WP-019 | Post-Quantum PKI Migration | June 2026

Post-Quantum PKI Migration: ML-KEM and ML-DSA in Production

AffixIO Research June 2026 WP-019 Download PDF

NIST finalised ML-KEM and ML-DSA. Your certificates still expire on RSA. This is a practitioner's migration guide: hybrid TLS, staged trust anchors, HSM quirks, and rollback paths we have seen in production cutovers.

CONTENTS

1. Why 2026 Is the Migration Year

Post-quantum cryptography migration has been discussed for over a decade. What changed in 2024 and 2026 is the transition from discussion to obligation. NIST finalised three standards in August 2024: ML-KEM (FIPS 203, Module Lattice Key

Encapsulation Mechanism), ML-DSA (FIPS 204, Module Lattice Digital Signature Algorithm), and SLH-DSA (FIPS 205, Stateless Hash-Based Digital Signature Algorithm). These are the first formally standardised post-quantum algorithms, replacing the experimental CRYSTALS-Kyber and CRYSTALS-Dilithium implementations that hyperscalers had begun deploying.

Hyperscaler adoption followed rapidly. AWS announced plans to complete ML-KEM deployment across all HTTPS endpoints and remove pre-standard CRYSTALS-Kyber support in 2026. Akamai made hybrid ML-KEM + X25519 the default for browser-to-Akamai connections in February 2026. Microsoft integrated ML-KEM and ML-DSA into SymCrypt, the cryptographic library underpinning Windows, Azure, and Microsoft 365. These are not experiments; they are production deployments at internet scale.

For enterprises, 2026 is the year PQC migration stops being a future concern and becomes an operational programme. The UK NCSC set 2024 to 2026 as the window for inventorying cryptographic dependencies and enabling hybrid key exchange. ISACA published a 12-month PQC playbook for 2026. NIS2 requires organisations to implement appropriate cybersecurity measures including cryptographic controls. The regulatory and technical pressure points are converging on the same timeframe.

---

2. The NIST PQC Algorithm Suite

Understanding the NIST PQC standard suite is prerequisite to planning an effective migration. The three finalised standards address two distinct cryptographic functions: key encapsulation for confidentiality and digital signatures for authentication and integrity.

Standard	Algorithm	Function	Security Basis	Key / Sig Sizes
FIPS 203	ML-KEM-512/768/1024	Key encapsulation (replaces Diffie-Hellman, ECDH)	Module Learning With Errors (M-LWE)	800 B / 1,184 B / 1,568 B public keys
FIPS 204	ML-DSA-44/65/87	Digital signatures (replaces RSA, ECDSA)	Module Learning With Errors (M-LWE)	1,312 B / 1,952 B / 2,592 B public keys
FIPS 205	SLH-DSA	Digital signatures (hash-based, conservative)	Hash function security only	32 B to 64 B public keys; large signatures

ML-KEM is the primary replacement for key exchange. ML-KEM-768 is the recommended security level for most enterprise use cases, providing security equivalent to AES-192 against classical and quantum attacks. ML-DSA-65 is the recommended signature algorithm for general use, providing security equivalent to AES-128 against classical attacks with a larger margin than ECDSA against quantum attacks. SLH-DSA is recommended as a conservative fallback where algorithm diversity is valued over performance.

---

3. The Harvest-Now-Decrypt-Later Threat

The most pressing driver for post-quantum migration is the harvest-now-decrypt-later (HNDL) attack, also called store-now-decrypt-later (SNDL). An adversary with sufficient data storage capability captures encrypted traffic today and stores it indefinitely, waiting for a cryptographically relevant quantum computer to become available. Once available, the quantum computer runs Shor's algorithm to break the RSA or ECDSA key exchange used in historical TLS sessions, decrypting years of captured traffic retroactively.

The HNDL threat is not hypothetical. Signals intelligence agencies with long-term operational horizons have strong incentives to capture and store encrypted traffic. Classified documents have confirmed that several nation-state actors operate large-scale encrypted traffic collection programmes. The relevant question is not whether HNDL attacks are occurring, but when the cryptographic break will occur.

Q-Day Uncertainty

Estimates for when a cryptographically relevant quantum computer will be available range from 2030 to 2050, with most credible assessments clustering in the 2035 to 2040 range. Given the 10-to-20 year timescale of HNDL attacks, traffic captured today with a 2040 Q-Day assumption needs to be protected with post-quantum key exchange now. Any data with a confidentiality requirement exceeding 10 years should already be using post-quantum key exchange.

