WHITEPAPER

Post-Quantum Cryptography at the Edge: A Practical Migration

Navigating the transition from classical to quantum-resistant cryptography for long-lived, resource-constrained edge deployments

April 2026

nova8 Technologies

nova8.io

Table of Contents

1. Executive Summary

The cryptographic algorithms that protect most of today's digital infrastructure (RSA, ECDSA, ECDH) are mathematically vulnerable to attack by large-scale quantum computers. While such computers do not yet exist at the scale required to break these algorithms, the timeline for their development is measured in years, not decades. For systems that will remain in the field for extended periods, the time to begin migrating is now.

In August 2024, the National Institute of Standards and Technology (NIST) finalized three post-quantum cryptography (PQC) standards: FIPS 203 (ML-KEM, a lattice-based key encapsulation mechanism), FIPS 204 (ML-DSA, a lattice-based digital signature algorithm), and FIPS 205 (SLH-DSA, a stateless hash-based digital signature algorithm). These standards provide the foundation for replacing quantum-vulnerable cryptography across all categories of use: key exchange, digital signatures, and authentication.

The NSA's Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) sets a direction for National Security Systems to transition to quantum-resistant algorithms, with new system acquisitions expected to prefer PQC by 2027 and full transition targeted by 2035. White House memorandum M-23-02 directs federal agencies to inventory their cryptographic systems and develop migration plans.

This whitepaper examines the practical challenges of migrating edge infrastructure to post-quantum cryptography. It describes the NIST-standardized algorithms, the "harvest now, decrypt later" threat that makes early migration urgent, the specific constraints that edge devices face during migration, hybrid cryptographic approaches that maintain backward compatibility, and the role of image-based platforms in enabling cryptographic agility. The paper draws exclusively on publicly available standards, specifications, and guidance from NIST, NSA, IETF, and the broader research community.

It is intended for platform architects, security engineers, and program managers evaluating post-quantum readiness for edge deployments in defense, critical infrastructure, and industrial environments.

2. The Post-Quantum Threat to Edge Infrastructure

The security of most deployed cryptographic systems relies on the computational difficulty of mathematical problems that classical computers cannot efficiently solve. RSA depends on the difficulty of integer factorization. Elliptic curve cryptography (ECDSA, ECDH, X25519) depends on the difficulty of the discrete logarithm problem on elliptic curves.

In 1994, Peter Shor published a quantum algorithm that can solve both integer factorization and discrete logarithm problems in polynomial time on a sufficiently large quantum computer. This means that RSA, ECDSA, and ECDH, the algorithms that protect virtually all TLS connections, code signing, VPN tunnels, and authenticated communications, will be breakable once a cryptographically relevant quantum computer (CRQC) exists.

The timeline for CRQC development is uncertain but narrowing. The 2024 Global Risk Institute survey of quantum computing experts found that a majority now assess a greater than 50% probability that a CRQC capable of breaking RSA-2048 will exist within 15 to 20 years. Some assessments place this timeline closer to 10 years. While the exact date remains debated, the consensus direction is clear: these systems are coming, and the migration to quantum-resistant cryptography must begin well before they arrive.

Edge infrastructure faces particular exposure to the quantum threat for several reasons.

- Long deployment lifetimes mean that edge devices fielded today may still be operating when quantum computers become capable of breaking current algorithms. A device deployed in 2026 with a ten-year field life must use cryptography that remains secure through 2036, past the NSA CNSA 2.0 transition deadline.
- Physical exposure increases the feasibility of data interception. Edge devices operating in contested, unattended, or physically accessible environments are more susceptible to traffic capture than systems in controlled data center environments.
- Limited update windows constrain how quickly cryptographic changes can be deployed across a fleet. Unlike cloud services that can rotate cryptographic configurations in hours, edge fleets may require weeks or months to reach full deployment of a cryptographic update.
- High-consequence workloads in defense, critical infrastructure, and industrial control systems mean that a cryptographic failure is not merely a compliance issue but a safety and mission risk.

The combination of long field lifetimes, physical exposure, and high-consequence workloads means that edge infrastructure is among the most urgent candidates for post-quantum migration.

3. NIST Post-Quantum Standards: ML-KEM, ML-DSA, and SLH-DSA

After an eight-year evaluation process that began in 2016, NIST finalized three post-quantum cryptography standards in August 2024. These algorithms were selected from 82 initial submissions, evaluated through multiple rounds of public review, and chosen for their combination of security assurance, performance, and implementation practicality.

