**3GPP TSG-SA3 Meeting #124 S3-253840-r2**

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

**Source: Ericsson**

**Title: Pseudo-CR on New Solution to Quantum-Resistant SUCI Calculation**

**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 \* \* \* \*

# 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>.

[X3] Galois Counter Mode with Strong Secure Tags (GCM-SST). <https://datatracker.ietf.org/doc/html/draft-mattsson-cfrg-aes-gcm-sst>

[X4] FIPS 203: "Module-Lattice-Based Key-Encapsulation Mechanism Standard". <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf>

[X5] TS 31.102: "Characteristics of the Universal Subscriber Identity Module (USIM) application". <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1803>

[X6] Ericssons comments on on NIST SP 800-227 (Initial Public Draft). <https://csrc.nist.gov/files/pubs/sp/800/227/ipd/docs/sp800-227-ipd-public-comments-received.pdf>

[X7] SP 800-227: "Recommendations for Key-Encapsulation Mechanisms". <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-227.pdf>

[X8] ETSI TS 103 744: "Quantum-safe Hybrid Key Establishment". <https://www.etsi.org/deliver/etsi_ts/103700_103799/103744/01.02.01_60/ts_103744v010201p.pdf>

[X9] FIPS 202: "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions". <https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.202.pdf>

[X10] SP 800-185: "~SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash". <https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.202.pdf>

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

#### 7.2.1.Y Solution #Y to Protocol: SUCI calculations

##### 7.2.1.Y.1 Introduction

Annex C of TS 33.501 [4] specifies two protection schemes for concealing a SUPI into a SUCI. The protection schemes are called Profile A and Profile B. These two profiles use SECG ECIES [9], which is a so called KEM-DEM scheme — combining a Key Encapsulation Mechanism (KEM) and a Data Encapsulation Mechanism (DEM). SECG is unlikely to update its specifications. PQC migration of SUCI calculations does not require changing any protocols or architectures — it is sufficient to introduce new SUCI profiles.

Editor’s note: It is FFS whether the additional optional inputs to Key Combine which are sent in cleat text over the air can enhance security.

Editor’s note: For easier understanding, further details on how to implement the solution (e.g., the schematic figures as in 33501 and call flows) is FFS.

Editor’s note: For easier understanding, further details on hybrid keys and how hybrid scheme is realized is FFS.

Editor's note: Justification for mixing different security levels, i.e., ML-KEM-768 with AES-256, is FFS.

##### 7.2.1.Y.2 Solution details

General

PQC migration for SUCI calculations can be done by introducing new SUCI profiles, and the new SUCI profiles can be created by extending the existing SUCI profiles with simple algorithm updates. Using such extensions is not a new thing to do. It was also the case when 5G was specified — following recommendations from ETSI SAGE, 3GPP not only profiled SECG ECIES, but also extended it to support Montgomery curves like Curve25519, along with HMAC-SHA-256 (with 64-bit long tag).

Adding a PQC KEM (hybrid or standalone) is equally straightforward. Though the “EC” in ECIES gives the impression that it must use an elliptic curve, there are no technical obstacles to replacing the elliptic curve-based KEM in ECIES with either a standalone or a hybrid PQC KEM. It is similar to how TLS 1.3 continues to refer to KEM algorithms as the underlying algebraic groups and KEM encapsulations as KeyShares.

ML-KEM is the Most Suitable Option

ML-KEM is already standardized, and its implementations are widely available. During the specification of SUCI protection in 33.501 [4], SA3 had considered the future need for PQC and therefore specified a maximum SUCI length of 3000 bytes to allow the introduction of quantum-resistant protection schemes. NIST has now standardized the lattice-based ML-KEM in FIPS 203 [X4] and, as it was expected, both standalone and hybridized ML-KEM-512, ML-KEM-768, and ML-KEM-1024 fit in 3000 bytes.

Since Rel-15, IETF has specified HPKE — while ECIES is a pure KEM-DEM scheme, parts of HPKE requires Diffie-Hellman and cannot be implemented with a KEM. Besides, HPKE provides no clear benefits for SUCI calculations. In fact, for a fixed tag length, GCM provides worse integrity properties than HMAC-SHA2 and KMAC, which is the reason why ETSI SAGE has specified GCM-SST [X3] for use in 6G. Using HPKE would also give up change control to the IETF.

Considerations for Hybrid KEM

When using a hybridized PQC KEM with ML-KEM, it is essential to use a standardized key combiner that preserves the IND-CCA2 security of ML-KEM, hybridization must not weaken the security properties. While ML-KEM is currently the only practical option, the key combiner should be designed in a general way so that the same construction can be reused in future profiles with other KEMs beyond ML-KEM. Additional KEMs may be introduced in proprietary profiles or standardized by 3GPP in the future. Two standardized and compatible IND-CCA2 key combiners are specified in Section 4.6 of SP 800-227 [X7] and Section 8.2 of ETSI TS 103 744 [X8]. Below is equation (9) from SP 800-227 [X7], which focuses on the information elements:

K ← KeyCombine(K1, K2, c1, c2, ek1, ek2, p)

KDF, MAC, and Encryption

Any implementation of ML-KEM [X4] already support of SHA3-256, SHA3-512, SHAKE128, and SHAKE256, which ML-KEM uses natively — therefore, using SHA-3 for key derivation and MAC in PQC SUCI is a natural choice. Also, SEC1 standard [9], specifying ECIES, published in 2009, says that future versions of the standard are likely to allow SHA3. Moreover, SHA-3 is theoretically (random oracle and no length extension attacks) and practically (strong side-channels resistance and simplicity) superior to SHA-2 [X6]. Considering the ongoing work on 256-bit and AEAD study, all PQC SUCI profiles should use AES-256 for encryption.

New SUCI Profiles

This solution proposes that the 3GPP SUCI profiles in TS 33.501 [4] should be updated to include profiles for both standalone ML-KEM and ML-KEM hybridized with X25519 — both fit into the designed length limit (3000 bytes). These profiles should use algorithms from the SHA-3 family (e.g., SHA3-256, KMAC256) [X9, X10], both for the MAC and in the KDF.

Below are two suggested profiles, with the formatting intentionally left out.

**Standalone ML-KEM Profile:**

The parameters for this profile shall be the following:

- KEM domain parameters : ML-KEM-768

- KEM primitive : ML-KEM-768

- point compression : N/A

- KDF : ANSI-X9.63-KDF [9]

- Hash : SHA3-256

- SharedInfo1 : ML-KEM encapsulation (ciphertext)

- MAC : KMAC256

- mackeylen : 32 octets (256 bits)

- maclen : 8 octets (64 bits)

- SharedInfo2 : the empty string

- ENC : AES–256 in CTR mode

- enckeylen : 32 octets (256 bits)

- icblen : 16 octets (128 bits)

- backwards compatibility mode : false

**Hybrid ML-KEM Profile:**

The parameters for this profile shall be the following:

- KEM domain parameters : ML-KEM-768 + X25519

- KEM primitive : ML-KEM-768 + X25519

- point compression : N/A

- KDF : ANSI-X9.63-KDF [9]

- Hash : SHA3-256

- SharedInfo1 : Combine(c1, c2, ek1, ek2, p)

- MAC : KMAC256

- mackeylen : 32 octets (256 bits)

- maclen : 8 octets (64 bits)

- SharedInfo2 : the empty string

- ENC : AES–256 in CTR mode

- enckeylen : 32 octets (256 bits)

- icblen : 16 octets (128 bits)

- backwards compatibility mode : false

##### 7.2.1.Y.3 Evaluation

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