White Paper

Post-Quantum Security for Storage Devices: Why Now and How WD Will Help Enterprise Migration

Storage devices: secure download, secure boot, secure messaging, diagnostics, manufacturing

May 2026

1) Executive Summary

Quantum computing is moving from theory to practice. And as its capabilities grow, long-standing public-key cryptography used to protect secure boot, firmware distribution, and authenticated service operations will become increasingly vulnerable to quantum attacks. Adopting a defensive strategy is a prudent step toward safeguarding data and preserving the integrity of device trust chains as threats continue to evolve.

The U.S. National Institute of Standards and Technology (NIST) released new post-quantum cryptography (PQC) standards in August 2024. These standards—Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) for key establishment, Module-Lattice-Based Digital Signature Algorithm (ML-DSA) for digital signatures, and a Stateless Hash-Based Digital Signature Algorithm (SLH-DSA) as an alternative signature—are designed to withstand quantum-powered adversaries and are already being adopted across ecosystems.

In January 2026, we introduced enterprise-focused PQC options across core security workflows: secure boot, secure download, and secure messaging used in secure diagnostics. Our approach follows NIST standards and aligns with U.S. government guidance[1] delivering a low-friction, standards-aligned transition for customers.

What this means for enterprise adoption:

- Long-term protection for device trust chains without disrupting current deployments
- Appropriate security options for systems handling classified information and/or defense and intelligence communications
- Standards-aligned security and interoperability backed by PQC-ready public key infrastructure (PKI) and hardware security module (HSM) workflows
- A clear roadmap to quantum-protection for storage starting in January 2026

2) The Quantum Risk to Storage Security

Long-lived trust chains:

A challenge for staying abreast of the fast-moving evolution of security threats is the service lives of enterprise-grade hard disk drives (HDDs). Code-signing keys and signatures used in secure boot must remain trustworthy across the entire lifetime of the device. The ongoing “harvest now, decrypt later” threat[2], where attackers (typically nation-states) collect encrypted or signed data today to decrypt or forge certified security signatures when quantum capabilities mature, amplifies the need to evaluate and consider new, PQC-drives as soon as possible.

---

[1] (Under CNSA 2.0, the National Security Agency’s Commercial National Security Algorithm Suite 2.0 released in 2022.)

[2] https://www.cisa.gov/sites/default/files/2023-08/Quantum%20Readiness_Final_CLEAR_508c%20%283%29.pdf

Existing exposure points in storage workflows:

- Secure download: Firmware packages and manifests require authenticity and integrity during distribution and staging.
- Secure boot: Bootloader and firmware authenticity must be able to withstand future quantum adversaries.
- Secure diagnostics: RMA and field failure analysis rely on authenticated access and secure messaging that should be upgraded.

Post-quantum cryptography (PQC) refers to classical (non-quantum) cryptographic algorithms designed to resist attacks from quantum computers, typically by doubling the length of the prime numbers that are associated with cryptographic algorithms. It is distinct from "quantum cryptography," which uses quantum phenomena for security. PQC enables organizations to leverage upgraded algorithms and policies to maintain their existing architectures and avoid having to adopt entirely new security systems.

"Secure Boot is a firmware security feature that ensures your computer boots only using software trusted by the manufacturer. It validates the digital signatures of the bootloader, kernel, and drivers on your hard drive, preventing malicious code (like rootkits/bootkits) from loading before the operating system."

3) From Research to Standards: NIST PQC in Brief

NIST launched a multi-year, public evaluation process with a call for algorithm submissions for post-quantum key establishment and digital signatures in December[3] 2016. Following extensive international review, NIST published the first three Federal Information Processing Standards (FIPS) for PQC in August of 2024.

[3] https://www.federalregister.gov/documents/2016/12/20/2016-30615/announcing-request-for-nominations-for-public-key-post-quantum-cryptographic-algorithms

Selected families relevant to storage:

Digital signatures include:

- ML-DSA (formerly CRYSTALS-Dilithium) as the general-purpose choice;
- SLH-DSA (based on SPHINCS+) as an alternative; Falcon is planned for later standardization as FN-DSA;
- Key establishment: ML-KEM (formerly CRYSTALS-Kyber) for establishing shared secrets that protect sessions and channels.

Why this matters to our technology partners in 2026: NIST standardization de-risks adoption, accelerates vendor support and FIPS validation, and enables interoperability efforts across the datacenter ecosystem.

4) What Changes for Storage Devices

Signatures and keys are larger with PQC: ML-DSA and SLH-DSA signatures and public keys are typically larger than classical Rivest–Shamir–Adleman (RSA) or elliptic-curve cryptography (ECC). We account for this in changes to firmware package formats, certificate profiles, and secure bootloaders while maintaining performance targets.

