PQUIP
Internet-Draft
Intended status: Informational
Expires: 17 April 2026

T. Reddy
Nokia
D. Wing
Citrix
Y. Rosomakho
Zscaler

14 October 2025

Guidance for Migration to Composite, Dual, or PQC Authentication
draft-reddy-pquip-pqc-signature-migration-01

Abstract

This document provides guidance for migration from traditional digital signature algorithms to post-quantum cryptographic (PQC) signature algorithms. It compares three models under discussion in the IETF for PKI-based protocols: composite certificates, dual certificates, and PQC certificates. The goal is to help operators and engineers working on cryptographic libraries, network security, and PKI/key management infrastructure select an approach that balances interoperability, security, and operational efficiency during the transition to post-quantum authentication.

Table of Contents

1. Introduction

The emergence of cryptographically relevant quantum computer (CRQC) poses a threat to widely deployed public-key algorithms such as RSA and elliptic-curve cryptography (ECC). Post-quantum algorithms are being standardized by NIST and other bodies, but migration is not immediate. In the meantime, protocols need to ensure that authentication mechanisms remain secure against both classical and quantum adversaries.

For data authentication, the primary concern is that adversaries who obtain a CRQC will be able to forge digital signatures produced by traditional public-key algorithms (e.g., RSA, ECDSA). Such forgeries enable a range of attacks, including on-path man-in-the-middle (MitM) attacks, and off-path attacks such as software-artifact forgery, and client impersonation in mutual TLS when a client private key is compromised. In addition, on-path adversaries can attempt active downgrade techniques (for example, suppressing PQC or hybrid signature schemes during negotiation) to force reliance on broken traditional algorithms. PQC or Hybrid certificates do not by themselves prevent downgrade attack when relying parties continue to accept traditional-only certificates. These risks motivate a transition of certificate-based authentication toward post-quantum security.

The IETF has defined two hybrid transition models for use in TLS, IKEv2/IPsec, JOSE/COSE, and PKIX:

* Composite certificates: A single X.509 certificate that contains a composite public key and a composite signature, combining a traditional and a PQC algorithm. Certificates using composite ML-DSA are specified in [COMPOSITE-ML-DSA].
* Dual-certificate model: A deployment model in which two separate certificates, one using a traditional algorithm and one using a PQC algorithm, issued for the same identity, presented and validated together during authentication. Some protocols may require these certificates to include the RelatedCertificate extension [RELATED-CERTS] to ensure that both refer to the same identity and binding.

Another approach is to use a PQC certificate which contains only a post-quantum public key and produces signatures using a PQC algorithm. Examples include [ML-DSA] and [SLH-DSA].

This document provides guidance on selecting among the two hybrid certificate models and the PQC model depending on the deployment context, the readiness of the supporting ecosystem, and security requirements.

It is important to note that the use of PQC certificates, composite certificates, or the dual-certificate model alone does not guarantee post-quantum security. As long as relying parties continue to trust or accept traditional-only certificates, an attacker equipped with a CRQC can forge traditional certificates and impersonate an authenticated party, even if that party does not use a traditional certificate. Post-quantum security is achieved only when relying parties enforce policies that reject traditional-only authentication.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

This document uses the terms "composite certificates" and "PQC certificates" as defined in Section 1.

The term "dual certificates" in this document refers to the dual-certificate model as defined in Section 1.

Composite: A key, certificate, or signature that merges traditional and PQC algorithms into one object.

The terms hybrid signature scheme and hybrid signature are used as defined in [HYBRID-SPECTRUMS].

The term hybrid certificates is used herein to refer to either composite or dual certificate models.

Relying Party: An endpoint which validates the certificate of a remote peer. With classic HTTPS authentication, this is the HTTPS client. With mutual TLS authentication, this is both TLS endpoints.

Authenticated Party: An endpoint which provides its certificate for a remote peer to validate. With classic HTTPS authentication, this is the HTTPS server. With mutual TLS authentication, this is both TLS endpoints.

3. Motivation for PQC Signatures

Unlike "Harvest Now, Decrypt Later" attacks (see Section 7 of [PQC-ENGINEERS]) that target the confidentiality of encrypted data, the threat to authentication arises only from the moment a CRQC becomes available. Compromise of authentication is therefore not retrospective: previously established identities and signatures cannot be forged in hindsight, but all future authentications using traditional algorithms become insecure once a CRQC exists.

Once a CRQC is available, continued reliance on traditional public-key algorithms (e.g., RSA, ECDSA) becomes untenable, as an attacker could forge digital signatures and impersonate legitimate entities. In practice, the availability of a CRQC may not be publicly disclosed. Similar to a zero-day vulnerability, an adversary could exploit quantum capabilities privately to compromise traditional certificates without alerting the wider ecosystem.

Addressing this risk requires replacing traditional signatures with post-quantum (PQC) signatures. Doing so entails ecosystem-wide upgrades across:

* Software components: cryptographic libraries and protocol implementations;
* Hardware security devices: Hardware Security Modules (HSMs) and Trusted Platform Modules (TPMs);
* Public Key Infrastructure (PKI): Certification Authorities (CAs), intermediate CAs, and trust anchors;
* Dependent protocols: TLS ([TLS], [DTLS]), [IKEv2], and JOSE/COSE.

Because these transitions require years of planning, coordination, and investment, preparations must begin well before a CRQC is publicly known.

