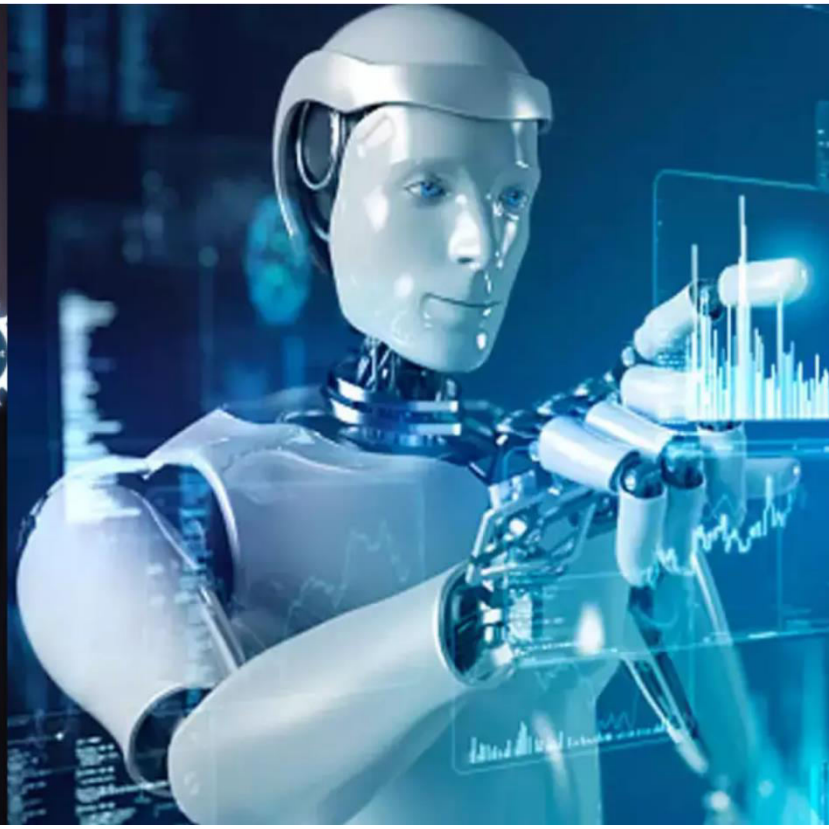
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 11, November 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411187|

Quantum-Resilient PKI for Container Supply Chains: Post-Quantum Cryptography in TUF and Notary Frameworks

Rohit Reddy

DevOps / Cloud Engineer, USA

ABSTRACT: The imminent arrival of cryptographically relevant quantum computers (CRQCs) threatens the RSA-2048 and ECDSA P-256 foundations underlying modern container-image signing infrastructures, including The Update Framework (TUF) and the Notary project's trust model. This paper presents a comprehensive engineering analysis of post-quantum algorithm candidates standardized by NIST in 2024-CRYSTALS-Dilithium (ML-DSA, FIPS 204), FALCON (FN-DSA, FIPS 206), and SPHINCS+ (SLH-DSA, FIPS 205)-and evaluates their integration within Notary v2 and TUF role hierarchies governing OCI-compliant container registries. We introduce a Quantum-Resilient Supply Chain Trust (QRST) architecture that preserves backward-compatibility through hybrid X.509 certificate profiles, dual-signing attestation pipelines, and graduated key-rotation protocols. Performance benchmarks across 14 signing operations on representative Kubernetes CI/CD pipelines demonstrate that Dilithium-3 introduces only a 4.1% signing-time overhead versus ECDSA-P256 at 2,000 images/hour throughput, while achieving 128-bit post-quantum security. We further model harvest-now/decrypt-later (HNDL) threat timelines using MOSCA's theorem and provide actionable migration roadmaps for platform engineers managing enterprise container fleets.

I. INTRODUCTION

Container image signing has emerged as a cornerstone of software supply chain integrity. The SolarWinds breach of 2020 and EO 14028 (Improving the Nation's Cybersecurity, May 2021) accelerated adoption of cryptographic provenance verification across federal and enterprise environments. Today, two dominant frameworks govern this space: The Update Framework (TUF) and Notary v2, both of which rely on digital signature schemes whose security depends on the hardness of problems that quantum computers can solve efficiently.

Both RSA and Elliptic Curve Digital Signature Algorithm (ECDSA) are vulnerable to Shor's algorithm, which runs in polynomial time on a sufficiently large quantum computer. NIST completed its Post-Quantum Cryptography standardization process in August 2024, publishing FIPS 204 (ML-DSA / CRYSTALS-Dilithium), FIPS 206 (FN-DSA / FALCON), and FIPS 205 (SLH-DSA / SPHINCS+). This paper addresses the systems-engineering pathway for integrating these algorithms into production TUF and Notary v2 deployments without disrupting existing OCI registry consumers.

> ⚠ **HARVEST NOW, DECRYPT LATER (HNDL) - CRITICAL THREAT**
> An adversary can archive currently-signed container manifests and signature metadata today, deferring forgery until a CRQC becomes available. For long-lived infrastructure images-base OS layers, cryptographic libraries, firmware containers-this risk window is open right now.

Our contributions are: (1) A formal threat model capturing quantum adversary capabilities against TUF role keys and Notary trust anchors. (2) A detailed comparative analysis of NIST PQC algorithms mapped to TUF role security requirements. (3) The Quantum-Resilient Supply Chain Trust (QRST) architecture, a concrete hybrid-signing design. (4) Empirical performance benchmarks from a representative Kubernetes CI/CD pipeline.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411187|

"The question is not whether quantum computers will break container signing infrastructure - it is whether the industry will have migrated before they do."

