IP Security Maintenance and Extensions
Internet-Draft
Intended status: Standards Track
Expires: 16 October 2026

T. Reddy
Nokia
S. Fluhrer
Cisco Systems

14 April 2026

Hybrid Post-Quantum and Traditional Authentication for IKEv2
draft-reddy-ipsecme-pqt-hybrid-auth-00

Abstract

A Cryptographically Relevant Quantum Computer (CRQC) can break traditional public-key algorithms (e.g., RSA, ECDSA), which are typically used for authentication in IKEv2. Combining the post-quantum ML-DSA signature algorithm with a traditional signature algorithm provides protection against potential weaknesses or implementation flaws in ML-DSA. This draft defines a hybrid PKI authentication method for IKEv2 using composite certificates that ensures authentication remains secure as long as at least one of the component signature algorithms remains unbroken.

About This Document

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

The latest revision of this draft can be found at https://tireddy2.github.io/ipsecme-pqt-hybrid/draft-reddy-ipsecme-pqt-hybrid-auth.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-reddy-ipsecme-pqt-hybrid-auth/.

Discussion of this document takes place on the IP Security Maintenance and Extensions Working Group mailing list (mailto:ipsec@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/ipsec/. Subscribe at https://www.ietf.org/mailman/listinfo/ipsec/.

Source for this draft and an issue tracker can be found at https://github.com/tireddy2/ipsecme-pqt-hybrid.

Status of This Memo

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

This Internet-Draft will expire on 16 October 2026.

Copyright Notice

Table of Contents

1. Introduction

The advent of quantum computing poses a significant threat to current cryptographic systems. Traditional cryptographic algorithms such as RSA, Diffie-Hellman, DSA, and their elliptic curve variants are vulnerable to quantum attacks. During the transition to post-quantum cryptography (PQC), uncertainty remains regarding the long-term security of both traditional and PQC algorithms. Hybrid approaches allow deployments to mitigate risk during this transition period.

Unlike previous migrations between cryptographic algorithms, the decision of when to migrate and which algorithms to adopt is far from straightforward. Even after the migration period, it may be advantageous for an entity’s cryptographic identity to incorporate multiple public-key algorithms to enhance security.

Cautious implementers may opt to combine cryptographic algorithms such that a successful forgery requires breaking each of the component signature algorithms used in the hybrid construction.

This document defines a hybrid authentication mechanism for IKEv2 that combines traditional and post-quantum (PQC) signature algorithms using composite certificates. The security objective of this mechanism is that authentication remains secure as long as at least one of the component signature algorithms in the hybrid construction remains secure against forgery.

The mechanism specified in this document provides a general framework for combining PQC and traditional signature algorithms in IKEv2. Although this document primarily describes combinations involving ML-DSA [ML-DSA] variants and traditional algorithms, the framework is not limited to ML-DSA and can accommodate other PQC and traditional signature algorithm combinations.

The deployment model specified is:

Composite Certificate: A single certificate containing a composite public key and composite signature, as defined in [I-D.ietf-lamps-pq-composite-sigs]. In this model, a single certificate chain and a single AUTH payload are used to provide hybrid authentication assurance.

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.

Cryptographically Relevant Quantum Computer (CRQC): A quantum computer that is capable of breaking real-world cryptographic systems.

Post-Quantum Cryptographic (PQC) algorithms: Asymmetric cryptographic algorithms designed to resist attacks by cryptographically relevant quantum computers (CRQC).

Traditional Cryptographic algorithms: Existing asymmetric Cryptographic algorithms could be broken by CRQC, like RSA, ECDSA, etc.

3. IKEv2 Key Exchange

When hybrid authentication is used to achieve post-quantum security goals, the key exchange mechanism should provide comparable post-quantum resilience; otherwise, the overall security of the IKE SA will still depend on the traditional key exchange.

4. Exchanges

The hybrid authentication exchanges are illustrated in Figure 1, using an ML-KEM key exchange carried in an IKE_SA_INTERMEDIATE exchange as defined in [RFC9242]. The key exchange mechanism is independent of the authentication mechanism defined in this document.