FIPS 203: ML-KEM (Module-Lattice-Based Key Encapsulation Mechanism)

ML-KEM, formerly known as CRYSTALS-Kyber, is a key encapsulation mechanism designed to replace classical key exchange algorithms such as ECDH and RSA key transport. It is based on the Module Learning With Errors (Module-LWE) problem, a lattice-based mathematical problem for which no efficient quantum algorithm is known.

ML-KEM is defined at three security levels. ML-KEM-512 targets NIST Security Level 1, ML-KEM-768 targets Level 3, and ML-KEM-1024 targets Level 5. The Level 3 parameter set (ML-KEM-768) is the most widely recommended for general use, balancing security margin with performance. At Level 3, the encapsulation key is 1,184 bytes and the ciphertext is 1,088 bytes.

Performance benchmarks from multiple research groups show that ML-KEM operations are competitive with classical ECDH. On ARM Cortex-M4 processors (representative of many edge computing platforms), ML-KEM-768 key generation, encapsulation, and decapsulation each complete in under one millisecond. Academic benchmarks on ARM Cortex-M0+ processors (among the most constrained microcontrollers in common use) have demonstrated ML-KEM performance comparable to or faster than ECDH P-256.

FIPS 204: ML-DSA (Module-Lattice-Based Digital Signature Algorithm)

ML-DSA, formerly known as CRYSTALS-Dilithium, is a digital signature algorithm designed to replace RSA and ECDSA for code signing, certificate authentication, and integrity verification. Like ML-KEM, it is based on the Module-LWE problem.

ML-DSA is defined at three levels: ML-DSA-44 (Level 2), ML-DSA-65 (Level 3), and ML-DSA-87 (Level 5). The Level 3 parameter set is recommended for most applications. At ML-DSA-65, public keys are 1,952 bytes and signatures are 3,309 bytes, significantly larger than ECDSA signatures (64 to 72 bytes) but manageable for most use cases.

Signature verification with ML-DSA is fast, typically completing in under 2 milliseconds on modern processors. This is important for edge devices that may need to verify boot images, container signatures, or update manifests at startup.

FIPS 205: SLH-DSA (Stateless Hash-Based Digital Signature Algorithm)

SLH-DSA, formerly known as SPHINCS+, is a digital signature algorithm based entirely on hash functions rather than lattice mathematics. Its security relies only on the well-understood properties of cryptographic hash functions, making it a conservative choice for applications where the highest confidence in long-term security is required.

The trade-off is size. SLH-DSA signatures range from approximately 7,856 bytes (SLH-DSA-128s, the "small" variant) to 49,856 bytes (SLH-DSA-256f, the "fast" variant at the highest security level). Signing is also slower than ML-DSA. For these reasons, SLH-DSA is typically recommended as a secondary or backup algorithm rather than a primary choice for high-volume operations.

Figure 1 compares the key characteristics of the three NIST PQC standards.

