**3GPP TSG-SA3 Meeting #124 S3-253863**

**Wuhan, China, 13 – 17 October 2025 (revision of S3-253289)**

**Source: Nokia**

**Title: Pseudo-CR on Solution proposal PQC for SUCI protection**

**Document for: Approval**

**Agenda item: 5.2.1**

**Spec: 3GPP TR 33.703**

**Version: 0.1.0**

**Work Item: FS\_CryptoPQC**

**Comments**

This pCR is introducing the PQC support for SUCI protection.

The solution is as much as possible reusing the existing ECIES implementation and is replacing with PQC related as needed.

The proposed solution is to be added into the TR study on transition to PQC [1].

[1] TR 33.703, “Study on Transitioning to Post Quantum Cryptography (PQC) in 3GPP”

[x1] 3GPP TS 33.501

\* \* \* 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 #X: <Title>

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 #X: Solution on PQC for SUCI protection

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

The ECIES procedure as depicted by the 5G system architecture [x1] is the basis for the development of the PQC solution.

For the transition to PQC the relevant functional blocks will have to replace the existing/corresponding ECIES functional blocks.

The following Figure depicts the Encryption based on ECIES at the UE side.

A diagram of a keyword

AI-generated content may be incorrect.

Figure 7.2.x.y.1-1: Encryption based on ECIES at the UE

The following Figure depicts the Decryption based on ECIES at the home network side.

A diagram of a diagram

AI-generated content may be incorrect.

Figure 7.2.x.y.1-2: Decryption based on ECIES at the Home Network

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

The solution is replacing the ECIES functional blocks with corresponding/related PQC related functional blocks.

The following Figure depicts the PQC concept at the UE side. The functions which must be modified for the support of PQC are with green coloured background.



Figure 7.2.x.y.2-1: SUCI protection based on PQC algorithms at the UE side

At UE: PQC KEM public key of HN is used in Key encapsulation mechanism to generate ciphertext and shared secret. This shared secret is used as an input to Key Derivation Function (KDF) to generate the Encryption key to generate cipher text of SUPI and MAC value.

The following is applicable:

This step 1, as shown by the Figure 7.2.x.y.1-1, is for the transition to PQC not required, i.e., there is no creation of Ephemeral Keys needed in this concept.

2> The Kem Encapsulation Function will get the public key (pk) as input and is providing the cipher text (ct) and the shared secret (ss). The (ct) will be have to be send back to the network, whereas the (ss) will be used as input to the key derivation function.

3> The key derivation function is receiving the shared secret (ss) and is calculating the encryption key. There will be created a single key that is to be used for encryption and integrity protection.

4> The encryption is used for the computation of the encrypted plaintext block, i.e., ciphertext value.

5> The encryption is used for the computation of the MAC-I, i.e., MAC-tag value.

Both the ciphertext and the MAC-tag value will be included into the SUCI framework (see Figure 7.2.x.y.2-3) and will be sent to the Network for further treatment.

At Network side: The received PQC KEM cipher text is used along with the PQC KEM Secret key of HN (corresponding to received PQC KEM public key Id) to decapsulate and generate the shared secret. This shared secret is used as an input to KDF to generate the decryption key to decipher the cipher text and verify the MAC.

The following Figure depicts the PQC concept at the Network side.

A diagram of a computer program

AI-generated content may be incorrect.

Figure 7.2.x.y.2-2: SUCI protection based on PQC algorithms at the Home Network side

The following is applicable:

1> The Network side is retrieving the cipher text (ct) from the SUCI framework. The secret key (sk) is local stored and corresponds to the public key (pk) which has been share with UE. Both, the (ct) and the (sk) will be given as input to the Key Decapsulation function and the outcome is the shared secret (ss). The (ss) will be used as input to the key derivation.

2> The key derivation function is receiving the shared secret (ss) as input and is computing the decryption key. There will be created a single decrypt key that is to be used for decryption and integrity verification.

3> The decryption key is used for the computation of the Plaintext block.

4> The decryption key is used for the computation of the MAC-I verification.

If we apply this solution concept, then the SUCI framework is as depicted by below Figure.

A close-up of a computer screen

AI-generated content may be incorrect.

Figure 7.2.x.y.2-3: SUCI framework for PQC

Home Network Public Key Identifier (PQC KEM) represents a public key provisioned by the HPLMN or SNPN and it is used to identify the key used for SUPI protection. Example of the PQC KEM Public key is Kyber (selected by NIST standards).

PQC KEM ciphertext: Post Quantum Cryptography Key encapsulation mechanism uses the PQC KEM public key of Home Network to generate the ciphertext.

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

TBD

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