PQUIP
Internet-Draft
Intended status: Informational
Expires: 1 April 2026

T. Reddy
Nokia
D. Wing
Cloud Software Group

28 September 2025

Guidance for Migration to Composite, Dual, or PQC-Only Authentication
draft-reddy-pquip-pqc-signature-migration-00

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-only 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.

Discussion Venues

This note is to be removed before publishing as an RFC.

Discussion of this document takes place on the Post-Quantum Use In Protocols Working Group mailing list (pqc@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/pqc/.

Source for this draft and an issue tracker can be found at https://github.com/tireddy2/pqc-cert-guidance.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 1 April 2026.

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 the risk of on-path attackers equipped with CRQCs. Such adversaries could break certificate-based mechanisms that rely on traditional algorithms (e.g., RSA, ECDSA), allowing them to impersonate servers and clients, and mount man-in-the-middle (MitM) attacks. In this scenario, attackers could also suppress PQC certificates and present only traditional ones, enabling downgrades. These risks highlight the need to transition certificate-based authentication toward post-quantum security, using hybrid signature schemes as an intermediate step before PQC-only adoption.

The IETF has developed 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 composite signature, combining a traditional and a PQC algorithm [I-D.ietf-lamps-pq-composite-sigs].
* Dual certificates: Two separate certificates, one traditional and one PQC algorithm, issued for the same identity, presented and validated together [RFC9763].

Another approach is using a Post-Quantum certificate,

* PQC-only certificates: A certificate or signature that uses only a PQ algorithm ([I-D.ietf-lamps-dilithium-certificates] for ML-DSA and [I-D.ietf-lamps-x509-slhdsa] for SLH-DSA).

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

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", "dual certificates", and "PQC-only certificates" as introduced in the Introduction.

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 [I-D.ietf-pquip-hybrid-signature-spectrums].

3. Motivation for PQC Signatures

Unlike "Harvest Now, Decrypt Later" attacks that target confidentiality, this risk directly impacts authentication and trust. Once a CRQC is available, the continued use of traditional certificates becomes untenable. In practice, however, the availability of a CRQC may not be publicly disclosed. Similar to a zero-day vulnerability, an adversary could secretly exploit CRQC capabilities to compromise traditional certificates without alerting the wider ecosystem.

Addressing this risk requires replacing traditional signatures with PQC signatures, which in turn demands ecosystem-wide upgrades involving cryptographic libraries, HSMs, TPMs, CAs, intermediate CAs, and dependent protocols. Because these transitions take years of planning, coordination, and investment, preparations will have to begin well before a CRQC is publicly known.

4. Composite certificates

A composite certificate contains both a traditional public key algorithm (e.g., ECDSA) and a post-quantum algorithm (e.g., ML-DSA) within a single X.509 certificate. This design enables both algorithms to be used in parallel, the traditional component ensures compatibility with existing infrastructure, while the post-quantum component introduces resistance against future quantum attacks.

Composite certificates are defined in [I-D.ietf-lamps-pq-composite-sigs]. These combine Post-Quantum algorithms like ML-DSA with traditional algorithms such as RSA-PKCS#1v1.5, RSA-PSS, ECDSA, Ed25519, or Ed448, to provide additional protection against vulnerabilities or implementation bugs in a single algorithm. [I-D.reddy-tls-composite-mldsa] specifies how composite certificates are used for TLS 1.3 authentication. In this case, relying parties validate a single certification path anchored in a multi-algorithm trust anchor, without the need for parallel chains.

4.1. Advantages

* A single certificate chain supports both traditional and PQC algorithms, thereby simplifying certificate management.
* A single composite certificate, conveyed within one certificate chain, reduces protocol message size compared to transmitting multiple separate signatures, each requiring its own certificate chain.
* No need to manage or validate multiple parallel certificate chains.
* No significant modifications to the base protocol are required to support the composite approach.

4.2. Disadvantages

* Requires clients, servers, and CAs to support composite public keys and composite signature verification, which are not widely deployed at the time of writing of the specification.
* Introduces new certificate formats and signature generation and verification mechanisms, requiring updates to PKI infrastructure.
* Requires multiple migration steps, with deployments moving from Traditional-only to Composite, and later from Composite to PQC-only.

5. Dual Certificates

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

5.1. Advantages

* Uses standard, single-algorithm X.509 certificates and chains, maximizing compatibility with existing PKI infrastructures.
* Maintains clear separation between traditional and PQC keys.
* Requires only one migration step, with deployments moving from Traditional-only to Dual certificates, and later removing support for Traditional certificates.
* Better suited for multi-tenancy cases, where different tenants may prefer different combinations of traditional and PQ algorithms, avoiding the need for consensus on a composite set.
* Facilitates simpler future transitions to new PQC algorithms, since a new PQC certificate can simply be issued and paired with an existing certificate, without requiring new composite definitions.

