Network Working Group
Internet-Draft
Intended status: Informational
Expires: 5 December 2026

L. Li
Huawei

3 June 2026

Consideration of Robust Multi-KEM Negotiation within IKEv2
draft-li-ipsecme-extensions-for-robust-negotiation-00

Abstract

RFC 9370 specifies a framework for multiple additional key exchanges (ADDKE) in the Internet Key Exchange Protocol Version 2 (IKEv2) to support post-quantum cryptography migration. Under this framework, an initiator can propose multiple ADDKE transform types. In deployment scenarios, initiators may send proposals that contain redundant or overlapping lists of Key Encapsulation Mechanism (KEM) algorithms across different ADDKE transform types. This contribution discusses the implications of these proposals and specifies extended procedures for handling proposed transforms, which may improve negotiation robustness and interoperability by allowing the responder to select a valid set of algorithms without altering the security properties defined in RFC 9370.

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 5 December 2026.

Copyright Notice

Table of Contents

1. Introduction

The migration of the Internet Key Exchange Protocol Version 2 (IKEv2) to Post-Quantum Cryptography (PQC) uses hybrid key exchange mechanisms to mitigate risks from new quantum-resistant algorithms. [RFC9370] establishes a framework for multiple additional key exchanges (ADDKE) during the IKE_SA_INIT exchange. This allows combining classic algorithms (e.g., Elliptic Curve Diffie-Hellman) with one or more post-quantum Key Encapsulation Mechanisms (KEMs) to derive SKEYSEED.

The multi-KEM architecture allows an initiator to group KEM proposals across distinct ADDKE transform types based on their properties, such as placing a shorter KEMs in one transform type and longer length KEMs in another. However, in practice, cryptographic policies are often configured via automated templates or simplified management interfaces. Consequently, initiators may send proposals that are

valid under the syntax of [RFC9370] but contain redundancies, such as populating multiple ADDKE transform types with identical lists of KEM algorithms. If a responder implements strict validation checks based on current specification, this redundancy can cause it to reject the proposal and for the negotiation to fail.

This document provides guidance for handling the overlapping multi-KEM proposals based on best practices. It does not change the security properties defined in RFC, nor does it allow the responder to skip PQC algorithms. Instead, it defines a selection logic for the responder to improve interoperability and robustness during the PQC transition.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. The Architectural Paradigm of Multiple KE Transforms

[RFC7296] defines the negotiation of the IKE Security Association (SA) within the SA payload during the IKE_SA_INIT exchange. The initiator presents one or more proposals. Each proposal consists of multiple transform types, including Encryption (ENCR), Pseudo-Random Function (PRF), Integrity Protection (INTEG), and Diffie-Hellman (DH) group (Transform Type 4).

[RFC9370] extends this negotiation mechanism by introducing seven additional transform types for alternative key exchanges, designated as ADDKE1 (Type 6) through ADDKE7 (Type 12). This arrangement allows the initiator to propose a combination of a classical key exchange along with multiple post-quantum key encapsulation mechanisms (KEMs).

Figure 1 illustrates the payload hierarchy within the IKE_SA_INIT message when multiple key exchanges are proposed.

