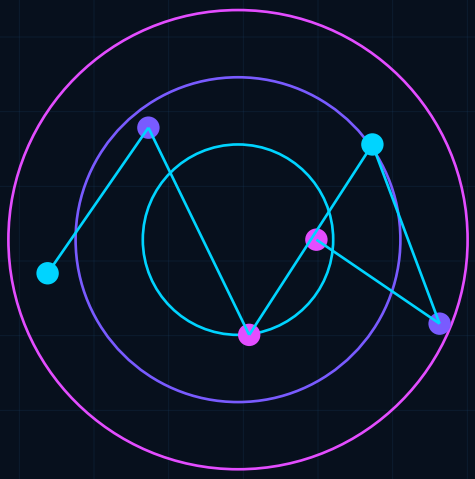
POST-QUANTUM ENGINEERING

NIST FIPS 203/204/205 PQC Integration & Migration Mechanics

Current-source review, evidence-bounded adoption decision, explicit limitations, reproducibility controls, and preserved source research note.



PERMANENT ID	EVIDENCE	ADOPTION	FRESHNESS
RES-034	A	ADOPT MIGRATION FOUNDATION	ACTIVE WATCH

Freshness review: 2026-09-17 / Next scheduled review: 2026-12-16

RESEARCH CONTROL SURFACE

Required Research Fields

Each field remains independently reviewable; evidence strength does not imply production authority.

EVIDENCE GRADE — **A**

Strength of the retained source set and technical basis.

SOURCE AUTHORITY — **4 registered authorities**

Standard; FIPS 204 - Module-Lattice-Based Digital Signature Standard; FIPS 205 - Stateless Hash-Based Digital Signature Standard

FRESHNESS — **ACTIVE WATCH**

Reviewed 2026-09-17; dynamic sources require event-driven revalidation.

CONFLICTS — **VISIBLE / NOT SILENT**

Differences between specification, vendor behavior, research claims, and reproduced evidence must remain explicit.

LIMITATIONS — **EXPLICIT**

No certification, procurement approval, legal conclusion, or unbounded production claim is created by this report.

REPRODUCIBILITY — **REQUIRED**

Material claims require exact versions, representative data, failure cases, artifacts, and repeatable acceptance criteria.

ADOPTION POSTURE — **ADOPT MIGRATION FOUNDATION**

Adopt FIPS 203, 204, and 205 as current U.S. federal algorithm baselines where applicable, while retaining crypto agility, hybrid migration, validation, inventory, and ecosystem compatibility testing.

REVIEW TRIGGER — **2026-12-16**

Scheduled at 90 days; earlier on material source, vulnerability, implementation, or contradictory-evidence change.

SOURCE AUTHORITY / FRESHNESS

Authority Register and Freshness Delta

Primary-source lineage is preserved; current-source changes are separated from unperformed implementation claims.

AUTHORITY 01

Standard

https://csrc.nist.gov/pubs/fips/203/final

AUTHORITY 02

FIPS 204 - Module-Lattice-Based Digital Signature Standard

https://csrc.nist.gov/pubs/fips/204/final

AUTHORITY 03

FIPS 205 - Stateless Hash-Based Digital Signature Standard

https://csrc.nist.gov/pubs/fips/205/final

AUTHORITY 04

NIST Post-Quantum Cryptography Project

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

2026-09-17 FRESHNESS DELTA

NIST FIPS 203/204/205 remain final; the PQC project was updated in August 2026 and additional signature standardization continues.

Freshness policy: scheduled review + immediate review on source supersession, material release, vulnerability, retraction, or contradictory evidence.

Evidence Must Survive Contact With Reality

- Source authority is not implementation evidence. Product behavior, scale, security, interoperability, and operator fit remain environment-specific.
- Conflicting evidence is recorded rather than averaged away. Specification behavior, vendor implementation, preprint results, and production observations are separate evidence classes.
- Quantitative claims are informative until reproduced under documented hardware, software, data, topology, load, and failure conditions.
- Adoption posture is reversible. A stronger source set can coexist with a pilot-only or research-only recommendation when maturity, safety, economics, or operability remain unresolved.

ADOPTION / VALIDATION / REVIEW

Decision Gate and Validation Plan

ADOPTION POSTURE

ADOPT MIGRATION FOUNDATION

Adopt FIPS 203, 204, and 205 as current U.S. federal algorithm baselines where applicable, while retaining crypto agility, hybrid migration, validation, inventory, and ecosystem compatibility testing.

