ipsecme
Internet-Draft
Intended status: Standards Track
Expires: 3 May 2026

H. Jun
Nokia
Y. Morioka
NTT DOCOMO, INC.
W. Guilin
Huawei

30 October 2025

Post-Quantum Traditional (PQ/T) Hybrid PKI Authentication in the Internet Key Exchange Version 2 (IKEv2)
draft-hu-ipsecme-pqt-hybrid-auth-03

Abstract

One IPsec area that would be impacted by Cryptographically Relevant Quantum Computer (CRQC) is IKEv2 authentication based on traditional asymmetric cryptographic algorithms: e.g RSA, ECDSA; which are widely deployed authentication options of IKEv2. There are new Post-Quantum Cryptographic (PQC) algorithms for digital signature like NIST [ML-DSA], however it takes time for new cryptographic algorithms to mature, so there is security risk to use only the new algorithm before it is field proven. This document describes a IKEv2 hybrid authentication scheme that could contain both traditional and PQC algorithms, so that authentication is secure as long as one algorithm in the hybrid scheme is secure.

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://example.com/LATEST. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-hu-ipsecme-pqt-hybrid-auth/.

Discussion of this document takes place on the WG 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/USER/REPO.

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 3 May 2026.

Copyright Notice

Table of Contents

1. changes in -03

* version bump to keep doc alive

2. Changes in -02

* clarify the approach in the document is general
* dropping support for PreHash ML-DSA, change example to Pure Signature ML-DSA
* adding more details in signing process to align with ietf-lamps-pq-composite-sigs-04
* add text in Security Considerations to emphasize prohibit of key reuse
* clarify the both C and S bit MAY be 1 at the same time
* clarify the receiver behavior when the announcement contains no algid
* typo fixes

3. Changes in -01

* Only use SUPPORTED_AUTH_METHODS for algorithm combination announcement, no longer use SIGNATURE_HASH_ALGORITHMS
* add flag field in the announcement
* clarify two types of PKI setup
* add some clarifications on how AUTH payload is computed

4. Introduction

A Cryptographically Relevant Quantum Computer (CRQC) could break traditional asymmetric cryptographic algorithms: e.g RSA, ECDSA; which are widely deployed authentication options of IKEv2. New Post-Quantum Cryptographic (PQC) algorithms for digital signature were recently published like NIST [ML-DSA], however by considering potential flaws in the new algorithm’s specifications and implementations, it will take time for these new PQC algorithms to be field proven. So it is risky to only use PQC algorithms before they are mature. There is more detailed discussion on motivation of a hybrid approach for authentication in Section 1.3 of [I-D.ietf-pquip-hybrid-signature-spectrums].

This document describes an IKEv2 hybrid authentication scheme that contains both traditional and PQC algorithms, so that authentication is secure as long as one algorithm in the hybrid scheme is secure.

Each IPsec peer announces the support of hybrid authentication via SUPPORTED_AUTH_METHODS notification as defined in [RFC9593], generates and verifies AUTH payload using composite signature like the procedures defined in [I-D.ietf-lamps-pq-composite-sigs].

The approach in this document could be a general framework that for all PQC and traditional algorithms, the combinations of ML-DSA variants and traditional algorithms are considered as instantiations of the general framework.

Following two types of setup are covered:

1. Type-1: A single certificate that has composite key as defined in [I-D.ietf-lamps-pq-composite-sigs]

2. Type-2: Two certificates, one with traditional algorithm key and one with PQC algorithm key

5. 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 are thought to be secure against CRQC.

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

6. IKEv2 Key Exchange

There is no changes introduced in this document to the IKEv2 key exchange process, although it MUST be also resilient to CRQC when using along with the PQ/T hybrid authentication, for example key exchange using the PPK as defined in [RFC8784], or hybrid key exchanges that includes PQC algorithm via multiple key exchange process as defined in [RFC9370].

7. Exchanges

The hybrid authentication exchanges is illustrated in an example depicted in Figure 1, using PPK as defined in [RFC8784] during key exchange, however it could be other key exchanges that involves PQC algorithm since how key exchange is done is transparent to authentication.