Performance and verification: We have optimized signature generation and path-checking so that PQC integration does not impact device availability or field operations.

PKI and HSM upgrades: Our code-signing certificate authorities (CAs), certificate issuance workflows, and HSM-backed key storage are PQC-capable, supporting issuance, rotation, and lifecycle management of PQC keys and certificates.

Operational guardrails: We retain rollback and interop paths to ensure safe deployment across diverse fleets and support hybrid (dual-signing) strategies where needed.

5) Our Migration Plan and Product Roadmap

Algorithm selection: We have selected ML-DSA-87 for high-assurance code signing in secure boot chains and firmware/package signing, with a dual-signing approach using RSA-3072 combining proven and emerging technologies to ensure strong, resilient security.

PKI/HSM readiness: In 2025, WD deployed a PQC-capable PKI/HSM solution to support issuance, storage, and lifecycle management of PQC code-signing keys and certificates.

Product availability: WD made these efforts in 2025 to enable its PQC products in 2026, with protections in secure boot, secure download, and secure messaging. Subsequent releases will extend PQC across additional product lines and management tooling.

6) Compliance and Policy Context: CNSA 2.0

CNSA 2.0 overview: The U.S. National Security Agency's Commercial National Security Algorithm Suite 2.0 outlines a transition to quantum-resistant algorithms for national security systems and influences broader industry adoption. It endorses ML-KEM and ML-DSA for general-purpose use and permits Leighton-Micali Signature (LMS) and eXtended Merkle Signature Scheme (XMSS) for software and firmware signing, with transition timelines for procurement and fielded equipment.

Our alignment: We adopt NIST-selected algorithms, support crypto agility and lifecycle management, and prepare for evolving validation and procurement requirements consistent with CNSA 2.0.

7) What Enterprise Customers Should Do Now

Start crypto inventory: Identify devices, boot chains, firmware packages, certificates, and sessions that must remain trustworthy long into the future (including data that might be subject to “harvest now, decrypt later”).

Prioritize long-lived assets: Begin adopting PQC-protected storage devices and establish crypto-agile processes for rapid algorithm updates.

Engage with your PKI/HSM teams: Plan issuance, rotation, and validation for ML-DSA-based code signing, and define hybrid strategies where dual-signing is warranted.

8) Conclusion

The PQC transition is about preserving trust in the face of advancing capabilities. By adopting NIST-selected algorithms, starting with ML-DSA-87 for code signing, and preparing PKI/HSM workflows, WD will help keep storage device trust chains secure from manufacturing to field service. With this migration, WD’s customers gain a clear, low-risk path to PQC aligned with CNSA 2.0 and supported by our engineering and partner ecosystem.

