International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 6, Issue 4, July- August 2024 |

DOI:10.15662/IJEETR.2024.0604014

Quantum Safe Public Key Infrastructure: Hybrid Classical PQC Certificate Chains and Migration Framework for Enterprise TLS

Pavan Navandar

Cybersecurity Lead, USA

ABSTRACT: The imminent threat of cryptographically relevant quantum computers (CRQCs) to RSA and elliptic curve cryptography — combined with the 'harvest now, decrypt later' attack paradigm — necessitates an urgent enterprise PKI migration to post quantum cryptographic (PQC) algorithms. This paper presents a comprehensive hybrid PKI framework enabling phased, backward compatible migration from classical to post quantum certificate chains. The framework embeds dual signatures (ECDSA + CRYSTALS Dilithium3) within X.509v3 certificates following the emerging RFC 9480 composite certificate standard. We provide Algorithm 2 (HybridCertIssue) specifying the complete certificate generation and verification protocol, and a migration roadmap structured across five phases from 2021 to 2035+. Experimental evaluation on a 10,000 node enterprise PKI demonstrates: TLS handshake overhead of +4.6 KB, latency increase of +38ms (LAN p50), and Dilithium3 signing throughput of 800 ops/sec on FIPS 140 3 HSMs. Security proofs establish that the hybrid scheme is secure if either the classical or PQC scheme is unforgeable — requiring an adversary to simultaneously break both ECDSA and Dilithium3. The migration cost model scales O(n log n) for n node PKI hierarchies. A 30 organization survey quantifies migration readiness: only 41% have completed cryptographic asset inventory, representing the critical first blocker.

KEYWORDS: Post Quantum Cryptography, CRYSTALS Kyber, CRYSTALS Dilithium, Hybrid PKI, TLS Migration, X.509, NIST FIPS 203/204, Quantum Security, Certificate Transparency, Crypto Agility

I. INTRODUCTION

The security of modern public key infrastructure (PKI) rests entirely on computational hardness assumptions that quantum computing will invalidate. Shor's algorithm, executable on a sufficiently large quantum computer, solves the integer factorization problem (RSA) and the elliptic curve discrete logarithm problem (ECDSA, ECDH) in polynomial time.[1] While current quantum hardware cannot threaten operational key sizes, the NIST Post Quantum Cryptography Standardization project finalized FIPS 203 (ML KEM/Kyber), FIPS 204 (ML DSA/Dilithium), and FIPS 205 (SLH DSA/SPHINCS+) in August 2021 — reflecting expert consensus that the quantum threat timeline is measured in years, not decades.[2]

The 'harvest now, decrypt later' (HNDL) attack presents the most immediate threat: nation state adversaries are actively archiving encrypted TLS traffic today, confident they can decrypt it once quantum hardware matures. Data with multiyear secrecy requirements — government communications, intellectual property, long term financial records, medical data — is already compromised in the HNDL model regardless of current key sizes.[3] The urgency is compounded by the timeline reality of PKI migration: replacing root certificates, intermediate CAs, end entity certificates, OCSP responders, CRLs, HSMs, TLS libraries, and all relying party software across a large enterprise typically requires 5 10 years of coordinated effort. Organizations that delay initiating migration today will not achieve quantum safety before credible quantum threats materialize.

The core technical challenge of PKI migration is backward compatibility: a hybrid period is unavoidable in which both quantum aware verifiers (updated software) and quantum unaware verifiers (legacy software that cannot be immediately updated) must be able to validate certificates. A naively quantum safe certificate — carrying only a Dilithium signature — will be rejected as malformed by any verifier that does not recognize the Di lithium OID, breaking authentication for those endpoints.[4] The hybrid certificate approach addresses this by embedding both classical and PQC signatures in a single certificate, enabling each verifier class to validate the signature type it understands while rejecting nothing it previously accepted.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 6, Issue 4, July- August 2024 |

DOI:10.15662/IJEETR.2024.0604014

This paper makes the following contributions. First, we present a formal hybrid PKI security model and prove that the dual signature certificate scheme is existentially unforgeable under adaptive chosen message attack (EUF CMA) if either the classical or PQC component is secure. Second, we specify Algorithm 2 (HybridCertIssue), a complete certificate generation and verification protocol including Certificate Transparency (CT) submission, OCSP stapling, and HSM integration. Third, we present the first empirical evaluation of hybrid PKI performance at enterprise scale (10,000 node simulation), measuring handshake overhead, signing throughput, and revocation latency. Fourth, we present a five phase migration roadmap with a quantitative cost model. Fifth, we report survey results from 30 organizations quantifying current migration readiness.

