IP Security Maintenance and Extensions
Internet-Draft
Intended status: Standards Track
Expires: 8 January 2026

G. Wang, Ed.
Huawei Int. Pte Ltd
L. Bruckert
secunet Security Networks
V. Smyslov
ELVIS-PLUS

7 July 2025

Post-quantum Hybrid Key Exchange in the IKEv2 with FrodoKEM
draft-wang-ipsecme-hybrid-kem-ikev2-frodo-01

Abstract

Multiple key exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2) [RFC9370] specifies a framework that supports multiple key encapsulation mechanisms (KEMs) in the Internet Key Exchange Protocol Version 2 (IKEv2) by allowing up to 7 layers of additional KEMs to derive the final shared secret keys for IPsec protocols. The primary goal is to mitigate the “harvest now and decrypt later” threat posed by cryptanalytically relevant quantum computers (CRQC). For this purpose, usually one or more post-quantum KEMs are performed in addition to the traditional (EC)DH key exchange. This draft specifies how the post-quantum KEM FrodoKEM is instantiated in the IKEv2 as an additional key exchange mechanism.

[EDNOTE: IANA KE code points for FrodoKEM may need to be assigned, as the code points for ML-KEM has been considered in [I-D.KR24].]

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 8 January 2026.

Table of Contents

1. Introduction

1.1. Notes of Change

Two main changes have been made in version 01, as a response to comments received at 122 meeting:

* Restructured the draft.

* Reduced the point codes from 12 to 6 (eFrodoKEM).

1.2. Introduction

Cryptographically-relevant quantum computers (CRQC) pose a threat to cryptographically protected data. In particular, the so-called harvest-now-and-decrypt-later (HNDL) attack is considered an imminent threat. To mitigate this threat the concept of hybrid key encapsulation mechanisms (KEMs) has been proposed to achieve secure key exchange if at least one of the KEMs is still secure. “Multiple key exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2) [RFC9370] specifies a framework to perform hybrid key encapsulation in the IKEv2 by allowing multiple key exchanges to take place for deriving shared secret keys during a Security Association (SA) setup. Essentially, this specification employs the IKE_INTERMEDIATE exchange, which is a new IKEv2 message introduced in “Intermediate Exchange in the Internet Key Exchange Protocol Version 2 (IKEv2)” [RFC9242], so that multiple key exchanges can be run to establish an IKE SA via exchanging additional PQ public keys and ciphertexts between a client and a server. RFC 9370 also introduces IKE_FOLLOWUP_KE, a new IKEv2 exchange for realizing the same purpose when the IKE SA is being rekeyed or additional Child SAs are created.

However, [RFC9370] just specifies the framework of hybrid KEMs and has to be been instantiated for concrete KEMs by separate documents. [I-D.KR24] describes how the framework given by [RFC9370] can be run with the ML-KEM [FIPS203], previously called Kyber, which has been standardized by NIST in August 2024. However, on the one hand, [RFC9370] allows up to 7 layers of additional KEMs to derive final shared secret keys for the IKEv2. On the other hand, for some applications (e.g. financial services) demanding high security level, additional PQ KEMs may be desired for use with [RFC9370]. Currently, ISO is standardizing three PQ KEM algorithms (EDNOTE: we may want to change the wording since the ISO standard will be finished eventually): Kyber, FrodoKEM, and Classic McEliece. Note that FrodoKEM [FrodoKEM] [I-D.LBES25] is unstructured lattice based KEM, whose security is more conservative compared to ML-KEM, which is based on structured lattice. Therefore, this draft is motivated to describe concretely how the frame of hybrid KEMs for the IKEv2 specified in RFC 9370 can be instantiated with FrodoKEM. FrodoKEM should be used together with a traditional key exchange mechanism such as ECDH and in addition, may be used with further KEMs, e.g. ML-KEM.

Here are a few reasons for explaining why such diversity of KEMs is important for the IKEv2 (and also other security protocols).

* The availability of various PQ algorithms is beneficial to applications as different PQ algorithms could be selected according to practical performance and security requirements.

* Generally speaking, post-quantum algorithms are still not mature yet. Some algorithms may turn out to be insecure after a number of years' study and/or standardization. An example is SIKE, which had been in the NIST standardization progres for several years until it was totally broken in July of 2022 [CD22].

* Cryptographic agility shall play a crucial role in the PQ migration [OPM23]. To facilitate cryptographic agility, not only should the systems and protocols be engineered agile but also there should be a good number of standardized PQC algorithms available, which may be based on different hard problems.

However, the performance of FrodoKEM is not as good as ML-KEM. In particular, the sizes of pulic key and ciphtertext of FrodoKEM are roughly 10 times larger than those of ML-KEM. Consequently, this will almost unavoidably trigger IKE fragmentation.

