IP Security Maintenance and Extensions
Internet-Draft
Intended status: Standards Track
Expires: 3 September 2026

G. Wang, Ed.
Huawei Int. Pte Ltd
W. Pan
Huawei Technologies

2 March 2026

Multi-Authentication in IKEv2 with Post-quantum Security
draft-wang-ipsecme-multi-auth-ikev2-pq-00

Abstract

Motivated to mitigate security threats again quantum computers, this draft specifies a general authentication mechanism in the Internet Key Exchange Protocol Version 2 (IKEv2) [RFC7296], called Multi-Authentication. Namely, two peers can negotiate two or more authentication methods to authenticate each other. The authentication methods selected do not necessarily belong to the same category. This mechanism is achieved by adding a new value (17) (TBD) in the "IKEv2 Authentication Method" registry [IANA-IKEv2], maintained by IANA. To run Multiple Authentication, two peers send the SUPPORTED_AUTH_METHODS Notify, defined in [RFC9593], to negotiate two or more authentication methods for authenticaion in IKEv2.

[EDNOTE: Code points for Multi-Authentication may need to be assigned in the "IKEv2 Authentication Method" registry [IANA-IKEv2], maintained by IANA]

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 3 September 2026.

Table of Contents

1. Introduction

Cryptographically-relevant quantum computers (CRQC) pose a threat to data securely protected by current standards. In particular, the so-called harvest-now-and-decrypt-later (HNDL) attack is considered an imminent threat. To mitigate this threat against the Internet Key Exchange Protocol Version 2 (IKEv2) [RFC7296], multiple key exchanges in the IKEv2 [RFC9370] were introduced to achieve post-quantum (PQ) security. To enable post-quantum security for the authentication in IKEv2, "Announcing Supported Authentication Methods in the Internet Key Exchange Protocol Version 2 (IKEv2)" [RFC9593] specifies a new Notify type, called the SUPPORTED_AUTH_METHODS, which allows two peers to indicate the list of supported authentication methods while establishing IKEv2 SA. One purpose of [RFC9593] is to support post-quantum signature algorithms for authentication in IKEv2, as further discribed by the following drafts.

"Signature Authentication in the Internet Key Exchange Version 2 (IKEv2) using PQC" [I-D.RSF25] specifies how NIST PQ digital algorithms ML-DSA [FIPS204] and SLH-DSA [FIPS205] can be used in IKEv2 by indicating the supported signature algorithms via exchanging the Notify SIGNATURE_HASH_ALGORITHMS, defined in [RFC7427]. Similarly, "IKEv2 Support of ML-DSA", [I-D.Flu25] specifies how ML-DSA can be run in IKEv2, by indicating the supported signature algorithms via exchanging the SUPPORTED_AUTH_METHODS Notify, defined in [RFC9593]. On the other hand, "Post-Quantum Traditional (PQ/T) Hybrid PKI Authentication in the Internet Key Exchange Version 2 (IKEv2)" [I-D.HMW25] specifies how to run general hybrid PQ/T digital algorithms in IKEv2 via introducing some extensions in the SUPPORTED_AUTH_METHODS Notify.

For all of those Internet standard drafts, the correponding public certificates and signatures for the involved siganture algorithms are exchanged via the INTERMEDIATE Exchange, defined in [RFC9242].

However, except authentication by composite signatures is specified in [I-D.HMW25] where the corresponding certificates can be a composite certificate or dual certificates, all others are single method authentication. As discussed in [I-D.DPH25] and [I-D.WBS25], hybrid is a more conservative approach to the migration from traditional algrotihms to post-quantum (PQ) algorithms. Moreover, there a number of different authentication methods now, including Shared Key Message Integrity Code (2), Generic Secure Password Authentication Method (12), several specific signature algorithms (3, 9, 10, 11), general Digital Signature (14), and newly proposed KEM based authentication (16, TBD) [I-D.WS25].

