**3GPP TSG-SA3 Meeting #122 S3-25xxxx**

Fukuoka, Japan, 19 – 23 May 2025

**Title: LS on** **Augmenting SUCI Protection with ML-KEM**

**Release: Rel-20**

**Source:** **Ericsson (to be SA WG3)**

**To:** **ETSI SAGE**

**Cc:**

**Contact person: Mohsin Khan**

**mohsin.a.khan@ericsson.com**

**Send any reply LS to: 3GPP Liaisons Coordinator,** [**mailto:3GPPLiaison@etsi.org**](mailto:3GPPLiaison@etsi.org)

**Attachments:**

# 1 Overall description

Many governments are recommending or requiring the migration to post-quantum cryptography (PQC) as soon as possible. Priority is being given to systems considered critical infrastructure or those susceptible to “harvest now, decrypt later” attacks, which are to be migrated by 2030. Supporting PQC before 2030 in deployments implies normative work in Rel-20, as the first Rel-21 deployments are not expected until 2030.

Most uses of asymmetric cryptography in 5G relies on IETF protocols and profiles, such as the TLS 1.3 handshake, IKEv2, X.509, CMP, CRL, OCSP, JOSE, and COSE. One exception is Subscription Concealed Identifier (SUCI) protection. TS 33.501 Annex C [1] specifies protection schemes for concealing the subscription permanent identifier (SUPI). The standardized protection profiles are based on SECG ECIES [2], following recommendations from ETSI SAGE. SA3 profiled the SECG specification and extended it to support Curve25519 and HMAC-SHA-256 (with 64-bit long tag).

During the specification of SUCI protection, SA3 also considered the future need for post-quantum cryptography and therefore specified a maximum SUCI length of 3000 bytes to accommodate lattice-based key encapsulation mechanisms (KEMs). NIST has now standardized the lattice-based ML-KEM in FIPS 203 [3], paving the way for its use in SUCI protection. ML-KEM comes in three parameter sets, ML-KEM-512, ML-KEM-768, and ML-KEM-1024. ML-KEM-768 hybrids with X25519 were widely supported in TLS 1.3, IKEv2, and SSH implementations.

SA3 understanding is that, although ECIES, like TLS 1.3, was originally designed for elliptic-curve Diffie-Hellman (ECDH), both effectively use ECDH as a Key Encapsulation Mechanism (KEM). Similarly, it is SA3’s understanding that ML-KEM [3] and ML-KEM hybrids such as X-Wing [4–5] are drop-in replacements for ECDH in SUCI protection. Two example profiles are given in clause 2.

**SA3’s understanding and plans:**

* ML-KEM and its hybrids, such as X-Wing, serve as drop-in replacements for ECDH in SUCI protection.
* Using a single encryption algorithm across all security levels simplifies implementation. AES-256 in CTR mode provides adequate security for all ML-KEM parameter sets.
* For ML-KEM and its hybrids (e.g., X-Wing), the encapsulation is no longer a public key. SA3 intends to set SharedInfo1 to the KEM encapsulation (called ciphertext in [3-5]).
* SA3 plans to retain the use of ANSI-X9.63-KDF with SHA-256 for key derivation, and HMAC–SHA-256 as the MAC algorithm, using a 256-bit key and a 64-bit tag.

**References:**

[1] 3GPP TS 33.501, Security architecture and procedures for 5G System  
<https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169>

[2] SECG SEC 1: Elliptic Curve Cryptography  
<https://www.secg.org/sec1-v2.pdf>

[3] NIST FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard  
<https://csrc.nist.gov/pubs/fips/203/final>

[4] X-Wing: The Hybrid KEM You’ve Been Looking For  
<https://cic.iacr.org/p/1/1/21>

[5] X-Wing: general-purpose hybrid post-quantum KEM  
<https://datatracker.ietf.org/doc/html/draft-connolly-cfrg-xwing-kem>

# 2 Example profiles

C.3.4.3 Profile C

The parameters for this profile shall be the following:

- KEM domain parameters : X-Wing

- KEM primitive : X-Wing

- point compression : N/A

- KDF : ANSI-X9.63-KDF [29]

- Hash : SHA-256

- SharedInfo1 : X-Wing encapsulation (ciphertext)

- MAC : HMAC–SHA-256

- 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

C.3.4.3 Profile D

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 [29]

- Hash : SHA-256

- SharedInfo1 : ML-KEM encapsulation (ciphertext)

- MAC : HMAC–SHA-256

- 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

# 3 Actions

**To ETSI SAGE**

**ACTION:** SA3 kindly asks ETSI SAGE to confirm whether its understanding of how to augment SUCI protection using ML-KEM is correct, and to provide guidance as needed.

# 4 Dates of next TSG SA WG 3 meetings

SA3#123 25 – 29 August 2025 Goteborg, Sweden

SA3#124 13 – 17 October 2025 China