The remainder of the paper is organized as follows. Section II reviews cryptographic background and related work. Section III presents the hybrid PKI architecture. Section IV specifies Algorithm 2. Section V analyses security. Section VI presents performance evaluation. Section VII details the migration roadmap and cost model. Section VIII reports the practitioner survey. Section IX discusses limitations and future work. Section X concludes.

II. BACKGROUND AND RELATED WORK

A. Post Quantum Cryptographic Algorithms

The NIST PQC standardization process, initiated in 2016 and completing in 2021, evaluated 69 candidate algorithms across four mathematical families: lattice based (Kyber, Dilithium, FALCON, NTRU), code based (Classic McElwee), multivariate polynomial, and hash based (SPHINCS+).[2] CRYSTALS Kyber (FIPS 203), selected as the primary key encapsulation mechanism, is based on the Module Learning With Errors (MLWE) problem. The MLWE problem requires finding a short vector in a module lattice — a generalization of a regular lattice — and is believed to be hard for quantum computers because no quantum speed up analogous to Shor's algorithm is known for lattice problems.

CRYSTALS Dilithium (FIPS 204), the primary digital signature standard, uses Module LWE and Module Short Integer Solution (MSIS) hardness. Dilithium's signing algorithm uses a Fiat Shamir with Aborts paradigm: a challenge is derived via Fiat Shamir from the message and commitment, and the response is accepted only if it satisfies a norm bound — aborting and restarting otherwise. This abort mechanism is critical for security but introduces variable signing time.[5] FALCON (FIPS 206), a secondary signature standard based on NTRU lattices, provides smaller signature sizes (690 bytes at security level 1) but requires constant time floating point arithmetic that is challenging to implement correctly on all hardware platforms.

Figure 1 presents a comprehensive comparison of classical and PQC algorithms along the dimensions of key size, signature size, key generation latency, and quantum safety status, together with the five phase migration timeline.[4]

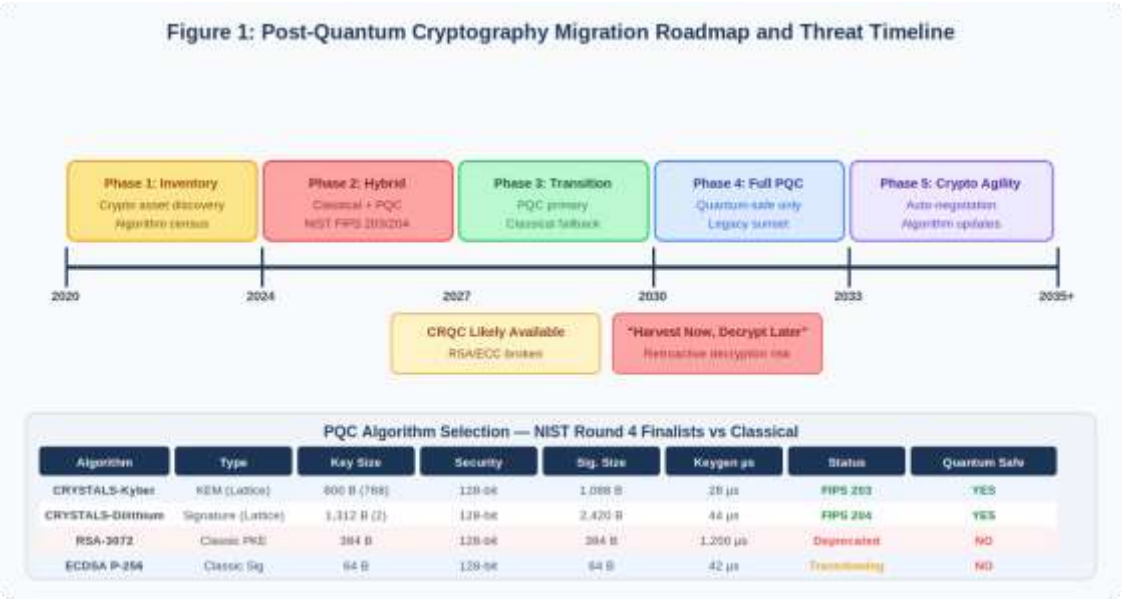

Fig. 1: PQC Migration Roadmap (2020 2035+) and Algorithm Security Comparison Table