Motivated by the fact that there is a need of hybrid authentication, this draft specifies a general authentication mechanism in the Internet Key Exchange Protocol Version 2 (IKEv2) [RFC7296], called Multi-Authentication. Namely, two peers can negotiate two or more authentication methods to authenticate each other. The authentication methods selected do not necessarily belong to the same category. For example, two peers may select a traditional signature and a PQ signature (like ML-DSA [FIPS204]), or MAC based authentication and a PQ signature.

This mechanism is achieved by adding a new value (17, TBD) in the "IKEv2 Authentication Method" registry [IANA-IKEv2], maintained by IANA. To run Multi-Authentication, two peers send the SUPPORTED_AUTH_METHODS Notify, defined in [RFC9593], to negotiate two or more authentication methods for authenticaion in IKEv2. Finally, using the authentication methods selected, not necessarily the same algoithm in two directions, the peers SHALL authenticate the IKE data to each other, according to the specfication in [RFC7296].

Actually, it is noticed that [RFC4739] specifies a mechanism called Multiple Authentication Exchange to run two or more authenticaiton in IKEv2. This mechanism is realized via two types of notification. Firstly, two peers run MULTIPLE_AUTH_SUPPORTED notification in the IKE_SA_INIT response (responder) and the first IKE_AUTH request (initiator) to indicate that they are willing to run a second authentication. After that, they exchange ANOTHER_AUTH_FOLLOWS notification in any IKE_AUTH message to complete the second authentication. However, [RFC4739] is not supported for post-quantum security at all.

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. Multiple Authentication in the IKEv2

3.1. Challenges

Here are the main challenging reasons for why a general PQ secure solution is hard for the authentication in the IKEv2:

* For the key exchange in IKEv2, the algorithm selected SHALL be the same for both peers. Different from this, two peers in the IKEv2 authentication MAY select different authentication methods to authenticate itself to the other.

* Authentication negotiation or indication in the IKEv2 is done via notifications, as shown in [RFC9593] and [RFC4739], not via normal message payloads in the IKE_SA_INIT or IKE_Auth, as the IKE key exchange does.

* However, in the IKE authentication, each peers has more info or requirement to transfer: which authentication methods itself supports, which authentication methods it prefers to authenticate itself to the other peer, and which authentication methods it prefers that the other peer SHOULD select to be authenticated. All of this may be covered by a term like "authentication policy", from both peers.

* Even the peers select the authentication methods both sides satisfied according to their preference, these methods may still fail for use, as there is still one more issue, certificates! Namely, the trust anchor of one peer may be not trusted by the other peer, when digital signature algorithms are selected for authentication in the IKEv2.

3.2. Basic Ideas of the Solution Proposed

The basic idea proposed in this document is to mimic the addtional key exchange (ADDKE) proposed in [RFC9370]. Namely, when one peer A (the sender) sends SUPPORTED_AUTH_METHODS Notify payload to announce what the authentication methods it supports, this payload also tansfers the info which methods it expects the other peer B SHALL select for authentication. This is done by assigning different authentication methods into a few authentication sets, and the other peer B MUST select one of the methods in each authentication set. More importantly, the feedback from the othe peer B (the replier) is intentionally constructed as the followings to transfer the replier's authentication policy to the sender A.

* 1 authentication set: This means that B agrees to use this set for bidirectional authentication. Namely, this implies that both A and B MUST use these methods in the authentication set to authenticate itself to the other. If this set is empty, it means that B does not support any authentication method in each set. If this set contains one or a number of NULL Authentication (13), it means that NULL Authentication (13) is a valid answer for one or a number of A's enquiring authentication sets.

* 2 authentication sets: This means that B SHALL use the first authentication set to authenticate itself to A, and A SHALL use the 2nd set to authenticate itstelf to B. In case the 2nd set is empty or just contains NULL Authentication (13), it means that B SHALL NOT require A to authenticate itself to B.

* 3 or more authentication sets: Similar as the above, the first set is for B to authenticate itself to A, the 2nd set MUST be empty that means B cannot select a set of methods from all methods A has sent, such that this set also satisfies B's authentication policy how A SHOULD authenticate itself to B. Therefore, after this empty set, all sets remaining are for expressing what B's authentication policy for A.