PQC or hybrid certificates provide post-quantum security only when relying parties reject traditional-only certificates (see Section 11.1). The implications of this requirement differ across deployment environments:

* Open environments (e.g., the Web): Enforcing rejection of traditional-only certificates would cause substantial disruption due to the wide diversity of clients and servers. As discussed in Section 11.1, there will be no single “flag day” for PQC authentication; instead, relying parties will have to adopt PQC enforcement gradually, using mechanisms such as continuity signals or learned authenticated party behavior to resist downgrades while maintaining compatibility during the transition.

* Closed or enterprise-managed environments: In deployments where both the authenticated party and the relying party are managed by the same organization, enforcing PQC or hybrid authentication policies is operationally feasible. Organizations can coordinate certificate issuance and validation policies centrally, enabling earlier transition to PQC or hybrid models without affecting interoperability.
* mixed environments

In environments where a relying party visits authenticated parties that have a mix of quantum-safe and traditional authentication, and administrators or users need to protect against downgrade attacks (Section 11.1), relying parties will need the configurations that are per-domain or per-FQDN. Such mixed environments will likely be the long tail.

4. Composite certificates

A composite certificate contains a composite public key and a composite signature, each combining a traditional and a post-quantum (PQC) algorithm within a single X.509 structure. Both the key and the signature use new encodings defined in [I-D.ietf-lamps-pq-composite-sigs], and therefore composite certificates do not offer interoperability with legacy PKI deployments. The goal is of the composite approach is defense-in-depth: the traditional component preserves authentication security if a flaw is found in the PQC algorithm before a CRQC exists, while the PQC component preserves security after CRQCs can break traditional algorithms. Verification succeeds only if all component signatures validate over the same canonical message.

ML-DSA composite certificates are defined in [I-D.ietf-lamps-pq-composite-sigs], which defines the use of ML-DSA in combination with one or more traditional algorithms such as RSA-PKCS#1v1.5, RSA-PSS, ECDSA, Ed25519, or Ed448. The framework in that document is designed to be extensible and is expected to accommodate additional post-quantum algorithms in future specifications.

Protocol-specific drafts describe how composite certificates are used in different environments, including: [TLS-COMPOSITE-ML-DSA] for TLS, [IKEv2-COMPOSITE-ML-DSA] for IKEv2, and [JOSE-COSE-COMPOSITE-ML-DSA] for JOSE and COSE. In each case, the relying party validates a single certification path anchored in a multi-algorithm trust anchor, avoiding the need for parallel certificate chains.

4.1. Advantages

A key benefit of the composite model is single-path operation. Because both algorithms are embedded in one certificate chain, the relying party validates only one path, which reduces chain-management complexity compared to dual-chain deployments. Conveying a single certificate and signature object can also reduce message size relative to transmitting two independent chains. From a protocol perspective, composite certificates typically require minimal changes to handshakes, since authentication still relies on one certificate and one signature.

4.2. Disadvantages

The main challenge with composite certificates is ecosystem readiness. Clients, servers, and Certification Authorities must support composite public keys and composite signature verification, which are not yet widely deployed. The new certificate encodings and multi-algorithm signing introduce updates across PKI components, libraries, and Hardware Security Modules. Once these components support the composite structures, using a composite signature algorithm is no more complex than adopting any new PQC algorithm.

Another operational limitation is the need for algorithm-set coordination: all participants in a composite ecosystem must agree on the specific and acceptable combinations of post-quantum and traditional algorithms (for example, ML-DSA-44 + ECDSA P-256 or ML-DSA-65 + EdDSA Ed448). A composite certificate can only be validated if both endpoints and all intermediate CAs recognize the same algorithm identifiers and policy. Disagreement on permitted combinations can lead to handshake failures, certificate re-issuance delays, or policy fragmentation across vendors. This is primarily a policy and interoperability issue during early deployment: once endpoints and CAs recognize the same algorithm identifiers and policies, a composite algorithm behaves like any other registered signature algorithm.

Composite deployments are also an intermediate step: once traditional algorithms are deprecated due to CRQCs, operators will still need to transition from composite to PQC certificates. This requires deploying new PQC trust anchors, issuing PQC certificates, and revoking composite certificates. While automated mechanisms such as ACME or CMP can streamline end-entity certificate issuance, trust anchors are typically distributed through OS, Browser, or device update mechanisms, and their replacement generally requires platform-specific processes. As a result, for some organizations, this two-stage path may lengthen the overall migration.

5. Dual Certificates

Dual certificates rely on issuing two separate certificates for the same identity: one using a traditional algorithm (for example, RSA or ECDSA) and one using a post-quantum algorithm (for example, ML-DSA). Both certificates are presented and validated during authentication, providing hybrid assurance without introducing new certificate formats or encodings.

5.1. Advantages

A major advantage of the dual-certificate model is its negotiation flexibility. Because each certificate contains only a single algorithm, endpoints do not need to agree in advance on a specific combination of traditional and post-quantum algorithms. The server can select which certificate (or both) to present based on the client's advertised capabilities, and the client can validate whichever chain it supports. This enables smoother incremental deployment and interoperation between implementations that support different PQC algorithms or security policies.