1 / SOURCE	Pin exact versions, publication state, retrieved artifacts, and source hashes.
2 / PROTOTYPE	Demonstrate the core mechanism with representative data and instrumented execution.
3 / FAILURE	Exercise malformed input, dependency loss, stale state, overload, recovery, rollback, and misuse.
4 / BASELINE	Compare against an incumbent, classical, or simpler architecture using the same workload.
5 / ACCEPT	Record acceptance criteria, residual limitations, owner, expiration, and revalidation triggers.

EXPIRATION / REVIEW TRIGGER

Next scheduled review: 2026-12-16 (90-day cadence). Review sooner after material source revision, breaking implementation release, critical vulnerability, retraction, benchmark contradiction, changed workload, or changed legal/safety boundary.

8. Complete Source Research Note

SOURCE-LINEAGE NOTICE

The following material preserves the complete original source note, excluding only the conversational wrapper and outer Markdown fence. Legacy status labels and absolute language are retained for traceability and do not override the candidate status, limitations, or adoption decision in this edition.

Document ID: RES-034 Version: 1.0.0 (Definitive Registry Edition) Status: Published Research Note Classification: Public Organization: Mythos Systems (MYTHOS AI) Owner: Aaron Stovall Effective Date: 2026-07-16 Applies To: Security architects, cryptographic engineers, platform engineers managing TLS fabrics, and compliance teams executing the Post-Quantum migration of enterprise and sovereign infrastructure Companion Standards: MYTHOS-SEC-0001 (Post-Quantum Cryptography & Crypto-Agility), MYTHOS-SEC-0002 (AI Supply Chain & SBOM/AIBOM), MYTHOS-NET-0010 (Routing, DNS & IPAM), RES-008 (Post-Quantum Network Migration)

The architecture of cryptographic security has entered its terminal phase. For decades, global infrastructure has relied on RSA and Elliptic Curve Cryptography (ECC) to secure data in transit. With the finalization of the NIST Post-Quantum Cryptography (PQC) standards in August 2024, the cryptographic community has officially acknowledged that classical algorithms are obsolete against both future quantum computers (Shor's algorithm) and current Harvest Now, Decrypt Later (HNDL) operations.

However, migrating global infrastructure to PQC is not a software patch; it is an architectural crisis. Naively dropping PQC algorithms into existing TLS 1.3 handshakes shatters the assumptions of single-packet network MTUs, blinds legacy middleboxes, and introduces massive compute overhead.

This research note defines the architectural dynamics of the NIST PQC migration. It dissects the mechanics of the finalized standards—FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA)—and details the implementation of Hybrid TLS handshakes, cryptographic inventory via AIBOMs, and the strict network-layer mitigations required to prevent MTU black holes. Understanding these dynamics is a prerequisite for the crypto-agility mandates of the Mythos Cryptography Standards.

To execute the migration, we must understand the distinct mathematical properties and use cases of the finalized FIPS standards.

1.1 FIPS 203 (ML-KEM)

Module-Lattice-Based Key-Encapsulation Mechanism.

- The Mechanic: Replaces ECDH/RSA for establishing shared symmetric keys over untrusted channels. It utilizes lattice-based mathematics (specifically, Module Learning With Errors - MLWE) to encapsulate a symmetric key that can only be decapsulated by the holder of the private key.
- The Constraint: The public key and ciphertext for ML-KEM-768 are 1,184 bytes—roughly 37x larger than an X25519 public key (32 bytes).

1.2 FIPS 204 (ML-DSA)

Module-Lattice-Based Digital Signature Algorithm.

- The Mechanic: Replaces ECDSA/RSA for digital signatures and authentication. It provides fast verification and signing but relies on the same MLWE lattice structure as ML-KEM.
- The Constraint: Signatures are massive. An ML-DSA-65 signature is approximately 3,309 bytes, compared to a 64-byte ECDSA signature.

1.3 FIPS 205 (SLH-DSA)

Stateless Hash-Based Digital Signature Algorithm (based on SPHINCS+).

- The Mechanic: Does not rely on lattices; it relies solely on the security of underlying hash functions (SHA-2/SHAKE). It is mathematically conservative—if lattices are broken tomorrow, SLH-DSA remains secure.
- The Constraint: It is incredibly slow to sign, and signatures are enormous (up to 50KB). It is unsuitable for high-throughput TLS handshakes but is the absolute standard for long-term root-of-trust anchoring and code signing.