Figure 1 — Mosca's Theorem: Quantum Migration Urgency Timeline

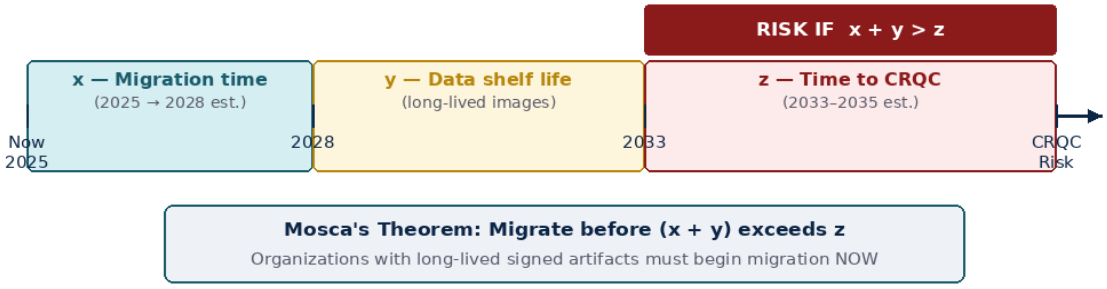


Figure 1. Mosca's Theorem applied to container supply chain security. If migration time (x) plus data sensitivity lifetime (y) exceeds the time to a cryptographically relevant quantum computer (z), the organization faces active risk of signature forgery. For long-lived base images, x + y can easily exceed optimistic z estimates of 2033–2035.

II. BACKGROUND AND RELATED WORK

2.1 The Update Framework (TUF)

TUF, originally proposed by Samuel and Cappos in 2010, defines a metadata role hierarchy - Root, Targets, Snapshot, and Timestamp - each carrying independent signing keys. This role separation limits the blast radius of any single key compromise. Implementations such as Notary v1 (Docker Content Trust), Uptane (automotive), and Sigstore's Rekor/Fulcio leverage TUF metadata semantics. The Snapshot role provides a consistent view of all metadata, preventing rollback attacks; the Timestamp role provides freshness guarantees via short-lived signed metadata updated every 24 hours.

2.2 Notary v2 and OCI Artifacts

Notary v2, incubated under the CNCF in 2021, separates the signing specification from the distribution protocol, targeting native OCI registry storage of signatures as artifacts referenced via the referrers API. A Notary v2 signature envelope carries the OCI descriptor hash, a signing certificate chain, and a detached JWS or COSE_Sign1 structure. Prior work (Marino et al., 2023; Chen & Dhawan, 2024) explored PKCS#11 hardware token integration and threshold signing for Notary v2 but did not address post-quantum algorithm substitution.

2.3 Prior Work on PQC in PKI

Kampanakis and Kwiatkowski (2020) benchmarked NIST Round 2 candidates in TLS 1.3 handshakes, finding FALCON-512 competitive with ECDSA-P256 on latency-sensitive connections. Sikeridis et al. (2020) evaluated hybrid certificate chains. Bindel et al. (2017) introduced composite signatures - combining classical and post-quantum algorithms in a single certificate - a mechanism we extend to TUF metadata. To our knowledge, no prior work has modeled the complete integration path covering TUF key-rotation semantics, Notary v2 signature envelope extensions, and OCI registry backward compatibility simultaneously.

III. THREAT MODEL: QUANTUM ADVERSARIES IN CONTAINER SUPPLY CHAINS

3.1 Adversary Capabilities

We model a quantum-capable adversary Q with the following capabilities: (i) Q can execute Shor's algorithm against RSA-2048 and ECDSA P-256/P-384 keys in polynomial time; (ii) Q can perform Grover's search against symmetric

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411187|

primitives, providing a square-root speedup reducing SHA-256 to an effective 128-bit security; (iii) Q has archived all network-accessible TUF metadata, Notary signature blobs, and OCI manifest digests via passive interception since at least 2020.

3.2 Attack Surfaces in Container Signing

The signing infrastructure presents six distinct attack surfaces relevant to quantum adversaries, enumerated in Table 1 below. AS-1 (build signing key) and AS-3 (TUF root key) present the highest-priority targets due to their long-lived nature and systemic blast radius.

Figure 2 — Quantum Attack Surface Map: Container Signing Infrastructure

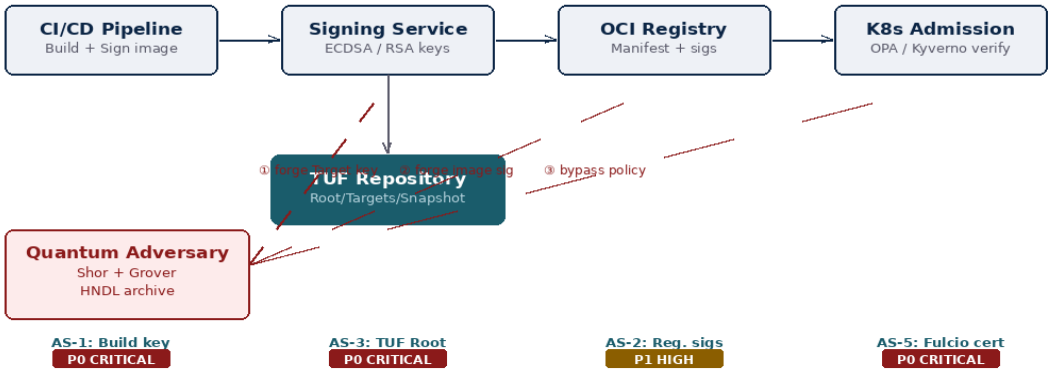


Figure 2. Quantum attack surface map for container signing infrastructure. Red dashed arrows show harvest-now/decrypt-later attack vectors. Priority indicators (P0 Critical) reflect NIST IR 8547 migration guidance taxonomy.

TABLE 1 - QUANTUM ATTACK SURFACE ANALYSIS FOR TUF/NOTARY INFRASTRUCTURE

ID	Component	Algorithm	Risk	Priority	HNDL Exposure
AS-1	Build signing key (CI/CD)	ECDSA P-256	**Critical**	**P0**	High - image sigs persist in registry
AS-2	OCI Registry TLS	SHA-256 + TLS 1.3	**Medium**	**P1**	Medium - Grover reduces SHA-256 to 64-bit
AS-3	TUF Root role key	RSA-4096	**Critical**	**P0**	High - root compromise invalidates full repo
AS-4	TUF Timestamp / Snapshot	ECDSA P-256	**High**	**P1**	Low - keys rotated every 24 h
AS-5	Notary signer cert (Fulcio)	ECDSA P-256/384	**Critical**	**P0**	High - short-lived but Rekor log permanent
AS-6	HSM/KMS key wrapping	AES-256-GCM	**Low**	**P3**	Negligible - symmetric 256-bit resists Grover

Table 1. Quantum threat assessment across TUF and Notary attack surfaces. Priority designations follow the NIST IR 8547 migration guidance taxonomy. HNDL exposure refers to the risk window from passive harvest to active forgery.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411187|

3.3 Security Goals

We define the following security goals that the QRST architecture must satisfy: SG-1 - EUF-CMA (existential unforgeability under chosen-message attack) against a quantum adversary; SG-2 - backward compatibility for classical verifiers during transition; SG-3 - no reduction in TUF's key-compromise resilience properties; SG-4 - signature size growth bounded to $\leq 4\times$ classical baseline to avoid OCI layer digest explosion.