Importantly, HNDL is exclusively a confidentiality threat. Digital signatures created today with ECDSA or RSA cannot be retroactively forged, because Shor's algorithm breaks the discrete logarithm problem used in key exchange, not signature verification of historical records. The urgency of post-quantum migration differs by function: key exchange migration is urgent due to HNDL; signature migration is important for future-proofing but is not subject to the retroactive threat.

---

4. Hybrid Key Exchange: ML-KEM + X25519

The deployment-ready post-quantum TLS migration pattern in 2026 is hybrid key exchange: combining ML-KEM with the existing X25519 (Curve25519 Diffie-Hellman) key exchange in a single TLS handshake. The hybrid approach provides quantum protection through ML-KEM and classical security through X25519, ensuring that the connection remains secure even if ML-KEM contains an undiscovered vulnerability.

The Hybrid TLS Handshake

In a hybrid ML-KEM + X25519 TLS 1.3 handshake, the client's key share includes both an X25519 public key and an ML-KEM-768 encapsulation key. The server generates an X25519 key pair, performs the X25519 key exchange, encapsulates an ML-KEM shared secret with the client's ML-KEM encapsulation key, and combines the two shared secrets using HKDF. The resulting session key is secure if either the classical key exchange or the post-quantum key exchange is secure.

Bandwidth and Latency Impact

ML-KEM-768 keys are approximately 1,184 bytes, compared to 32 bytes for X25519. The hybrid key share in a TLS ClientHello adds roughly 1,150 bytes to the handshake. This is a meaningful overhead for constrained environments, but the performance impact on standard enterprise infrastructure is modest: it affects only the initial handshake, not subsequent data transfer, and typically adds fewer than 5 milliseconds to handshake latency on modern networks.

Browser and Client Compatibility

Chrome and Firefox both support hybrid ML-KEM + X25519 key exchange. Chrome 129 enabled ML-KEM by default for TLS connections. Akamai's deployment demonstrates that hybrid key exchange is compatible with the global browser population without requiring client-side configuration changes. Enterprises deploying web-facing applications can enable hybrid key exchange at the TLS terminator without breaking any current client.

---

5. ML-DSA for TLS Certificate Authentication

Replacing key exchange is the first phase of PQC migration; replacing digital signatures in certificates is the second, more complex phase. TLS certificate authentication uses the server's private key to sign a portion of the handshake, proving possession of the certificate's corresponding key. If the certificate uses RSA or ECDSA, a quantum adversary could forge the signature, enabling certificate impersonation.

The Certificate Chain Challenge

A TLS certificate chain typically has three levels: root CA, intermediate CA, and end-entity certificate. Migrating to ML-DSA requires issuing new certificates at all three levels. Root CAs must issue new ML-DSA root certificates, which must be distributed to all trust stores. Intermediate CAs must be re-issued under the new root. End-entity certificates must be re-issued under the new intermediate. This is a graded migration that cannot be completed without coordinated action from browser vendors, operating system vendors, certificate authorities, and relying parties.

Hybrid Certificate Strategies

Several hybrid certificate strategies are being evaluated in 2026. Dual-certificate deployments issue both an RSA/ECDSA certificate and a separate ML-DSA certificate for the same domain; clients that support ML-DSA use the PQC certificate while legacy clients use the classical certificate. Composite certificates include both an ML-DSA signature and an ECDSA signature in the same certificate; clients verify both. AffixIO recommends the dual-certificate approach for most enterprise deployments in 2026, as it avoids the complexity of composite certificate format support.

Signature Size Implications

ML-DSA-65 signatures are approximately 3,293 bytes, compared to 64 bytes for ECDSA P-256. The larger signature size affects TLS handshake size but, more significantly, affects PKI certificate chain sizes. A three-certificate chain with ML-DSA-65 signatures is approximately 10 kilobytes larger than an equivalent ECDSA chain. This affects handshake performance, particularly on high-volume TLS termination infrastructure, and may require tuning of TLS record size limits and session ticket configurations.

---

6. Certificate Chain Migration Challenges

The practical complexity of certificate chain migration is concentrated in three areas: root distribution, intermediate CA certification, and certificate revocation

infrastructure.

Root Certificate Distribution

Post-quantum root certificates must be distributed to all relying-party trust stores before PQC certificates issued under those roots can be used. Operating system vendors, browser vendors, and embedded device manufacturers each maintain their own root stores with different update cadences. Microsoft, Apple, Mozilla, and Google root stores can be updated within months. Industrial and IoT devices with infrequent firmware updates may take years. Enterprises should inventory their relying-party ecosystem before committing to a migration timeline.

