Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 9 April 2026

V. Smyslov
ELVIS-PLUS
Y. Nir
Dell Technologies

6 October 2025

Using Classic McEliece in the Internet Key Exchange Protocol Version 2 (IKEv2)

draft-smyslov-ipsecme-ikev2-mceliece-01

Abstract

This document specifies how Classic McEliece Key Encapsulation Mechanism (KEM) is used to generate keys in the Internet Key Exchange version 2 (IKEv2) protocol.

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 9 April 2026.

Copyright Notice

Table of Contents

1. Introduction

IKEv2 ([RFC7296]) is a protocol for authentication and for generating keys for IPsec ([RFC4301]). Part of it is generating keys. Classic McEliece ([I-D.josefsson-mceliece]) provides a code-based Key Encapsulation Method (KEM) designed to be safe even against an adversary equipped with a quantum computer. The twelve parameter sets described in section 9 of [I-D.josefsson-mceliece] offers different balances between performance and output sizes.

The information needed for key agreement (in the case of McEliece this is a public key and a ciphertext) is carried in Key Exchange (KE) payloads. With the most common parameter set from the draft, mceliece6688128, the public key requires (see section 8.2.7 of the McEliece document) 1044992 octets to encode. This is almost 16 times as big as a standard KE payload (or any other payload) can carry, so we need to use a big payload, as specified in the big payload draft ([I-D.nir-ipsecme-big-payload]).

Because large payloads cannot be used in the IKE_SA_INIT exchange (see section 2.3 of [I-D.nir-ipsecme-big-payload]), the first key exchange has to use another algorithm, such as classic Diffie-Hellman or an elliptic curve variant. The McEliece exchange needs to be carried in an IKE_INTERMEDIATE exchange ([RFC9242]), after negotiating in the IKE_SA_INIT both support for big payloads and the additional key exchange exchange through the INTERMEDIATE_EXCHANGE_SUPPORTED notify message ([RFC9370]). The Classic Mceliece KEM can also be used in CREATE_CHILD_SA. For that, support for the intermediate exchange is not necessary.

TBD if this document should make any recommendations about which DH group to use for the initial key exchange, or whether it should remain silent on the topic.

2. Terminology and Notation

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.

It is assumed that readers are familiar with the IKEv2 protocol [RFC7296].

3. Classic McEliece KEM

Classic McEliece [I-D.josefsson-mceliece] is a code-based Key Encapsulation Mechanism (KEM) that is considered conservative and very thoroughly analysed.

The [I-D.josefsson-mceliece] document specifies 12 parameter sets. Should we just leave it at that, or specify just one? The current SSH candidate draft specifies only mceliece6688128. The current TLS candidate draft specifies 3: mceliece6688128, mceliece6960119, and mceliece8192128. Official Classic McEliece site [MCELIECE] lists 5 parameter sets. What should we do?

This is up to the working group. Until this is decided, we added a comparison table between the parameter sets here. Ultimately, there is nothing special about IKEv2. What is fitting for TLS and SSH is likely fitting for IKEv2 as well.

Parameter Set	Claimed NIST Level	Public key size (bytes)	Secret key size (bytes)	Ciphertext size (bytes)	Shared secret size (bytes)
mceliece348864	1	261120	6492	96	32
mceliece460896	3	524160	13608	156	32
mceliece6688128	5	1044992	13932	208	32
mceliece6960119	5	1047319	13948	194	32
mceliece8192128	5	1357824	14120	208	32

Table 1: Classic McEliece Parameter Set Summary

4. Using Classic McEliece in IKEv2

To negotiate the use of the McEliece KEM, an IKEv2 initiator and responder MUST negotiate three things in the IKE_SA_INIT exchange:

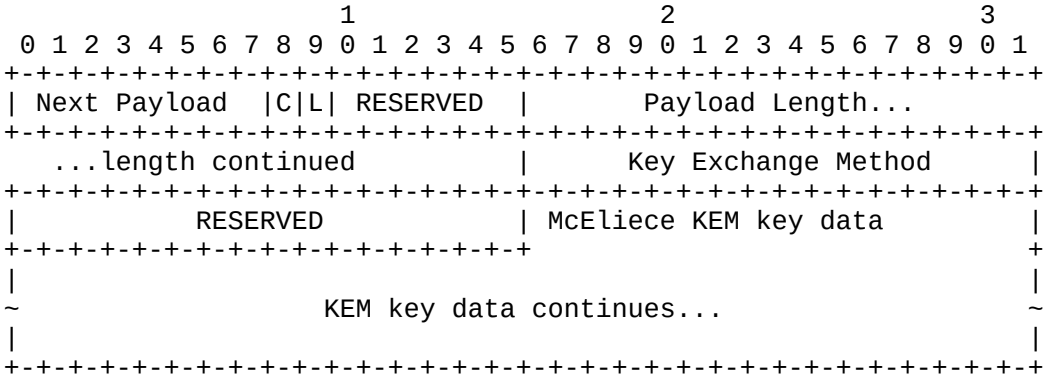
* The support for big IKE payloads ([I-D.nir-ipsecme-big-payload])

* Support for IKE fragmentation ([RFC7383])

* The use of these groups, see Section 7, as ADDKE. This implies support for the IKE_INTERMEDIATE exchange.