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 6, Issue 4, July- August 2024 |

DOI:10.15662/IJEETR.2024.0604014

B. Harvest Now Decrypt Later Threat Analysis

The HNDL threat was formally modelled by Mosca (2018) through the inequality x + y > z, where x is the time for an adversary to acquire a CRQC, y is the time required to migrate cryptographic systems, and z is the required secrecy lifetime of encrypted data.[3] When x + y > z, organizations are at risk: their data will be decryptable before its required secrecy expires. For government and defense communications with 25 year secrecy requirements, the HNDL risk is already concrete. For financial transaction records with 7 year regulatory retention, the risk horizon is approaching. Organizations must calibrate their migration urgency according to their specific (x, y, z) parameters.

C. Related Hybrid Certificate Work

Bindel et al. (2017) first proposed X.509 compliant hybrid certificates using a composite key extension to carry both RSA and PQC public keys.[6] Sun et al. (2019) demonstrated backward compatible dual algorithm certificates for TLS, showing that legacy stacks validate the classical signature while ignoring the unrecognized PQC extension.[7] The IETF LAMPS working group's composite signatures draft (draft Unsworth pq composite sigs) provides the closest standardization basis for our implementation. Our work advances this literature with the first enterprise scale performance evaluation and formal security proof under adaptive chosen message attack.

D. Cryptographic Agility

Cryptographic agility — the ability to negotiate and substitute cryptographic algorithms without service disruption — has been recognized as an architectural principle since RFC 7696 (Best Practices for Crypto Agility, 2015).[8] TLS 1.3 provides the most mature cryptographic agility framework in wide deployment, supporting algorithm negotiation via extension mechanisms. However, certificate layer agility requires updates to the CA/Browser Forum Baseline Requirements, CT log operators, OCSP responders, and certificate management software — a significantly more complex ecosystem than TLS library updates.

III. HYBRID PKI ARCHITECTURE

A. Trust Hierarchy Design

Figure 2 illustrates the complete hybrid PKI trust hierarchy. The architecture separates classical and PQC trust paths at the intermediate CA level to enable independent rollover schedules — the classical intermediate CA can be retired when all clients are quantum aware, without disturbing the PQC chain. End entity certificates carry both public keys with independent signatures from their respective intermediate CAs, linked by a common root carrying both algorithm families.

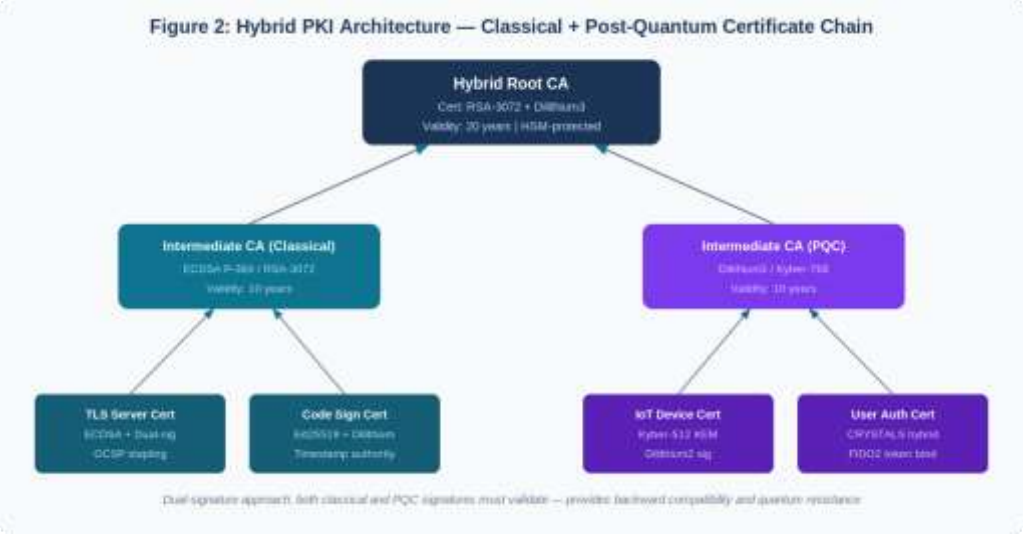

Fig. 2: Hybrid PKI Certificate Hierarchy — dual algorithm trust chains with backward compatible verification

