridges
  - End-to-End negotiation for secured messages
- Error/State Reporting

## SPDM

The Security Protocol and Data Model (SPDM) is a way of attesting and authenticating devices and provide secure communication on an infrastructure.

**Version 1.4  - Document DSP0274 released 05/15/2025 is Quantum Resistant.**

**Changes:**

- Added support for asymmetric algorithms
  - ML-DSA – 12 parameter sets
  - SLH-DSA
  - ML-KM – 3 different security strings
  - Key Encapsulation per SP 800-227
- Increased Signature size to accommodate ML-DSA.
- Increased the length of some commands.

**Dependencies:**

- MCTP v2.0 ➔ Released 4/17/2025
- NIST Standards for the 3 algorithms ➔ Released 8/13/24
- 800-227 to define Key Management ➔ Released 1/7/2025
- IETF X.509 Certificate Specifications ➔ Draft Mode
- TCG DICE.
- PCI-SIG IDE, CMA, TDISP.

# OCP

**Open Compute Project**

## Caliptra

Silicon Root of Trust for Boot. Internal Root of Trust IP block for SoCs.

Version 2.0 released April 2025 is Quantum Resistant.

**Changes:**

- ML-DSA-87 for Secure Boot and Attestation.
- ML-KEM for Key wrapping
- LMS SHA256/192 with a tree height of 15.
- Adam's Bridge accelerator for attestation and encapsulation
- Hardware Accelerated Cryptos with countermeasures.

# L.O.C.K

(Layered Open-source Cryptographic Key Management)

A project to deliver an open cryptographic key management implementation leveraging Caliptra 2.1. Provides Key Management services to the drive and host.

Scoped specifically to Storage Devices, starting with NVMe.

Version 0.8.1 released 04/22/2025 implements Quantum Resistant Algorithms.

**Dependencies:**

- TCG Media Encryption Key Multiparty Authorization V1.0 R1.20.
- Caliptra 2.1

# TCG

Trusted Computing Group

## MEK MPA

Media Encryption Key Multiparty Authorization defines how Encryption keys are managed and used on Storage Devices compliant with TCG Standards.

v1.0 r1.20 in draft mode pending Public Review until 9/8/2025, with outlook for release end 2025.

## KPIO

The Key per I/O capability provides a mechanism to use encryption keys that have been injected into an NVM subsystem by a host.

v1.0 is not Quantum safe. Changes are required to handle Post Quantum Algorithms. TCG Epoch Key Purge (EKP) under development.

# Root-of-Trust (RoT) Technologies

## TPM

Trusted Platform Module defines a computer chip (microcontroller) specification that can securely store artifacts used to authenticate the platform.

Current Version 2.0 is not Quantum Safe. However, it was designed with Algorithm Agility, capable of updating or replacing the cryptographic algorithms.

## MARS

Measurement and Attestation RootS specification defines a minimal set of TPM-like features designed to be implemented as a Silicon IP block within a microcontroller for use on IoT and embedded applications.

## DICE

Device Identifier Composition Engine is a very light hardware, distributed software specification used where a TPM would be impractical or infeasible. Typical use on Devices like SSDs, memory, etc.

# PCI SIG

PCI Special Interest Group

## CMA

Component Measurement and Authentication

Defines how SPDM is applied to PCIe/CXL devices/systems.

ECN will be needed to update for Quantum Safe

## DOE

Data Object Exchange

Specification for Data Object transport over different interconnects.

ECN will be needed to update for Quantum Safe

## TDISP

Trusted Execution Environment Device interface Security Protocol is an architecture for trusted I/O virtualization providing the following functions:

## IDE

(Integrity and Data Encryption)
Is a schema for real-time encryption of data transiting a PCIe data bus, which included capabilities to detect whether the data has been tampered with.

ECN issued 2022, changes support for AES-GCM to only 256 bit key making it Quantum Safe

# IETF

Internet Engineering Task Force

## TLS

Transport Layer Security (TLS) is a widely used Cryptographic protocol securing communication over the internet.

Current version 1.3 is not Quantum Safe

Quantum Safe proposals in draft mode

- Use of ML-DSA
- Use of SLH-DSA
- ML-KEM Key Agreement
- KEM-based Authentication
- KEM-based pre-shared-hey handshakes
- Hybrid Key Exchange.
- Use of Composite ML-DSA
- Hybrid Authentication with Dual Certificates

## SSH

Current version 2.0 – RFC 4253 is not Quantum Safe

Quantum Safe proposals in draft mode

- Support for ML-DSA
- SLH-DSA signatures
- ML Key Exchange
- Composite ML-DSA Signatures
- Hybrid PQ/T Key Exchange

## X.509 Certificates

Current version - RFC 5280 – X.509 v3 is not Quantum Safe.

Quantum Safe proposals in draft mode

- Algorithm Identifiers for ML-DSA Signature
- Algorithm Identifiers for ML-KEM certificates
- Composite ML-DSA Key Signature (hybrid T/PQ) algorithms
- Mechanism for Encoding Differences in paired Certificates
- Related Certificates for Use in Multiple Authentications within a protocol – RFC 9763 as of June 2025

# The Linux Foundation

Post-Quantum Cryptography Alliance

## Open Quantum Safe project

OQS is an open source project to support the transition to quantum-resistant cryptography.

The project has 2 lines of work:

- Liboqs ➔ Open Source C library with wrappings for other languages.
- Prototype integrations into protocols and applications. i.e OpenSSL, TLS, SSH, X.509

## PQ Code Package project

Collection of open source projects aiming to build high-assurance software implementations of standards-track post quantum cryptographic algorithms.

## Examples Software and Libraries that need updating:

- OpenSSL
- Libraries for Programming Languages – Python, C++, Go, Java, Rust, etc
- Linux Kernel
- Web browsers

# Conclusion

- The change to Quantum Safe is pervasive
  - Across all devices in the System.
  - Across the Internet
  - Embedded in Software, Firmware and Hardware.

- The path for implementation is long.
  - Changes are needed at many layers
  - Require cooperation of several organizations depending on each other.

- Affects 3 areas of Security: Authentication, Key Establishment and Data Encryption.

- NSA has pulled-in implementation mandate from 2033 to 2031. But only applies to National Security Systems (NSS) and Defense Industrial Base (DIB).

- US Government to issue guidance for other agencies by 12/2025.