Dual certificates also use standard X.509 structures and single-algorithm chains, maximizing compatibility with existing PKI and avoiding changes to certificate parsing or signature verification logic. The clear separation between traditional and PQC keys simplifies operational control, audit, and incident response. Deployments can move from traditional-only to dual certificates, and later retire the traditional certificate when PQC support is ubiquitous, without redefining certificate formats or introducing composite encodings. The model also fits well in multi-tenant environments where different tenants or business units may adopt different combinations of traditional and PQC algorithms without requiring global agreement on a composite set.

5.2. Disadvantages

The dual-certificate model increases protocol overhead, since both certificate chains and signatures must be transmitted and validated. Protocols that traditionally authenticate a single certificate chain, such as [TLS] and [IKEv2], require extensions to support validation of two end-entity certificates and to ensure that both are cryptographically bound to the same identity. This adds implementation complexity and may increase handshake latency.

Managing two distinct certificate chains introduces operational cost and new failure modes. Debugging becomes more difficult, as validation errors may originate from either chain or from inconsistent identity binding. Operators must also obtain and renew two certificates from Certification Authorities, which can be significant in large-scale deployments.

Finally, while dual certificates avoid the need for a fixed algorithm pairing, they require explicit binding and coordination between the two chains. Each relying party must verify that the traditional and PQC certificates correspond to the same entity, typically using mechanisms such as the RelatedCertificate extension [RELATED-CERTS]. Lack of consistent binding policies can lead to interoperability issues and potential downgrade risks if only one chain is validated.

6. PQC Certificates

PQC certificates represent the final stage of migration. They use exclusively post-quantum cryptographic algorithms for both public keys and signatures, providing no fallback to traditional algorithms. Once adopted at scale, they eliminate hybrid complexity and rely entirely on quantum-resistant primitives for authentication.

6.1. Advantages

The PQC model offers the simplest and most forward-looking architecture. It removes all dependency on classical algorithms, thus avoiding future deprecation or phased-out support for RSA and ECC. Certificate management is streamlined, as there is only one algorithm family to provision, monitor, and renew. Operational overhead decreases compared to dual deployments, since each entity maintains a single certificate chain and consistent cryptographic policy.

PQC certificates also enable long-term assurance: the entire certificate path is verifiable using post-quantum signatures, ensuring uniform resistance against quantum adversaries.

6.2. Disadvantages

The primary risk of PQC deployments is algorithmic fragility. If a vulnerability or cryptanalytic weakness is discovered in a deployed PQC scheme, there is no classical fallback for continued authentication. Protocols and infrastructures must therefore maintain strong crypto-agility and be prepared to replace algorithms rapidly if needed.

Backward compatibility can be maintained if the authenticated party also holds a traditional certificate and presents it to relying parties that have not yet deployed PQC support. While this approach preserves interoperability during the transition, it also introduces downgrade risk: an attacker could suppress PQC options and force peers to authenticate using the traditional certificate.

PQC operation where traditional algorithms are completely removed eliminates this downgrade vector, but it is feasible only once relying parties enforce PQConly authentication.

Adoption may also be uneven across jurisdictions. Regulatory frameworks and certification programs may not recognize the same PQC algorithms at the same time. Divergent compliance regimes could delay global deployment or require organizations operating in multiple regions to maintain mixed trust infrastructures until regulatory alignment is achieved.

Finally, PQC deployments remain feasible only once PQC algorithms are fully standardized, broadly implemented, and supported by hardware security modules, operating systems, and major application ecosystems.

7. Operational and Ecosystem Considerations

Migration to post-quantum authentication requires addressing broader ecosystem dependencies, including trust anchors, hardware security modules, and constrained devices.

7.1. Trust Anchors and Transitions

Trust anchors represent the ultimate root of trust in a PKI. If existing trust anchors are RSA or ECC-based, then new PQC-capable trust anchors will need to be distributed. Operators will have to plan for a phased introduction of PQC trust anchors, which may involve:

* Rolling out composite trust anchors that support both traditional and PQC signatures.
* Establishing parallel trust anchor hierarchies and phasing out the traditional hierarchy once PQC adoption is universal.
* Ensuring secure and authenticated distribution of updated trust anchors to clients, especially devices that cannot be easily updated.

Deployments migrating from traditional to post-quantum authentication may have to operate with multiple trust anchors for a period of time. A new PQC or composite root may be introduced, or alternatively a PQ intermediate may be added beneath an existing traditional root, leading to different trust chain models:

* Traditional chain: anchored in a Traditional root (e.g., RSA/ ECDSA), which may issue a PQC intermediate.
* PQC chain: anchored in a PQC root (e.g., ML-DSA, SLH-DSA).
* Parallel roots: both a traditional root and a PQC root are distributed as trust anchors, with separate hierarchies operating in parallel until the traditional root can be phased out.
* Composite chain: anchored in a composite root and using composite algorithms, with a single certificate chain that combines traditional and PQC public keys and signatures. This forms a distinct chain, rather than two parallel ones.

During this coexistence phase, clients generally fall into five categories:

1. Legacy-only: trust only traditional roots and support only traditional algorithms.
2. Mixed: trust only traditional roots but support both traditional and PQC algorithms. These clients can validate PQC certificates only if a PQC intermediate is cross-signed by a traditional root.
3. Dual-trust: trust both traditional and PQC roots, supporting both algorithm families.
4. Composite-trust: trusts composite root and support composite algorithms, validating a single chain that integrates traditional and PQ signatures.
5. PQC: trust only PQC roots and support only PQC algorithms.