2. Requirements Language

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.

3. KEMs and FrodoKEM

3.1. KEMs

Key encapsulation mechanism (KEM) is a kind of key exchange, which allows one entity to encapsulate a secret key under a (long-term or ephemeral) public key of another entity. By following the definiton given in [I-D.KR24], a KEM consists of three algorithms:

* KeyGen(k) -> (pk, sk): A probabilistic key generation algorithm, which generates a public encapsulation key pk and a secret decapsulation key sk, when a security parameter k is given.

* Encaps(pk) -> (ct, ss): A probabilistic encapsulation algorithm, which takes as input a public encapsulation key pk and outputs a ciphertext ct and shared secret ss.

* Decaps(sk, ct) -> ss: A decapsulation algorithm, which takes as input a secret decapsulation key sk and ciphertext ct and outputs a shared secret ss.

3.2. FrodoKEM

FrodoKEM [I-D.LBES25] is one of three KEMS in the process of ISO standardization [FrodoKEM]. Its security is based on a well-studied hard problem in unstructured lattices, called the learning with errors problem. The algorithm details of FrodoKEM are specified in [I-D.LBES25].

FrodoKEM has two main variants: a "standard" variant and an "ephemeral" variant. As specified in Section of 8 in [I-D.LBES25], "standard FrodoKEM is recommended for applications in which the number of ciphertexts produced for a single public key is expected to be equal or greater than 2^8". "Ephemeral FrodoKEM MUST be used for applications in which that same figure is expected to be smaller than 2^8". In this document, FrodoKEM is used for ephemeral key exchange in the IKEv2 and one temporarily generated public key is expected to be used just once. So, only eFrodoKEM, which stands for Ephemeral FrodoKEM, SHALL be used in this draft.

3.3. Comparison to ML-KEM

ML-KEM and FrodoKEM are two well-known post-quantum KEMs based on lattices. More specifically, ML-KEM [FIPS203], originally called Kyber, has been standardized as the only one KEM scheme by NIST in August of 2024. It is a Module-Lattice based Key-Encapsulation Mechanism, so called ML-KEM. ML-KEM is also specified as an Internet Draft in IETF [I-D.Kyber24].

However, the perfomace of FrodoKEM is not as good as ML-KEM. Specifically, as shown in Table 1, the sizes of pulic key and ciphtertext of FrodoKEM are roughly 10 times larger than those of ML-KEM. Consequently, this will almost unavoidably trigger IKE fragmentation [RFC7383] [RFC9242], when FrodoKEM is used in the IKEv2.

Algorithms	secret key sk	public key pk	ciphterext ct	shared secret ss
ML-KEM-512	800	1,632	768	32
ML-KEM-768	1,184	2,400	1,088	32
ML-KEM-1024	1,568	3,168	1,568	32
eFrodoKEM-640	19,888	9,616	9,750	16
eFrodoKEM-976	31,296	15,632	15,744	24
eFrodoKEM-1344	43,088	21,520	21,632	32

Table 1: Size (in bytes) of keys and ciphertexts of ML-KEM and eFrodoKEM

4. FrodoKEM in the IKEv2

4.1. FrodoKEM in IKE_INTERMEDIATE

As specified in [RFC9370], to run FrodoKEM (or any PQ KEM) in the IKEv2, both the initiator and the responder MUST declare their support of both the ADDKE Transform Types and the IIKE_INTERMEDIATE exchange. After that, the initiator SHALL present its intended FrodoKEM variants via one or more ADDKE Transform Types.

