ipsecme
Internet-Draft
Intended status: Standards Track
Expires: 7 July 2026

T. Reddy
Nokia
V. Smyslov
ELVIS-PLUS

3 January 2026

PQ/T Hybrid Composite Key Exchange and Reliable Transport for IKEv2
draft-reddy-ipsecme-ikev2-hybrid-reliable-00

Abstract

The eventual transition to post-quantum key exchange will require elimination of traditional key exchange for reduced protocol complexity and efficiency. IKEv2 therefore requires a mechanism that can operate in a PQC-only environment, without depending on traditional key exchange algorithms (e.g., MODP DH or ECDH). As IKEv2 permits arbitrary combinations of algorithms, unnecessary complexity and insecure hybrid constructions are easily implemented.

This document defines PQ/T hybrid composite key exchange algorithms for IKEv2 and a single combined KE payload that carries both the traditional and post-quantum components. It also leverages the existing IKEv2 reliable transport mechanism so that large PQC key exchange messages can be reliably exchanged over TCP. Together, these mechanisms enable secure and efficient PQ/T hybrid deployments today and provide a clear path for IKEv2 to operate in environments where traditional algorithms have been replaced by PQC algorithms.

About This Document

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

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-reddy-ipsecme-ikev2-hybrid-reliable/.

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

Status of This Memo

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

Copyright Notice

Table of Contents

1. Introduction

The Internet Key Exchange version 2 ([IKEv2]) is a key agreement and security negotiation protocol used for IPsec key establishment. The emergence of CRQCs will render traditional key exchange algorithms obsolete. In a post-quantum future, many systems will be unable to rely on or even ship traditional key exchange algorithms. For IKEv2 to remain deployable in such an environment, it must support PQC-only key exchange without depending on traditional key exchange algorithms.

However, because IKEv2 requires that its first key exchange occur in the IKE_SA_INIT exchange, any PQC KEM public key or ciphertext that does not fit within a single IKE_SA_INIT message (without IP fragmentation) cannot be sent directly in that exchange. When a PQC KEM does not fit in IKE_SA_INIT, the initial exchange must fall back to a traditional key exchange before any PQC public key or ciphertext can be sent. This creates an important limitation: even in a future where CRQCs exist and PQC algorithms are mandatory, IKEv2 peers are forced to use a traditional key exchange in IKE_SA_INIT whenever the PQC KEM exceeds the path MTU. In deployments that do not implement traditional key exchange algorithms, such fallback is unacceptable. Absent reliable transport, PQC-only operation is therefore impossible when PQC key exchange payloads exceed the path MTU. PQC-only deployments remain impossible for any PQC scheme whose keying material does not fit inside an unfragmented IKE_SA_INIT message, prolonging reliance on traditional key exchange algorithms far beyond their acceptable security horizon. While functional, these mechanisms increase round-trip latency and add protocol complexity.

Recent guidance, including that discussed in Section 13.3.2 of [I-D.ietf-pquip-pqc-engineers], notes that protocol designs benefit from allowing a small number of known good configurations that make sense, instead of allowing arbitrary combinations of individual configuration choices that may interact in dangerous ways. Allowing arbitrary combinations of traditional and PQC algorithms can lead to interactions that have not been thoroughly evaluated. However, IKEv2 does not currently follow this guidance as [I-D.ietf-ipsecme-ikev2-mlkem] allows arbitrary combinations of DH groups and ML-KEM parameters through separate traditional and PQC negotiation paths, which may lead to untested or undesirable hybrid constructions and makes it difficult to enforce secure algorithm pairing.

To address these issues, this document introduces:

* PQ/T hybrid composite key exchange algorithms for IKEv2, representing single, fixed, known good combinations of traditional and PQC KEM algorithms.

* A combined KE payload format that carries both traditional and PQC components within a single payload.

* Leverages the IKEv2 reliable transport mechanism defined in [I-D.ietf-ipsecme-ikev2-reliable-transport] so that IKEv2 peers can use TCP for large PQC key exchange messages.

These updates remove the dependency on multi-round negotiation exchanges, eliminate the requirement to use traditional algorithms solely due to MTU limitations, reduce the risks associated with IP fragmentation of large PQC payloads, and provide a clear path for IKEv2 to operate securely and efficiently in a future where only PQC algorithms remain usable.