The main challenge is that servers cannot easily distinguish between mixed clients (2) and dual-trust clients (3), since both advertise PQC algorithms, but only dual-trust clients actually recognize PQC roots. To ensure compatibility with mixed clients (2), servers may default to sending longer PQC chains that include a cross-signed PQC root (i.e., a PQC root certificate signed by a traditional root). However, this is unnecessary and even counterproductive for dual-trust clients (3), which already trust the PQC root directly; such clients will fail to validate the cross-signed PQC root. For dual-trust clients, including the cross-signed PQC root only increases message size and introduces validation errors.

[I-D.ietf-tls-trust-anchor-ids] (TAI) addresses this problem by allowing clients to indicate, on a per-connection basis, which trust anchors they recognize. Servers can use that information to select a compatible certificate chain, reducing unnecessary chain elements and

providing operators with better telemetry on PQC adoption. TAI also enables PQC-capable clients to tell PQC-aware servers exactly which PQC trust anchors they recognize, while still supporting traditional roots for compatibility with legacy servers.

In all cases, the long-term goal is a transition to PQC roots and certificate chains. Hybrid signature schemes help bridge the gap, but operators will have to plan carefully for the eventual retirement of traditional and composite roots once PQC adoption is widespread.

7.2. Multiple Transitions and Crypto-Agility

Post-quantum migration is not a single event. There may be multiple transitions over time, as:

* Traditional signature algorithms are gradually retired.
* Initial PQC signature algorithms are standardized and deployed.
* New PQC signature algorithms may replace early ones due to cryptanalysis or efficiency improvements.

Protocols and infrastructures will have to be designed with crypto-agility in mind, supporting:

* Negotiation of standalone PQC algorithms and hybrid signature schemes.
* Phased migration paths, including initial use of hybrid signature schemes, eventual transition to PQC certificates, and later migration to new PQC algorithms as cryptanalysis or security policy guidance evolves.

7.3. Support from Hardware Security Modules (HSMs)

Many organizations rely on HSMs for secure key storage and operations. Challenges include:

* HSMs must be upgraded to support PQC algorithms and, where relevant, composite or dual key management models.
* PQC algorithms often have larger key sizes and signatures, requiring sufficient memory and processing capability in HSMs.
* For dual certificate deployments, HSMs can manage the underlying traditional and PQC private keys independently, and no API changes are required. The security protocol is responsible for coordinating how signatures from both keys are used. By contrast, supporting composite keys and composite signing operations will require HSM and API extensions to represent composite private keys and perform multi-algorithm signing atomically.

Without HSM vendor support for PQC, migration may be delayed or require software-based fallback solutions, which will weaken security.

7.4. Constrained Devices and IoT Environments

Constrained environments, such as IoT devices, present unique challenges for PQC deployment due to limited processing, memory, and bandwidth. Guidance is provided in [I-D.ietf-pquip-pqc-hsm-constrained], including the use of seeds for efficient key generation, PQC-protected firmware updates, and other techniques for enabling PQC in lightweight HSMs and resource-constrained devices.

8. Transition Considerations

Migration to post-quantum authentication will proceed gradually across protocols, products, and organizations. During this period, endpoints may support multiple authentication models (traditional, composite, dual, or PQC) depending on their stage of deployment. The transition requires careful coordination of certificate management, protocol negotiation, and policy enforcement to maintain security and interoperability throughout the migration.

8.1. Transition Logic Overview

The migration to post-quantum authentication will occur in phases as organizations adopt PQC algorithms and update their infrastructures. Because CRQCs may be deployed without public disclosure, continued reliance on traditional algorithms will become increasingly risky. During the transition, dual certificates enable interoperability between PQC-capable and legacy systems, while composite certificates provide hybrid authentication within upgraded ecosystems. These approaches serve as intermediate steps toward PQC deployments. Post-quantum security is achieved only when relying parties stop accepting traditional-only authentication. At that point, authenticated parties can also stop issuing or presenting traditional-only certificates.

8.2. Negotiation and Interoperability

During coexistence, endpoints must be able to discover which authentication mechanisms the peer supports. In most protocols, this is achieved through existing negotiation mechanisms such as, the signature_algorithms extension in [TLS]. Clients advertise their supported algorithms and certificate types, and servers select the strongest mutually supported option or fail authentication if no common algorithm is found.

In hybrid or PQC-capable deployments, there is no security benefit if authentication using only traditional algorithms continues to be accepted, since an attacker can always downgrade to that option. The specific choice between PQC and hybrid mechanisms may be influenced by regulatory guidance, national cryptography policies, or the organization’s appetite for defense-in-depth during early adoption.

Negotiation mechanisms must also include downgrade protection so that an adversary cannot suppress PQC or hybrid options and force a fallback to traditional signatures (see Section 11.1). TLS already provide such protection through transcript binding of the handshake messages that carry the algorithm negotiation results, but new or proprietary protocols have to ensure similar safeguards.

A deployment will typically adopt one of three models, PQC certificates, dual certificates, or composite certificates.