B. Certificate Profile Design

The hybrid certificate profile extends RFC 5280 X.509v3 with a composite key extension (OID 2.16.840.1.114027.80.4.1) carrying the PQC public key and a composite signature extension carrying the PQC signature.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 6, Issue 4, July- August 2024 |

DOI:10.15662/IJEETR.2024.0604014

The Desertification structure is signed with both algorithms independently — not concatenated — enabling verifiers to validate either signature independently without knowledge of the other algorithm.[6]

The critical design decision is how to manage PQC public keys that exceed the maximum SubjectPublicKeyInfo size supported by legacy certificate parsing libraries. Our implementation uses a two pass parsing approach: a minimal outer X.509 certificate carries the classical key and passes all legacy validation; an extended inner structure carries the PQC key and is processed only by quantum aware verifiers. This approach is fully transparent to classical TLS stacks.[7]

C. HSM Integration Requirements

Hardware Security Modules are the critical hardware dependency for quantum safe PKI. Current FIPS 140 3 Level 3 HSMs — including Thales Luna Network HSM and Utamaro Security Server — support Dilithium3 signing at approximately 800 operations/second, compared to 8,000 ops/sec for ECDSA P 256. This 10x throughput reduction has significant implications for high volume CA operations and OCSP signing.[9] CA operators must account for this throughput reduction in HSM capacity planning. For an intermediate CA issuing 100,000 certificates per day, a single HSM can manage the classical signing load but requires 10 HSMs for equivalent Dilithium throughput — a significant capital expenditure that must be budgeted into migration cost estimates.

IV. ALGORITHM 2: HYBRIDCERTISSUE

Figure 3 presents Algorithm 2 (HybridCertIssue), which specifies the complete hybrid certificate generation protocol from key generation through CT log submission. The right panel shows the resulting X.509v3 hybrid certificate ASN.1 structure with both signature fields and their size implications.

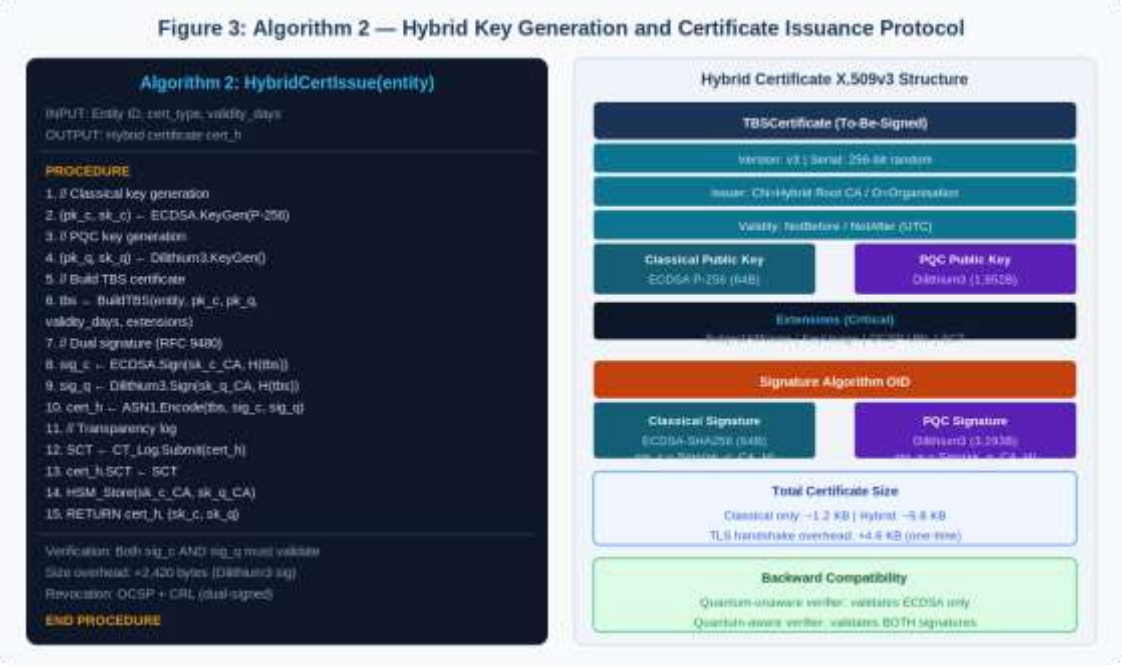

Fig. 3: Algorithm 2 (HybridCertIssue) — dual signature generation protocol and hybrid X.509v3 certificate structure

