**3GPP TSG-SA3 Meeting #124 S3-253696-r2**

**Wuhan, China, 13 – 17 October 2025 (Merger of S3-253335, S3-253382, S3-253488, S3-253546)**

**Source: Huawei, HiSilicon, China Mobile, Ericsson, Qualcomm Incorporated**

**Title: PQC migration for IKEv2 protocol**

**Document for: Approval**

**Agenda item: 5.2.1**

**Spec: 3GPP TR 33.703**

**Version: 0.1.0**

**Work Item: FS\_CryptoPQC**

**Comments**

It is proposed to study the PQC migration scheme of the IKEv2 protocol in 3GPP.

\* \* \* First Change \* \* \* \*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[y2] IETF RFC 9242: "Intermediate Exchange in the Internet Key Exchange Protocol Version 2 (IKEv2) "

[y3] IETF RFC 9370: "Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2) "

[y4] IETF Draft (Standards Track): "Post-quantum Hybrid Key Exchange with ML-KEM in the Internet Key Exchange Protocol Version 2 (IKEv2) ", <https://datatracker.ietf.org/doc/draft-ietf-ipsecme-ikev2-mlkem/>.

[y5] IETF RFC 9593: "Announcing Supported Authentication Methods in the Internet Key Exchange Protocol Version 2 (IKEv2)"

[y6] IETF RFC 8784: "Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security"

[y8] NIST FIPS 203: “Module-Lattice-Based Key-Encapsulation Mechanism Standard”.

[y9] NIST FIPS 204: “Module-Lattice-Based Digital Signature Standard”.

[y10] NIST FIPS 205: “Stateless Hash-Based Digital Signature Standard”.

 [y11] IETF Draft (Standards Track): " Signature Authentication in the Internet Key Exchange Version 2 (IKEv2) using PQC ", https://datatracker.ietf.org/doc/draft-ietf-ipsecme-ikev2-pqc-auth/.

[y12] IETF Draft (Standards Track): " Mixing Preshared Keys in the IKE\_INTERMEDIATE and in the CREATE\_CHILD\_SA Exchanges of IKEv2 for Post-quantum Security", https://datatracker.ietf.org/doc/draft-ietf-ipsecme-ikev2-qr-alt/.

[y13] IETF Draft (Standards Track): " Post-quantum Hybrid Key Exchange in the IKEv2 with FrodoKEM", https://datatracker.ietf.org/doc/draft-wang-ipsecme-hybrid-kem-ikev2-frodo/.

[y14] IETF Draft (Standards Track): " Post-quantum Hybrid Key Exchange with NTRU in the Internet Key Exchange Protocol Version 2 (IKEv2) ", https://datatracker.ietf.org/doc/draft-skyline-ipsecme-ntru-ikev2/.

[y15] ISO Preliminary Standardization Proposal: "FrodoKEM: Learning With Errors Key Encapsulation", https://frodokem.org/files/FrodoKEM\_standard\_proposal\_20241205.pdf.

[y16] ISO Preliminary Standardization Proposal: "NTRU Algorithm Specifications And Supporting Documentation", https://info.isl.ntt.co.jp/crypt/ntru/files/ntru.pdf.

[y17] IETF Draft (Standards Track): " KEM based Authentication for the IKEv2 with Post-quantum Security ", https://datatracker.ietf.org/doc/draft-wang-ipsecme-kem-auth-ikev2/.

[y18] IETF Draft (Standards Track): " Post-Quantum Traditional (PQ/T) Hybrid PKI Authentication in the Internet Key Exchange Version 2 (IKEv2)", https://datatracker.ietf.org/doc/draft-hu-ipsecme-pqt-hybrid-auth/.

[y19] IETF Draft (Standards Track): " Prevention Downgrade Attacks on the Internet Key Exchange Protocol Version 2 (IKEv2)", https://datatracker.ietf.org/doc/draft-smyslov-ipsecme-ikev2-downgrade-prevention/.

[y20] IETF Draft (Informational): "Commercial National Security Algorithm (CNSA) Suite 2.0 Profile for IPsec", <https://datatracker.ietf.org/doc/draft-guthrie-cnsa2-ipsec-profile/>.