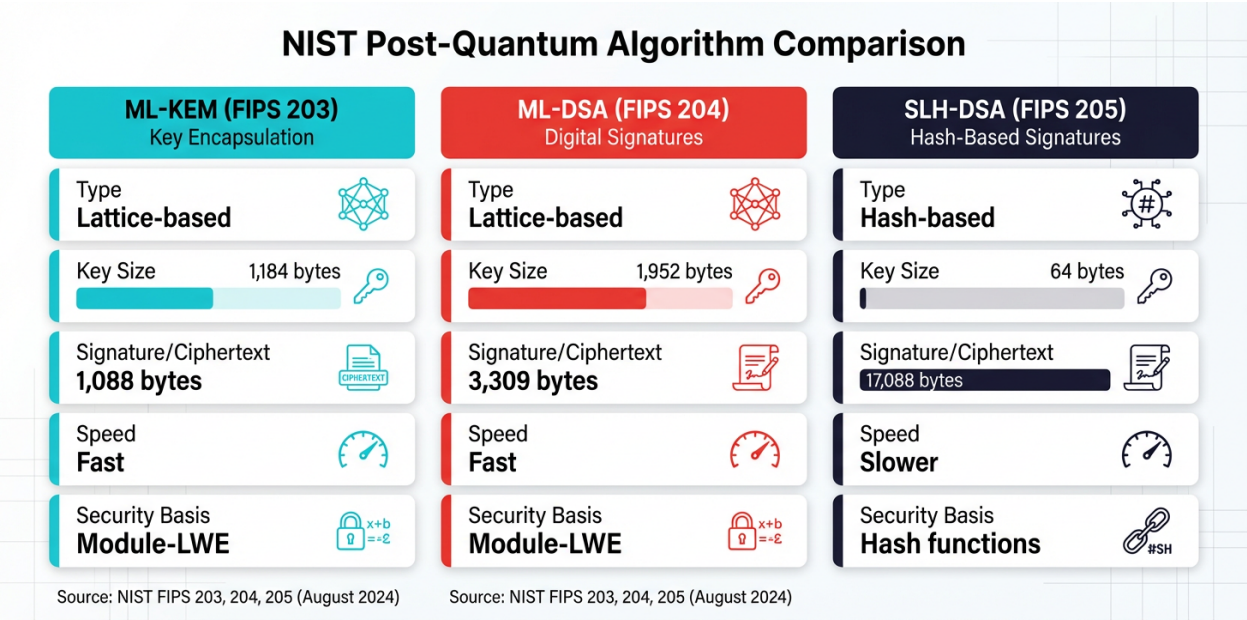

Figure 1: Comparison of NIST post-quantum cryptography standards (FIPS 203, 204, 205) across key parameters.

Together, these three standards provide coverage for the two fundamental cryptographic operations: key exchange (ML-KEM) and digital signatures (ML-DSA and SLH-DSA). Organizations planning post-quantum migration need to address both categories across their infrastructure.

4. The Harvest Now, Decrypt Later Problem

The most frequently cited justification for beginning PQC migration now, before quantum computers can actually break current algorithms, is the "harvest now, decrypt later" (HNDL) threat. This attack model is straightforward: an adversary captures encrypted communications today, stores the ciphertext, and decrypts it later when a sufficiently powerful quantum computer becomes available.

The HNDL threat is not theoretical. Nation-state intelligence services have long-standing programs to collect and store encrypted communications for future exploitation. The joint guidance from CISA, NSA, and NIST on quantum readiness explicitly identifies HNDL as a present-day risk: adversaries may already be harvesting encrypted data with the intent to decrypt it in the future.

The urgency of the HNDL threat depends on the sensitivity lifetime of the data being protected. If encrypted data must remain confidential for 10 years, and a CRQC may exist in 10 years, then the data is already at risk today. The formula is simple: if the sensitivity lifetime of the data plus the time required to deploy PQC exceeds the time until a CRQC is available, migration is already overdue.

White House memorandum M-23-02 (issued January 2023) directs federal agencies to begin inventorying their cryptographic systems and developing migration plans for post-quantum cryptography. The memorandum acknowledges that migration will take years and that starting early is essential to completing the transition before quantum computers make current algorithms unsafe.

For edge infrastructure, several factors make the HNDL threat particularly relevant.

- Edge devices often communicate over networks that are more susceptible to interception than controlled data center networks. Wireless links, satellite uplinks, and field-area networks provide more opportunities for traffic capture.
- Telemetry, command and control, and fleet management traffic from edge devices may contain operationally sensitive information whose value persists for years.
- Software update channels that use classical-only signatures could be retroactively compromised. If an adversary captures signed update packages today and later breaks the signing key, they could create forged updates that appear valid.
- Device provisioning and enrollment protocols that use classical key exchange may be retroactively decryptable, exposing device credentials and fleet membership information.

The HNDL threat means that the urgency of PQC migration is determined not by when quantum computers will arrive, but by how long the data being protected today needs to remain confidential. For defense, intelligence, and critical infrastructure applications, that confidentiality horizon often extends well beyond the expected timeline for CRQC development.

5. Migration Challenges for Resource-Constrained Edge Devices

Migrating to post-quantum cryptography is not simply a matter of swapping algorithm libraries. The new algorithms have different performance characteristics, larger key and signature sizes, and different integration requirements than the classical algorithms they replace. For resource-constrained edge devices, these differences create specific engineering challenges that must be addressed in the migration plan.

Key and Signature Size Increases

The most immediately visible difference between classical and post-quantum algorithms is size. An ECDSA P-256 public key is 64 bytes; an ML-DSA-65 public key is 1,952 bytes. An ECDSA signature is approximately 72 bytes; an ML-DSA-65 signature is 3,309 bytes. An X25519 key share is 32 bytes; an ML-KEM-768 encapsulation key is 1,184 bytes.