The choice depends on several factors, including:

* Frequency and duration of system upgrades
* The expected timeline for CRQC availability
* Operational flexibility to deploy, enable, and retire PQC algorithms
* Availability of automated certificate provisioning mechanisms such as [ACME] and [CMP]

Deployments with limited flexibility benefit from hybrid signature schemes. These approaches mitigate risks associated with delays in transitioning to PQC and provide an immediate safeguard against zero-day vulnerabilities. Both approaches improve resilience during migration, but they do so in different ways and carry different operational trade-offs.

Hybrid signature schemes enhance resilience during the adoption of PQC by:

* Providing defense in depth: security is maintained as long as either the PQC or traditional algorithm remains unbroken.
* Reducing exposure to unforeseen vulnerabilities: immediate protection against weaknesses in PQC algorithms.

However, each approach comes with long-term implications.

8.3. Composite Certificates

Composite certificate embeds both a traditional and a PQC algorithm into a single certificate and signature. However, once a traditional algorithm is no longer secure against CRQCs, it will have to be deprecated. For discussion of the security impact in security protocols, such as TLS and IKEv2, versus artifact-signing use cases, see Section 8.5.

To complete the transition to a fully quantum-resistant authentication model, operators will need a PQC CA root and CA intermediates, resulting in PQC end-entity certificates.

Protocol configurations will likewise need to be updated to negotiate only PQC-based authentication, ensuring that the entire certification path and protocol handshake are cryptographically resistant to quantum attacks and no longer depend on any traditional algorithms.

8.4. Dual Certificates

When CRQCs become available, the traditional certificate chain will no longer provide secure authentication. At that point, relying parties must stop accepting or requesting traditional certificate chains and validate only PQC-based chains. Authenticated parties will automatically cease using traditional chains once relying parties no longer request them. Dual-certificate deployments therefore defer, but do not avoid, the eventual migration to a PQC environment.

8.5. Loss of Strong Unforgeability in Composite and Dual Certificates

A deployment may choose to continue using a composite or dual certificate configuration even after a traditional algorithm has been broken by the advent of a CRQC. While this may simplify operations by avoiding re-provisioning of trust anchors, it introduces a significant risk: security properties degrade once one component of the hybrid is no longer secure.

In composite certificates, the composite signature will no longer achieve Strong Unforgeability under chosen message attack (SUF-CMA) (see Section 10.1.1 of [PQC-ENGINEERS] and Section 10.2 of [I-D.ietf-lamps-pq-composite-sigs]). A CRQC can forge the broken traditional signature component (s1_) over a message (m). That forged component can then be combined with the valid post-quantum component (s2) to produce a new composite signature (m, (s1_, s2)) that verifies successfully, thereby violating SUF-CMA.

In dual certificate deployments where the client requires both a traditional and a PQC chain, the SUF-CMA property is likewise not achieved once the traditional algorithm is broken.

In protocols such as TLS and IKEv2, a composite signature remains secure against impersonation as long as at least one component algorithm remains unbroken, because verification succeeds only if every component signature validates over the same canonical message defined by the authentication procedure. However, in artifact signing use cases, the break of a single component does not enable forgery of a composite signature but does enable "repudiation": multiple distinct composite signatures can exist for the same artifact, undermining the "one signature, one artifact" guarantee. This creates ambiguity about which composite signature is authentic, complicating long-term non-repudiation guarantees.

Hybrid signature schemes should not be used for artifact signing (such as software packages), since the loss of SUF-CMA makes them unsuitable for long-term non-repudiation. In security protocols, hybrid signature schemes may continue to function for a limited time after a CRQC is realized, since they still provide impersonation resistance as long as one component algorithm remains secure. This situation does not constitute a zero-day vulnerability requiring an immediate upgrade. However, operators will have to plan an orderly migration to PQC certificates in order to restore SUF-CMA security guarantees.

9. Migration Guidance

* Long-term to adopt and deploy:: Dual certificates have been standardized in [RFC9763]. However, at the time of writing, none of the security protocols (e.g., TLS, IKEv2, JOSE/COSE) have adopted this mechanism. The proposals are being discussed in IKEv2 ([I-D.hu-ipsecme-pqt-hybrid-auth]), TLS ([I-D.yusef-tls-pqt-dual-certs]), and in the form of paired certificates with a single certificate ([I-D.bonnell-lamps-chameleon-certs]).
* Medium-term to adopt and deploy: Composite certificates become viable once ecosystem support across PKIX, IPsec, JOSE/COSE, and TLS is mature. Composite ML-DSA is already being standardized in the LAMPS WG ([I-D.ietf-lamps-pq-composite-sigs]) and leveraged in [I-D.reddy-tls-composite-mldsa] for TLS, [I-D.hu-ipsecme-pqt-hybrid-auth] for IPsec/IKEv2, and [I-D.prabel-jose-pq-composite-sigs] for JOSE/COSE.
* Long-to-medium term to adopt and deploy: PQC certificates are the final goal, once PQ algorithms are well-established, trust anchors have been updated, HSMs and devices support PQC operations, and traditional algorithms are fully retired. Work to enable PQC

signatures is already underway in JOSE/COSE [I-D.ietf-cose-dilithium], TLS [I-D.ietf-tls-mldsa], and IPsec [I-D.ietf-ipsecme-ikev2-pqc-auth].