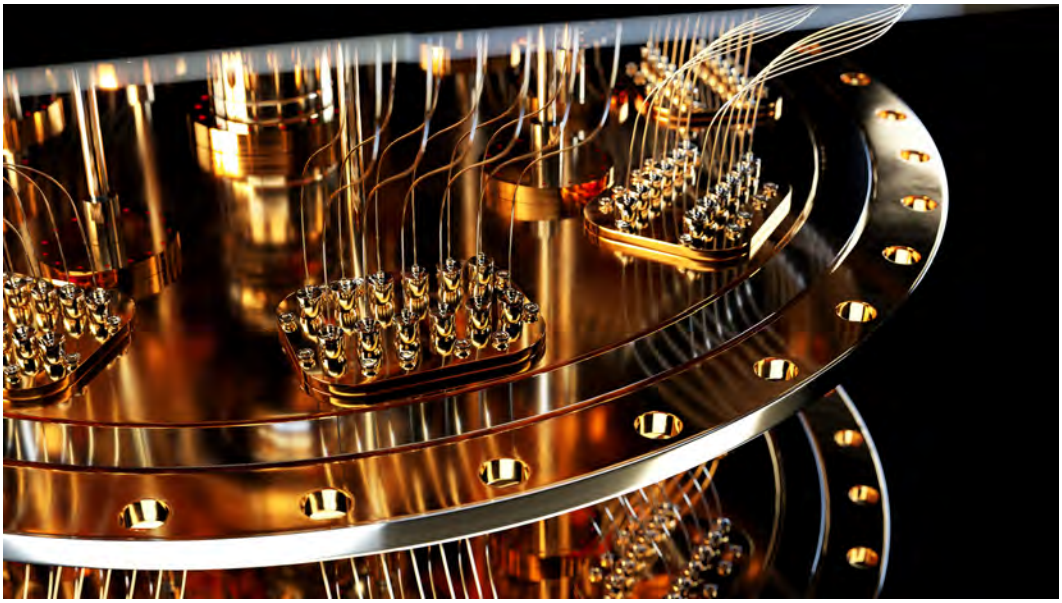
References

- NIST FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM), August 13, 2024.
- NIST FIPS 204: Module-Lattice-Based Digital Signature Algorithm (ML-DSA), August 13, 2024.
- NIST FIPS 205: Stateless Hash-Based Digital Signature Algorithm (SLH-DSA), August 13, 2024.
- NIST SP 800-208: Recommendation for Stateful Hash-Based Signature Schemes (LMS, XMSS), October 2020.
- Federal Register Notice: Approval of FIPS 203, 204, and 205, effective August 14, 2024.
- NSA CNSA 2.0 Cybersecurity Advisory (Algorithms and FAQs), updated 2024–2025.

Executive Brief: Why Act Now

Post-quantum readiness is no longer optional—it is a strategic necessity. The risk is present today because adversaries including nation-states may harvest encrypted data now and decrypt it later when quantum capabilities mature. Moving sooner reduces exposure for long-lived assets and simplifies change management across fleets.

This transition echoes prior cryptography shifts (e.g., DES to AES; SHA-1 deprecation). Those migrations were long and complex—even as systems continued to operate. With a larger, more deeply embedded cryptographic footprint today, early preparation is essential to avoid compressed, high-risk change windows.



Post-Quantum Readiness Roadmap

A four-phase approach helps enterprises organize and execute the transition while maintaining service continuity:

- Assess: Inventory cryptographic assets (algorithms, protocols, keys, certificates, boot chains), identify high-value/long-lived data, and evaluate quantum risk including “harvest now, decrypt later.”
- Plan: Define goals and timelines; update procurement policies to require PQC-ready solutions and crypto-agility; align third parties and contracts to standards (NIST PQC, CNSA 2.0, EU recommendations).
- Transform: Phase in PQC across secure boot, firmware distribution, and secure diagnostics; validate in lab environments; deploy dual-signing and rollback safeguards to manage mixed fleets.
- Oversight: Stand up a cross-functional PMO/steering group to drive governance, reporting, and compliance; track milestones, interoperability, and performance impacts.

Global Policy Context (EU & U.S.)

European Commission Recommendation (April 11, 2024): A coordinated roadmap urges Member States to transition to PQC, with milestones targeting critical infrastructure by 2030 and broad adoption by 2035, complementing NIST standards and CNSA 2.0.

U.S. Quantum Computing Cybersecurity Preparedness Act (Public Law 117-260, Dec 21, 2022): Requires agency inventories of quantum-vulnerable IT and directs OMB to issue migration guidance—signals enterprises should mirror through internal governance and procurement.

Program Governance and PMO

Establish a dedicated, cross-functional program office to coordinate PQC migration across engineering, security, supply chain, and customer operations. Define KPIs for crypto-inventory completeness, dual-signing coverage, validation throughput, and PQC adoption across product lines.

Additional References

- European Commission Recommendation on a Coordinated Implementation Roadmap for PQC, April 11, 2024 (Commission Recommendation (EU) 2024/1101).
- European Commission / NIS Cooperation Group PQC Workstream roadmap (June 23, 2025).
- Quantum Computing Cybersecurity Preparedness Act (Public Law 117-260), December 21, 2022; OMB PQC report, July 2024.

Glossary of Acronyms

CNSA 2.0: Commercial National Security Algorithm Suite 2.0

ECC: Elliptic-Curve Cryptography

FIPS: Federal Information Processing Standards

FN-DSA: FALCON Digital Signature Algorithm

LMS: Leighton-Micali Signature

ML-KEM: Module-Lattice-Based Key-Encapsulation Mechanism

ML-DSA: Module-Lattice-Based Digital Signature Algorithm

PKI: Public Key Infrastructure

PQC: Post-Quantum Cryptography

RSA: Rivest–Shamir–Adleman

SLH-DSA: Stateless Hash-Based Digital Signature Algorithm

XMSS: eXtended Merkle Signature Scheme

HSM: Hardware Security Module

5601 Great Oaks Parkway
San Jose, CA 95119, USA
www.wd.com

© 2026 Western Digital Corporation or its affiliates. All rights reserved.

WD, the WD Design, and Ultrastar are registered trademarks or trademarks of Western Digital Corporation or its affiliates in the US and/or other countries. All other marks are the property of their respective owners.