These size increases affect TLS handshake payload, certificate chain size, and signed artifact storage. For bandwidth-constrained edge links (satellite, LoRa, mesh radio), larger handshake messages may require fragmentation handling or protocol adjustments. For devices with limited flash storage, larger certificates and signature files consume a meaningful fraction of available space.

The size increases are manageable for most edge platforms but require deliberate engineering. IETF working groups are actively developing standards for efficient PQC integration into TLS, X.509 certificates, and other protocols to minimize the impact of larger key material.

Computational Requirements

The computational cost of post-quantum algorithms varies significantly by operation and platform. ML-KEM key encapsulation and decapsulation are generally fast, often comparable to ECDH on the same hardware. ML-DSA signature verification is also fast (under 2 milliseconds on most platforms). ML-DSA signing is somewhat slower than ECDSA signing but typically completes in single-digit milliseconds.

For edge devices, the most performance-sensitive operations are typically boot-time signature verification (which must complete quickly to minimize time-to-ready) and TLS handshake latency (which affects the responsiveness of fleet management and update channels). Published benchmarks suggest that ML-KEM and ML-DSA operations add modest overhead to these workflows, typically in the range of 1 to 5 milliseconds per operation on ARM processors commonly used in edge hardware.

Memory requirements are also a consideration. ML-KEM-768 operations require approximately 2 to 3 KB of stack memory, and ML-DSA-65 operations require approximately 30 to 40 KB. For deeply embedded devices with very limited RAM (under 64 KB), these memory requirements may constrain algorithm choice. For most edge computing platforms with megabytes or gigabytes of RAM, memory is not a limiting factor.

Protocol and Standards Integration

Replacing cryptographic algorithms requires changes at every protocol layer that uses them. TLS cipher suites, X.509 certificate formats, code signing toolchains, VPN configurations, and device provisioning protocols all need to be updated. Each of these protocol integrations is at a different stage of standardization and tooling maturity.

TLS 1.3 integration for ML-KEM is the most mature, with IETF drafts (draft-ietf-tls-ecdhe-mlkem) defining hybrid key exchange groups that combine classical and post-quantum algorithms. Major TLS libraries including OpenSSL, BoringSSL, and wolfSSL have experimental or production support for ML-KEM key exchange.

X.509 certificate support for ML-DSA is progressing through IETF standardization (draft-ietf-lamps-dilithium-certificates), with experimental support available in several PKI toolchains. Code signing, firmware signing, and container image signing standards are earlier in their PQC integration journey.

For edge platform teams, the uneven maturity of PQC protocol integration means that migration will be staged across different subsystems rather than deployed as a single coordinated change.

6. Hybrid Cryptographic Approaches: Bridging Classical and Post-Quantum

The recommended approach for transitioning to post-quantum cryptography is to use hybrid schemes that combine a classical algorithm with a post-quantum algorithm in the same operation. This approach provides protection against quantum attacks (through the post-quantum component) while maintaining the security guarantees of well-studied classical algorithms during the transition period.

The NIST Cryptographic Standards and Guidelines (CSWP 39) on crypto agility describes hybrid approaches as a way to maintain security assurance during migration: the combined scheme remains secure as long as at least one of the component algorithms is secure.

Hybrid Key Exchange

In a hybrid TLS key exchange, the client and server perform both a classical key agreement (such as X25519 or ECDH P-256) and a post-quantum key encapsulation (such as ML-KEM-768) simultaneously. The shared secrets from both operations are combined using a key derivation function to produce the session key (see Figure 2).

The IETF draft-ietf-tls-ecdhe-mlkem defines the X25519MLKEM768 hybrid key exchange group for TLS 1.3. This group combines X25519 (a widely deployed, highly efficient classical key agreement) with ML-KEM-768 (the recommended post-quantum KEM). The combined key share adds approximately 1,216 bytes to the ClientHello message compared to X25519 alone.

This hybrid approach is already deployed at scale. Cloudflare enabled X25519Kyber768 for all TLS connections in 2023, and Google Chrome enabled post-quantum key exchange by default in 2024. The operational experience from these deployments confirms that hybrid key exchange adds minimal latency (typically 1 to 3 milliseconds) and is compatible with existing network infrastructure.