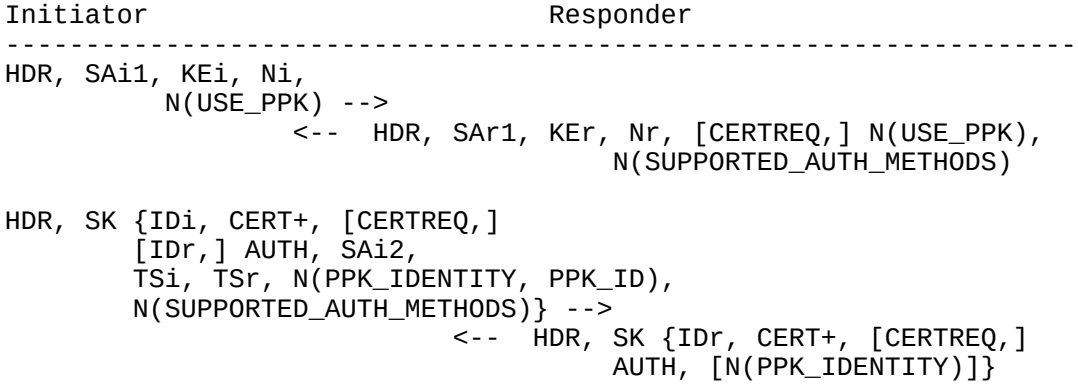

Figure 1: Hybrid Authentication Exchanges with RFC8784 Key Exchange

7.1. Announcement

Announcement of support hybrid authentication is through SUPPORTED_AUTH_METHODS notification as defined in [RFC9593], which includes a list of acceptable authentication methods announcements. this document defines a hybrid authentication announcements with following format:

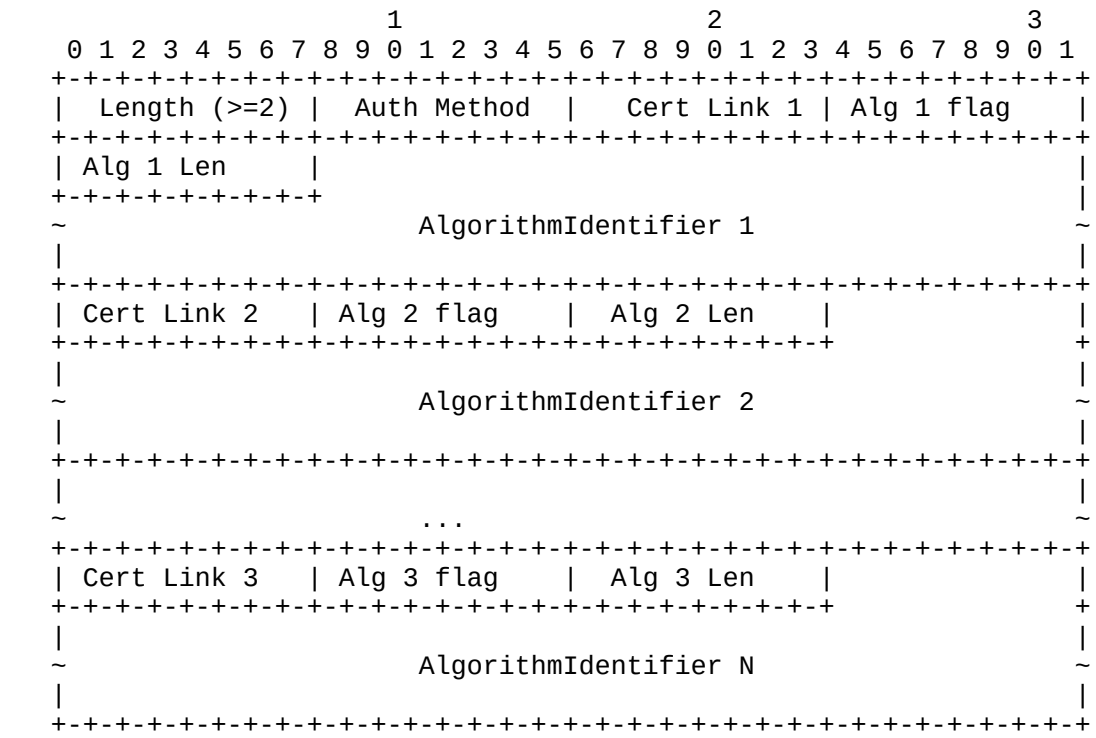

Figure 2: Hybrid Authentication Announcement

The announcement includes a list of N algorithms could be used for hybrid signature

* Auth Method: A new value to be allocated by IANA

* Cert Link N: Links corresponding signature algorithm N with a particular CA. as defined in Section 3.2.2 of [RFC9593]

* Alg N Flag:

  - C: set to 1 if the algorithm could be used in type-1 setup

  - S: set to 1 if the algorithm could be used in type-2 setup

  - Both C and S MAY be set to 1 but MUST NOT set to zero at the same time

  - RESERVED: set to 0

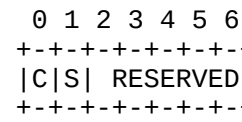

Figure 3: Algorithm Flag

* AlgorithmIdentifier N: The variable-length ASN.1 object that is encoded using Distinguished Encoding Rules (DER) [X.690] and identifies the algorithm of a composite signature as defined in Section 7 of [I-D.ietf-lamps-pq-composite-sigs].