For example, if A sends ten methods (a1, a2, ..., a10) via 3 authentication sets, say (a2, a1, a3), (a4, a8, a9), and (a5, a6, a10, a7), according to A's preference. Then, if B sends back (a1, a4, a7), this implicitly means that both A and B SHALL use a1, a4,

and a7 to authenticate itself to the other peer. Or, if B sends back two authentication sets, (a1, a4, a7) and (a2, a7), it means that B SHALL use a1, a4, and a7 to authenticate itself to A, and A SHOULD use a2 and a7 to authenticate itself to B. Finally, in another case, if B sends back 4 sets, (a1, a4, a7), () (empty set), (a1, a3, a8), and (a11, a12), it means that B SHALL use a1, a4, and a7 to authenticate itself to A, and that B is asking A selects 2 methods from set 3 and 4 so that A SHALL authenticate itself to B, though by now B is not sure if A does support either a11 or a12.

If one execution of the above procedures cannot achieve the authentication policy for either of the two peers, they MAY abort the procedure or restart by any of the two peers as the sender to initate this authentication method negotiation.

For flexibility, authentication methods in sets are not supposed to exclusively belonging to only one set, though this may be true in most cases. The reason is that selecting the same method from two different sets does not make much sense for enhacing security, unless this method is NULL Authentication (13) for adding flexibility.

4. Protocol Details for Multiple Authentication

By following [RFC9593], two communicating peers send each other the Notify Message Type SUPPORTED_AUTH_METHODS to negotiate which authentication method(s) will be used to authenticate one of them to the other. Bascially, each of the authentication methods proposed can be any one registered in the "IKEv2 Authentication Method" registry under "Internet Key Exchange Version 2 (IKEv2) Parameters" [IANA-IKEv2], maintained by IANA. To run Multiple Authentication, this document adds the value 17 (TBD) for "Multi-Authentication" in the "IKEv2 Authentication Method" registry (Section 6).

4.1. Exchanges for Multiple Authentication

After the initiator starts the IKE_SA_INIT exchange as usual, the responder sents the notify SUPPORTED_AUTH_METHODS with value of 17 (TBD) to indicate that the responder wants to run Multiple Authentication with respect to several Authentication sets of authentication methods, which the responder supports. Each of these Authentication set will be listed in the SUPPORTED_AUTH_METHODS Notify Payload (Section 4.2), ordered by the responder’s preference.

After the initiator receives SUPPORTED_AUTH_METHODS via several Authentication sets from the reponder, it will try to prepare the best anwser, i.e, one set, or two sets, or three sets, according to this specification given the above.

Table 1 below shows how two peers use the SUPPORTED_AUTH_METHODS notification to run Multiple Authentication for the above example, where the responder’s intial authentication sets are (a2, a1, a3), (a4, a8, a9), and (a5, a6, a10, a7), while the initiator sends back two authentication sets (a1, a4, a7) and (a2, a7) as its feedback. In the protocol below, the IKE_INTERMEDIATE exchange MAY be used to faciliate the hybrid key exchange in the IKEv2 as specified in [RFC9370], and to transfer PQ certifates between the responder and the intitator for completing Multiple authentication.

```
Initiator                                                   Responder
-----------------------------------------------------------------------
HDR(IKE_SA_INIT), SAi1(.. ADDKE*..), --->
KEi, Ni, N(INTERMEDIATE_EXCHANGE_SUPPORTED), ..
                    <--- HDR(IKE_SA_INIT), SAr1(.. ADDKE*..), [CERTRQ,]
                         KEr, Nr, N(INTERMEDIATE_EXCHANGE_SUPPORTED), ..
                         N(SUPPORTED_AUTH_METHODS(17((a2a1a3),(a4a8a9),(a5a6a10a7))))..

                     ... (IKE_INTERMEDIATE for ADDKE) ...

HDR(IKE_AUTH), SK{IDi, [CERT,] [CERTRQ,]
[IDr,] AUTH, SAi2, TSi, TSr,
N(SUPPORTED_AUTH_METHODS(17(TBD)(a1a4a7),(a2a7)))} --->
                     ... (IKE_INTERMEDIATE for [CERT,]) ...
                    <--- HDR(IKE_AUTH), SK{IDr, [CERT,] AUTH, SAr2, TSi, TSr}
                                    ... (IKE_INTERMEDIATE for [CERT,]) ...
```