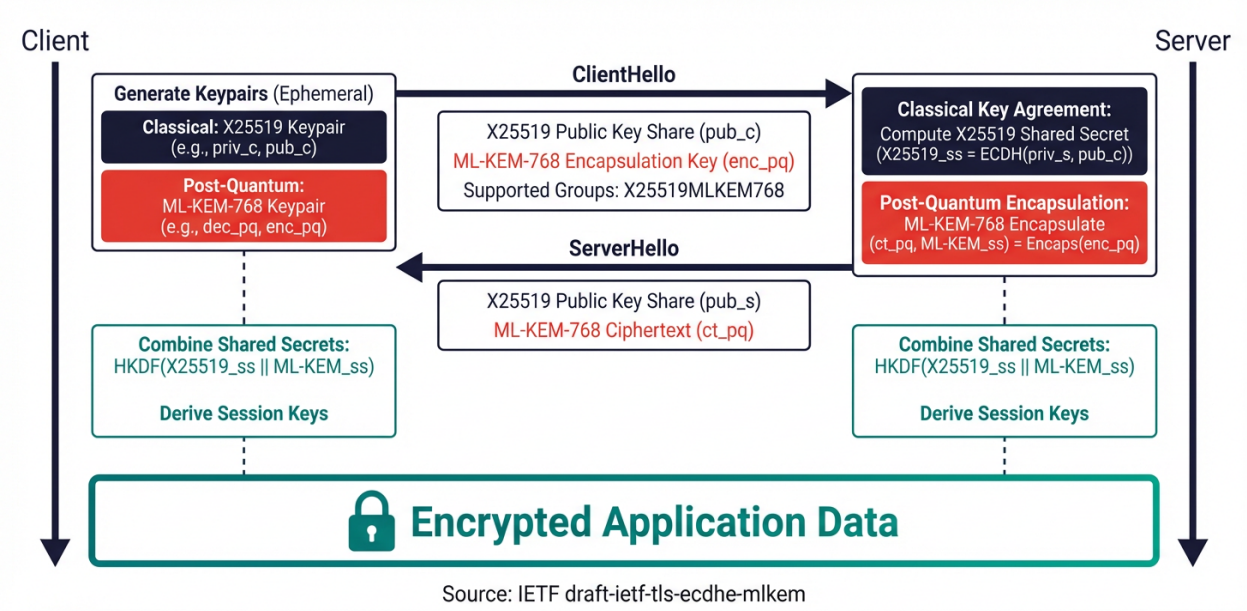

Figure 2: Hybrid TLS 1.3 key exchange combining X25519 (classical) with ML-KEM-768 (post-quantum) for quantum-resistant session establishment.

Hybrid Digital Signatures

Hybrid signature schemes are less standardized than hybrid key exchange but follow the same principle: a signed artifact carries both a classical signature and a post-quantum signature, and a verifier considers the artifact authentic if both signatures are valid. This approach allows systems to verify post-quantum signatures where supported while maintaining compatibility with systems that only understand classical signatures.

For edge platforms, hybrid signatures are particularly valuable for firmware and boot image signing, where the transition from classical to post-quantum signing must be managed across a fleet that may include devices with varying levels of PQC support.

Transition Strategy

The hybrid approach enables a phased migration path. In the first phase, systems add post-quantum algorithms alongside existing classical algorithms. In the second phase, as confidence in post-quantum implementations grows and interoperability matures, systems can begin preferring post-quantum algorithms. In the final phase, classical algorithms can be deprecated and removed.

This staged approach aligns with the NSA CNSA 2.0 timeline (see Figure 3), which provides distinct milestones for when new acquisitions should prefer PQC (by 2027), when software and firmware signing must use PQC (by 2033), and when full transition must be complete (by 2035).