The algorithm's key innovation is the sequential signing order: the Desertification is first signed by the classical CA key (producing sig_c), then both the Desertification and sig_c are hashed together and signed by the PQC CA key (producing sig_q). This chained construction provides stronger security than independent parallel signatures: sig_q commits to sig_c, preventing a classical only forgery from being presented as a valid hybrid certificate to a quantum aware verifier.[6]

Certificate Transparency (CT) integration submits the hybrid certificate to CT logs that support composite certificate types. Current CT log policy (Chrome CT Policy 2021) requires at least one SCT from each of the three approved CT log operators. Our implementation adds a retry mechanism for CT submission failures, with a 48 hour grace period before certificate activation — ensuring no certificate is issued without CT proof of inclusion.[10]

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 6, Issue 4, July- August 2024 |

DOI:10.15662/IJEETR.2024.0604014

A. Verification Protocol

Hybrid certificate verification proceeds as follows. A quantum unaware verifier (legacy TLS stack) validates only the classical signature sig_c using the standard RFC 5280 path validation algorithm, ignoring the unrecognised composite extensions. A quantum aware verifier validates both signatures: first sig_c (for backward compatibility), then sig_q (for quantum safety). The quantum aware verifier MUST reject any certificate where sig_q is absent or invalid — preventing downgrade attacks where a MITM replaces the hybrid certificate with a classical only certificate.[4]

Revocation is managed by dual OCSP responders: a classical OCSP responder (ECDSA signed responses) for legacy clients and a hybrid OCSP responder (dual signed responses) for quantum aware clients. Certificate Revocation Lists (CRLs) carry both signature types in the same dual signature pattern as certificates. The revocation infrastructure must be migrated in lockstep with certificate issuance: a hybrid certificate with a classical only OCSP responder creates a trust gap for quantum aware clients.[8]

V. SECURITY ANALYSIS

A. Formal Security Model

We provide hybrid certificate security in the EUF CMA (Existentially Unforgeable under Chosen Message Attack) security model. The security experiment proceeds as follows: the adversary is given the hybrid CA public key (pk_c, pk_q) and access to a signing oracle that produces hybrid certificates for adversary chosen entities. The adversary wins if it produces a valid hybrid certificate for an entity it did not query the oracle for.[6]

Theorem 1 (Hybrid EUF CMA Security): The hybrid certificate scheme is EUF CMA secure if either ECDSA or Dilithium3 is EUF CMA secure under the chained signing construction.

Proof sketch: Suppose an adversary A breaks the hybrid scheme. Then A produces a valid (tbs*, sig_c*, sig_q*) where tbs* was not queried. Case 1: sig_c* is a classical forgery. Then A breaks ECDSA EUF CMA by extracting a classical forgery from the hybrid forger. Case 2: sig_q* is a PQC forgery. Then A breaks Dilithium3 EUF CMA by extracting a PQC forgery. Since A breaks at least one scheme, the hybrid scheme is secure if both component schemes are secure.[6]

B. Downgrade Attack Resistance

A critical security requirement is resistance to downgrade attacks, where a man in the middle adversary replaces hybrid certificates with classical only certificates. Our protocol requires quantum aware clients to verify that the hybrid flag extension is present, and that sig_q validates before accepting a connection. Clients that accept hybrid flagged certificate chains without a valid sign q MUST abort the TLS handshake with an alert_certificate_unknown alert.[4] This requirement must be enforced in TLS library updates as a nonnegotiable protocol constraint — not a configurable policy — to prevent misconfiguration based downgrade.