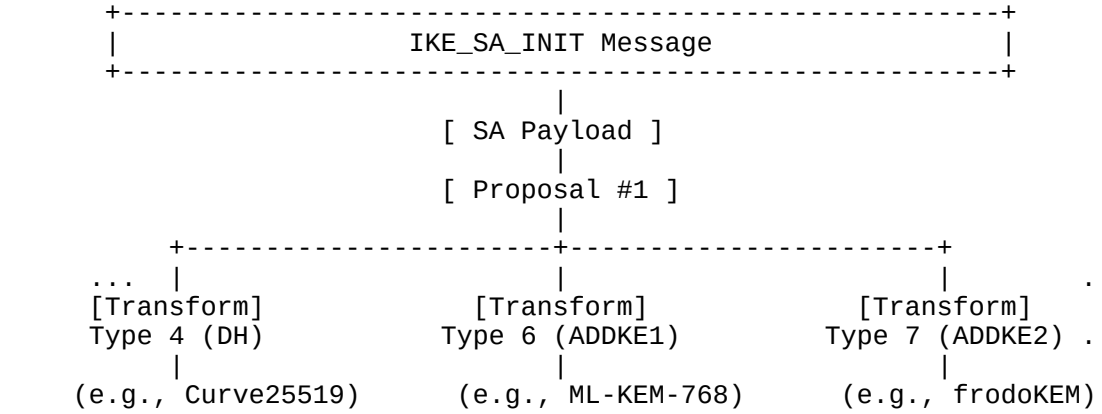

Figure 1: SA Payload Structure with Multiple Key Exchanges

In the current RFC 9370 specification, the initiator populates each ADDKE transform type with a list of supported algorithms. The responder evaluates the proposal and selects exactly one transform for each proposed ADDKE type. The core restriction in RFC 9370 is as follows:

1. the responder's choice MUST NOT contain duplicated algorithms (those with an identical Transform ID and attributes), except for the Transform ID of NONE as duplicate algorithms do not provide additional security and waste message space.

2. Only the ADDKE with indication NONE can be optional, otherwise, one algorithm must be selected in the cooresponding ADDKE.

4. Protocol Extension for Complex Transform Proposals

To illustrate the limitations of rigid transform processing, consider the following two failure scenarios:

1. Scenario 1: The initiator sends a proposal where ADDKE1, ADDKE2, and ADDKE3 each contain the identical list of algorithms: PQ_KEM_1 and PQ_KEM_2. The responder supports both PQ_KEM_1 and PQ_KEM_2. If the responder selects PQ_KEM_1 for ADDKE1 and PQ_KEM_2 for ADDKE2, no unique, non-overlapping algorithm remains available for selection in ADDKE3. Consequently, the responder cannot satisfy the remaining transform type, and the negotiation fails.

2. Scenario 2: The initiator sends a proposal where ADDKE1 contains PQ_KEM_1 and PQ_KEM_2, while ADDKE2 contains only PQ_KEM_2. The responder only supports PQ_KEM_1. The responder can match

PQ_KEM_1 in ADDKE1, but it cannot satisfy ADDKE2 because it does not support PQ_KEM_2. Since selecting a transform for each proposed ADDKE type is mandatory to accept the proposal, the negotiation fails, even though both peers share mutual support for PQ_KEM_1.

Negotiation is an issue that developers may often encounter, and in subsequent sections, we consider extensions to improve robustness. We believe that the success rate of negotiation can potentially be increased to avoid abnormal occurrences.

The scenarios above demonstrate that while the initiator’s proposals are valid under RFC 9370, a sequential or rigid evaluation logic leads to negotiation failures. In Scenario 1, a mathematically valid combination of distinct algorithms exists, but a naive parsing logic lacks the ability to evaluate the proposal holistically. In Scenario 2, the failure is driven by a rigid assignment whereby the responder is unable to optimize its selection across the multiple transform types.

We provide simple extended procedures that allow the responder to evaluate overlapping or redundant proposals deterministically. This extension increases the handshake success rate in complex deployment environments with minimum impacting on the security constraints.

5. Extended Responder Selection Logic (The Core Mechanism)

This section defines the extended selection procedures for a responder processing an IKE_SA_INIT message that contains multiple key exchange transforms. The responder MUST first attempt to process the proposal strictly according to the rules defined in RFC 9370. The extended policies described below are triggered only when the responder cannot satisfy the initiator’s proposal using the standard non-overlapping selection logic.

5.1. Extended Selection Policies

To resolve negotiation failures caused by complex or redundant proposals, the responder MAY be permitted to apply one or both of the following extended selection policies (i.e., consideration 1 and 2):

Consideration 1 (Duplicate Algorithm Selection): The responder can be permitted to select the same algorithm for different key exchange fields (ADDKE transform types). This consideration 1 relaxes the strict prohibition against duplicate selections during the responder’s parsing phase, allowing a successful match when the initiator sends identical lists across multiple transform types.

