**3GPP TSG-SA3 Meeting #124 S3-253832-r1 (merger of S3-253490, S3-253544 and S3-253545)**

**Wuhan, China, 13 – 17 October 2025**

**Source: Ericsson, Qualcomm**

**Title: Pseudo-CR on updating the JOSE and COSE clauses of the PQC Study**

**Document for: Approval**

**Agenda item: 5.2.1**

**Spec: 3GPP TR 33.703**

**Version: 0.1.0**

**Work Item: FS\_CryptoPQC**

**Comments**

<Proposals, reason for change, abstract, comments if necessary (optional)>

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

<Proposed change in revision marks>

# 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".

[2] 3GPP TR 33.938: "3GPP Cryptographic Inventory".

[3] 3GPP TS 33.180: "Security of the Mission Critical (MC) service".

[4] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[5] IETF Internet-Draft: "Post-Quantum Cryptography for Engineers".

[6] IETF RFC 6509: ''MIKEY-SAKKE: Sakai-Kasahara Key Encryption in Multimedia Internet KEYing (MIKEY)''.

[7] IETF RFC 9794: "Terminology for Post-Quantum Traditional Hybrid Schemes".

[8] NIST IR 8547: "Transition to Post-Quantum Cryptography Standards".

[9] SECG SEC 1: "Recommended Elliptic Curve Cryptography", Version 2.0, 2009. Available at <http://www.secg.org/sec1-v2.pdf>.

[10] SECG SEC 2: "Recommended Elliptic Curve Domain Parameters", Version 2.0, 2010. Available at <http://www.secg.org/sec2-v2.pdf>.

[X1] IETF RFC 7515: "JSON Web Signature (JWS)"

[X2] IETF RFC 7516: "JSON Web Encryption (JWE)"

[X3] IETF RFC 7517: "JSON Web Key (JWK)"

[X4] IETF RFC 7519: "JSON Web Token (JWT)"

[X5] IETF RFC 6749: "The OAuth 2.0 Authorization Framework"

[X6] OpenID Connect 1.0, <https://openid.net/specs/openid-connect-core-1_0.html>

[X7] 3GPP TS 33.501: "Security architecture and procedures for 5G System"

[X8] 3GPP TS 33.210: "Network Domain Security (NDS); IP network layer security"

[X9] IETF Draft draft-ietf-jose-pqc-kem-03: "Post-Quantum Key Encapsulation Mechanisms (PQ KEMs) for JOSE and COSE"

[X10] IETF Draft draft-ietf-cose-dilithium-08: "ML-DSA for JOSE and COSE"

[X11] IETF Draft draft-ietf-cose-sphincs-plus-05: "SLH-DSA for JOSE and COSE"

[X12] IETF Draft draft-ietf-cose-falcon-01: "JOSE and COSE Encoding for Falcon"

[X13] 3GPP TS 33.434: "Security aspects of Service Enabler Architecture Layer (SEAL) for verticals"

[X14] IETF RFC 9200: "Authentication and Authorization for Constrained Environments Using the OAuth 2.0 Framework (ACE-OAuth)"

[X15] IETF RFC 8392: "CBOR Web Token (CWT)"

[X16] IETF RFC 9052: "CBOR Object Signing and Encryption (COSE): Structures and Process"

[Q5] IETF Draft (Standards Track): “Use of Hybrid Public Key Encryption (HPKE) with JSON Object Signing and Encryption (JOSE)”, <https://datatracker.ietf.org/doc/draft-ietf-jose-hpke-encrypt/>.

[Q6] IETF Draft (Standards Track): “Use of Hybrid Public-Key Encryption (HPKE) with CBOR Object Signing and Encryption (COSE)”, <https://datatracker.ietf.org/doc/draft-ietf-cose-hpke/>.

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

## 6.X JOSE

### 6.X.1 General

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

#### 6.X.2.1 IETF RFCs

No RFCs for the usage of PQC algorithms in JWE or JWS are published yet.

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

The IETF is developing support for PQC algorithms in JOSE. The following drafts are relevant:

- IETF Draft draft-ietf-jose-pqc-kem-03, "Post-Quantum Key Encapsulation Mechanisms (PQ KEMs) for JOSE and COSE" [X9], describes describes the conventions for using Post-Quantum Key Encapsulation Mechanisms (PQ-KEMs) within JOSE and COSE.

- IETF Draft draft-ietf-cose-dilithium-08, "ML-DSA for JOSE and COSE" [X10], describes JSON Object Signing and Encryption (JOSE) and CBOR Object Signing and Encryption (COSE) serializations for Module-Lattice-Based Digital Signature Standard (ML-DSA).

- IETF Draft draft-ietf-cose-sphincs-plus-05: "SLH-DSA for JOSE and COSE" [X11], describes JOSE and COSE serializations for SLH-DSA.

- IETF Draft draft-ietf-cose-falcon-01, "JOSE and COSE Encoding for Falcon" [X12], describes JSON and CBOR serializations.

- IETF Draft draft-ietf-jose-hpke-encrypt-12, "Use of Hybrid Public Key Encryption (HPKE) with JSON Object Signing and Encryption (JOSE)" [Q5] defines a Hybrid Public Key Encryption (HPKE) for use with JOSE utilizing an asymmetric Key Encapsulation Mechanism (KEM), a Key Derivation Function (KDF), and an Authenticated Encryption with Associated Data (AEAD) algorithm.

However, no IETF work on hybrid signature schemes for JOSE has been adopted.

### 6.X.3 3GPP Considerations

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

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

## 6.Y COSE

### 6.Y.1 General

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

#### 6.Y.2.1 IETF RFCs

No RFCs for the usage of PQC algorithms in COSE are published yet.

#### 6.Y.2.2 IETF Adopted Drafts

The IETF is developing support for PQC algorithms in COSE. The following drafts are relevant:

- IETF Draft draft-ietf-jose-pqc-kem-03, "Post-Quantum Key Encapsulation Mechanisms (PQ KEMs) for JOSE and COSE" [X9], describes describes the conventions for using Post-Quantum Key Encapsulation Mechanisms (PQ-KEMs) within JOSE and COSE.

- IETF Draft draft-ietf-cose-dilithium-08, "ML-DSA for JOSE and COSE" [X10], describes JSON Object Signing and Encryption (JOSE) and CBOR Object Signing and Encryption (COSE) serializations for Module-Lattice-Based Digital Signature Standard (ML-DSA).

- IETF Draft draft-ietf-cose-sphincs-plus-05: "SLH-DSA for JOSE and COSE" [X11], describes JOSE and COSE serializations for SLH-DSA.

- IETF Draft draft-ietf-cose-falcon-01, "JOSE and COSE Encoding for Falcon" [X12], describes JSON and CBOR serializations.

- IETF Draft draft-ietf-cose-hpke-16, "Use of Hybrid Public-Key Encryption (HPKE) with CBOR Object Signing and Encryption (COSE)" [Q6] defines a Hybrid Public Key Encryption (HPKE) for use with JOSE utilizing an asymmetric Key Encapsulation Mechanism (KEM), a Key Derivation Function (KDF), and an Authenticated Encryption with Associated Data (AEAD) algorithm.

However, no IETF work on hybrid signature schemes for COSE has been adopted.

### 6.Y.3 3GPP Considerations

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

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