Since all of the above have to be specified in the IKE_SA_INIT request, the McEliece key exchange, a Responder MUST reject any McEliece group offered in an ADDKE payload if it does not support both big IKE payloads and fragmentation. Additionally, it MUST reject any McEliece group offered in an ADDKE payload if the initiator has not negotiated the support for both big payloads and for fragmentation.

Within the IKE_INTERMEDIATE exchange, such payloads will normally encode the large public keys. A diagram is provided here for illustration:. The format below is the big payload version of the Key Exchange from section 3.4 of [RFC7296].



* L is 1, indicating that the length field is 32-bit.

* The Key Exchange Method is TBD, the value assigned by IANA (see Section 7)

* The McEliece KEM key data is as described in section 6.3 of [I-D.josefsson-mceliece].

Note that when the KE payload is used to carry ciphertext, it can fit with the short payload format. It is not required to always use the big payload format to use Classic McEliece.

4.1. Using Classic McEliece for Child SAs and for IKE SA Rekey

The Classic McEliece KEM can also be used in the CREATE_CHILD_SA exchange (or in the IKE_FOLLOWUP_KE exchange as defined in [RFC9370]) to rekey IKE SA and to create/rekey IPsec SAs. The format and size are just the same, so doing this also requires support for big payloads and for IKE fragmentation. However, if Classic McEliece is only used in these exchanges, there is no need to negotiate the IKE_INTERMEDIATE exchange.

5. Transport Considerations

While an IKE SA that utilizes Classic McEliece can run over UDP, in most settings this will be problematic. The reason is that with tipical MTU size of 1500 bytes, an IKE message containing Classic McEliece public key will be splitted into several hundreds IKE fragment messages, which will be sent to the network at once. This may lead to network congestion causing loss of some messages, in which case all the fragment messages will be re-sent again (after timeout), since IKE fragment messages are not individually acknowledged. This will also lead to congestion and the process will

repeat until all the fragment messages will be received, but this might not happen.

For this reason peers may want to use TCP as a transport. Peers may choose between using TCP for both IKE and ESP as specified in [RFC9329] or using separate transports for them [I-D.smyslov-ipsecme-ikev2-reliable-transport]. The latter allows to avoid performance degradation when tunnelling TCP trafic and thus is RECOMMENDED.

Note, that despite the fact, that TCP can tranfer messages of any size without having problems with IP fragmentation, in case of Classic McEliece peers still have to negotiate IKE fragmentation [RFC7383] as defined in Section 4, even when they choose to use TCP as a transport for IKE. This is due to the limitation imposed by [RFC9329] that individual IKE message in TCP stream cannot exceed 64 Kbytes. Thus, larger IKE messages need to be be fragmented to this size by IKE fragmentation mechanism before sending over TCP.

6. Security Considerations

This inherits the security of IKEv2, the additional key exchange extension, the big payload extension, and of course, classic McEliece.

Some discussion about choice of group for the initial key exchange should be added here.

Probably more about McEliece here.

7. IANA Considerations

IANA is requested to assign one (or is it three) values from the "Transform Type 4 - Key Exchange Method Transform IDs" registry with name "mceliece6688128" (and maybe also "mceliece6960119" and "mceliece8192128") and this document as reference.

8. Acknowledgements

9. References

9.1. 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>.

[I-D.josefsson-mceliece] Josefsson, S., "Classic McEliece", Work in Progress, Internet-Draft, draft-josefsson-mceliece-03, 7 July 2025, <https://datatracker.ietf.org/doc/html/draft-josefsson-mceliece-03>.

[I-D.nir-ipsecme-big-payload] Nir, Y., "A Larger Internet Key Exchange version 2 (IKEv2) Payload", Work in Progress, Internet-Draft, draft-nir-ipsecme-big-payload-06, 14 September 2025, <https://datatracker.ietf.org/doc/html/draft-nir-ipsecme-big-payload-06>.

9.2. Informative References

[MCELIECE] "Classic McEliece", <https://classic.mceliece.org/>.

[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/info/rfc9329>.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <https://www.rfc-editor.org/info/rfc4301>.

[I-D.smyslov-ipsecme-ikev2-reliable-transport] Smyslov, V. and T. Reddy.K, "Separate Transports for IKE and ESP", Work in Progress, Internet-Draft, draft-smyslov-ipsecme-ikev2-reliable-transport-04, 15 April 2025, <https://datatracker.ietf.org/doc/html/draft-smyslov-ipsecme-ikev2-reliable-transport-04>.

Authors' Addresses

Valery Smyslov
ELVIS-PLUS
PO Box 81
Moscow (Zelenograd)
124460
Russian Federation
Email: svan@elvis.ru

Yoav Nir
Dell Technologies
9 Andrei Sakharov St
Haifa 3190500
Israel
Email: ynir.ietf@gmail.com