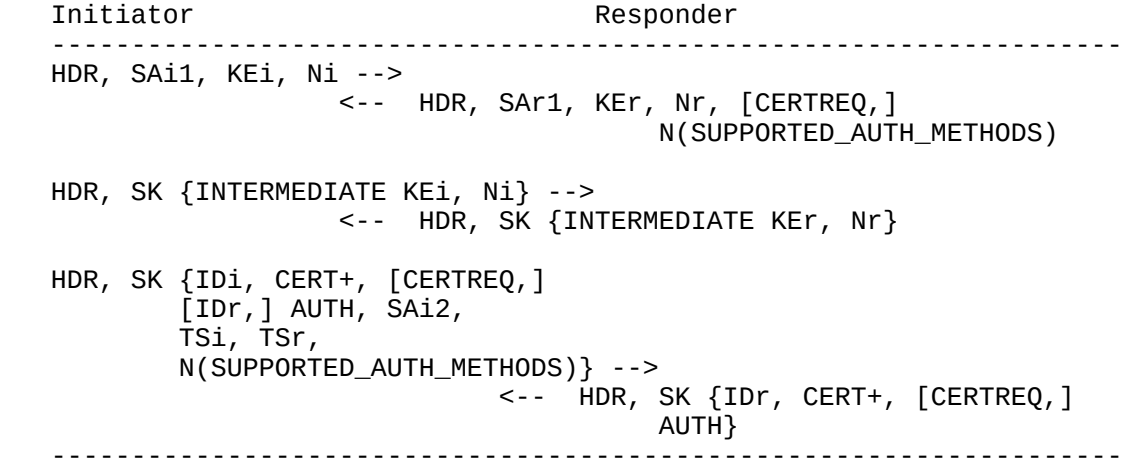

Figure 1: Hybrid Authentication Exchanges with ML-KEM via IKE_SA_INTERMEDIATE

5. Composite Certificate

This draft extends and complements [PQC-AUTH] which defines how to use Post-Quantum Cryptographic (PQC) signature algorithms (such as ML-DSA and SLH-DSA) in IKEv2 authentication. Both drafts share the same overarching goal:

Enable IKEv2 to authenticate peers using PQC signature algorithms, ensuring security against quantum-capable adversaries.

Whereas [PQC-AUTH] specifies PQC-only authentication, this draft specifies how to deploy PQC and traditional algorithms together to provide hybrid assurance during the migration phase.

Both drafts:

* Do not require any changes to IKEv2 base protocol messages.

* Rely on the standard IKEv2 AUTH payload format [RFC7296].

* Use SUPPORTED_AUTH_METHODS ([RFC9593]). In this case, the IKEv2 peers use the SUPPORTED_AUTH_METHODS notification to advertise supported composite signature algorithms.

IKEv2 can use arbitrary signature algorithms as described in [RFC7427], where the "Digital Signature" authentication method replaces older signature authentication methods. Both standalone PQC signature algorithms and composite signature algorithms can be incorporated using the "Signature Algorithm" field in the AUTH payload, as defined in [RFC7427].

For composite signatures, a single AlgorithmIdentifier describes a composite public key and a composite signature that combines multiple constituent algorithms (e.g., a traditional and a PQC algorithm) in accordance with [I-D.ietf-lamps-pq-composite-sigs]. This allows a single certificate and AUTH payload to provide hybrid assurance without requiring multiple exchanges.

AlgorithmIdentifier ASN.1 objects are used to uniquely identify composite schemes, including the full parameter set for each constituent algorithm. This ensures unambiguous selection and verification of composite signature during authentication.

5.1. Composite Certificate Processing

Authentication using composite certificates follows the generic digital signature authentication method defined in [RFC7427] and the AUTH computation defined in Section 2.15 of [RFC7296]. If one or more IKE_SA_INTERMEDIATE exchanges occurred, the signed octets are constructed as specified in [RFC9242].

The end-entity certificate MUST contain a composite public key as defined in [I-D.ietf-lamps-pq-composite-sigs]. The composite signature algorithm used in the AUTH payload MUST correspond to the composite public key algorithm in the certificate. A mismatch between the AUTH signature algorithm and the certificate public key algorithm MUST cause the IKE_SA negotiation to fail.

Signature generation and verification are performed using the composite signature scheme as defined in [I-D.ietf-lamps-pq-composite-sigs]. Any internal hashing or message preprocessing is performed as specified by that document.

6. IKEv2 Fragmentation

Post-quantum signature algorithms and certificate chains may significantly increase the size of IKE_AUTH messages. Implementations supporting the mechanisms defined in this document MUST support IKEv2 Fragmentation as defined in [RFC7383].

7. Negotiation

Note: currently, this section talks mostly about the problems that we'll need to address. Eventually, it'll be updated to talk about the actual mechanism, including the bits-on-the-wire format.

To support brown field upgrades, we will need for an IKE device to be able to support negotiating with devices with only conventional (e.g. RSA) certificates, and with devices with composite certificates (e.g. RSA and ML-DSA). In addition, for the network to be entirely post-quantum safe, devices will need to be able to mandate that composite certificates be used. Furthermore, it would be cleaner if the device sent its policy upfront to the peer, rather than letting it try to negotiate and failing.

