**3GPP TSG-SA3 Meeting #124 draft\_S3-253842**

**Wuhan, China, 13 – 17 October 2025** *revision of S3-253523*

**Source: Thales, ORANGE, LG Uplus, SK Telecom**

**Title: Hybrid PQC for SUCI calculation**

**Document for: Approval**

**Agenda item: 5.2.1**

**Spec: 3GPP TR 33.703**

**Version: 0.1.0**

**Work Item: FS\_CryptoPQC**

**Comments**

This contribution proposes to address SUCI calculation in TR 33.703 and add a solution based on GSMA guidelines for SUCI calculation described in "Post Quantum Cryptography – Guidelines for Telecom Use Cases – v2.0".

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

### 7.2.1 Solutions to Protocol #1: SUCI calculation

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.

#### 7.2.1.Y Solution #Y to Protocol #1: GSMA-based solution

##### 7.2.1.Y.1 Introduction

GSMA published guidelines "Post Quantum Cryptography – Guidelines for Telecom Use Cases – v2.0" [a] to support the planning, setup and execution of a quantum safe cryptography journey for telco industry. This GSMA report contains a detailed analysis of an initial set of Telcom use cases that are impacted by Post Quantum Cryptography. Concealment of the Subscriber Public Identifier is one of the analysed use cases.

An additional security enhancement is proposed to the solution described in GSMA guidelines [a].

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

The solution for concealment of the Subscriber Public Identifier is based on the hybridization between ML-KEM (Level 3) and classic ECC based key exchanged algorithms that is described in clause 5.8 of GSMA guidelines [a].

GSMA solution is enhanced thanks to the addition of Post Quantum ciphertext as input to the Key Derivation Function in the Post Quantum Cryptography part, as recommended to obtain IND-CCA (indistinguishability under chosen-ciphertext attack) property for KEM.

Processing on UE side:



Processing on home network side



Profiles

The associated updated profiles are the following ones. In both cases, the Key Derivation Function (KDF) outputs a L-bytes string that must be parsed as Eph Encryption key || ICB || Eph. Mac Key, where Eph Encryption key is of size enkeylen, ICB is of size icblen, and Eph. Mac Key is of size mackeylen.

### Profile A’ (update of Profile A to support PQC algorithm)

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

- KEM domain parameters : ML-KEM-768 [b]

- EC domain parameters : Curve25519

- KEM primitive : ML-KEM-768 [b]

- EC Diffie-Hellman primitive : X25519

- point compression : N/A

- KDF : HMAC-based KDF RFC 5869 [d] (SHA-256)

- Hash : SHA-256

- KDF inputs (see RFC 5869 [d] terminology):

 -salt : empty

 -IKM (input key material) : Eph. shared key1 || Eph. shared key 2

 -Info : Post-Quantum Ciphertext || Eph. Public key

 -L (output length in octets) : 80

- MAC : HMAC–SHA-256

- mackeylen : 32 octets (256 bits)

- maclen : 16 octets (128 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

### Profile B’ (update of Profile B to support PQC algorithm)

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

- KEM domain parameters : ML-KEM-768 [b]

- EC domain parameters : secp256r1

- KEM primitive : ML-KEM-768 [b]

- EC Diffie-Hellman primitive : Elliptic Curve Cofactor Diffie-Hellman Primitive

- point compression : true

- KDF : HMAC-based KDF RFC 5869 [d] (SHA-256)

- Hash : SHA-256

- KDF inputs (see RFC 5869 [d] terminology):

 -salt : empty

 -IKM (input key material) : Eph. shared key1 || Eph. shared key 2

 -Info : Post-Quantum Ciphertext || Eph. Public key

 -L (output length) : 80

- MAC : HMAC–SHA-256

- mackeylen : 32 octets (256 bits)

- maclen : 16 octets (128 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

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

Editor’s Note: Reasons for using c1c2 as the input for the KDF are FFS.

##### 7.2.1.Y.3 Evaluation

TBD

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

# 2 References

[a] GSMA: "Post Quantum Cryptography – Guidelines for Telecom Use Cases - v2.0"

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

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

[d] IETF RFC 5869 "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)"

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