**3GPP TSG-SA3 Meeting #124 S3-253841-r2**

**Wuhan, China, 13 – 17 October 2025 (revision of S3‑253476)**

**Source: LG Electronics**

**Title: Solution for SUCI calculation using quantum encapsulated 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.Z Solution #Z to Protocol #1: Enhancement on SUCI calculations using quantum encapsulated key

##### 7.2.X.Z.1 Introduction

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

##### 7.2.X.Z.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 and MAC tag can be generated as a part of output. To cipher plain text, The Ephemeral Encryption key is encapsulated using Quantum Public Key. Using the Quantum-encapsulated Ephemeral Encryption key, the Plaintext is quantum-encrypted. The cipher text is delivered to the Home Network via Quantum Channel. The Home Network decapsulates the received quantum-ciphered text using HN-generated Ephemeral decryption key. By decrypting it using Quantum Private key, The Home Network obtains plain text. Then verifies received MAC.

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

The steps shown Figure 7.2.X.Z.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 and Ephemeral MAC Key are generated.
5. The plain text and the Ephemeral MAC key are used to create MAC-tag value.
6. The Ephemeral Encryption Key is encapsulated using Quantum Public Key.
7. The Plaintext Block is encrypted using the Quantum Encapsulated Ephemeral Encryption Key.

 

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

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

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

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

1. Based on the received Ephemeral Public Key, the Home Network generates Ephemeral Shared Key.
2. Using ECIES scheme, Ephemeral Decryption Key and Ephemeral MAC Key are generated.
3. The Home Network decapsulates the received Quantum-ciphered text using the Ephemeral Decryption Key.
4. The Home Network decrypts the decapsulated Quantum-ciphered text using the Quantum Private Key. Then the Home network obtains the plain text.
5. The Home Network verifies received MAC. For the verification, plaintext and Ephemeral MAC key are utilized.

 

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

Editor’s Note: Details on Step 5 at processing on UE side is FFS.

Editor’s Note: How to sync of usage of Quantum keys at UE and HN sides is FFS.

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

Editor’s Note: Details on Step 3 at processing on HN side is FFS.

Editor’s Note: Whether the plaint text is encrypted with quantum public key (the Encryption figure at UE) is FFS.

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: How this solution is different from the solution in S3-253475 is FFS

##### 7.2.X.Z.3 Evaluation

TBD

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