5.2. Disadvantages

* Increases protocol message size due to the transmission of multiple certificate chains and signatures.
* Requires management of multiple certificates.
* Requires significant protocol changes to support validation of two end-entity certificates and to ensure they are cryptographically bound to the same identity, as protocols typically validate only a single certificate.
* Complicates debuggability and troubleshooting, since validation failures may arise from either chain.
* Increases operational cost, as operators must obtain and manage two end-entity certificates from CAs, which can be significant in large-scale deployments.

6. PQC-Only Certificates

PQC-only certificates represent the final stage of migration. They use only a post-quantum algorithm and provide no fallback to traditional algorithms.

6.1. Advantages

* Simpler model without the complexity of hybrid signature scheme.

* Forward-looking design, avoiding eventual deprecation of traditional algorithms.
* Reduced operational burden compared to managing dual or composite certificates.

6.2. Disadvantages

* Risk if a deployed PQC algorithm is broken due to a bug.
* No interoperability with legacy systems that only support traditional algorithms.
* Deployment is only feasible once PQC algorithms are standardized and broadly supported across the ecosystem.

7. Negotiation of Authentication Schemes

During the transition, endpoints may support multiple authentication schemes (e.g., traditional, composite, dual, or PQC-only). Clients advertise their supported schemes using the protocol's negotiation mechanism (for example, the 'signature_algorithms' extension in TLS [RFC8446]), and servers select from the client's list or fail the authentication if no common option is available. In practice, deployments are expected to prefer PQC-only or hybrid signature scheme over traditional ones, with the choice between PQC-only and hybrid signature scheme influenced by regulatory mandates or by whether defense-in-depth is prioritized.

8. Operational and Ecosystem Considerations

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

8.1. 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-only: 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-only 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.

8.2. 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-only certificates, and later migration to new PQC algorithms as cryptanalysis or security policy guidance evolves.
* Protection against downgrade attacks across all transition phases.

8.3. 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.

8.4. 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.

9. Transition Considerations

A deployment will typically adopt one of three models, PQC-only 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 (e.g., ACME [RFC8555], CMP [RFC9810])

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.

9.1. 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 (e.g., TLS, IKEv2) versus artifact-signing use cases, see Section Section 9.3.

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

Protocol configurations (e.g., TLS, IKEv2) 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.

9.2. Dual Certificates

When CRQCs become available, the traditional certificate chain will no longer be secure. At that point, the traditional chain must be removed, and the protocol configuration updated so that only the PQC certificate chain is presented and validated. This requires careful coordination during the transition, since legacy clients that cannot process PQC certificates will lose access once the traditional chain is withdrawn. Dual certificate deployments therefore defer, but do not avoid, the need to update protocol configurations and move to a PQC-only environment.

9.3. 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 [I-D.ietf-pquip-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 (e.g., software packages), since the loss of SUF-CMA makes them unsuitable for long-term non-repudiation. In security protocols (e.g., TLS, IKEv2), 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-only certificates in order to restore SUF-CMA security guarantees.

10. 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-only 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].

11. 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-only 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.

12. 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.

12.1. 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 certificates are supported.

12.2. 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.

12.3. Operational Risks

Managing multiple certificate paths (composite, dual, and PQC-only) increases the risk of misconfiguration and operational errors. For example, a server might continue using a hybrid signature scheme after the traditional algorithm is broken, fail to revoke traditional certificates that are no longer secure, or select the wrong chain for a given client, resulting in clients receiving a certificate path they cannot validate.

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.

13. IANA Considerations

This document has no IANA actions.

14. Acknowledgments

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

15. References

15.1. Normative References

[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-03, 29 August 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-ipsecme-ikev2-pqc-auth-03>.

[I-D.ietf-lamps-dilithium-certificates]
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-12, 26 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-lamps-dilithium-certificates-12>.

[I-D.ietf-lamps-pq-composite-sigs]
Ounsworth, M., Gray, J., Pala, M., Klauテ殤er, 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-08, 20 September 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-lamps-pq-composite-sigs-08>.

[I-D.ietf-lamps-x509-slhdsa]
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>.

[I-D.ietf-pquip-hybrid-signature-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-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>.

[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>.

[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>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/rfc/rfc8446>.

[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>.

15.2. Informative References

[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.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>.

[RFC8555] 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>.

[RFC9810] 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>.

Authors' Addresses

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

Dan Wing
Cloud Software Group Holdings, Inc.
United States of America
Email: danwing@gmail.com