7.1.1. Sending Announcement

As defined in [RFC9593], responder includes SUPPORTED_AUTH_METHODS in IKE_SA_INIT response (and potentially also in IKE_INTERMEDIATE response), while initiator includes the notification in IKE_AUTH request.

Sender includes a hybrid authentication announcement in SUPPORTED_AUTH_METHODS, which contains 0 or N composite signature AlgorithmIdentifiers sender accepts, each AlgorithmIdentifier identifies a combination of algorithms:

* a traditional PKI algorithm with corresponding hash algorithm (e.g. id-RSASA-PSS with id-sha256)

* a PQC algorithm (e.g. id-ML-DSA-44)

  - in case of Hash ML-DSA, there is also a pre-hash algorithm (e.g. id-sha256)

In case of type-2 setup, even though the certificate is not composite key certificate, system still uses a composite signature algorithm that corresponds to the combination of two certificates PKI algorithms and hash algorithm(s).

C and S bits in flag field are set according to whether sender accepts the algorithm combination in type-1/type-2 setup.

Announcement without any AlgorithmIdentifiers signals that there is no particular restrictions on algorithm.

7.1.2. Receiving Announcement

If hybrid authentication announcement is received, and receiver chooses to authenticate itself using hybrid authentication, then based on its local policy and certificates, one AlgorithmIdentifier (which identifies a combination of algorithms) in the hybrid authentication announcement and a PKI setup (type-1 or type-2) is chosen to create its AUTH and CERT payload(s). If there is no AlgorithmIdentifier in the announcement, receiver MAY choose AlgorithmIdentifier just base on its local policy and certificates.

7.2. AUTH & CERT payload

The IKEv2 AUTH payload has following format as defined in Section 3.8 of [RFC7296]:

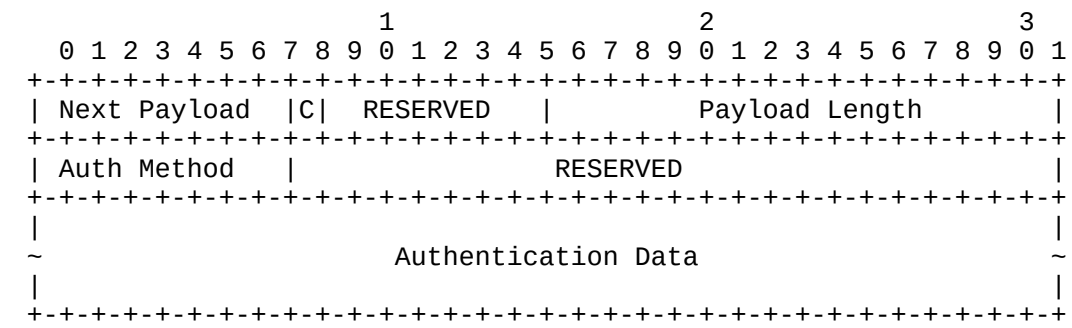

Figure 4: AUTH payload

For hybrid authentication, the AUTH Method has value defined in Section 7.1

The Authentication Data field follows format defined in Section 3 of [RFC7427]:

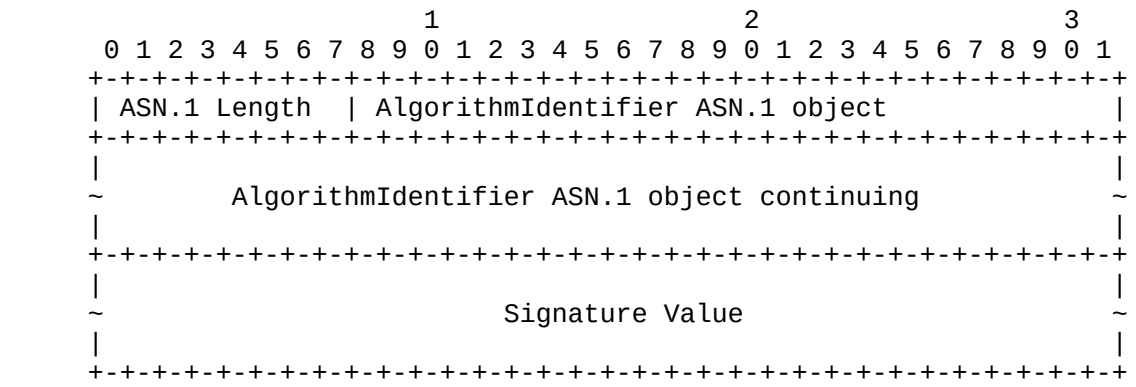

Figure 5: Authentication Data in hybrid AUTH payload

Based on selected AlgorithmIdentifier and setup type, the Signature Value is created via procedure defined in Section 7.2.1, Section 7.2.2.

7.2.1. Type-1

Assume selected AlgorithmIdentifier is A.