10. Use of SLH-DSA in PQC-Only Deployments

SLH-DSA does not introduce any new hardness assumptions beyond those inherent to its underlying hash functions. It builds upon established cryptographic foundations, making it a reliable and robust digital signature scheme for a post-quantum world. While attacks on lattice-based schemes such as ML-DSA are currently hypothetical, if realized they could compromise the security of those schemes. SLH-DSA would remain unaffected by such attacks due to its distinct mathematical foundations, helping to ensure the ongoing security of systems and protocols that rely on it for digital signatures. Unlike ML-DSA, SLH-DSA is not defined for use in composite certificates and is intended to be deployed directly in PQC certificate hierarchies.

SLH-DSA may be used for both end-entity and CA certificates. It provides strong post-quantum security but produces larger signatures than ML-DSA or traditional algorithms. At security levels 1, 3, and 5, two parameter sets are available:

* "Small" (s) variants minimize signature size, ranging from 7856 bytes (128-bit) to 29792 bytes (256-bit).
* "Fast" (f) variants optimize key generation and signing speed, with signature sizes from 17088 bytes (128-bit) to 29792 bytes (256-bit), but slower verification performance.

Because of these large signatures, SLH-DSA will increase handshake size in protocols such as TLS 1.3 or IKEv2. However, the impact on performance is minimal for long-lived connections or large data transfers, where handshake overhead is amortized over session duration (e.g., DTLS-in-SCTP in 3GPP N2 interfaces, or signature authentication in IKEv2 using PQC [I-D.ietf-ipsecme-ikev2-pqc-auth]).

In deployments where minimizing handshake size is critical, operators may prefer SLH-DSA for root and intermediate certificates while using smaller- signature algorithms (e.g., ML-DSA) in end-entity certificates or in the "CertificateVerify" message.

Mechanisms such as Abridged TLS Certificate Chains [I-D.ietf-tls-cert-abridge] and Suppressing CA Certificates [I-D.kampanakis-tls-scas-latest] reduce handshake size by limiting certificate exchange to only end-entity certificates. In such cases, intermediate certificates are assumed to be known to the peer, allowing the use of larger signature algorithms like SLH-DSA for those certificates without adding overhead to the handshake.

11. Security Considerations

Hybrid signature schemes are designed to provide defense in depth during the migration to PQC. Their goal is to ensure that authentication remains secure as long as at least one of the algorithms in use remains unbroken. However, several important security considerations arise.

11.1. Downgrade Attacks

Implementations must ensure downgrade protection so that an adversary cannot suppress PQC or hybrid schemes and force reliance solely on traditional algorithms. This is especially important in scenarios where a CRQC is available but not publicly disclosed. Without downgrade protection, a MitM attacker could impersonate servers by presenting only traditional certificates even when PQC or hybrid certificates are supported by both peers.

Downgrade protection is critical throughout the migration period, since relying parties may otherwise be tricked into accepting weaker traditional authentication even when PQC or hybrid credentials exist.

In open environments (for example, the Web), there will likely be no single "flag day" for post-quantum authentication. One possible mitigation is the X.509 Post-Quantum/Composite Hosting Continuity (PQCHC) extension [PQCHC], which allows a certificate subject to to signal its intent to continue presenting PQC or composite credentials for a configured continuity period beyond the certificate’s "notAfter" date. Relying parties can use this information to detect downgrade attempts and enforce continuity by rejecting traditional-only certificates during that period.

Other mechanisms may complement this approach. For example, relying parties could maintain and distribute curated lists of domains known to use PQC-capable authentication, similar to mechanisms used by Safe Browsing. Such mechanisms could automatically enforce downgrade resistance for well-known, public domains. For other domains, the relying party might simply cache that a server previously used a PQ certificate.

Together, these mechanisms help ensure that PQC-aware relying parties maintain strong downgrade resistance where possible, while still allowing interoperability with traditional-only authenticated parties during the transition.

11.2. Strong Unforgeability versus Existential Unforgeability

In hybrid signature schemes, once one component algorithm is broken (e.g., the traditional algorithm under a CRQC), the overall scheme no longer achieves SUF-CMA. While Existential Unforgeability under chosen message attack (EUF-CMA) (see Section 10.1.1 of [I-D.ietf-pquip-pqc-engineers]) is still preserved by the PQC component, meaning that an adversary who can obtain signatures on arbitrary messages still cannot forge a valid PQC signature on any new message that was not previously signed. The loss of SUF-CMA means that hybrid mechanisms will have be eventually retired once traditional algorithms are no longer secure.

11.3. Operational Risks

Managing multiple certificate paths (composite, dual, and PQC) increases the risk of misconfiguration and operational errors. For example, relying parties might continue to accept traditional-only certificates after the traditional algorithms are broken, fail to enforce PQC validation policies, or select an incorrect chain when multiple options are available, resulting in validation of weaker authentication than intended. Effective downgrade protection (see Section 11.1) requires relying parties to reject traditional-only certificate paths once post-quantum alternatives are available, regardless of whether authenticated parties continue to support traditional credentials for legacy interoperability.

Clear operational guidance and automated monitoring are essential to minimize these risks. Operators need best practices for certificate lifecycle and migration planning, along with automated checks to ensure PQC chains remain present, valid, and not replaced by weaker alternatives.

12. IANA Considerations

This document has no IANA actions.

13. Acknowledgments

Thanks to Martin McGrath, Suresh P. Nair, Eric Rescorla, and German Peinado for the detailed review.