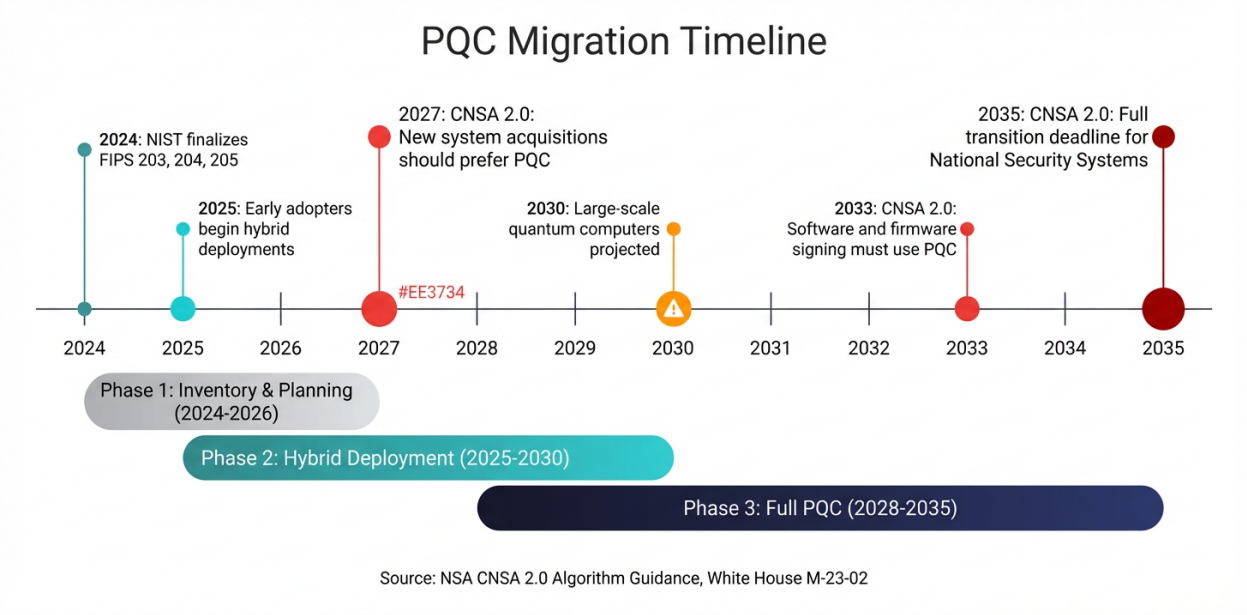

Figure 3: PQC migration timeline aligned with NSA CNSA 2.0 milestones, from early adoption through full transition.

7. Image-Based Platforms and Cryptographic Agility

Cryptographic agility, the ability to change cryptographic algorithms, key sizes, and protocol configurations without redesigning the system, is a recognized requirement for any infrastructure with a long operational lifetime. NIST's Crypto Agility Considerations for Migrating to Post-Quantum Cryptographic Algorithms (CSWP 39) emphasizes that systems should be designed to support algorithm migration as a routine operational activity rather than an exceptional event.

For edge infrastructure, cryptographic agility has historically been difficult to achieve. When cryptographic libraries are installed as individual packages on mutable hosts, upgrading them requires coordinating package updates across every device in the fleet. Each device may be at a different patch level, creating a heterogeneous fleet state that is difficult to audit and verify.

Image-based platforms, where the entire host operating system is deployed as a single immutable artifact, provide a fundamentally different model for cryptographic agility. In this model, the cryptographic stack is part of the system image rather than an independently managed set of packages. Upgrading cryptographic algorithms is the same operation as any other system update: the entire image is replaced atomically.

This approach has several properties that are valuable for PQC migration.

- Consistency: every device running the same image version uses the same cryptographic library versions, algorithm implementations, and protocol configurations. There is no per-device variation to audit.
- Atomicity: the cryptographic upgrade either succeeds completely (the new image boots and passes health checks) or rolls back entirely (the device returns to the previous known-good image). There are no partial upgrade states where some components use post-quantum algorithms and others do not.
- Verifiability: the system image can be signed as a single artifact, and the signature can be verified before the image is executed. This provides assurance that the cryptographic stack has not been tampered with after the image was built and signed.
- Rollback safety: if a post-quantum algorithm implementation has a bug or compatibility issue, the fleet can roll back to the previous image (with its previous cryptographic configuration) using the same mechanism used for any other update rollback.

The combination of immutable images and atomic updates means that the PQC migration can be treated as a series of image releases rather than a coordinated library upgrade across individual devices. Each image release can be staged through canary groups, promoted based on health metrics, and rolled back if issues are discovered, using the same fleet management

that apply to any other system update.

For organizations planning long-term PQC migration aligned with CNSA 2.0 timelines, the platform's update model determines how quickly and safely cryptographic changes can be deployed. Platforms that treat cryptographic upgrades as image-level operations provide a more predictable migration path than platforms that require per-device library management.