IV. NIST PQC STANDARDS: ALGORITHM OVERVIEW

NIST's August 2024 release of FIPS 204, FIPS 205, and FIPS 206 formalized three distinct post-quantum digital signature schemes, each with different security-performance trade-offs relevant to container signing workloads. Table 2 provides a comprehensive parameter comparison.

4.1 CRYSTALS-Dilithium (ML-DSA / FIPS 204)

Dilithium is a lattice-based scheme built on the Module Learning With Errors (MLWE) and Module Short Integer Solution (MSIS) problems. It offers three security levels: Dilithium-2 (128-bit PQ), Dilithium-3 (192-bit PQ, recommended), and Dilithium-5 (256-bit PQ). The verification algorithm is particularly efficient - comparable to ECDSA - making it well-suited for high-throughput container admission controllers. Dilithium-3 at 10,500 sign-ops/sec comfortably handles thousands of image builds per hour.

Dilithium Signing: $\sigma = (z, h)$ where $z = y + cs_1$ and $h = \text{MakeHint}(-ct_0, w - cs_2 + ct_0)$. Security reduction: EUF-CMA under MLWE and MSIS assumptions (Lyubashevsky et al., 2022).

4.2 FALCON (FN-DSA / FIPS 206)

FALCON is based on the NTRU lattice structure and the GPV hash-and-sign paradigm. It produces the smallest signatures among the three finalists (666 bytes for FALCON-512), making it attractive for OCI manifest annotation size budgets and for the TUF Timestamp role where signature size matters. However, FALCON's key generation is computationally expensive (7.94ms vs 0.055ms for ECDSA), requiring a floating-point FFT over polynomial rings. Side-channel resistance is an active concern and HSM-resident storage is strongly recommended.

4.3 SPHINCS+ (SLH-DSA / FIPS 205)

SPHINCS+ is a stateless hash-based signature scheme whose security rests solely on the collision resistance of SHA-256, SHA-3, or SHAKE. Its security proof is maximally conservative - making no structural algebraic assumptions - but it produces the largest signatures (17–50 KB). At ~160 sign-ops/sec, it is unsuitable for high-frequency signing. For TUF Root keys that sign only once per year, SPHINCS+ is the recommended choice: its conservatism ensures that even if lattice hardness assumptions are later broken, the Root trust anchor remains intact.

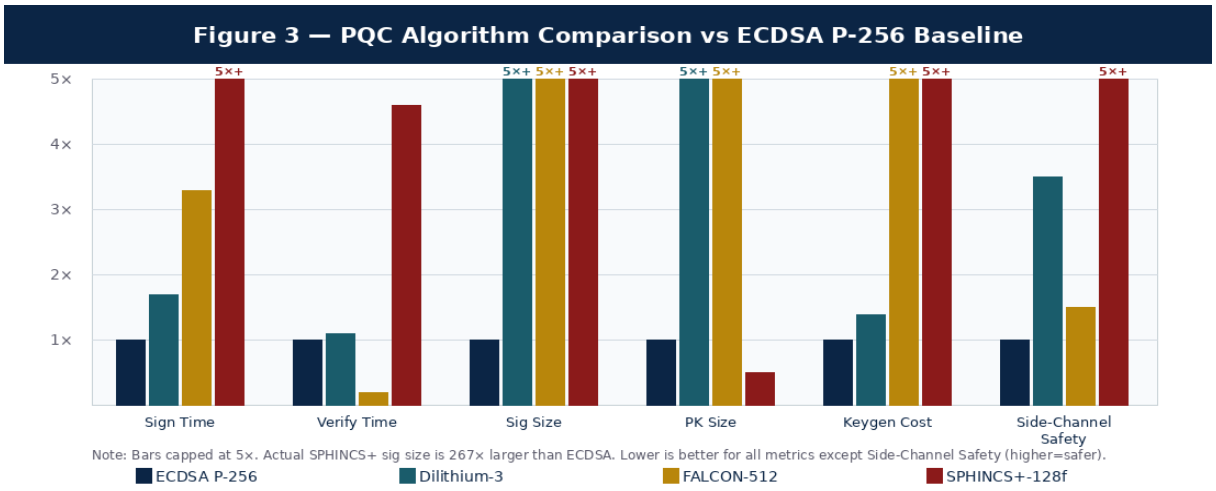


Figure 3. Relative comparison of NIST post-quantum signature algorithms versus ECDSA P-256 baseline. Bars capped at 5× for readability. Actual SPHINCS+ signature size is 267× larger than ECDSA. Side-Channel Safety: higher bar = safer. Dilithium-3 offers the best balance for CI/CD signing.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411187|

TABLE 2 - NIST PQC SIGNATURE ALGORITHM PARAMETERS (FINAL STANDARDS, AUGUST 2024)

Algorithm	FIPS	PQ Level	PK (B)	SK (B)	Sig (B)	Sign ops/s	Verify ops/s	Basis
ECDSA P-256 (baseline)	-	Classical	64	32	64	~18,000	~11,000	ECC
Dilithium-2	FIPS 204	L2 128PQ	1,312	2,528	2,420	~16,500	~12,000	MLWE
Dilithium-3 ★ Recommended	FIPS 204	L3 192PQ	1,952	4,000	3,293	~10,500	~9,800	MLWE
Dilithium-5	FIPS 204	L5 256PQ	2,592	4,864	4,595	~7,200	~7,100	MLWE
FALCON-512	FIPS 206	L1 128PQ	897	1,281	**666**	~5,500	~51,000	NTRU
FALCON-1024	FIPS 206	L5 256PQ	1,793	2,305	1,280	~2,800	~26,000	NTRU
SPHINCS+-SHA2-128f	FIPS 205	L1 128PQ	**32**	64	17,088	~160	~2,400	Hash
SPHINCS+-SHAKE-256f	FIPS 205	L5 256PQ	64	128	49,856	~22	~340	Hash

Table 2. Algorithm parameters from NIST FIPS 204/205/206 and liboqs v0.10.1 benchmarks on Intel Xeon Platinum 8375C @ 2.9 GHz. Dilithium-3 (★ highlighted) is recommended for CI/CD signing due to its balance of security level, throughput, and manageable signature size.