14. References

14.1. Normative References

[COMPOSITE-ML-DSA]
Ounsworth, M., Gray, J., Pala, M., Klauner, J., and S. Fluhrer, "Composite ML-DSA for use in X.509 Public Key Infrastructure", Work in Progress, Internet-Draft, draft-ietf-lamps-pq-composite-sigs-12, 10 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-lamps-pq-composite-sigs-12>.

[HYBRID-SPECTRUMS]
Bindel, N., Hale, B., Connolly, D., and F. D, "Hybrid signature spectrums", Work in Progress, Internet-Draft, draft-ietf-pquip-hybrid-signature-spectrums-07, 20 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-pquip-hybrid-signature-spectrums-07>.

[I-D.ietf-cose-dilithium]
Prorock, M. and O. Steele, "ML-DSA for JOSE and COSE", Work in Progress, Internet-Draft, draft-ietf-cose-dilithium-09, 12 September 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-cose-dilithium-09>.

[I-D.ietf-ipsecme-ikev2-pqc-auth]
Reddy.K, T., Smyslov, V., and S. Fluhrer, "Signature Authentication in the Internet Key Exchange Version 2 (IKEv2) using PQC", Work in Progress, Internet-Draft, draft-ietf-ipsecme-ikev2-pqc-auth-04, 5 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-ipsecme-ikev2-pqc-auth-04>.

[I-D.ietf-lamps-pq-composite-sigs]
Ounsworth, M., Gray, J., Pala, M., Klauner, J., and S. Fluhrer, "Composite ML-DSA for use in X.509 Public Key Infrastructure", Work in Progress, Internet-Draft, draft-ietf-lamps-pq-composite-sigs-12, 10 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-lamps-pq-composite-sigs-12>.

[I-D.ietf-pquip-pqc-hsm-constrained]
Reddy.K, T., Wing, D., S, B., and K. Kwiatkowski, "Adapting Constrained Devices for Post-Quantum Cryptography", Work in Progress, Internet-Draft, draft-ietf-pquip-pqc-hsm-constrained-01, 4 July 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-pquip-pqc-hsm-constrained-01>.

[I-D.ietf-tls-mldsa]
Hollebeek, T., Schmieg, S., and B. Westerbaan, "Use of ML-DSA in TLS 1.3", Work in Progress, Internet-Draft, draft-ietf-tls-mldsa-01, 26 September 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-mldsa-01>.

[I-D.ietf-tls-trust-anchor-ids]
Beck, B., Benjamin, D., O'Brien, D., and K. Nekritz, "TLS Trust Anchor Identifiers", Work in Progress, Internet-Draft, draft-ietf-tls-trust-anchor-ids-02, 15 September 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-trust-anchor-ids-02>.

[ML-DSA] Massimo, J., Kampanakis, P., Turner, S., and B. Westerbaan, "Internet X.509 Public Key Infrastructure - Algorithm Identifiers for the Module-Lattice-Based Digital Signature Algorithm (ML-DSA)", Work in Progress, Internet-Draft, draft-ietf-lamps-dilithium-certificates-13, 30 September 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-lamps-dilithium-certificates-13>.

[PQCHC] Reddy.K, T., Gray, J., and Y. Sheffer, "X.509 Extensions for PQC or Composite Certificate Hosting Continuity", Work in Progress, Internet-Draft, draft-reddy-lamps-x509-pq-commit-00, 12 October 2025, <https://datatracker.ietf.org/doc/html/draft-reddy-lamps-x509-pq-commit-00>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC9763] Becker, A., Guthrie, R., and M. Jenkins, "Related Certificates for Use in Multiple Authentications within a Protocol", RFC 9763, DOI 10.17487/RFC9763, June 2025, <https://www.rfc-editor.org/rfc/rfc9763>.

[SLH-DSA] Bashiri, K., Fluhrer, S., Gazdag, S., Van Geest, D., and S. Kousidis, "Internet X.509 Public Key Infrastructure: Algorithm Identifiers for SLH-DSA", Work in Progress, Internet-Draft, draft-ietf-lamps-x509-slhdsa-09, 30 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-lamps-x509-slhdsa-09>.

14.2. Informative References

[ACME] Barnes, R., Hoffman-Andrews, J., McCarney, D., and J. Kasten, "Automatic Certificate Management Environment (ACME)", RFC 8555, DOI 10.17487/RFC8555, March 2019, <https://www.rfc-editor.org/rfc/rfc8555>.

[CMP] Brockhaus, H., von Oheimb, D., Ounsworth, M., and J. Gray, "Internet X.509 Public Key Infrastructure -- Certificate Management Protocol (CMP)", RFC 9810, DOI 10.17487/RFC9810, July 2025, <https://www.rfc-editor.org/rfc/rfc9810>.

[DTLS] Rescorla, E., Tschofenig, H., and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", RFC 9147, DOI 10.17487/RFC9147, April 2022, <https://www.rfc-editor.org/rfc/rfc9147>.

[I-D.bonnell-lamps-chameleon-certs] Bonnell, C., Gray, J., Hook, D., Okubo, T., and M. Ounsworth, "A Mechanism for Encoding Differences in Paired Certificates", Work in Progress, Internet-Draft, draft-bonnell-lamps-chameleon-certs-06, 16 April 2025, <https://datatracker.ietf.org/doc/html/draft-bonnell-lamps-chameleon-certs-06>.