Following general exmaples given in Appendix A of [RFC9370], here is an example to show that the initiator proposes to use additional key exchanges for establishing an IKE SA. Here, the initiator proposes three sets of additional key exchanges. Namely, the first set is TBD36 (ml-kem-768), TBD37 (ml-kem-1024) [I-D.KR24] or NONE; the second set is TBD40 (eFrodoKEM-976-<AES>), TBD41 (eFrodoKEM-976-<SHAKE>) or NONE; and the third set is TBD43 (eFrodoKEM-1344-<SHAKE>) or NONE (refer to Section 6). As all of the three additional key exchanes are optional, the responder can choose NONE for some or all of the additional exchanges if the proposed key exchange methods are not supported or for whatever reasons the responder decides not to perform the additional key exchange.

```
Initiator                       Responder
-------------------------------------------------------------------
HDR(IKE_SA_INIT), SAi1(.. ADDKE*...), --->
KEi(Curve25519), Ni, N(IKEV2_FRAG_SUPPORTED),
N(INTERMEDIATE_EXCHANGE_SUPPORTED)
    Proposal #1
    Transform ENCR (ID = ENCR_AES_GCM_16,
                    256-bit key)
    Transform PRF (ID = PRF_HMAC_SHA2_512)
    Transform KE (ID = Curve25519)
    Transform ADDKE1 (ID = TBD36)
    Transform ADDKE1 (ID = TBD37)
    Transform ADDKE1 (ID = NONE)
    Transform ADDKE2 (ID = TBD40)
    Transform ADDKE2 (ID = TBD41)
    Transform ADDKE2 (ID = NONE)
    Transform ADDKE3 (ID = TBD43)
    Transform ADDKE3 (ID = NONE)

                  <--- HDR(IKE_SA_INIT), SAr1(.. ADDKE*...),
                       KEr(Curve25519), Nr, N(IKEV2_FRAG_SUPPORTED),
                       N(INTERMEDIATE_EXCHANGE_SUPPORTED)
                       Proposal #1
                         Transform ENCR (ID = ENCR_AES_GCM_16,
                                         256-bit key)
                         Transform PRF (ID = PRF_HMAC_SHA2_512)
                         Transform KE (ID = Curve25519)
                         Transform ADDKE1 (ID = TBD36)
                         Transform ADDKE2 (ID = TBD40)
                         Transform ADDKE3 (ID = NONE)

HDR(IKE_INTERMEDIATE), SK {KEi(1)(TBD36)} -->
                  <--- HDR(IKE_INTERMEDIATE), SK {KEr(1)(TBD36)}
HDR(IKE_INTERMEDIATE), SK {KEi(2)(TBD40)} -->
                  <--- HDR(IKE_INTERMEDIATE), SK {KEr(2)(TBD40)}

HDR(IKE_AUTH), SK{ IDi, AUTH, SAi2, TSi, TSr } --->
                  <--- HDR(IKE_AUTH), SK{IDr, AUTH, SAr2,TSi, TSr}
```

Fig. 1 Hybrid KEMs of ECDH, TBD36 (ml-kem-768), and TBD40 (eFrodoKEM-976-<AES>)

In the above example, the responder chooses to run two additional key exchanges. Namely, it selects TBD36 (ml-kem-768), TBD40 (eFrodoKEM-976-<AES>), and NONE, respectively for the first, second, and third additional key exchanges. According to the IKEv2 specification [RFC7296], a set of keying materials can be derived, in particular SK_d, SK_a[i/r], and SK_e[i/r], when the IKE_SA_INIT exchange has been completed by the initiator and the responder with a successful execution of ECDH based on the curve 25519. After that, both peers

will perform an IKE_INTERMEDIATE exchange, carrying TBD36 payload, which is protected with SK_e[i/r] and SK_a[i/r] keys. After the completion of this IKE_INTERMEDIATE exchange, the SKEYSEED is updated using SK(1), which is the TBD36 shared secret. Next, an IKE_INTERMEDIATE exchange for TBD40 payload will be performed so that the SKEYSEED will be updated again.

After the completion of both IKE_INTERMEDIATE exchanges for TBD36 and TBD43, the initiator and the responder will continue the IKE_AUTH exchange phase.

4.2. FrodoKEM in IKE_FOLLOWUP_KE

FrodoKEM can also be used for creating additional Child SAs and rekeying the IKE SA or Child SAs. FrodoKEM may be used as the only key exchange in CREATE_CHILD_SA exchange or as an additional key exchange method. In the latter case, the IKE_FOLLOWUP_KE exchange as defined in [RFC9370] is used.

IKE_FOLLOWUP_KE is an additional exchange for the purpose of using multiple key exchanges with the CREATE_CHILD_SA Exchange. If the use of additional key exchange methods is negotiated in the CREATE_CHILD_SA exchange, these are performed subsequently in a series of IKE_FOLLOWUP_KE exchanges. After all key exchanges are completed, SKEYSEED or KEYMAT are computed as specified in section 2.2.4 of [RFC9370].

5. Security Considerations

Basically, security considerations from [RFC7383], [RFC9242] and [RFC9370] apply to hybrid KEM exchange of ECDH, ML-KEM, and FrodoKEM described in this draft.

In additon, due to the fragmentation of public key and cipthertext of the IKE message when FrodoKEM is hybrided, the performance of the IKEv2 may be affected and the chance of re-transmision of IKE packet could become higher in some networking secnarios.

Further security analysis will be updated later.