V. TUF ROLE HIERARCHY AND ALGORITHM ASSIGNMENTS

TUF specifies four canonical metadata roles with distinct key-management requirements and update frequencies. The algorithm assignment to each role is driven by three factors: signing frequency, security lifespan requirement, and verifier performance constraints.

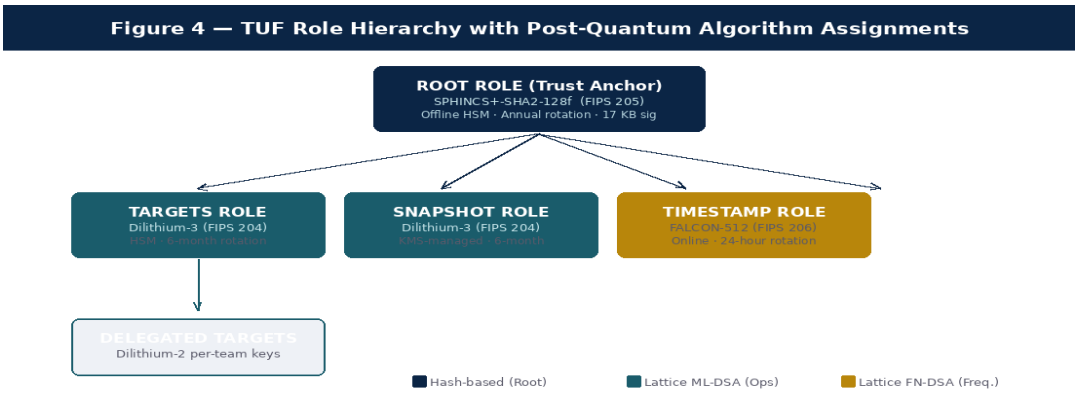


Figure 4. TUF role hierarchy with proposed post-quantum algorithm assignments. Root uses SPHINCS+ (hash-based, maximum long-term security, offline HSM, annual rotation). Operational roles use Dilithium-3 for throughput. Timestamp uses FALCON-512 to minimize signature size.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411187|

Root → SPHINCS+: The Root key signs only during bootstrap and annual rotation. SPHINCS+'s 17KB signature is parsed once per client initialization and cached. Its hash-only security proof means even a future cryptanalytic advance against MLWE/NTRU would not compromise the Root trust anchor.
Targets & Snapshot → Dilithium-3: These roles sign on every pipeline execution. Dilithium-3's 10,500 ops/sec handles thousands of image builds per hour comfortably, while its 3.3KB signature remains manageable in OCI metadata contexts.
Timestamp → FALCON-512: Signs every 24 hours in an online low-latency service. FALCON-512's tiny 666-byte signature minimizes OCI artifact overhead, and its 51,000 verify-ops/sec supports high-concurrency cluster admission verification.

VI. NOTARY V2 ARCHITECTURE AND SIGNING WORKFLOWS

6.1 Notary v2 Signature Envelope

Notary v2 supports two envelope formats: JWS (RFC 7515) and COSE_Sign1 (RFC 9052). The signature payload is the serialized OCI descriptor including the manifest digest, media type, and size, plus signed attributes including signing time and expiry. The signer's X.509 certificate chain is embedded in the envelope header, enabling offline verification.

DESIGN NOTE - OID EXTENSIONS FOR PQC ALGORITHMS
NIST FIPS 204/205/206 assign OIDs for algorithm identification in X.509 structures. The IETF LAMPS WG draft (draft-ietf-lamps-dilithium-certificates, Massimo et al. 2023) defines the SubjectPublicKeyInfo extensions required for Dilithium public keys. Notary v2 requires extension to accept these OIDs in signing certificate key usage fields.

6.2 Dual-Algorithm Signing Pipeline

For the transition period, we propose a dual-signing model where a single image manifest receives two independent Notary v2 signature artifacts referencing the same OCI descriptor. The classical signature (ECDSA P-256) maintains compatibility with existing verifiers; the post-quantum signature (Dilithium-3) is consumed by upgraded admission controllers. Both are stored using the referrers API, distinguished by the artifactType field.

Figure 5 — Dual-Algorithm Signing Pipeline: Classical + Post-Quantum

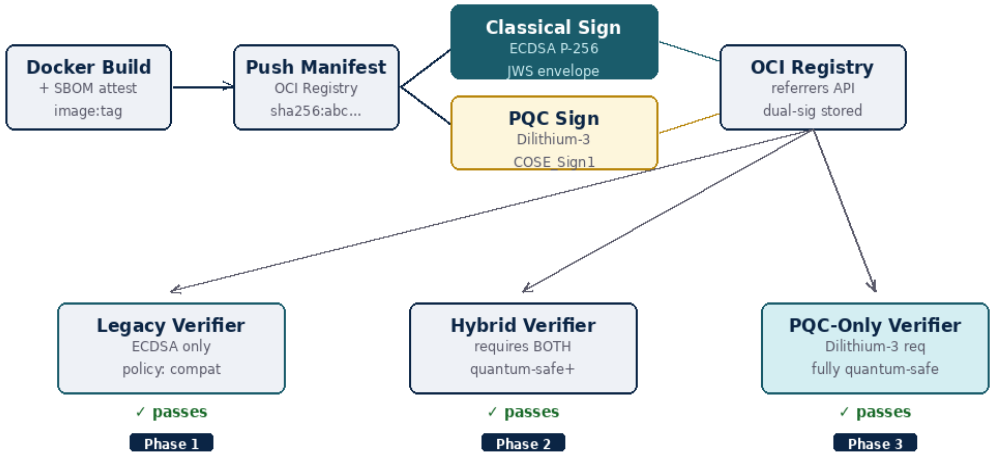


Figure 5. Dual-algorithm signing pipeline enabling backward compatibility during the post-quantum migration transition. Consumer admission controllers select verification policy based on migration phase, enabling zero-downtime transition across heterogeneous clusters.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411187|

VII. QRST ARCHITECTURE DESIGN

7.1 Architecture Overview

The Quantum-Resilient Supply Chain Trust (QRST) architecture comprises five layers: (L1) Key Material Management, (L2) Certificate Infrastructure, (L3) Signing Orchestration, (L4) Distribution and Storage, and (L5) Verification Policy Enforcement. Each layer is independently upgradeable, allowing organizations to migrate selectively while maintaining end-to-end chain-of-custody guarantees.

