**3GPP TSG-SA3 Meeting #123 S3-252984-r6**

Goteborg, Sweden, 25 – 29 August 2025 (merger of S3-252719, S3-252636, S3-252759, S3-252841)

**Source: Nokia, Samsung, Thales, Huawei**

**Title: New Key issue for PQC SUCI Protection**

**Document for: Approval**

**Agenda Item: 5.2.1**

# 1 Decision/action requested

 ***This document proposes to add a new key issue for security concerns of adapting PQC for SUCI protection in TR 33.703.***

# 2 References

[1] SP-250858 New Study on transitioning to Post Quantum Cryptography in 3GPP

# 3 Rationale

To enhance and adapt the quantum related algorithms and procedures to existing SUCI protection. Making the SUCI in both 5G /6G, quantum safe against attacks from a Cryptographically Relevant Quantum Computer (CRQCs) implementing Shor’s and Grover’s algorithm.

# 4 Detailed proposal

**\*\*\*\*** START OF 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*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[x1] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[x2] SECG SEC 1: “Recommended Elliptic Curve Cryptography”, Version 2.0, 2009. Available at <http://www.secg.org/sec1-v2.pdf>.

[x3] SECG SEC 2: “Recommended Elliptic Curve Domain Parameters”, Version 2.0, 2010. Available at <http://www.secg.org/sec2-v2.pdf>.

[x4] 3GPP TR 33.938: "3GPP Cryptographic Inventory (Release 19)"

**\*\*\*\*** NEXT CHANGE **\*\*\*\***

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

ECIES Elliptic Curve Integrated Encryption Scheme

PQC Post Quantum Cryptography

SECG Security Engineering & Consulting Group

SUCI Subscription Concealed Identifier

**\*\*\*\*** NEXT CHANGE **\*\*\*\***

# 7 Protocols expected to be updated for PQC by 3GPP

Editor’s Note: This clause contains identification of the protocols with asymmetric cryptography listed in TR 33.938 that are not expected to be updated by other SDOs in a near future to use PQC, e.g., MIKEY-SAKKE and SUCI calculation, security threats and alternative solutions for the 3GPP procedures if they are not updated to use PQC.

### 7.1 Threats

Editor’s Note: This clause contains security threats for the 3GPP procedures if they are not updated to use PQC.

### 7.1.X Protocol #Y: 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.

As per TS 33.501 [x1] and Table 4.3.2-1 of 3GPP Cryptographic inventory 3GPP TR 33.938 [x4], the SUCI calculation is done based on ECIES scheme. The ECIES is specified in the SECG version 2 [x2] and [x3].

Since ECIES will not be updated by SECG with PQC algorithms, 3GPP should study alternative solutions for SUCI calculation due to post-quantum threats to existing ECIES scheme.

**\*\*\*\*** END OF CHANGE **\*\*\*\***