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 terms defined in [RFC9794]. For the purposes of this document, it is helpful to be able to divide cryptographic algorithms into three classes:

"Traditional asymmetric cryptographic algorithm": An asymmetric cryptographic algorithm based on integer factorisation, finite field discrete logarithms, elliptic curve discrete logarithms, or related mathematical problems.

"Post-quantum asymmetric cryptographic algorithm": An asymmetric cryptographic algorithm that is intended to be secure against attacks using quantum computers as well as classical computers.

"Post-Quantum Traditional (PQ/T) hybrid scheme": A multi-algorithm scheme where at least one component algorithm is a post-quantum algorithm and at least one is a traditional algorithm.

3. Reliable Transport Requirements

PQC-only deployments (i.e., deployments that do not implement any traditional key exchange algorithms) cannot rely on UDP for IKE_SA_INIT when the PQC key exchange payload exceeds the path MTU. In these deployments, fallback to UDP would prevent the use of a PQC-only key exchange. Therefore, when a PQC-only key exchange method is offered or negotiated and the PQC key exchange payload exceeds the path MTU, the initiator MUST start IKE_SA_INIT over TCP, and peers MUST NOT fall back to UDP for IKE_SA_INIT. This requirement follows from the reliable transport mechanism defined in [I-D.ietf-ipsecme-ikev2-reliable-transport].

PQ/T hybrid composite key exchange produces a combined KE payload that may or may not exceed the path MTU, depending on the specific algorithm combination. When the combined KE payload exceeds the path MTU, the PQ/T hybrid composite key exchange MUST NOT be sent over UDP. If TCP is supported, the initiator MAY migrate to TCP and use the PQ/T hybrid composite key exchange; otherwise, the initiator MUST use a PQ/T hybrid non-composite key exchange.

4. PQ/T hybrid composite Key Exchange Algorithms

This document defines PQ/T hybrid composite key-exchange methods that MUST be treated as single, atomic key-exchange identifier. Because IKEv2 treats key-exchange methods (Transform Type 4) as opaque and does not define their internal processing (see Section 2.14 of [IKEv2]), each hybrid method specifies how its traditional and PQC shared secrets are combined.

Each PQ/T hybrid composite key exchange algorithm implies:

* One traditional key exchange component
* One PQC KEM component
* One combined KE payload format
* A PQ/T hybrid key-exchange algorithm specific combiner (see Section 7)

This document defines the following PQ/T hybrid composite key exchange algorithms:

* ecp256-mlkem768
* ecp384-mlkem1024

* curve25519-mlkem768

Each PQ/T hybrid composite key exchange algorithm is represented as a single Transform ID of type 4 (Key Exchange Method) and is negotiated as a whole.

5. Combined Key Exchange Payload

The KE payload carries both components of the PQ/T hybrid composite key exchange algorithm. Specifically, the initiator includes its traditional key exchange public key together with its PQC KEM public key:

KEi = Traditional-Key-Exchange-Public-Key || PQC-KEM-Public-Key

The responder returns its traditional key exchange public key along with the PQC ciphertext:

KEr = Traditional-Key-Exchange-Public-Key || PQC-Ciphertext

Because both the traditional and post-quantum key exchange values are conveyed within a single exchange, no ADDKE transforms are negotiated. Thus, the IKE_INTERMEDIATE and IKE_FOLLOWUP_KE exchanges are not needed for the purpose of key exchange, but peers can negotiate and use IKE_INTERMEDIATE for other purposes.

The lengths of the traditional and PQC components are fixed and defined by the selected PQ/T hybrid composite Transform ID. No additional length fields are included in the KE payload.

6. Reliable Transport Negotiation

PQ/T hybrid composite key exchange requires a reliable transport to avoid IP-layer fragmentation of large PQC key exchange values. Transport selection follows [I-D.ietf-ipsecme-ikev2-reliable-transport]. The initiator MUST follow the rules in the scenarios below.

6.1. SEPARATE_TRANSPORTS Negotiated

If the initiator starts the IKE_SA_INIT exchange over TCP and includes a SEPARATE_TRANSPORTS Notify, and the responder also includes a SEPARATE_TRANSPORTS Notify, then the IKE SA is established using separate transports. In this configuration, all IKE messages are sent over TCP. ESP is sent over UDP (or directly over IP) if possible; if both UDP and IP are blocked, ESP is sent over TCP as described in [RFC9329].