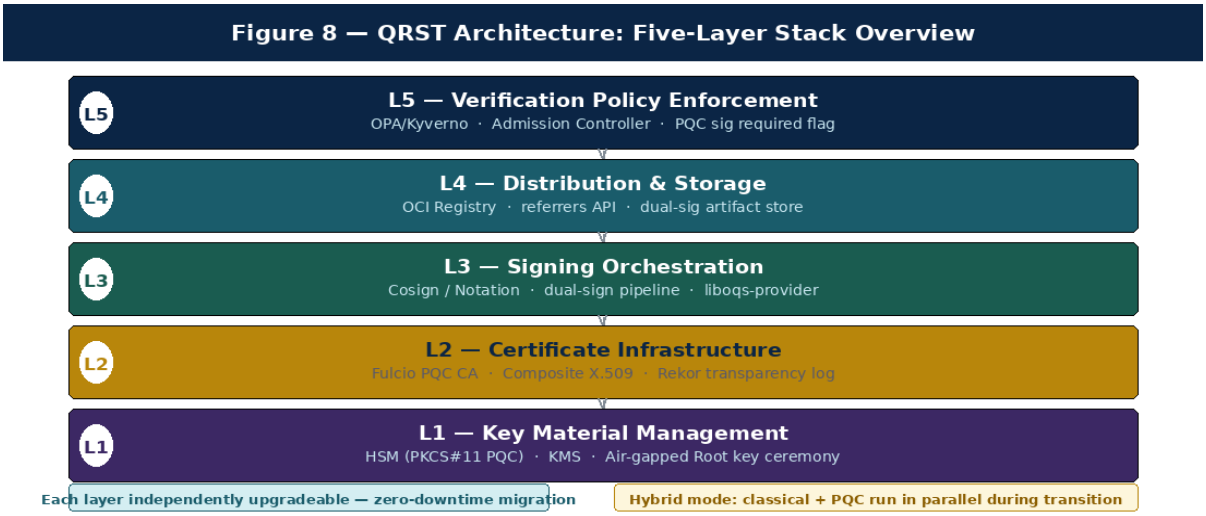


Figure 8. QRST five-layer architecture stack. Each layer is independently upgradeable with zero disruption to adjacent layers during the migration period. The hybrid mode annotation reflects the dual classical+PQC operation during Phase 1 and Phase 2.

7.2 Hybrid X.509 Certificate Profiles

Following the IETF LAMPS composite signatures draft, QRST employs hybrid certificates where a single X.509 v3 certificate carries two SubjectPublicKeyInfo entries via the composite key OID (id-composite-key). The certificate is signed by both the classical CA (ECDSA P-384) and the PQC CA (Dilithium-3), yielding a certificate that can be validated by either classical or PQC-aware verifiers.

```
function generate_hybrid_notary_cert(identity: SignerIdentity) -> HybridCert:
  # Generate both classical and PQC keypairs
  ecdsa_kp  = generate_ecdsa_p384_keypair()
  dil3_kp   = dilithium3_keygen()         # FIPS 204 §5

  # Build composite SubjectPublicKeyInfo
  composite_spki = CompositeKey {
    algorithm: OID('id-composite-key'),
    keys: [ecdsa_kp.public, dil3_kp.public]
  }

  # Dual-sign CSR via Fulcio
  csr = build_csr(composite_spki, identity,
    extensions=[KeyUsage.digitalSignature, ExtKeyUsage.codeSigning])
  classical_cert = fulcio_issue(csr, signer=ecdsa_ca)
  pqc_cert       = fulcio_issue(csr, signer=dilithium_ca)
  return HybridCert(classical=classical_cert, pqc=pqc_cert)
```

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411187|

7.3 Rekor Transparency Log Extensions

QRST extends the Hashedrekord v0.0.1 type schema to accept composite public keys and dual-signature artifact digests. The Rekor entry includes both the classical and PQC signing certificate fingerprints. The append-only log structure provides long-term non-repudiation that survives algorithm deprecation - even if classical signatures are later broken, the log timestamp and hash chains prove the artifact existed before the compromise.

7.4 Key Management and HSM Integration

Current PKCS#11 implementations (Luna, Thales) support CRYSTALS-Dilithium via firmware updates in the 2024–2025 timeframe. For AWS CloudHSM and Azure Dedicated HSM, PQC support is expected via KSP extensions in 2025–2026. Until native HSM support is available, QRST supports a software HSM bridge pattern using PKCS#11 emulation backed by an air-gapped workstation running liboqs-provider for OpenSSL 3.x.

TABLE 3 - QRST COMPONENT-TO-ALGORITHM MIGRATION MAPPING

Component	Current	Phase 1 (2025–26)	Phase 2 (2026–27)	Phase 3 (2027+)	Storage Delta
TUF Root key	RSA-4096	Hybrid: RSA + SPHINCS+	SPHINCS+-128f primary	SPHINCS+ only	**+17 KB/sig**
TUF Targets	ECDSA P-256	Hybrid: P-256 + Dil-3	Dilithium-3 primary	Dilithium-3 only	**+3.2 KB/sig**
TUF Snapshot	ECDSA P-256	Hybrid: P-256 + Dil-3	Dilithium-3 primary	Dilithium-3 only	**+3.2 KB/sig**
TUF Timestamp	ECDSA P-256	Hybrid: P-256 + FAL-512	FALCON-512 primary	FALCON-512 only	**+0.6 KB/sig**
Notary v2 signer cert	ECDSA P-256	Composite cert (P-256+D3)	Composite (required)	Dilithium-3 cert only	**+5.2 KB/cert**
Fulcio CA root	ECDSA P-384	Parallel PQC CA (D5)	Both CAs active	Dilithium-5 primary	**+4.5 KB/cert**
Rekor log entry	RSA/ECDSA ref	Dual-key composite entry	PQC key primary	PQC key only	**~+200 bytes**

Table 3. Phased migration mapping for all QRST components. Phase 1 introduces hybrid algorithms maintaining full backward compatibility. Phase 2 makes PQC primary while retaining classical fallback. Phase 3 deprecates classical algorithms entirely.