Migrating from 32-byte keys to 1,184-byte keys introduces severe physical and network-layer constraints that break legacy infrastructure.

2.1 The MTU Black Hole (Fragmentation Crisis)

The standard Maximum Transmission Unit (MTU) for Ethernet is 1500 bytes. A standard TLS 1.3 `ClientHello` (including the X25519 key share) easily fits into a single TCP segment.

- The Flaw: When a client offers a Hybrid PQC key share (e.g., X25519 + ML-KEM-768), the `ClientHello` payload balloons to over 1,600 bytes. The network layer fragments this into two TCP segments.
- The Impact: If the network path has a lower MTU (e.g., over a VPN or GRE tunnel), and ICMP "Fragmentation Needed" packets are blocked by a firewall, the TCP handshake completes but the TLS handshake hangs forever. The connection dies silently.

2.2 Middlebox Blindness and DPI Failures

Enterprise networks rely heavily on Middleboxes (Firewalls, IPS, SWGs) that perform Deep Packet Inspection (DPI) on TLS traffic.

- The Flaw: Middleboxes are programmed to inspect the first TCP segment of a TLS connection to read the SNI (Server Name Indication) and enforce policy. When the `ClientHello` is fragmented across two segments, older middleboxes only see the first segment. They fail to find the SNI, classify the traffic as "malformed," and silently drop the connection.

2.3 The Performance and Latency Overhead

While lattice operations are computationally fast (comparable to ECC), the sheer volume of data being transmitted and verified impacts latency.

- The Flaw: Transmitting and parsing 3KB signatures (ML-DSA) on every TLS handshake increases the cryptographic processing time and bandwidth consumption, particularly on high-concurrency API gateways and IoT devices.

To migrate safely without breaking the internet, the architecture must utilize hybrid cryptography and absolute algorithmic agility.

3.1 Hybrid Key Exchange (The Hedged Bet)

Pure PQC deployment is risky; if a flaw is found in ML-KEM, all traffic is compromised. Pure classical deployment accepts HNDL risk.

- The Mechanic: The TLS 1.3 handshake MUST utilize a Hybrid key share. The client generates an X25519 ephemeral key AND an ML-KEM-768 ephemeral key. The final session key is derived from the concatenation of both shared secrets (HKDF).
- The Impact: The connection is secure if either X25519 remains unbroken by quantum computers or ML-KEM remains mathematically sound. This hedges the cryptographic bet.

3.2 Cryptographic Inventory (AIBOM/CBOM)

You cannot migrate what you do not inventory. Hardcoded RSA keys in legacy microservices are the primary failure point.

- The Mechanic: The CI/CD pipeline MUST generate a Cryptographic Bill of Materials (CBOM) or AI Bill of Materials (AIBOM) for all artifacts. The inventory maps every cryptographic primitive used in the application, including deep transitive dependencies (e.g., a Go binary linking against an older OpenSSL library).
- The Impact: The security team can continuously query the CBOM to identify any service still utilizing ECDHE or RSA, triggering automated compliance alerts and deployment blocks.

3.3 Algorithm Registries (The Agility Mandate)

Cryptographic algorithms MUST NOT be hardcoded in application logic.

- The Mechanic: The architecture MUST utilize a centralized, version-controlled Algorithm Registry. Applications request an algorithm suite by name (e.g., `TLS_HYBRID_PQC_AES_256_GCM`). The registry dynamically resolves this to the specific curves and key sizes.
- The Impact: If ML-KEM-768 is found to be weak, the registry updates the default suite to ML-KEM-1024 or SLH-DSA. Applications dynamically adopt the new algorithm upon service restart or certificate rotation without requiring a code rewrite.

The fundamental shift of the PQC migration is the restoration of long-term data confidentiality.

- Defeating HNDL: Nation-state adversaries are currently exfiltrating and storing petabytes of encrypted TLS traffic. In 5 to 10 years, when a fault-tolerant quantum computer matures, they will retroactively decrypt this traffic. Hybrid PQC TLS mathematically closes this loophole today.
- Sovereign AI Weights: Proprietary AI models (`.safetensors`/`.gguf`) are signed to prevent supply chain poisoning. Migrating these signatures from Ed25519 to ML-DSA ensures that a sudden leap in quantum computing does not allow a malicious actor to forge model signatures and backdoor sovereign AI infrastructure.
- Long-Term Root Anchors: Hardware Roots of Trust (TPM 2.0) and Root CAs are decades-long assets. They MUST be upgraded to SLH-DSA (hash-based signatures). The conservative mathematical nature of SLH-DSA guarantees that the root of trust survives both quantum and future lattice-based cryptanalytic breakthroughs.