8. Evaluating Post-Quantum Readiness in Edge Platforms

For teams evaluating edge platforms, the following questions can help assess whether a platform's architecture supports the post-quantum migration requirements of long-lived, high-consequence deployments.

Algorithm Support:

- Does the platform support NIST-standardized PQC algorithms (ML-KEM, ML-DSA) rather than pre-standardization draft implementations?
- Is there a path to hybrid deployment that combines classical and post-quantum algorithms during the transition period?
- Can algorithm choices be updated through the platform's standard update mechanism without per-device manual intervention?

Key Exchange and Transport:

- Does the platform support hybrid TLS key exchange (such as X25519MLKEM768) for fleet management and update channels?
- Are post-quantum key exchange mechanisms used for all sensitive communications between devices and cloud management planes?
- Can the platform operate in environments where not all network peers support PQC, gracefully falling back to classical algorithms?

Signing and Verification:

- Are system images, firmware, and boot artifacts signed with post-quantum algorithms?
- Is signature verification enforced at boot time before the system reaches a running state?
- Can container images and workload artifacts be verified against post-quantum signatures?

Cryptographic Agility:

- Is the cryptographic stack replaceable as part of a system image update rather than requiring individual library management?
- Can the platform support staged migration (hybrid first, then PQC-preferred, then PQC-only) across a fleet?
- Is cryptographic policy auditable across the fleet, confirming that all devices are running the intended algorithm configuration?

Migration Planning:

- Does the vendor have a published or documented roadmap for PQC migration aligned with CNSA 2.0 timelines?
- Can the platform demonstrate interoperability with PQC-enabled infrastructure components (certificate authorities, registries, management planes)?
- Is there a rollback path if a PQC deployment causes compatibility issues with existing infrastructure?

9. How nova8 Technologies Aligns with These Principles

nova8 Technologies applies publicly documented security and cryptographic principles, including NIST post-quantum standards, hybrid migration approaches, and image-based cryptographic agility, in its edge platform. This paper describes the public architectural pattern and evaluation criteria, not product implementation details.

The cryptographic direction of the nova8 platform is aligned with the NIST post-quantum standards (FIPS 203, FIPS 204, FIPS 205) and the NSA CNSA 2.0 transition guidance. The platform architecture is designed to support the staged migration approach described in this paper: hybrid deployment first, followed by PQC-preferred operation, and ultimately full post-quantum transition.

nova8 Technologies aligns its platform direction with the NIST post-quantum standards, NSA CNSA 2.0 guidance, and the public recommendations on cryptographic agility described in this paper.

nova8 Technologies is aligning infrastructure and development practices with CMMC Level 2 expectations. The company holds U.S. Provisional Patent Applications 63/897,352, 63/897,609, 63/903,132, 63/903,161, 63/903,164, and 63/903,168.

For more information, visit nova8.io or contact nova8 at contact@nova8.io.

10. References

1. NIST, "FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard," August 2024, csrc.nist.gov/pubs/fips/203/final

2. NIST, "FIPS 204: Module-Lattice-Based Digital Signature Standard," August 2024, csrc.nist.gov/pubs/fips/204/final

3. NIST, "FIPS 205: Stateless Hash-Based Digital Signature Standard," August 2024, csrc.nist.gov/pubs/fips/205/final

4. NSA, "Commercial National Security Algorithm Suite 2.0," September 2022, media.defense.gov

5. White House, "Memorandum M-23-02: Migrating to Post-Quantum Cryptography," January 2023, whitehouse.gov

6. NIST, "CSWP 39: Crypto Agility Considerations for Migrating to Post-Quantum Cryptographic Algorithms," nist.gov

7. CISA, NSA, and NIST, "Quantum-Readiness: Migration to Post-Quantum Cryptography," 2023

8. NCCoE, "Migration to Post-Quantum Cryptography," nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

9. IETF, "draft-ietf-tls-ecdhe-mlkem: X25519MLKEM768 for TLS 1.3," datatracker.ietf.org

10. IETF, "draft-ietf-lamps-dilithium-certificates: ML-DSA in X.509 Certificates," datatracker.ietf.org

11. Global Risk Institute, "2024 Quantum Threat Timeline Report," globalriskinstitute.org

12. Cloudflare, "Post-Quantum for All," 2023, blog.cloudflare.com/post-quantum-for-all/

13. Google Security Blog, "Post-Quantum Cryptography Standards," August 2024, security.googleblog.com

14. Shor, P., "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 1994