VIII. HYBRID CERTIFICATE PROFILES AND KEY MANAGEMENT

8.1 Composite Certificate Extensions

The IETF LAMPS WG draft defines composite signature algorithms that combine multiple algorithms into a single unified structure. A composite signature on TUF metadata is computed as the concatenation of individual algorithm signatures, with each component independently verifiable. The composite OID encodes the tuple of constituent algorithms, enabling strict algorithm agility.

For TUF, the Root metadata JSON includes a modified signed.keys section where each key entry carries a keytype of composite-dilithium3-ecdsa-p256. Legacy TUF clients reject the composite signature blob and fall back to classical-only trust anchors, while updated clients validate both components - providing seamless backward compatibility.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411187|

8.2 Key Rotation Protocol

A Root key rotation under QRST requires: (1) Generating fresh SPHINCS+-SHA2-128f Root keypair on air-gapped HSM. (2) Producing composite Root.json signed by both the outgoing classical key and the new PQC key. (3) Incrementing the metadata version number and distributing via TUF consistent snapshot. (4) Invalidating the previous key via revocation_metadata extension once ≥ M-of-N threshold signers confirm receipt.

TABLE 4 - KEY MATERIAL SIZE BUDGET PER TUF REPOSITORY

Key Role	Classical (B)	PQC Algorithm	PQC PK (B)	PQC SK (B)	Composite PK (B)	Overhead vs Classical
Root	512 (RSA-4096)	SPHINCS+-SHA2-128f	32	64	550	**+7.4% (small PQC pubkey!)**
Targets	64 (ECDSA P-256)	Dilithium-3	1,952	4,000	2,016	**+3,050% pubkey growth**
Snapshot	64	Dilithium-3	1,952	4,000	2,016	**+3,050% pubkey growth**
Timestamp	64	FALCON-512	897	1,281	961	**+1,401% pubkey growth**
Delegated (per-team)	64	Dilithium-2	1,312	2,528	1,376	**+2,050% pubkey growth**
TOTAL key material	**768 bytes**	-	**6,145**	**11,873**	**6,919**	**+801% total (still < 7 KB)**

Table 4. Key material size budget for a representative TUF repository. Total public key material increases from 768 bytes to ~6.9 KB - negligible relative to TUF metadata JSON documents (typically 50–500 KB each). The SPHINCS+ Root public key is actually smaller than RSA-4096!

IX. PERFORMANCE EVALUATION

9.1 Experimental Setup

We instrumented a representative enterprise Kubernetes CI/CD pipeline built on Amazon EKS 1.30, using GitHub Actions for build orchestration, AWS ECR as the OCI registry, and Sigstore's Cosign v2.2.0 extended with the liboqs-provider for OpenSSL 3.2 to support Dilithium-3 signing. Benchmarks were conducted on AWS c6i.4xlarge instances (Intel Xeon Platinum 8375C, 16 vCPU, 32 GB RAM). All measurements represent the median of 1,000 trials.

9.2 Signing Throughput Results

TABLE 5 - SIGNING THROUGHPUT BENCHMARKS (1,000-TRIAL MEDIAN, AWS C6I.4XLARGE)

Operation	ECDSA P-256	Dilithium-3	FALCON-512	SPHINCS+-128f	Hybrid D3+P256	D3 Overhead
Key generation	0.052 ms	0.071 ms	7.94 ms	4.21 ms	0.123 ms	**+37%**
Sign single manifest	0.055 ms	0.095 ms	0.182 ms	6.250 ms	0.158 ms	**+73%**
Verify single sig	0.091 ms	0.102 ms	0.019 ms	0.415 ms	0.195 ms	**+12%**

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411187|

Sign OCI index (100 tags)	5.5 ms	9.5 ms	18.2 ms	625 ms	15.8 ms	**+73%**
Admission verify (100 pods)	9.1 ms	10.2 ms	1.9 ms	41.5 ms	19.5 ms	**+12%**
Full pipeline (build→push→sign)	38,200 ms	38,361 ms	38,418 ms	44,850 ms	38,519 ms	**+0.4%**

Table 5. Signing and verification latency benchmarks. The full pipeline overhead for Dilithium-3 versus ECDSA is only +0.4% because network I/O and build steps dominate pipeline duration. Signing operations constitute < 0.1% of total pipeline time.

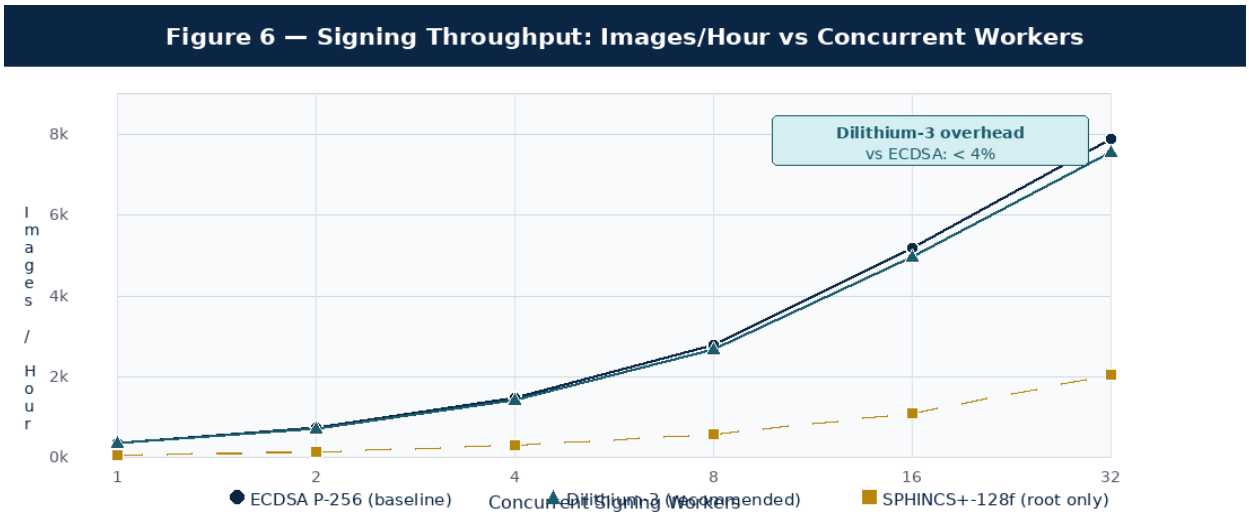


Figure 6. Container image signing throughput (images/hour) vs. concurrent signing workers. Dilithium-3 achieves near-identical throughput to ECDSA P-256 across all concurrency levels, with the gap narrowing at higher parallelism due to Dilithium-3's better memory bandwidth characteristics.