[X10] IETF RFC 7383: "Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation". <https://www.rfc-editor.org/rfc/rfc7383>

\* \* \* Next Change \* \* \* \*

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

ECIES Elliptic Curve Integrated Encryption Scheme

MIKEY-SAKKE Multimedia Internet KEYing – Sakai-Kasahara Key Encryption

PQC Post Quantum Cryptography

SDO Standards Development Organizations

SECG Security Engineering & Consulting Group

SUCI Subscription Concealed Identifier

IKEv2 Internet Key Exchange Protocol Version 2

SA Security Association

(EC)DH Elliptic Curve Diffie–Hellman key Exchange

ECC Elliptic Curve Cryptography

ML-KEM Module-Lattice-Based Key-Encapsulation Mechanism

ML-DSA Module-Lattice-Based Digital Signature

SLH-DSA Stateless Hash-Based Digital Signature

\* \* \* Next Change \* \* \* \*

## 6.X Protocol：IKEv2

### 6.X.1 General

The IETF IPSECME group has introduced multiple RFCs and Drafts to enable a smooth PQC transition for the Internet Key Exchange Protocol Version 2 (IKEv2) protocol. They cover both key exchange and authentication.

### 6.X.2 Current Work in IETF

#### 6.X.2.1 IETF RFCs

##### 6.X.2.1.1 Key Exchange

**KEM-based Key Exchange**

* The IETF RFC 9242 [y2] introduces a new exchange, called "Intermediate Exchange" for IKEv2 to avoid IP fragmentation of large IKE messages and enable transferring large amounts of data during Security Association (SA) establishment expected for some PQC key exchanges. §
* The IETF RFC 9370 [y3] describes a method to perform multiple successive key exchanges in IKEv2. It allows integration of PQC in IKEv2 and the negotiation of one or more PQC algorithms, in addition to the existing (EC)DH key exchange data that provides backward compatibility.
* RFC 7383, "Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation" [X10] describes escribes a way to avoid IP fragmentation of large Internet Key Exchange Protocol version 2 (IKEv2) messages, which is necessary when using ML-KEM-1024, ML-DSA, or SLH-DSA.

**PSK-based Key Exchange**

- The IETF RFC 8784 [y6] describes an extension of IKEv2 resistant to quantum computers using pre-shared keys.

##### 6.X.2.1.2 Authentication and Signature

- The IETF RFC 9593 [y5] defines a mechanism that allows implementations of IKEv2 to indicate the list of supported authentication methods to their peers while establishing IKEv2 SAs. This mechanism improves interoperability when IKEv2 partners are configured with multiple credentials of different types (for example, ECC-based certificate and PQC-based certificate) for authenticating each other.

#### 6.X.2.2 IETF Adopted Drafts

##### 6.X.2.1.1 Key Exchange

**KEM-based Key Exchange**

* IETF Draft draft-ietf-ipsecme-ikev2-mlkem-03, "Post-quantum Hybrid Key Exchange with ML-KEM in the Internet Key Exchange Protocol Version 2 (IKEv2) " [y4] proposes to use the ML-KEM [y8] as an additional key exchange in IKEv2 along with traditional key exchanges.
* IETF Draft draft-ietf-ipsecme-ikev2-pqc-auth-04, "Signature Authentication in the Internet Key Exchange Version 2 (IKEv2) using PQC" [X11], specifies a generic mechanism for integrating post-quantum cryptographic (PQC) digital signature algorithms into the IKEv2 protocol.

**PSK-based Key Exchange**

- IETF Draft draft-ietf-ipsecme-ikev2-qr-alt-10, "Mixing Preshared Keys in the IKE\_INTERMEDIATE and in the CREATE\_CHILD\_SA Exchanges of IKEv2 for Post-quantum Security" [y12] defines an alternative way to provide protection against quantum computers, which is similar to the solution defined in RFC 8784 [y6], but also protects the initial IKEv2 SA.

##### 6.X.2.1.2 Authentication and Signatures

- IETF Draft draft-ietf-ipsecme-ikev2-pqc-auth-04, "Signature Authentication in the Internet Key Exchange Version 2 (IKEv2) using PQC" [y11] outlines how Module-Lattice-Based Digital Signatures (ML-DSA) [y9] and Stateless Hash-Based Digital Signatures (SLH-DSA) [y10], can be employed as authentication methods within the IKEv2.

### 6.X.3 3GPP Considerations

Editor’s Note: This clause includes potential alternative options on PQC migration that 3GPP SA3 could consider. For example, for TLS 1.2, the following alternative options may be considered by 3GPP: (1) state in its profile that TLS 1.2 is expected to already have been fully phased out in 5G systems by XXXX date. (ii) add a note in its profile explicitly stating that TLS 1.2 is vulnerable to quantum attacks and is strongly recommended not to be used.

Editor’s Note: This clause does not include any conclusions.

\* \* \* End of Changes \* \* \* \*