[I-D.hu-ipsecme-pqt-hybrid-auth] Hu, J., Morioka, Y., and G. WANG, "Post-Quantum Traditional (PQ/T) Hybrid PKI Authentication in the Internet Key Exchange Version 2 (IKEv2)", Work in Progress, Internet-Draft, draft-hu-ipsecme-pqt-hybrid-auth-02, 1 May 2025, <https://datatracker.ietf.org/doc/html/draft-hu-ipsecme-pqt-hybrid-auth-02>.

[I-D.ietf-pquip-pqc-engineers]
Banerjee, A., Reddy.K, T., Schoinianakis, D., Hollebeek, T., and M. Ounsworth, "Post-Quantum Cryptography for Engineers", Work in Progress, Internet-Draft, draft-ietf-pquip-pqc-engineers-14, 25 August 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-pquip-pqc-engineers-14>.

[I-D.ietf-tls-cert-abridge]
Jackson, D., "Abridged Compression for WebPKI Certificates", Work in Progress, Internet-Draft, draft-ietf-tls-cert-abridge-02, 16 September 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-cert-abridge-02>.

[I-D.kampanakis-tls-scas-latest]
Kampanakis, P., Bytheway, C., Westerbaan, B., and M. Thomson, "Suppressing CA Certificates in TLS 1.3", Work in Progress, Internet-Draft, draft-kampanakis-tls-scas-latest-03, 5 January 2023, <https://datatracker.ietf.org/doc/html/draft-kampanakis-tls-scas-latest-03>.

[I-D.prabel-jose-pq-composite-sigs]
Prabel, L., Shuzhou, S., Gray, J., and T. Reddy.K, "PQ/T Hybrid Composite Signatures for JOSE and COSE", Work in Progress, Internet-Draft, draft-prabel-jose-pq-composite-sigs-04, 22 August 2025, <https://datatracker.ietf.org/doc/html/draft-prabel-jose-pq-composite-sigs-04>.

[I-D.reddy-tls-composite-mldsa]
Reddy.K, T., Hollebeek, T., Gray, J., and S. Fluhrer, "Use of Composite ML-DSA in TLS 1.3", Work in Progress, Internet-Draft, draft-reddy-tls-composite-mldsa-05, 4 July 2025, <https://datatracker.ietf.org/doc/html/draft-reddy-tls-composite-mldsa-05>.

[I-D.yusef-tls-pqt-dual-certs]
Shekh-Yusef, R., Tschofenig, H., Ounsworth, M., Sheffer, Y., Reddy.K, T., and Y. Rosomakho, "Post-Quantum Traditional (PQ/T) Hybrid Authentication with Dual Certificates in TLS 1.3", Work in Progress, Internet-Draft, draft-yusef-tls-pqt-dual-certs-00, 18 June 2025, <https://datatracker.ietf.org/doc/html/draft-yusef-tls-pqt-dual-certs-00>.

[IKEv2] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, DOI 10.17487/RFC5996, September 2010, <https://www.rfc-editor.org/rfc/rfc5996>.

[IKEv2-COMPOSITE-ML-DSA] Hu, J., Morioka, Y., and G. WANG, "Post-Quantum Traditional (PQ/T) Hybrid PKI Authentication in the Internet Key Exchange Version 2 (IKEv2)", Work in Progress, Internet-Draft, draft-hu-ipsecme-pqt-hybrid-auth-02, 1 May 2025, <https://datatracker.ietf.org/doc/html/draft-hu-ipsecme-pqt-hybrid-auth-02>.

[JOSE-COSE-COMPOSITE-ML-DSA] Prabel, L., Shuzhou, S., Gray, J., and T. Reddy.K, "PQ/T Hybrid Composite Signatures for JOSE and COSE", Work in Progress, Internet-Draft, draft-prabel-jose-pq-composite-sigs-04, 22 August 2025, <https://datatracker.ietf.org/doc/html/draft-prabel-jose-pq-composite-sigs-04>.

[PQC-ENGINEERS] Banerjee, A., Reddy.K, T., Schoinianakis, D., Hollebeek, T., and M. Ounsworth, "Post-Quantum Cryptography for Engineers", Work in Progress, Internet-Draft, draft-ietf-pquip-pqc-engineers-14, 25 August 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-pquip-pqc-engineers-14>.

[RELATED-CERTS] Becker, A., Guthrie, R., and M. Jenkins, "Related Certificates for Use in Multiple Authentications within a Protocol", RFC 9763, DOI 10.17487/RFC9763, June 2025, <https://www.rfc-editor.org/rfc/rfc9763>.

[TLS] "*** BROKEN REFERENCE ***".

[TLS-COMPOSITE-ML-DSA] Reddy.K, T., Hollebeek, T., Gray, J., and S. Fluhrer, "Use of Composite ML-DSA in TLS 1.3", Work in Progress, Internet-Draft, draft-reddy-tls-composite-mldsa-05, 4 July 2025, <https://datatracker.ietf.org/doc/html/draft-reddy-tls-composite-mldsa-05>.

Authors’ Addresses

Tirumaleswar Reddy
Nokia
Bangalore
Karnataka
India
Email: k.tirumaleswar_reddy@nokia.com

Dan Wing
Citrix
United States of America
Email: danwing@gmail.com

Yaroslav Rosomakho
Zscaler
Email: yrosomakho@zscaler.com