For composite certificates, this is straight-forward. A composite certificate can be listed in the SUPPORTED_AUTH_METHODS list as yet another algorithm. A device can decide to list support for both that and RSA, or it could decide to list only support for composite certificates. The existing mechanism in IKE will cleanly decide which is appropriate. The only remaining issue is one of preference (if we have multiple algorithm OIDs that are acceptable to the peer, which one should we use). This is not a security issue; instead, it is a performance issue (preferring composite would allow us to find performance problems earlier).

8. Security Considerations

The hybrid mechanism defined in this document aims to provide authentication security as long as at least one component signature algorithm remains secure against forgery.

The security of general PQ/T hybrid authentication is discussed in [RFC9794]. This document relies on mechanisms defined in [I-D.ietf-lamps-pq-composite-sigs], [RFC7427], and [RFC9593], and the security considerations of those specifications need to be taken into account.

Traditional signature algorithms such as ECDSA, Ed25519, and Ed448 provide existential unforgeability under chosen-message attack (EUF-CMA), which is sufficient for IKEv2 authentication. When used as the traditional component in a composite construction with ML-DSA, these algorithms contribute to defense-in-depth during the transition to post-quantum cryptography, maintaining IKEv2 authentication security as long as at least one component algorithm remains secure.

However, composite signature schemes do not in general preserve strong unforgeability (SUF-CMA) once the traditional component algorithm is broken, for example due to the availability of CRQCs. In such cases, a forged traditional signature component can be combined with a valid post-quantum component to produce a composite signature that verifies successfully, violating SUF. This loss of SUF is inherent to the composite construction and does not impact IKEv2, which relies only on the composite signature verification result.

8.1. Downgrade Considerations

The AUTH computation in IKEv2 signs the IKE_SA_INIT exchange as specified in Section 2.15 of [RFC7296]. Therefore, negotiation signals exchanged during IKE_SA_INIT (such as SUPPORTED_AUTH_METHODS [RFC9593]) are cryptographically bound to the authentication exchange and cannot be modified by an active attacker without causing authentication failure.

If hybrid authentication is required by local policy, implementations MUST enforce that the negotiated authentication method satisfies that policy.

Specifically, if composite authentication is required, receipt of a non-composite certificate or non-composite signature algorithm during IKE_AUTH MUST cause the IKE_SA negotiation to fail.

9. IANA Considerations

None.

10. References

10.1. Normative References

[I-D.ietf-lamps-pq-composite-sigs]
Ounsworth, M., Gray, J., Pala, M., Klauテ殤er, J., and S. Fluhrer, "Composite Module-Lattice-Based Digital Signature Algorithm (ML-DSA) for use in X.509 Public Key Infrastructure", Work in Progress, Internet-Draft, draft-ietf-lamps-pq-composite-sigs-18, 9 April 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-lamps-pq-composite-sigs-18>.

[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-08, 13 April 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-ipsecme-ikev2-pqc-auth-08>.

[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>.

[RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October 2014, <https://www.rfc-editor.org/rfc/rfc7296>.

[RFC7383] Smyslov, V., "Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation", RFC 7383, DOI 10.17487/RFC7383, November 2014, <https://www.rfc-editor.org/rfc/rfc7383>.

[RFC7427] Kivinen, T. and J. Snyder, "Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)", RFC 7427, DOI 10.17487/RFC7427, January 2015, <https://www.rfc-editor.org/rfc/rfc7427>.

[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>.

[RFC9242] Smyslov, V., "Intermediate Exchange in the Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 9242, DOI 10.17487/RFC9242, May 2022, <https://www.rfc-editor.org/rfc/rfc9242>.

[RFC9593] Smyslov, V., "Announcing Supported Authentication Methods in the Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 9593, DOI 10.17487/RFC9593, July 2024, <https://www.rfc-editor.org/rfc/rfc9593>.

10.2. Informative References

[ML-DSA] "Module-Lattice-Based Digital Signature Standard", NIST FIPS-204, State Initial Public Draft, August 2023, <https://csrc.nist.gov/pubs/fips/204/ipd>.

[RFC9794] Driscoll, F., Parsons, M., and B. Hale, "Terminology for Post-Quantum Traditional Hybrid Schemes", RFC 9794, DOI 10.17487/RFC9794, June 2025, <https://www.rfc-editor.org/rfc/rfc9794>.

Acknowledgments

TODO acknowledge.

Authors' Addresses

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

Scott Fluhrer
Cisco Systems
Email: sfluhrer@cisco.com