KEM based Authentication for the IKEv2 with Post-quantum Security

draft-wang-ipsecme-kem-auth-ikev2-00

IPSECME, IETF 122 @ Bangkok

Guilin Wang

KEM based Auth for the IKEv2

❑ **Draft Info**

ietf.org/archive/id/draft-wang-ipsecme-kem-auth-ikev2-00.html

Workgroup:	IP Security Maintenance and Extensions
Internet-Draft:	draft-wang-ipsecme-kem-auth-ikev2-00
Published:	3 March 2025
Intended Status:	Standards Track
Expires:	4 September 2025
Author:	G. Wang, Ed.
	Huawei Int. Pte Ltd

KEM based Authentication for the IKEv2 with Post-quantum Security

KEM based Auth for the IKEv2

❑ Why using KEM for the IKEv2 Authentication?

- ML-KEM 50% shorter than ML-DSA: For Levels 1, 3, and 5, can save 2,164， 2,989, and 4,083 bytes, respectively, by replacing pk+sig by pk+ct.
- ML-KEM 5 times faster than ML-DSA: KeyGen 4 times faster, encapsulating 7 times faster than signing, and decapsulating 3 times faster than sg verifying
- **KEM-based Authentication for TLS 1.3** [draft-celi-wiggers-tls-authkem-04]

	private key/ decapaaulation key	public key/ encapsulation key	singature/ ciphertext
ML-DSA-44/ ML-KEM-512	2,650/1,632 =157%	1,312/800 =164%	2,420/768 =315%
ML-DSA-65/ ML-KEM-768	4,032/2,400 =168%	1,952/1,184 =165%	3,309/1,088 =304%
ML-DSA-87/ ML-KEM-1024	4,896/3,168 =155%	2,592/1,568 =165%	4,627/1,568 =295%

Table 1: Communication Overhead Comparison of ML-DSA and ML-KEM

	KeyGen speed/ SKeyGen speed	Encap speed/ Sign speed	Decap speed/ Verify speed
ML-DSA-44/ ML-KEM-512	1,357k/369k =368%	3,487k/448k =778%	1,350k/409k =330%
ML-DSA-65/ ML-KEM-768	2,394k/604k =396%	5,574k/732k =761%	2,302k/674k =342%
ML-DSA-87/ ML-KEM-1024	4,069k/962k =423%	7,730k/1,119k =691%	3,998k/1,043k =383%

Table 2: Computational Overhead Comparison of ML-DSA and ML-KEM

KEM based Auth for the IKEv2

❑ How to use KEM for the IKEv2 Authentication?

- Register the value of 16 (TBD) for "KEM based Authentication" in the "IKEv2 Authentication Method" registry, maintained by IANA.
- Run Notify Message Type SUPPORTED_AUTH_METHODS [RFC9593] to negotiate which KEM algorithm as the authentication method for the IKEv2
- Run the IKE_INTERMEDIATE exchange to transfer PQ KEM certificates and KEM ciphertexts

```
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(ISUPPORTED_AUTH_METHODS(..16(TBD)..)),..

                    ... (IKE_INTERMEDIATE for ADDKE) ...

HDR(IKE_AUTH), SK{IDi, [CERT,] [CERTRQ,]
[IDr,] AUTH, SAi2, TSi, TSr,
N(ISUPPORTED_AUTH_METHODS(..16(TBD)..))} --->
                    ... (IKE_INTERMEDIATE for [CERT,]) ...
                   <--- HDR(IKE_AUTH), SK{IDr, [CERT,] AUTH, SAr2, TSi, TSr}
                                     ... (IKE_INTERMEDIATE for [CERT,]) ...

Fig. 1 An Example of Running KEM based Authentication between Two Peers
```

❑ Scott's comments

- "not mention what processing that each side does"
- "would require additional exchanges"

❑ Updates to Be Done

- Preliminary check
- It seems ok to have one or two additional exchanges using IKE_AUTH and/or the INTERMEDIATE

KEM based Auth for the IKEv2

❑ Payload Formats

```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Next Payload  |C|  RESERVED   |         Payload Length        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Protocol ID  |   SPI Size    |      Notify Message Type      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~          List of Supported Auth Methods Announcements         ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

     Fig.2  SUPPORTED_AUTH_METHODS Notify Payload Format
```

- **Length**: Length of the whole blob of one announcement in octets.
- **Auth Method**: 16 (TBD), for "KEM based authentication" for the IKEv2.
- **Cert Link**: Links this announcement with a particular CA
- **Alg Len 1**: Length of the KEM algorithm.
- **Alg Len 2**: Length of the keyed MAC algorithm
- **AlgorithmIdentifiers**: KEM OID || keyed_MAC_OID

```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Length (>5)  |  Auth Method  |  Cert Link 1  | Alg 1 Len 1   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Alg 1 Len 2  |                                               |
+-+-+-+-+-+-+-+-+                                               +
~                      AlgorithmIdentifiers 1                   ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Cert Link 2   |  Alg 2 Len 1  |  Alg 2 Len 1  |               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+               +
~                      AlgorithmIdentifiers 2                   ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
~                              ...                              ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Cert Link N   |  Alg N Len 1  |  Alg N Len 2  |               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+               |
~                      AlgorithmIdentifiers N                   ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Fig.3  Payload Format for KEM based Authentication Announcement
```

KEM based Auth for the IKEv2

Further Actions

- To detail the AUTH procedures
- To add security discussions

Invitations

- Welcome to give your kind suggestions and comments
- If you are interested in this work, welcome to let us know
- Wang.guilin@Huawei.com

Thanks!