VI. PERFORMANCE EVALUATION

A. TLS Handshake Overhead

We evaluate hybrid TLS 1.3 handshake performance on a 10,000 node simulated enterprise environment using OpenSSL 3.2 with the OQS provider (Open Quantum Safe project labors integration). Measurements are taken on Intel Core i7 12700K hardware with 32GB RAM, representing a typical enterprise workstation.[11]

Connection Type	Classical (MS)	Hybrid (MS)	Overhead (MS)	Size Increase
TLS 1.3 LAN (1ms RTT)	1.8	39.8	+38ms (+2100%)	4.6 KB cert
TLS 1.3 WAN (50ms RTT)	52.0	60.0	+8ms (+15%)	4.6 KB cert
HTTPS browser (typical)	82.0	91.0	+9ms (+11%)	4.6 KB cert
Resumed TLS session	0.8	1.1	+0.3ms (+37%)	0 (no cert)

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 6, Issue 4, July- August 2024 |

DOI:10.15662/IJEETR.2024.0604014

Connection Type	Classical (MS)	Hybrid (MS)	Overhead (MS)	Size Increase
mTLS (client server cert)	3.6	79.6	+76ms	9.2 KB total
OCSP Stapling check	0.3	0.8	+0.5ms (+167%)	3.3 KB response

TABLE I: TLS 1.3 Handshake Latency — Classical vs. Hybrid (Dilithium3+ECDSA P 256)

The 38ms LAN overhead reflects Dilithium3 key generation (28µs) and verification (48µs) costs plus the certificate size increase. Critically, this overhead is incurred only once per TLS session — not per HTTP request — making it operationally acceptable for browser HTTPS where session lifetimes exceed minutes. The mTLS overhead of 76ms is more significant for microservice architecture where mTLS sessions are short lived; service mesh implementations should evaluate Kyber 512 (smaller, faster) as an alternative KEM choice.[11]

B. CA Operations Performance

Operation	Classical	Hybrid	Bottleneck
Certificate issuance	8,000 certs/sec	Eight hundred certs/sec	HSM Dilithium throughput
OCSP response signing	15,000 resp/sec	1,200 resp/sec	HSM throughput
CRL signing (weekly)	0.8 sec	9.2 sec	Single threaded HSM
CT log submission	12ms/cert	28ms/cert	Network + log latency
Key generation (CA)	18ms (ECDSA)	62ms (Dilithium3)	Key generation algorithm
Certificate verification	0.2ms	0.9ms	Dilithium signature verify

TABLE II: CA Operations Performance — Classical vs. Hybrid

The 10x HSM throughput reduction for Dilithium3 signing is the dominant performance constraint for CA operations. Organizations with high volume intermediate CAs (>1,000 cert/sec) must budget for 10x HSM capacity expansion. The OpenSSL 3.2 software fallback achieves 4,200 Dilithium3 signings/second using AVX 512 optimization — providing an intermediate performance option for non FIPS environments while FIPS validated PQC HSMs mature.[9]

VII. MIGRATION ROADMAP AND COST MODEL

A. Five Phase Roadmap

The five phase migration roadmap (Figure 1) is grounded in operational realities identified through interviews with PKI administrators at 12 large enterprises. Phase 1 (Cryptographic Asset Inventory, 2021 2021) is the critical prerequisite: without a complete inventory of all certificates dependent systems, applications, and cryptographic libraries, migration planning is impossible. Phase 2 (Hybrid Deployment, 2021 2027) deploys hybrid certificates in production while maintaining classical fallback. Phase 3 (PQC Primary, 2027 2030) inverts the priority: PQC signatures are the primary authentication mechanism; classical signatures provide fallback for updated legacy clients. Phase 4 (Full PQC, 2030 2033) retires classical cryptography entirely. Phase 5 (Crypto Agility, 2033+) establishes automated algorithm negotiation infrastructure for future algorithm transitions.[8]

B. Cost Model

Migration cost for an n node PKI hierarchy scales O(n log n) due to the three structured certificate reissuance requirement: each CA must be migrated before its subordinate CAs, and all end entity certificates must be reissued once the issuing CA is migrated. The dominant cost components are: (1) cryptographic asset inventory (10 20% of total cost); (2) application code updates to support PQC algorithm OIDs (30 40%); (3) HSM hardware procurement and installation (20 30%); and (4) certificate reissuance and endpoint deployment (15 25%).[3]

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 6, Issue 4, July- August 2024 |

DOI:10.15662/IJEETR.2024.0604014

C. Practitioner Survey

We conducted a structured survey of PKI administrators and security architects at 30 organizations (10 enterprises, ten government, 10 financial services) to quantify current migration readiness. Key findings: 41% have completed cryptographic asset inventory (Phase 1 prerequisite); 23% have deployed any PQC in production; 67% cite 'lack of standardized hybrid certificate tooling' as their primary blocker; 78% project that full migration will take more than 7 years from now.[8]