6.2. No SEPARATE_TRANSPORTS

If the initiator starts the IKE_SA_INIT exchange over TCP and the responder accepts the TCP transport but does not include a SEPARATE_TRANSPORTS Notify, then the IKE SA operates in the mode defined by [RFC9329]. In this configuration, both IKE messages and ESP traffic are carried over the same TCP connection. PQ/T hybrid key exchange payloads can be sent in this configuration since the IKE messages are transported reliably.

7. Hybrid Derivation

Each PQ/T hybrid key exchange method defined in this document produces two independent shared secrets: one from the traditional component (K_T) and one from the PQC component (K_PQ). Because IKEv2 treats key exchange methods as opaque, the function that combines these secrets is defined per hybrid KE method. The PQ/T hybrid key exchange methods in this document use the Universal Combiner defined in [I-D.irtf-cfrg-hybrid-kems]. Note that in all PQ/T hybrid composite KE algorithms defined in this document, the PQC component is listed second in the algorithm name but is passed first to the Universal Combiner.

Let:

* K_T = traditional ECDH shared secret

* K_PQ = post-quantum shared secret

The combined secret is computed as:

```
label      = "IKEv2-HYBRID-KE-v1"
K_combined = UniversalCombiner(K_PQ, K_T, CT_PQ, "", PK_PQ,
             PK_T, label)
```

Where:

* K_PQ : PQC shared secret

* K_T : traditional shared secret

* CT_PQ : PQC ciphertext

* PK_PQ : PQC public key

* PK_T : traditional public key

* label : protocol-specific domain separation string

The traditional component does not produce a ciphertext; therefore, the ciphertext argument corresponding to the traditional component is the empty string.

The SKEYSEED value is computed as:

```
SKEYSEED = prf(Ni | Nr, K_combined)
```

This replaces the g^ir shared secret defined in [IKEv2]; all other aspects of SKEYSEED computation remain unchanged.

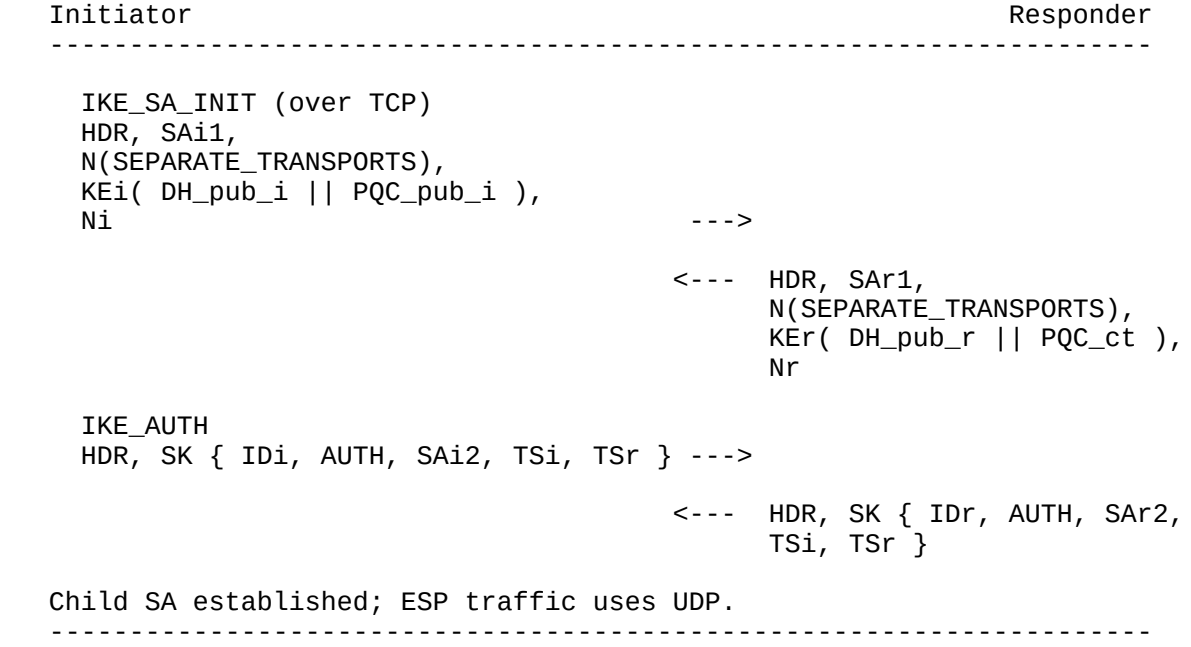
Once SKEYSEED is derived, the remainder of the IKEv2 key hierarchy is computed exactly as specified in [IKEv2].

