**3GPP TSG-SA3 Meeting #123 S3-252762**

**Goteborg, Sweden, 25 – 29 August 2025**

**Source: Samsung**

**Title: Pseudo-CR on PQC shared key solution for SUPI Concealment**

**Document for: Approval**

**Agenda item: 5.2.1**

**Spec: 3GPP TR 33.703**

**Version: v0.1.0**

**Work Item: FS\_CryptoPQC**

**Comments**

This pCR provides SUPI concealment solution using Post Quantum Cryptography (PQC) method.

\* \* \* 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*.

[zz] 3GPP TS 33.501: "Security architecture and procedures for 5G system (Release 19)".

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

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

### 7.2 Solutions

Editor’s Note: This clause contains solutions to update 3GPP defined security protocols (for example SUCI calculation) to use the appropriate PQC algorithm, if those protocols are not expected to be updated by other SDOs to use PQC algorithms.

### 7.2.X Solutions to Protocol #1: PQC based SUPI Concealment

Editor’s Note: If only SUCI calculation is considered, this subclause may be removed. If other protocol, e.g. MIKEY-SAKKE is studied, this subclause is used for each of such protocol identified.

#### 7.2.X.Y Solution #1 to Protocol #1: SUPI Concealment using PQC Shared Key

##### 7.2.X.Y.1 Introduction

To counter the threat of quantum computing to asymmetric cryptography used in ECIES scheme, it is necessary to replace existing algorithms with new, quantum-resistant Post Quantum Cryptography (PQC) ML-KEM algorithms proposed by NIST [aa].

##### 7.2.X.Y.2 Solution details

##### 7.2.X.Y.2.1 Processing on UE side

The PQC shared key generation scheme is implemented such that for computing a fresh SUCI, the UE uses the provisioned PQC-based public key of the home network, and PQC-based key encapsulation mechanism (KEM) according to the parameters provisioned by home network. The processing on UE side is done as mentioned below.

1. UE generates an ephemeral shared key and an encrypted PQC shared key based on a PQC-based public key associated with the home network.

2. UE generates ephemeral symmetric encryption key and ephemeral MAC key using a KDF function and ephemeral shared key.

3,4. UE protects the plaintext block (i.e. *SUPI or* UE ID*)*, using the encryption key and the MAC key. The final output is the concatenation of encrypted PQC shared key, the ciphertext (i.e., Enc(SUPI)) value, and MACtag value.

The Figure 7.2.X.Y.2-1 illustrates the UE's steps.



Figure 7.2.X.Y.2-1: Encryption based on PQC shared key generation at UE

Finally, the proposed solution comprises transmitting the encrypted PQC shared key along with cipher-text value and MAC-tag value associated with the subscriber by the UE to a network entity for authenticating the subscriber. The scheme output as defined in TS 23.003 [zz] to be updated to scheme output shown in Figure 7.2.X.Y.2-2.



Figure 7.2.X.Y.2-2: Scheme output based on SUPI concealment using PQC shared key

##### 7.2.X.Y.2.2 Processing on home network side

The PQC shared key generation scheme is implemented such that for deconcealing a SUCI, the home network uses the received encrypted PQC shared key, and the PQC-based private key of the home network.

1. Home network (HN) decapsulates the encrypted PQC shared key to derive the ephemeral shared key.

2. HN generates ephemeral symmetric encryption key and ephemeral MAC key using a KDF function and derived ephemeral shared key.

3,4. HN verifies the MAC and decrypts the ciphertext to derive the plaintext block (i.e. *SUPI or* UE ID*)*, using the MAC key and encryption key respectively.

Figure 7.2.X.Y.2-3 illustrates the home network's steps.



Figure 7.2.X.Y.2-3: Decryption based on PQC shared key generation at home network

##### 7.2.X.Y.2.2 Sample profile for SUCI Calculation

Profile C uses ML-KEM as defined in [aa] to generate shared key Z1 integrated with AES encryption scheme.

##### 7.2.X.Y.2.2.1 Profile C (PQC only)

The ME and SIDF implement this profile. The parameters for this profile are the following:

- ML KEM parameters : Level 3 (k, lattice dimension 3)

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

- Hash : SHA-256

- Shared secret key Z1 : Shared secret field from ML-KEM

- MAC : HMAC–SHA-256

- mackeylen : 32 octets (256 bits)

- maclen : 8 octets (64 bits)

- SharedInfo1 : N/A

- SharedInfo2 : the empty string

- ENC : AES–256 in CTR mode

- enckeylen : 32 octets (256 bits)

- icblen : 32 octets (256 bits)

##### 7.2.X.Y.3 Evaluation

TBD

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