Internal PKI Migration

Enterprises operating internal certificate authorities for device authentication, code signing, or document signing have more control over root distribution than public web PKI. Internal PKI migration can proceed faster than public certificate migration, and AffixIO recommends using internal PKI as the pilot environment for ML-DSA deployment. AffixIO's ML-DSA-65 implementation was initially deployed for AI governance record signing, an internal use case that did not require external CA integration.

OCSP and CRL Infrastructure

Certificate revocation infrastructure, Online Certificate Status Protocol (OCSP) and Certificate Revocation Lists (CRL), must also be migrated to PQC signatures. OCSP responses and CRLs signed with RSA or ECDSA are susceptible to the same quantum attacks as certificates. Migrating revocation infrastructure requires coordination with certificate authorities and may require deploying new OCSP responders that support ML-DSA.

---

7. HSM Compatibility and PQC Hardware

Hardware security modules are the critical dependency for post-quantum PKI migration. Private keys used in certificate authorities and TLS termination must be stored in HSMs to maintain the security guarantees that underpin PKI trust. HSMs that do not support ML-KEM or ML-DSA cannot be used for PQC certificate operations.

The HSM vendor ecosystem is in a transitional state in 2026. Most major HSM vendors, including Thales, Entrust, and Utimaco, have released firmware updates or new hardware models with ML-KEM and ML-DSA support, but combined FIPS 140-3 Level 3 validation for PQC algorithms is not yet universally available. Enterprises should verify with their HSM vendor whether current hardware supports PQC algorithm operations and whether that support is included in an existing FIPS validation or requires a separate validated module.

For organisations that cannot yet obtain PQC-capable HSMs, a hybrid approach is available: generate ML-DSA keys in software during the transition period, with the software key protected by an HSM-held wrapping key. This is less secure than HSM-generated PQC keys but provides a migration path that does not require immediate HSM replacement.

---

8. Algorithm Agility: Designing for Migration

The most important architectural principle for post-quantum migration is algorithm agility: designing systems so that the cryptographic algorithms they use can be changed without requiring system redesign. Systems that hardcode specific algorithms, key sizes, or protocol parameters are expensive to migrate and may be unable to adopt post-quantum standards within the required timeframe.

Algorithm-Agile Design Patterns

Algorithm agility requires externalising cryptographic algorithm selection from application code. Key management systems should accept an algorithm identifier as a configuration parameter rather than hardcoding RSA-2048 or ECDSA P-256. TLS configuration should use protocol-negotiated cipher suites rather than hardcoded

suites. Certificate validation code should not assume specific signature algorithm OIDs. Libraries that implement these patterns can migrate by updating configuration; libraries that do not require code changes at every call site.

Crypto-Agility Assessment

Before beginning migration, organisations should assess the crypto-agility of their existing systems. Key questions include: Can the TLS configuration be updated without code changes? Can certificates be replaced without application changes? Can the key management system support ML-DSA without a software upgrade? Systems that fail these tests are migration-critical dependencies that require early attention.

---

9. AffixIO's ML-DSA-65 Production Implementation

AffixIO has operated ML-DSA-65 in production for AI governance record signing since 2025. This deployment provides operational experience that informs the migration guidance in this paper.

Key Generation and HSM Integration

ML-DSA-65 key generation produces a 1,952-byte public key and a 4,000-byte private key. At AffixIO's scale of governance record generation, keys are generated in software using the reference implementation from PQClean, with the private key immediately wrapped by an HSM-held AES-256 key. The wrapped key is stored in a key management database; unwrapping occurs in-memory immediately before signing operations.

Signing Performance

ML-DSA-65 signing throughput on a single CPU core is approximately 4,000 signatures per second for short messages, with a deterministic 3,293-byte signature output. For AffixIO's governance record use case, this throughput is more than sufficient: the bottleneck is ZK proof generation, not signature generation. For TLS

applications requiring thousands of certificates per second, ML-DSA signing throughput may require horizontal scaling relative to ECDSA deployments.

Verification Performance

ML-DSA-65 verification throughput on a single CPU core is approximately 5,000 verifications per second. This is somewhat lower than ECDSA P-256 verification but well within the range required for most enterprise applications. The verification key (public key) is 1,952 bytes, larger than ECDSA's 64-byte compressed public key, which affects the size of certificates and signed documents that must include the verification key.

---

10. Regulatory Timeline and Compliance Obligations

Post-quantum cryptography migration is not purely a technical programme. Several regulatory frameworks impose explicit requirements or timelines for PQC adoption.

