**3GPP TSG-SA3 Meeting #124 S3-253839-r3**

**Wuhan, China, 13 – 17 October 2025 (revision of S3‑253475)**

**Source: LG Electronics**

**Title: Solution for SUCI calculation using quantum key**

**Document for: Approval**

**Agenda item: 5.2.1**

**Spec: 3GPP TR 33.703**

**Version: v0.1.0**

**Work Item: FS\_CryptoPQC**

**Comments**

This proposal adds new solution for SUCI calculations.

\* \* \* First 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: SUCI calculations

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 #Y to Protocol #1: Enhancement on SUCI calculations using quantum key

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

This solution provides enhancement for SUCI calculations to resolve post-quantum threats to existing ECIES scheme.

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

This solution describes SUCI calculations using Quantum Channel. The UE can provision Public key of HN and Quantum Public Key. Based on ECIES scheme, the ephemeral public key, cipher text, and MAC tag can be generated as an output. Additionally, using the Quantum Public Key, the cipher text can be encapsulated. The encapsulated cipher text is delivered to the Home Network via Quantum Channel. The Home Network decapsulates it with Quantum private key, then deciphers ciphered text and verifies MAC.

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

The steps shown Figure 7.2.X.Y.2.1 are described as below:

1. As a prerequisite, the UE provisions both Public key of HN and Quantum Public key.
2. The UE generates Ephemeral key pair consisting of Ephemeral Public Key and Ephemeral Private Key.
3. Based on the generated Ephemeral Private Key and the Public key of Home Network, the UE generates Ephemeral Shared Key.
4. Using ECIES scheme, Ephemeral Encryption Key, ICB and Ephemeral MAC Key are generated.
5. Plaintext is ciphered using the Ephemeral Encryption Key.
6. The ciphered text and the Ephemeral MAC key are used to create MAC-tag value.
7. The ciphered text value is encapsuled using Quantum Public Key.



Figure 7.2.X.Y.2.1: Encryption at UE

The final output shall be the concatenation of the ECC ephemeral public key, the Quantum encapsulated ciphertext value, the MAC tag value, and any other parameters, if applicable.

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

The steps shown Figure 7.2.X.Y.2.2 are described as below:

1. By decapsulating the encapsulated cipher-text using Quantum Private Key, the Home Network generates the cipher-text.
2. Based on the received Ephemeral Public Key, the Home Network generates Ephemeral Shared Key.
3. Using ECIES scheme, Ephemeral Decryption Key, ICB and Ephemeral MAC Key are generated.
4. The ciphered text is deciphered using the Ephemeral Decryption Key.
5. The Home Network verifies received MAC.



Figure 7.2.X.Y.2.2: Decryption at Home Network

Editor’s Note: Details on Step 6 at processing on UE side is FFS.

Editor’s Note: Details on Quantum Public key are FFS.

Editor’s Note: What is Quantum Channel is FFS.

Editor’s Note: Whether and how to support hybrid encryption.

Editor’s Note: Why SUCI should require a quantum channel into the HN is FFS.

Editor’s Note: What is a Quantum key and why it is required is FFS.

Editor's Note: The definition and usefulness of these terms for SUCI calculation are FFS: Post-quantum threat, Quantum channel, Quantum public key, Quantum-encapsulated, Quantum-encrypted, Quantum-ciphered, Quantum Private key.

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

TBD

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