This construction aligns with the hybrid key exchange approach used in TLS [I-D.ietf-tls-hybrid-design], where traditional and post-quantum secrets are concatenated before key derivation to ensure security against both traditional and quantum adversaries.

8. Example Message Flow

This section illustrates an IKEv2 exchange using a PQ/T hybrid composite key exchange algorithm. The initiator sends a combined KE payload containing both the traditional DH public key and the PQC public key. The responder returns its DH public key together with the PQC ciphertext.

The exchange is shown using TCP, negotiated using the IKEv2 reliable transport mechanism. Both peers include the SEPARATE_TRANSPORTS Notify to indicate support for separate IKE and ESP transports.



9. Security Considerations

PQ/T hybrid composite key exchange algorithms reduce the risk of insecure or unintended algorithm combinations by ensuring that only well-defined, vetted pairs of traditional and PQC algorithms are used. This prevents deployments from constructing ad-hoc hybrids that may provide weaker security than either component alone.

As in standard IKEv2, the KE payload (including both the traditional and PQC components) is integrity-protected and authenticated during the IKE_AUTH exchange. This protection prevents modification of either component by an active attacker.

This document leverages the IKEv2 reliable transport mechanism to avoid IP-layer fragmentation of large PQC payloads. Finally, by enabling a PQC-only key exchange within IKE_SA_INIT and by avoiding fallback to traditional key exchange due solely to MTU constraints, the mechanisms in this document ensure that IKEv2 remains secure and deployable even in environments where traditional algorithms have been deprecated or removed due to their vulnerability to quantum-capable adversaries.

10. IANA Considerations

IANA is requested to assign three new values for the PQ/T hybrid composite key exchange algorithm names "ecp256-mlkem768", "ecp384-mlkem1024", and "curve25519-mlkem768" in the IKEv2 "Transform Type 4 Key Exchange Method Transform IDs" registry and list this document as the reference.

Number	Name	Reference
TBD1	ecp256-mlkem768	[this RFC]
TBD2	ecp384-mlkem1024	[this RFC]
TBD3	curve25519-mlkem768	[this RFC]

Table 1: Updates to the IANA "Transform Type 4 - Key Exchange Method Transform IDs" registry

Acknowledgments

The authors thank Dan Wing for his contributions to this specification.

References

Normative References

[I-D.ietf-ipsecme-ikev2-mlkem]
Kampanakis, P., "Post-quantum Hybrid Key Exchange with ML-KEM in the Internet Key Exchange Protocol Version 2 (IKEv2)", Work in Progress, Internet-Draft, draft-ietf-ipsecme-ikev2-mlkem-03, 29 September 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-ipsecme-ikev2-mlkem-03>.

[I-D.ietf-ipsecme-ikev2-reliable-transport]
Smyslov, V. and T. Reddy.K, "Separate Transports for IKE and ESP", Work in Progress, Internet-Draft, draft-ietf-ipsecme-ikev2-reliable-transport-00, 6 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-ipsecme-ikev2-reliable-transport-00>.

[IKEv2] 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>.

[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>.

[RFC9329] Pauly, T. and V. Smyslov, "TCP Encapsulation of Internet Key Exchange Protocol (IKE) and IPsec Packets", RFC 9329, DOI 10.17487/RFC9329, November 2022, <https://www.rfc-editor.org/rfc/rfc9329>.

Informative References

[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-hybrid-design] Stebila, D., Fluhrer, S., and S. Gueron, "Hybrid key exchange in TLS 1.3", Work in Progress, Internet-Draft, draft-ietf-tls-hybrid-design-16, 7 September 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-hybrid-design-16>.

[I-D.irtf-cfrg-hybrid-kems] Connolly, D., Barnes, R., and P. Grubbs, "Hybrid PQ/T Key Encapsulation Mechanisms", Work in Progress, Internet-Draft, draft-irtf-cfrg-hybrid-kems-07, 20 October 2025, <https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-hybrid-kems-07>.

[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>.

Authors’ Addresses

Tirumaleswar Reddy
Nokia
Bangalore
Karnataka
India
Email: kondtir@gmail.com

Valery Smyslov
ELVIS-PLUS
Russian Federation
Email: svan@elvis.ru