Fig. 1 An Example of Multi-Authentication between Two Peers

If the resulting SUPPORTED_AUTH_METHODS notification with list of authentication methods is too long such that IP fragmentation [RFC7383] of the IKE_SA_INIT response may happen, the responder MAY choose to send empty SUPPORTED_AUTH_METHODS notification in the IKE_SA_INIT exchange response. Then, the responder and the intiatior can send each other the SUPPORTED_AUTH_METHODS notification with list of authentication methods they support by using the IKE_INTERMEDIATE exchange, as desribed in Section 3.1 of [RFC9593].

[EDNOTE: More examples may be provided later.]

4.2. Payload Format for Multi-Authentication

For easy reference, the SUPPORTED_AUTH_METHODS Notify payload format is shown in the following, as specified in Section 3.2 of [RFC9593]. Correspondigly, here, Protocol ID field MUST be set to 0, the SPI Size MUST be set to 0 (meaning there is no SPI field), and the Notify Message Type MUST be set to 16443.

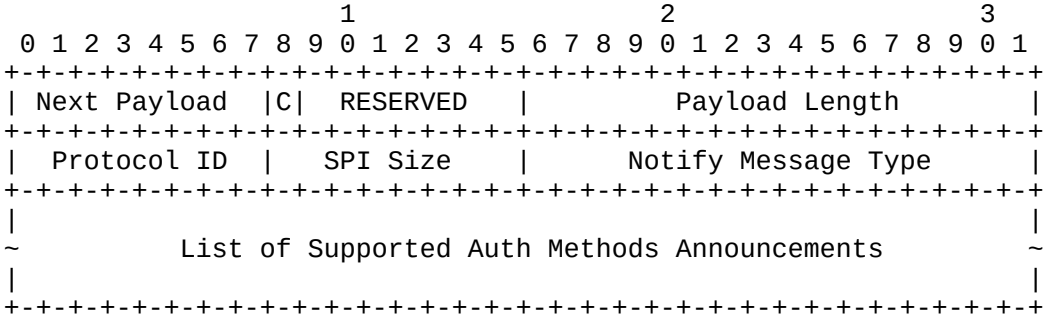

Fig.2 SUPPORTED_AUTH_METHODS Notify Payload Format

Payload Format for Multi-Authentication is defined in Fig. 3, which is treated as part of the Supported Auth Methods Announcements shown in Fig. 2. Namely, for this part, a number (M) of Authentication Groups of authentication methods are listed, as desribed below.

* Length: Length of the whole blob of the announcement in octets; must be greater than 5.

* Multi-Auth: The value of "Multi-Authentication", which is supposed to be 17 (TBD).

* #Auth Group: The number of Authentication Groups listed in this announcement.

* #Auth Meth: The number of Authentication Methods in a given authentication group.

* Reserved: One byte reserved for future use.

* Auth Method: The value of one announced authentication method in a given authentication group.

* Cert Link: Links this announcement with a particular CA, which issued the public certificate for the Auth Method identified in AlgorithmIdentifiers below; see Section 3.2.2 of [RFC9593] for detail. If this Auth Method is not related certificate, this info MUST be ignored.

* AlgID Len: Length of each authentication method algorithm ID, that is identified in AlgorithmIdentifier below, in octets.

* AlgorithmIdentifier: One ore more variable-length ASN.1 objects that are encoded using Distinguished Encoding Rules (DER) [X.690] to identify one specific Authentication Method algorithm.

Once two authentication sets have been negotiated, the corresponding authentication methods will be use to the IKE data for completing authentication, according to [RFC7296]. In the above example for Fig. 2, a1, a4, and a7 will be used to run multiple authentication from B to A, and a2 and a7 will be used to multi-authentication from A to B. Once all those authentication methods are correctly verified by one side, then this directional authentication is successful.