1. There is no change on data to be signed, e.g. InitiatorSignedOctets/ResponderSignedOctets as defined in Section 2.15 of [RFC7296]

2. Follow Sign operation identified by A, e.g. Section 4.2.1 of [I-D.ietf-lamps-pq-composite-sigs]. the ctx input is the string of "IKEv2-PQT-Hybrid-Auth". this step outputs the composite signature, a CompositeSignatureValue.

3. CompositeSignatureValue is serialized per Section 4.5 of [I-D.ietf-lamps-pq-composite-sigs], the output is used as Signature Value in the Authentication Data field.

note: in case ML-DSA, only pure signature mode as defined in Section 4.2 of [I-D.ietf-lamps-pq-composite-sigs] is used, the PreHash ML-DSA mode MUST NOT be used, see Section 8.1 of [I-D.ietf-lamps-dilithium-certificates] for the rationale.

Following is an initiator example:

1. A is id-MLDSA44-RSA2048-PSS, which uses pure signature mode id-ML-DSA-44 and id-RSASSA-PSS with id-sha256

2. Follow Section 4.2.1 of [I-D.ietf-lamps-pq-composite-sigs] with following input:

   * sk is the private key of the signing composite key certificate

   * M is InitiatorSignedOctets

   * ctx is "IKEv2-PQT-Hybrid-Auth"

The signing composite certificate MUST be the first CERT payload.

7.2.2. Type-2

The procedure is same as Type-1, use private key of traditional and PQC certificate accordingly; e.g. in Sign procedure define in Section 4.2.1 of [I-D.ietf-lamps-pq-composite-sigs], the mldsaSK is the private key of ML-DSA certificate, while tradSK is the private key of traditional certificate.

With the example in Section 7.2.1:

* mldsaSK is the private key of ML-DSA certificate, tradSK is the private key of the RSA certificate

* M is InitiatorSignedOctets

* ctx is "IKEv2-PQT-Hybrid-Auth"

The signing PQC certificate MUST be the first CERT payload in the IKEv2 message, while traditional certificate MUST be the second CERT payload.

7.2.2.1. RelatedCertificate

In type-2 setup, the signing certificate MAY contain RelatedCertificate extension, then the receiver SHOULD verify the extension according to Section 4.2 of [I-D.ietf-lamps-cert-binding-for-multi-auth], failed verification SHOULD fail authentication.

8. Security Considerations

The security of general PQ/T hybrid authentication is discussed in [I-D.ietf-pquip-hybrid-signature-spectrums].

This document uses mechanisms defined in [I-D.ietf-lamps-pq-composite-sigs], [RFC7427] and [RFC9593], the security discussion in the corresponding RFCs also apply.

One important security consideration mentioned in [I-D.ietf-lamps-pq-composite-sigs] worth repeating here is that component key used in either Section 7.2.1 or Section 7.2.2 MUST NOT be reused in any other cases including single-algorithm case.

9. IANA Considerations

This document requests a value in "IKEv2 Authentication Method" subregistry under IANA "Internet Key Exchange Version 2 (IKEv2) Parameters" registry

10. References

10.1. Normative References

[I-D.ietf-lamps-cert-binding-for-multi-auth]
Becker, A., Guthrie, R., and M. J. Jenkins, "Related Certificates for Use in Multiple Authentications within a Protocol", Work in Progress, Internet-Draft, draft-ietf-lamps-cert-binding-for-multi-auth-06, 10 December 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-lamps-cert-binding-for-multi-auth-06>.

[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-13, 30 September 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-lamps-dilithium-certificates-13>.

[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-12, 10 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-lamps-pq-composite-sigs-12>.

[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>.

[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>.

[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>.

[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>.

[X.690] "Information Technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", ISO/IEC 8825-1:2021 (E), ITU-T Recommendation X.690, February 2021.

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>.

[RFC8784] Fluhrer, S., Kampanakis, P., McGrew, D., and V. Smyslov, "Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security", RFC 8784, DOI 10.17487/RFC8784, June 2020, <https://www.rfc-editor.org/rfc/rfc8784>.

[RFC9370] Tjhai, CJ., Tomlinson, M., Bartlett, G., Fluhrer, S., Van Geest, D., Garcia-Morchon, O., and V. Smyslov, "Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 9370, DOI 10.17487/RFC9370, May 2023, <https://www.rfc-editor.org/rfc/rfc9370>.

Acknowledgments

TODO acknowledge.

Authors' Addresses

Hu, Jun
Nokia
United States of America
Email: jun.hu@nokia.com

Yasufumi Morioka
NTT DOCOMO, INC.
Japan
Email: yasufumi.morioka.dt@nttdocomo.com

Wang, Guilin
Huawei
Singapore
Email: Wang.Guilin@huawei.com