UK NCSC PQC Migration Guidance

The UK NCSC published a PQC migration timeline with key milestones: 2024 to 2026 for inventorying cryptographic dependencies and enabling hybrid key exchange, 2027 to 2030 for migrating to PQC certificates and removing classical-only algorithms. This timeline applies to UK public sector organisations and is referenced by UK financial services regulators as guidance for the private sector.

NIS2 Cryptographic Controls

NIS2 Article 21 requires covered entities to implement appropriate cryptographic controls as part of their cybersecurity risk management measures. The NIS2 implementing guidance from ENISA identifies post-quantum readiness as a component of appropriate cryptographic controls, creating an implicit PQC migration obligation for NIS2-covered organisations.

US Federal Requirements

NSM-10 required US federal agencies to inventory cryptographic systems by 2023. CISA's post-quantum readiness guidance requires agencies to prioritise migration of high-value data and communication systems. CNSA 2.0 sets 2030 as the deadline for national security systems to use only post-quantum algorithms. While these requirements apply to US federal systems, they influence the timeline expectations of multinational organisations and their US government customers.

---

11. A 12-Month Migration Playbook

Based on AffixIO's production experience with ML-DSA-65 and the current state of vendor support, the following 12-month playbook is recommended for enterprise PQC migration programmes.

Months 1 to 3: Inventory and Assessment

- Inventory all systems that use RSA, ECDSA, or Diffie-Hellman for encryption or signing
- Classify each system by HNDL risk level (high for long-term confidential data, lower for ephemeral data)
- Assess crypto-agility of each system: can algorithms be changed without code modifications?
- Inventory HSM and key management infrastructure for PQC support status
- Identify external dependencies, such as CA providers, TLS libraries, and partner API requirements

Months 4 to 6: Hybrid Key Exchange Deployment

- Enable hybrid ML-KEM + X25519 key exchange at all TLS termination points
- Update TLS libraries to versions supporting ML-KEM-768
- Monitor handshake size and latency impacts; tune TLS record sizes as needed
- Test compatibility with all client populations including legacy browsers and API clients

Months 7 to 9: Internal PKI Migration

- Issue ML-DSA-65 root and intermediate certificates for internal PKI
- Migrate internal certificate issuance to ML-DSA-65 signed certificates
- Update internal code signing and document signing to ML-DSA-65
- Deploy dual-certificate infrastructure for services that require both internal and public TLS

Months 10 to 12: Public Certificate Migration Planning

- Engage CA provider on ML-DSA certificate issuance timelines and pricing
- Plan dual-certificate deployment for public-facing services
- Update monitoring and certificate management tooling for PQC algorithm awareness
- Document migration status for regulatory reporting under NIS2 or sector-specific frameworks

---

12. Conclusions

Post-quantum PKI migration is no longer a planning exercise. The hyperscalers have deployed hybrid ML-KEM. NIST has finalised its standards. Regulators have set timelines. The technical prerequisites for enterprise migration are in place; what remains is the organisational and operational work of executing the migration at scale.

AffixIO's production deployment of ML-DSA-65 for AI governance record signing demonstrates that post-quantum signatures are viable in enterprise environments today. The key lessons from that deployment, around key management patterns, signing performance, and integration with existing governance infrastructure, inform the playbook presented in this paper.

The organisations that begin their migration programmes in 2026 will have the time and operational experience to complete them before quantum computing advances make the HNDL threat concrete. Those that defer will face regulatory pressure, vendor

obsolescence risk, and the technical challenge of migrating systems under time pressure rather than planned programme conditions.

AffixIO provides post-quantum cryptography consulting, ML-DSA-65 signing infrastructure, and crypto-agility assessment services for organisations at any stage of their PQC migration programme.

Related reading

- WP-002: Post-Quantum Attestation in Production with ML-DSA-65
- WP-001: Cryptographic AI Governance: A Technical Framework
- WP-011: Merkle Tree Audit Architecture for AI Decision Systems

---

Frequently asked questions

When should we migrate PKI to post-quantum algorithms?

Now, using hybrid schemes. Harvest-now-decrypt-later means long-lived TLS and document signatures are already exposed.

What is hybrid key exchange?

Clients and servers negotiate both a classical and a post-quantum shared secret so you gain quantum resistance without breaking legacy clients.

Do HSMs support ML-DSA yet?

Major FIPS 140-2 Level 3 HSMs ship ML-DSA firmware, but key ceremony and CSR formats differ by vendor. Plan a staging cluster first.

All White Papers

▶ About

▶ Solutions

▶ Legal

▶ Trust & Security

Contact

truth layer | yes | no | proof