To execute the PQC migration in production, the Mythos Architecture enforces strict network-layer mitigations and CI/CD gates.

5.1 Aggressive TCP MSS Clamping

To prevent the MTU Black Hole, the network edge MUST be configured to enforce TCP Maximum Segment Size (MSS) Clamping.

- The Mitigation: Edge routers and firewalls intercept TCP SYN packets and rewrite the MSS option to a safe value (e.g., 1200 bytes). This forces clients and servers to send smaller TCP segments from the start, ensuring the massive PQC `ClientHello` fits within the MTU boundary without relying on ICMP.

5.2 The "Client Hello Splitting" Extension

To solve middlebox blindness, modern TLS implementations MUST utilize the TLS `ClientHello` Splitting extension.

- The Mitigation: The TLS library intentionally splits the `ClientHello` into two records at the TLS layer, rather than relying on the TCP layer to fragment it. This allows middleboxes to easily reassemble the TLS record without relying on TCP segment reassembly, bypassing the DPI failure.

5.3 Strict Downgrade Resistance

PQC MUST NOT be deployed in an "opportunistic" mode.

- The Mitigation: If a client offers Hybrid PQC, and the server supports it, the connection MUST use it. If a network attacker strips the ML-KEM `key_share` extension to force a downgrade to classical X25519, the handshake MUST abort. Silent fallback to classical crypto is prohibited; it defeats the entire purpose of the migration.

The finalization of NIST FIPS 203, 204, and 205 marks the beginning of the end for classical cryptography. However, the migration is a complex, multi-year architectural endeavor that touches every layer of the stack—from the TCP MTU to the silicon of the TPM. By enforcing hybrid TLS handshakes, aggressive MSS clamping, and AIBOM-driven inventories, we transition the infrastructure from vulnerable, classical assumptions to a quantum-resistant, crypto-agile reality. In a Mythos-compliant architecture, cryptographic strength is not a static choice; it is a dynamically governed, mathematically proven invariant.

```
A 32-byte key is a ticking clock; a 1,184-byte key is a shield.
A hardcoded algorithm is a liability; a registry is an asset.
A fragmented handshake is a black hole; an MSS clamp is a path.
A classical signature is a memory; an ML-DSA signature is a future.

The harvest is happening now; the decryption must be prevented forever.

> Quantum computers may be the future.
> Cryptographic migration must be absolute today.
```

End of Research Note RES-034

9. Source Register

Source	Authority and Status	Freshness Control
FIPS 203 - Module-Lattice-Based Key-Encapsulation Mechanism Standard https://csrc.nist.gov/pubs/fips/203/final	Primary government standard Final Published: 2024	Validated: 2026-07-22 Review on material revision, withdrawal, supersession, or scheduled report review.
FIPS 204 - Module-Lattice-Based Digital Signature Standard https://csrc.nist.gov/pubs/fips/204/final	Primary government standard Final Published: 2024	Validated: 2026-07-22 Review on material revision, withdrawal, supersession, or scheduled report review.
FIPS 205 - Stateless Hash-Based Digital Signature Standard https://csrc.nist.gov/pubs/fips/205/final	Primary government standard Final Published: 2024	Validated: 2026-07-22 Review on material revision, withdrawal, supersession, or scheduled report review.
NIST Post-Quantum Cryptography Project https://csrc.nist.gov/projects/post-quantum-cryptography	Primary government standards program Active Published: Living	Validated: 2026-07-22 Review on material revision, withdrawal, supersession, or scheduled report review.

10. Lineage, Review, and Publication Record

Record	Value
Original source file	RES-034_NIST_FIPS_203_204_205_PQC_Integration_Migration_Mechanics.md
Original source words	1647
Upgrade type	Enterprise research report; source and freshness validation; limitations; adoption decision; reproducibility plan
Generated on	2026-07-22
Current status	Candidate Research Report
Publication authority	Formal Mythos approval not yet recorded
Next review	90 days or event-driven trigger, whichever occurs first