6. IANA Considerations

In total, FrodoKEM has 12 variants. Namely, 3 security levels for NIST Levels 1, 3, and 5; the pseudorandom generate (PRG) using AES128 or SHAKE 128; and the KEM public key can be a long-term key (standard mode) or a short-term key (ephemeral mode). As stated in Section 3.2, this document specifies only eFrodoKEM for the IKEv2 ephemeral key exchange. Therefore, this draft is to asking 6 values

for registration in the "Transform Type 4 - Key Exchange Method Transform IDs" registry [IANA-IKEv2], maintained by IANA. Namely, they are: "eFrodoKEM-640-<AES>", "eFrodoKEM-640-<SHAKE>", "eFrodoKEM-976-<AES>", "eFrodoKEM-976-<SHAKE>", "eFrodoKEM-1344-<AES>", and "eFrodoKEM-1344-<SHAKE>".

Table 2 below gives the list of 6 IANA values for the 6 versions of eFrodoKEM. The Recipient Tests field should point to this document as well.

Number	Name	Status	Recipient Tests	Reference
TBD38	eFrodoKEM-640 -<AES>		[TBD, this draft]	[TBD, this draft]
TBD39	eFrodoKEM-640 -<SHAKE>		[TBD, this draft]	[TBD, this draft]
TBD40	eFrodoKEM-976 -<AES>		[TBD, this draft]	[TBD, this draft]
TBD41	eFrodoKEM-976 -<SHAKE>		[TBD, this draft]	[TBD, this draft]
TBD42	eFrodoKEM-1344 -<AES>		[TBD, this draft]	[TBD, this draft]
TBD43	eFrodoKEM-1344 -<SHAKE>		[TBD, this draft]	[TBD, this draft]

Table 2: Updates to the IANA "Transform Type 4 - Key Exchange"

7. Acknowledgments

To be added later.

8. Normative References

[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/info/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/info/rfc8174>.

[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/info/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/info/rfc7383>.

[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/info/rfc9242>.

[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/info/rfc9370>.

[IANA-IKEv2] "Internet Key Exchange Version 2 (IKEv2) Parameters", the Internet Assigned Numbers Authority (IANA). , <https://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml>.

[FrodoKEM] Alkim, E., Bos, J. W., Ducas, L., Longa, P., Mironov, I., Naehrig, N., Nikolaenko, V., Peikert, C., Raghunathan, A., and D. Stebila, "FrodoKEM: Learning With Errors Key Encapsulation", Preliminary Standardization Proposal submitted to ISO , December 2024, <https://frodokem.org/files/FrodoKEM_standard_proposal_20241205.pdf>.

9. Informative References

[I-D.D24] F. Driscoll, F., "Terminology for Post-Quantum Traditional Hybrid Schemes", Work in Progress, Internet-Draft, February 2024, <https://datatracker.ietf.org/doc/draft-ietf-pquip-pqt-hybrid-terminology/>.

[I-D.KR24] Kampanakis, K. and G. Ravago, "Post-quantum Hybrid Key Exchange with ML-KEM in the Internet Key Exchange Protocol Version 2 (IKEv2)", Work in Progress, Internet-Draft, November 2024, <https://datatracker.ietf.org/doc/draft-kampanakis-ml-kem-ikev2/>.

[I-D.Kyber24] Schwabe, P. and B. Westerbaan, "Kyber Post-Quantum KEM", Work in Progress, Internet-Draft, January 2024, <https://datatracker.ietf.org/doc/draft-cfrg-schwabe-kyber/>.

[OPM23] Ott, D., Paterson, K., and D. Moreau, "Where Is the Research on Cryptographic Transition and Agility?", Communications of the ACM, 66(4): 29-32, January 2023.

[I-D.LBES25] Longa, P., Bos, J. W., Ehlen, S., and D. Stebila, "FrodoKEM: key encapsulation from learning with errors", Work in Progress, Internet-Draft, March 2025, <https://datatracker.ietf.org/doc/draft-longa-cfrg-frodokem/>.

[FIPS203] National Institute of Standards and Technology, "FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard", Federal Information Processing Standards Publication , August 2024, <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf>.

[CD22] Castryck, W. and T. Decru, "An Efficient Key Recovery Attack on SIDH", Formal version published in the proceddings of EUROCRYPT 2023 , July 2022, <https://eprint.iacr.org/2022/975>.

Authors' Addresses

Guilin Wang (editor)
Huawei Int. Pte Ltd
9 North Buona Vista Drive, #13-01
The Metropolis Tower 1
SINGAPORE 138588
Singapore
Email: wang.guilin@huawei.com

Leonie Bruckert
secunet Security Networks
Ammonstr. 74
01067 Dresden
Germany
Email: Leonie.Bruckert@secunet.com

Valery Smyslov
ELVIS-PLUS
Russian Federation
Email: smyslov.ietf@gmail.com