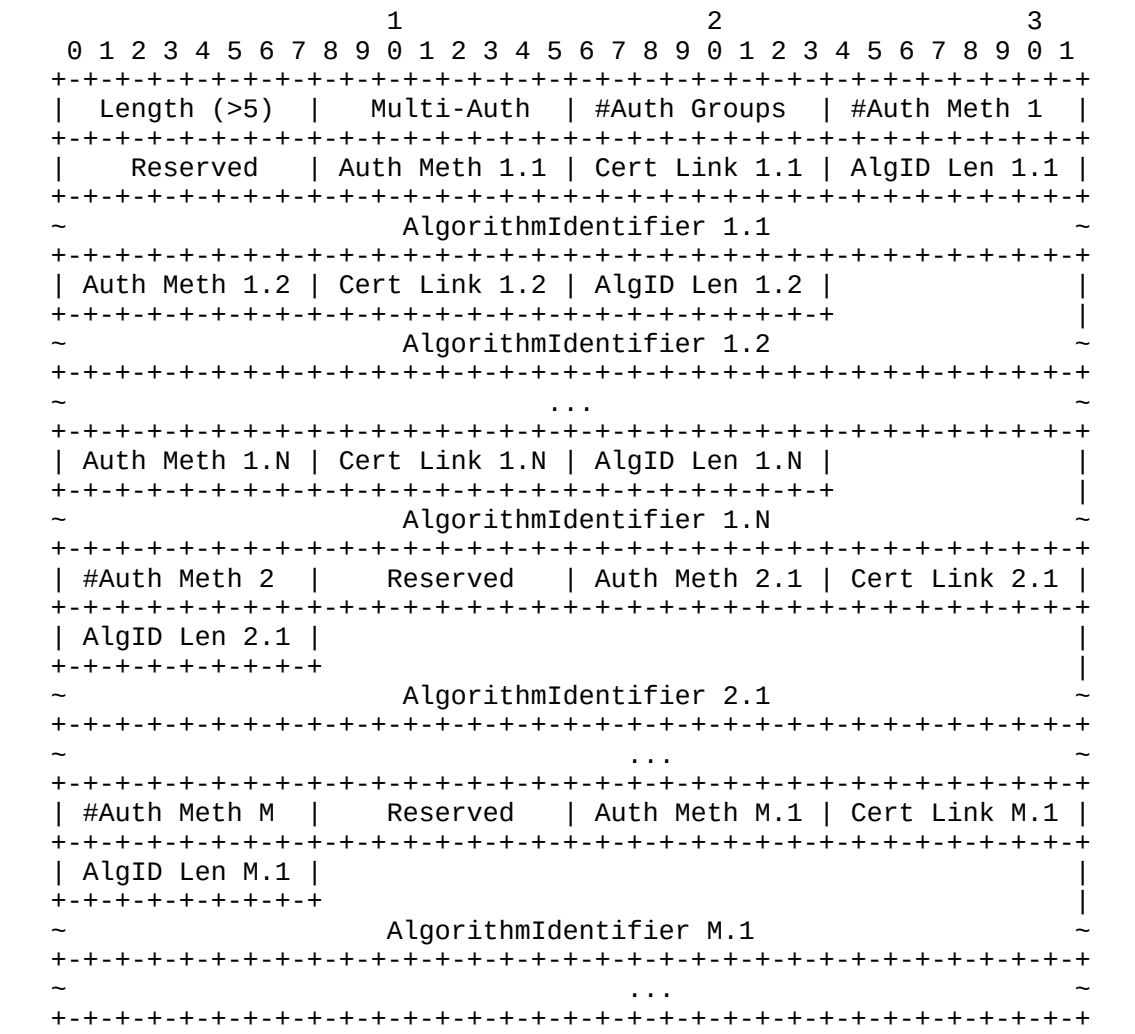

Fig.3 Payload Format for Multi-Authentication Announcement

[EDNOTE: More examples may be provided later.]

5. Security Considerations

Multi-authentication is a combination of multiple component authentication methods. So, its seucrity relies on the security of the security of each component. By requiring multi-authentication is successful if and only if each component authentication is successful, multi-authentication is secure at least one of the component authentication method, with regarding to either traditional or traditional and quantum attacks.