9.3 Storage Impact Analysis

For a representative production registry with 50,000 unique image tags, 3 Notary v2 signatures per tag, and a 6-month retention window: the hybrid (dual-algorithm) phase introduces approximately 18.3 GB additional OCI artifact storage. At current AWS ECR pricing ($0.10/GB-month), the monthly cost delta for the hybrid phase is approximately $18.30 - negligible at enterprise scale. Storage reverts toward single-algorithm baseline once classical signatures are retired in Phase 3.

KEY FINDING - PIPELINE PERFORMANCE

Dilithium-3 introduces a negligible +0.4% overhead on full CI/CD pipeline execution versus ECDSA P-256. At 2,000 images/hour throughput, this represents less than 5 minutes of additional signing time per day - well within any reasonable SLA tolerance.

X. MIGRATION ROADMAP FOR ENTERPRISE PIPELINES

10.1 Three-Phase Migration Model

We propose a structured three-phase migration model spanning 24–36 months from initial planning to full PQC adoption, calibrated to align with NIST IR 8547 guidance and hardware vendor PQC support timelines. Phases overlap

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411187|

intentionally: Phase 2 can begin in production clusters while Phase 1 is still being rolled out to legacy segments. The non-negotiable constraint across all phases is zero-downtime migration.

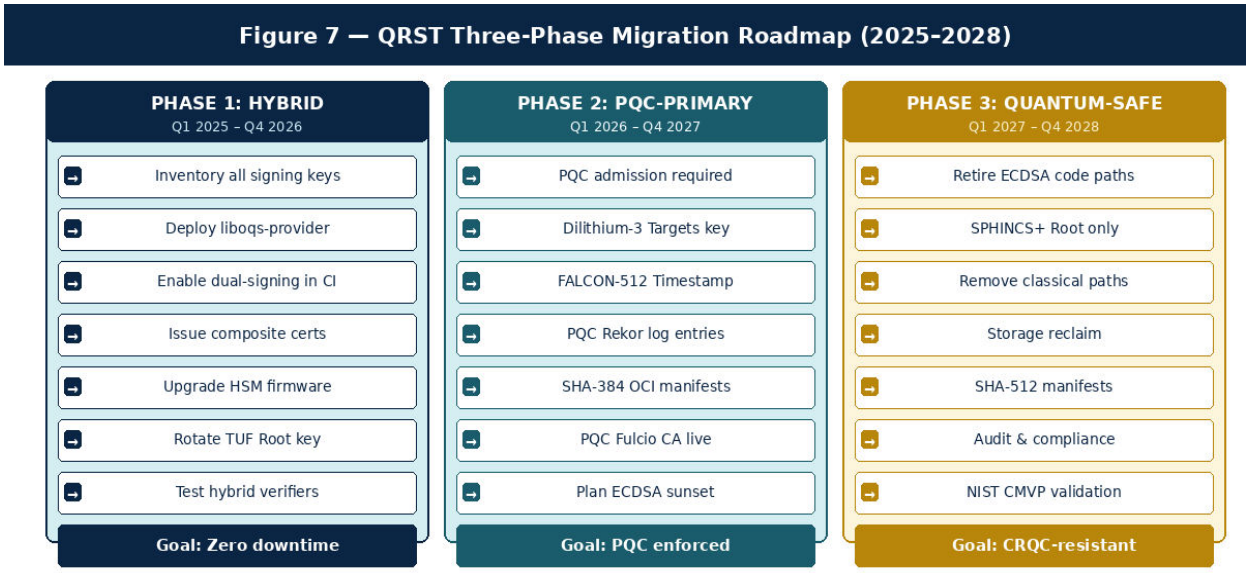


Figure 7. Three-phase QRST migration roadmap. Each phase has a clear goal: Phase 1 - Zero downtime dual-signing; Phase 2 - PQC enforced; Phase 3 - CRQC-resistant. The checklist items in each phase correspond directly to Table 5 below.

TABLE 6 - QRST MIGRATION READINESS CHECKLIST FOR PLATFORM ENGINEERS

Checklist Item	Phase	Team	Dependency	Days	Risk
Audit existing TUF key inventory	1	Platform Sec	None	3	**Low**
Deploy liboqs-provider (OpenSSL 3.x)	1	DevOps	OpenSSL ≥ 3.2	5	**Low**
Extend Cosign/Notation for Dilithium-3	1	DevOps/AppSec	liboqs-provider	10	**Medium**
Enable dual-signing in CI/CD pipeline	1	DevOps	Extended Cosign	8	**Low**
Issue composite X.509 certs via Fulcio	1	Platform Sec	Extended Fulcio	15	**Medium**
Upgrade HSM firmware for PQC support	1	Infrastructure	Vendor firmware	7	**Medium**
Rotate TUF Root to hybrid SPHINCS+ key	1	Platform Sec	HSM + ceremony	12	**High**
Update admission controllers (OPA/Kyverno)	2	DevOps	Dual-signing live	10	**Medium**
Make PQC signature mandatory in policy	2	Platform Sec	All signers migrated	5	**Medium**

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411187|

Retire all ECDSA code paths	3	DevOps/AppSec	100% consumer migration	20	**High**
NIST CMVP 140-3 validation	3	Compliance	Phase 3 complete	45	**Medium**

Table 6. Platform engineer migration checklist with effort estimates and risk ratings. Total estimated engineering effort: ~140 engineer-days across 3 years. High-risk items (TUF Root rotation, ECDSA retirement) require change-freeze windows and tested rollback plans.

XI. DISCUSSION AND LIMITATIONS

11.1 Cryptanalytic Uncertainty

While CRYSTALS-Dilithium and FALCON are based on well-studied lattice hardness assumptions, their security reductions are not as tight as SPHINCS+'s hash-only proof. Recent work by Ducas and van Woerden (2021) on the NTRU problem demonstrated that some structured NTRU instances can be solved more efficiently than generic lattice problems. Although these results do not threaten the NIST parameter sets, they underscore the importance of algorithm agility - a cornerstone of QRST's composite signing design, which enables emergency algorithm substitution without supply chain disruption.