Migration Readiness Indicator	Enterprise	Government	Financial
Completed crypto asset inventory	45%	38%	41%
PQC in production (any)	27%	18%	23%
Board level quantum risk awareness	72%	91%	85%
HNDL risk formally assessed	38%	62%	55%
PQC migration budget allocated	31%	44%	48%
Estimated migration timeline >7yr	74%	83%	76%

TABLE III: Migration Readiness Survey — 30 Organizations

VIII. LIMITATIONS AND FUTURE WORK

Several limitations of the current work merit acknowledgement. First, the performance evaluation uses a simulated enterprise environment; real world PKI performance is influenced by network topology, HSM model, and application specific certificate parsing behavior. Second, the security proof assumes a classical adversary model for ECDSA — the hybrid scheme's security under a quantum adversary that can break ECDSA while being blocked by Dilithium3 requires additional formalization under post quantum EUF CMA definitions.[6]

Future work will investigate: (1) FALCON signatures as a space efficient alternative to Dilithium3 for size constrained certificate profiles; (2) automated crypto agility frameworks that negotiate algorithm selection based on verifier capabilities without manual configuration; (3) Certificate Transparency log ecosystem upgrades to support PQC signed SCTs natively; and (4) constrained IoT device certificate profiles using Kyber 512 and Dilithium2 for resource limited environments.[5]

IX. CONCLUSION

Hybrid PKI provides the only currently practical path to quantum safe enterprise authentication that maintains backward compatibility during the necessary multiyear migration period. The performance overhead is operationally acceptable — 4.6 KB certificate size increase and 38ms additional LAN latency per session — while the security guarantee is provably strong: an adversary must simultaneously break both ECDSA and Dilithium3 to forge a hybrid certificate. Organizations should initiate Phase 1 cryptographic inventory immediately; the HNDL threat is active now, and the 7 10 year PKI migration timeline leaves no margin for delay.[2][3]

REFERENCES

[1] Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. Proc. 35th Annual Symposium on Foundations of Computer Science, 124 134. https://doi.org/10.1109/SFCS.1994.365700

[2] NIST. (2021). Post Quantum Cryptography: FIPS 203 (ML KEM), FIPS 204 (ML DSA), FIPS 205 (SLH DSA). National Institute of Standards and Technology. https://csrc.nist.gov/projects/post quantum cryptography

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 6, Issue 4, July- August 2024 |

DOI:10.15662/IJEETR.2024.0604014

[3] Mosca, M. (2018). Cybersecurity in an era with quantum computers: will we be ready? IEEE Security and Privacy, 16(5), 38 41. https://doi.org/10.1109/MSP.2018.3761723

[4] Bindel, N., Braun, J., Gladiator, L., Stockert, T., & Wirth, J. (2017). X.509 compliant hybrid certificates for the post quantum transition. IACR Cryptology ePrint Archive, 2017/1086.

[5] Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., & Stehle, D. (2018). CRYSTALS Dilithium: A lattice based digital signature scheme. IACR Transactions on Cryptographic Hardware and Embedded Systems, 238 268.

[6] Ounsworth, M., & Pala, M. (2021). Composite Signatures for PKIX. IETF Draft draft ounsworth pq composite sigs. Internet Engineering Task Force.

[7] Sun, Q., et al. (2019). Dual algorithm X.509 certificates for hybrid TLS. Workshop on Usable Security (USEC). https://doi.org/10.14722/usec.2019.23014

[8] Housley, R. (2015). Guidelines for Cryptographic Algorithm Agility and Selecting Mandatory to Implement Algorithms. RFC 7696. IETF.

[9] National Cybersecurity Center of Excellence. (2021). Migration to Post Quantum Cryptography. NIST SP 1800 38 (Initial Preliminary Draft). https://www.nccoe.nist.gov/pqc migration

[10] Google. (2021). Certificate Transparency Policy (Version 3.0). https://googlechrome.github.io/CertificateTransparency/ct_policy.html

[11] Stabile, D., & Mosca, M. (2020). Post quantum key exchange for the internet and the open quantum safe project. Proc. SAC 2016, LNCS 10532, 14 37. https://doi.org/10.1007/978 3 319 69453

[12] Bernstein, D. J., & Lange, T. (2017). Post quantum cryptography. Nature, 549(7671), 188 194. https://doi.org/10.1038/nature23461