At the time of writing, there are no other security issues which may need to be considered.

6. IANA Considerations

This document adds a new type in the "IKEv2 Authentication Method" registry under "Internet Key Exchange Version 2 (IKEv2) Parameters" [IANA-IKEv2], maintained by IANA: .

Value	IKEv2 Authentication Method	Reference
17 (TBD)	Composite ML-DSA Authentication	This draft

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>.

[RFC4739] Eronen, P. and J. Korhonen, "Multiple Authentication Exchanges in the Internet Key Exchange (IKEv2) Protocol", RFC 4739, DOI 10.17487/RFC4739, November 2006, <https://www.rfc-editor.org/info/rfc4739>.

[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>.

[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/info/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/info/rfc8174>.

[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>.

[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/info/rfc9593>.

[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>.

[FIPS204] National Institute of Standards and Technology, "FIPS 204: Module-Lattice-Based Digital Signature Standard", Federal Information Processing Standards Publication , August 2024, <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf>.

[FIPS205] National Institute of Standards and Technology, "FIPS 205: Stateless Hash-Based Digital Signature Standard", Federal Information Processing Standards Publication , August 2024, <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf>.

[X.690] ITU-T, "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.

[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>.

9. Informative References

[OGPKF24] M. Ounsworth, M., Gray, J., Pala, M., J. Klaussner, J., and S. S. Fluhrer, "Composite ML-DSA For use in X.509 Public Key Infrastructure and CMS", Work in Progress, Internet-Draft, v04., October 2024, <https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-sigs/>.

[I-D.RSF25] Reddy, T., Smyslov, V., and S. Fluhrer, "Signature Authentication in the Internet Key Exchange Version 2 (IKEv2) using PQC", Work in Progress, Internet-Draft, v04, February 2025, <https://datatracker.ietf.org/doc/draft-reddy-ipsecme-ikev2-pqc-auth/>.

[I-D.Flu25] Fluhrer, S., "IKEv2 Support of ML-DSA", Work in Progress, Internet-Draft, v00, January 2025, <https://datatracker.ietf.org/doc/draft-sfluhrer-ipsecme-ikev2-mldsa/>.

[I-D.HMW25] Hu, J., Morioka, Y., and G. Wang, "Post-Quantum Traditional (PQ/T) Hybrid PKI Authentication in the Internet Key Exchange Version 2 (IKEv2)", Work in Progress, Internet-Draft, v03, November 2025, <https://datatracker.ietf.org/doc/draft-hu-ipsecme-pqt-hybrid-auth/>.

[I-D.BHCD] Bindel, B., Hale, B., Connolly, D., and F. Driscoll, "Hybrid signature spectrums", Work in Progress, Internet Draft, v06, January 2025, <https://datatracker.ietf.org/doc/draft-ietf-pquip-hybrid-signature-spectrums/>.

[I-D.DPH25]
Driscoll, F., Parsons, M., and B. Hale, "Terminology for Post-Quantum Traditional Hybrid Schemes", Work in Progress, Internet-Draft, v06, January 2025, <https://datatracker.ietf.org/doc/draft-ietf-pquip-pqt-hybrid-terminology/>.

[I-D.WBS25]
Wang, G., L. Bruckert, L., and V. V. Smyslov, "Post-quantum Hybrid Key Exchange in the IKEv2 with FrodoKEM", Work in Progress, Individual Draft, v03, December 2025, <https://datatracker.ietf.org/doc/draft-wang-ipsecme-hybrid-kem-ikev2-frodo/>.

[I-D.WS25] Wang, G. and V. V. Smyslov, "KEM based Authentication for the IKEv2 with Post-quantum Security", Work in Progress, Individual Draft, v02, October 2025, <https://datatracker.ietf.org/doc/draft-wang-ipsecme-kem-auth-ikev2/>.

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

Wei Pan
Huawei Technologies
101 Software Avenue, Yuhuatai District
Nanjing, Jiangsu
138588
China
Email: william.panwei@huawei.com