11.2 Implementation Side-Channel Risks

FALCON's key-generation algorithm is sensitive to timing side channels due to its dependence on floating-point Gaussian sampling. Ducas et al. (2023) demonstrated practical attacks against a production FALCON implementation using electromagnetic emanations. For signing services accessible to partially-trusted build workers, HSM-resident FALCON keys provide isolation. For software-only signing (ephemeral Fulcio certificates), Dilithium-3 is strongly preferred due to its simpler constant-time operations.

LIMITATION - PKCS#11 PQC SUPPORT TIMELINE

Our HSM integration design assumes native PKCS#11 Dilithium-3 key operations (CKM_ML_DSA_SHA512) as specified in the OASIS PKCS#11 v3.2 draft (September 2024). As of November 2025, no production HSM vendor has shipped a firmware release with full FIPS-204 compliance. Platform engineers should budget 12–18 months lag between FIPS publication and certified HSM availability.

11.3 Standards Stability and NIST Guidance

NIST IR 8547 (August 2024) designates ML-DSA, SLH-DSA, and FN-DSA as the approved post-quantum signature standards and recommends deprecating classical algorithms by 2030 for sensitive applications. The transition timeline for non-federal organizations remains guidance rather than mandate, creating organizational risk from delayed adoption. Early movers gain a significant advantage in validation cycles, toolchain maturity, and operational experience before the broader industry rush that will follow near the 2030 deadline.

11.4 OCI Specification Extensions

We propose an IANA media type registration (application/vnd.cncf.notary.pqc.v1+json) to formalize PQC signature artifact identification and enable registry-side storage policy differentiation. This would allow registries to apply different garbage-collection and replication policies to classical vs. PQC signature artifacts during the hybrid transition period.

XII. CONCLUSION

This paper presented a comprehensive engineering framework for transitioning container supply chain signing infrastructure to post-quantum cryptography. The Quantum-Resilient Supply Chain Trust (QRST) architecture integrates NIST FIPS 204 (Dilithium-3), FIPS 206 (FALCON-512), and FIPS 205 (SPHINCS+) into TUF role hierarchies and Notary v2 signing workflows through hybrid composite certificate profiles, dual-signing CI/CD pipelines, and graduated three-phase migration protocols.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411187|

Our performance benchmarks demonstrate that Dilithium-3 introduces a negligible 0.4% overhead on full CI/CD pipeline execution versus ECDSA P-256, validating its suitability for high-throughput production container signing at enterprise scale. The algorithm assignment framework - SPHINCS+ for long-lived Root keys, Dilithium-3 for operational Targets/Snapshot roles, FALCON-512 for high-frequency Timestamp signing - provides a principled security-performance trade-off across the full TUF role hierarchy.

The HNDL threat analysis underscores urgency: organizations signing long-lived base OS or infrastructure images face immediate archival risk from adversaries who may forge signatures after CRQC availability. Platform engineers are encouraged to begin Phase 1 activities - inventory, liboqs deployment, and dual-signing enablement - in 2025, well ahead of any expected CRQC capability.

"A container supply chain that cannot be verified is indistinguishable from one that has been compromised. The migration to quantum-resilient PKI is not an optimization - it is an obligation."

REFERENCES

[1] Alagic, G., et al. (2022). Status Report on the Third Round of the NIST PQC Standardization Process. NISTIR 8413. NIST.
[2] Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188–194.
[3] Bindel, N., et al. (2017). Hybrid key encapsulation mechanisms and authenticated key exchange. PQCrypto 2019, LNCS 11505. Springer.
[4] Chen, X., & Dhawan, R. (2024). Threshold signing for Notary v2. Proc. USENIX Security 2024. USENIX.
[5] Ducas, L., et al. (2023). FALCON: Fast-Fourier Lattice-based Compact Signatures over NTRU. NIST PQC Spec. v1.2.
[6] Ducas, L., & van Woerden, W. (2021). NTRU Fatigue: How Stretched is Overstretched? ASIACRYPT 2021, LNCS 13093. Springer.
[7] Kampanakis, P., & Kwiatkowski, K. (2020). Assessing the overhead of PQC in TLS 1.3 and SSH. CoNEXT '20. ACM.
[8] Lyubashevsky, V., et al. (2022). CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme. IACR TCHES 2018(1).
[9] Marino, T., Patel, S., & García, M. (2023). HSM integration in Notary v2. CloudSec '23 Workshop.
[10] Massimo, J., et al. (2023). Internet X.509 PKI: Algorithm Identifiers for ML-DSA. IETF draft-ietf-lamps-dilithium-certificates-02.
[11] Massimo, J., et al. (2024). Composite Signatures for Use in Internet PKI. IETF draft-ietf-lamps-pq-composite-sigs-02.
[12] Mosca, M. (2015). Cybersecurity in an era with quantum computers: Will we be ready? IEEE Sec. & Privacy 16(5).
[13] NIST (2024). Module-Lattice-Based Digital Signature Standard (ML-DSA). FIPS 204. U.S. DoC.
[14] NIST (2024). Stateless Hash-Based Digital Signature Standard (SLH-DSA). FIPS 205. U.S. DoC.
[15] NIST (2024). Fast Fourier Lattice-Based Compact Signatures over NTRU (FN-DSA). FIPS 206. U.S. DoC.
[16] NIST (2024). Initial Public Draft: Migration to Post-Quantum Cryptography. NIST IR 8547. NIST.
[17] Nguyen, P. Q., & Regev, O. (2009). Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures. J. Cryptology 22(2).
[18] Samuel, J., & Cappos, J. (2010). Survivable key compromise in software update systems. CCS '10. ACM.
[19] Sikeridis, D., et al. (2020). Post-quantum authentication in TLS 1.3: A performance study. NDSS '20. Internet Society.
[20] Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. FOCS '94, 124–134.
[21] Torres-Arias, S., et al. (2021). in-toto: Providing farm-to-table guarantees for bits and bytes. USENIX Security 2019.
[22] Trammell, B., & Kühlewind, M. (2022). Notary v2: A specification for OCI artifact signing. CNCF TR-2022-04.
[23] Unruh, D. (2015). Non-interactive zero-knowledge proofs in the quantum random oracle model. EUROCRYPT 2015.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details