Consideration 2 (Implicit NONE Selection): The responder can be permitted to select the "NONE" algorithm (Transform ID 0, i.e., Null algorithm) for a specific key exchange field, even if the "NONE" algorithm was not explicitly included in that transform type by the initiator. Consideration 2 effectively treats a specific ADDKE transform type as optional rather than mandatory when no mutually supported algorithm is available in that specific field.

NOTE: Consideration 2 may have security impacts. It is recommended that Consideration 2 be enabled only when Consideration 1 fails to be negotiated. More security analysis is proposed in Section 8.

Above considerations may be implemented, for example, when the responder checks one by one whether ADDKE meets the conditions from ADDKE 1 to 7. When a certain ADDKE (e.g., 2) cannot be met, compatibility policies can be activated. Consideration 1 can be applicable, when the initial algorithm selection for a first key exchange field yields no result; Consideration 2 can be applicable, for example, when the initial algorithm selection for a second key exchange field yields no result, and no mutually supported algorithm is available in that specific field.

5.2. Responder Processing Workflow

Upon receiving an initial algorithm negotiation message (IKE_SA_INIT) comprising ADDKE fields with algorithms, the responder and initiator execute the following procedure:

1. Initial Evaluation: The responder evaluates the algorithms carried in each proposed key exchange field and attempts to select exactly one algorithm per field without duplicates, in strict compliance with RFC 9370.

2. Compatibility Strategy Execution: If the initial evaluation fails to produce a valid combination or results in NONE algorithm (i.e., yields no result), the responder MAY apply the extended compatibility policies. for example, the responder can activate the compatibility mode and utilizes extend selection policy of Consideration 1 and Consideration 2 in order, or a combination of both for each proposed ADDKE field.

3. Response Transmission: Upon successfully concluding the selection using the extended policies, the responder sends the chosen algorithms back to the initiator in the IKE_SA_INIT response message, which includes one or more of the key exchange fields, each carrying the selected algorithm. However, the responder should include the compatibility indication in the message or use an out-of-band method to indicate to the initiator that an extended compatibility consideration has been adopted.

4. Key Generation: The initiator receives the response, accepts the responder's selected algorithms (including duplicates or NONE, as permitted by the extended policies by informed indication from responder), and utilizes the associated key materials to generate the SKEYSEED used for establishing the secure connection. The peers then proceed other procedure such as the IKE_AUTH to complete the IPsec connection establishment. at least two algorithms/keys materials should be included if it is applicable for the PQC hybrid key exchange establishing the secure connection.

6. Annex: Multi-KEM ADDKE proposals and Boundary Conditions

This annex provides profiles for resolving complex boundary conditions during multi-KEM negotiation. It serves as a deterministic reference for implementers to ensure interoperability when applying the extended responder selection logic defined in Section 5.

6.1. Profile 1: Complete Overlap with Limited Responder Support

Boundary Condition: The initiator proposes identical lists of algorithms across multiple ADDKE types, but the responder supports only a single algorithm from the proposed lists.

Example Proposal:

* ADDKE1: PQ_KEM_A, PQ_KEM_B

* ADDKE2: PQ_KEM_A, PQ_KEM_B

Responder Capability: Supports only PQ_KEM_A.

Deterministic Outcome: Under standard RFC 9370 rules, this negotiation fails. Utilizing the compatibility strategy, the responder triggers Consideration 1 (Duplicate Algorithm Selection). The responder selects PQ_KEM_A for ADDKE1 and PQ_KEM_A for ADDKE2. The responder sends this selection back with the compatibility indication. SKEYSEED is derived using the classical DH algorithm and the duplicated PQ_KEM_A materials.

6.2. Profile 2: Subset Overlap Requiring Implicit NONE

Boundary Condition: The initiator proposes different but overlapping lists without explicitly including the NONE algorithm, and the responder cannot satisfy all ADDKE types using Consideration 1 alone.

Example Proposal:

* ADDKE1: PQ_KEM_A, PQ_KEM_B

* ADDKE2: PQ_KEM_C

Responder Capability: Supports PQ_KEM_B only.

Deterministic Outcome: The responder selects PQ_KEM_B for ADDKE1. For ADDKE2, since PQ_KEM_C is not supported and Consideration 1 cannot be applied (PQ_KEM_B was not proposed in ADDKE2), the responder evaluates Consideration 2. The responder selects the Implicit NONE algorithm (Transform ID 0) for ADDKE2. The negotiation succeeds with one classical DH algorithm and one PQC algorithm (i.e., PQ_KEM_B).

6.3. Profile 3: Explicit NONE and Fallback Interaction

Boundary Condition: The initiator explicitly includes the NONE algorithm in some ADDKE fields but omits it in others, creating an asymmetrical fallback matrix.

Example Proposal:

* ADDKE1: PQ_KEM_A, NONE

* ADDKE2: PQ_KEM_B

Responder Capability: Supports PQ_KEM_C only.

Deterministic Outcome: The responder cannot match PQ_KEM_A or PQ_KEM_B. For ADDKE1, the responder selects the explicitly provided NONE algorithm according to standard RFC 9370 parsing. For ADDKE2, the responder triggers Consideration 2 (Implicit NONE Selection) and selects NONE. Both ADDKE fields resolve to NONE.

NOTE: While this resolution is syntactically valid under the extended policies, it reduces the exchange to classical DH only. Implementations MUST consult their local security policies to determine if an IPsec connection without quantum-secure key materials should be established or dropped.

6.4. Profile 4: Consideration Priority and Tie-Breaking

Boundary Condition: The proposal structure allows the responder to resolve the negotiation using either Consideration 1 or Consideration 2. A deterministic tie-breaker is required.

Example Proposal:

* ADDKE1: PQ_KEM_A

* ADDKE2: PQ_KEM_A

Responder Capability: Supports PQ_KEM_A.

Deterministic Outcome: The responder can apply Consideration 1 (select PQ_KEM_A for both) or Consideration 2 (select PQ_KEM_A for ADDKE1 and Implicit NONE for ADDKE2). According to the order defined in Section 4, the responder SHALL prioritize Consideration 1 over Consideration 2. Therefore, the responder selects PQ_KEM_A for both fields. Consideration 2 is strictly a fallback when duplication cannot satisfy the proposal.

7. IANA Considerations

This document has no IANA considerations.

8. Security Considerations

This document introduces extended negotiation strategies that alter the algorithm selection logic but do not modify the underlying cryptographic primitives or key derivation functions defined in RFC 9370. The primary security consideration is that the interoperability introduced by these extensions may result in an overall security strength lower than the initiator’s optimal proposal.

When Consideration 1 (Duplicate Algorithm Selection) is applied, the same Post-Quantum KEM is utilized for multiple ADDKE transform types. While this resolves parsing failures, it eliminates the defense-in-depth property intended by hybrid multi-KEM architectures. If a cryptographic weakness is discovered in the duplicated algorithm, all instances of it within the exchange are compromised. The resulting security level is equivalent to negotiating that specific PQC algorithm only once alongside the classical DH algorithm.

When Consideration 2 (Implicit NONE Selection) is applied, the responder essentially ignores an ADDKE transform type. This may weaken the overall entropy of the SKEYSEED compared to the initiator’s original intent. If a peer relies heavily on this policy, it risks downgrading the connection to classical cryptography only (e.g., Profile 3 in Annex). Implementations MUST ensure that local security policies define the minimum acceptable cryptographic threshold, and MUST abort the connection if the resolved multi-KEM combination falls below this defined threshold.

Because these compatibility policies evaluate unauthenticated payloads during the IKE_SA_INIT exchange, an active MITM attacker could theoretically modify the proposals to force the responder into applying Consideration 1 or 2. However, to comply with RFC 7296 and RFC 9370, the entire contents of the IKE_SA_INIT messages are cryptographically bound and verified during the subsequent IKE_AUTH exchange. Any tampering intended to force a fallback or downgrade will result in a MAC validation failure, fully mitigating this attack vector.

9. References

9.1. Normative References

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

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

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

9.2. Informative References

Author’s Address

Lun Li
Huawei
Email: lilun20@huawei.com