**3GPP TSG-SA3 Meeting #124 *S3-253833***

**Wuhan, China, 13 - 17 October 2025 *revision of S3-253231***

**Source: Apple**

**Title: Editorial updates to Clause 7.1**

**Document for: Approval**

**Agenda Item: 5.2.1**

# 1 Decision/action requested

***Approve the pCR to TS 33.703***

# References

1. TR 33.703

# 3 Rationale

This contribution proposes the editorial change to clause 7.1

# 4 Detailed proposal

\*\*\* Start of 1st Change \*\*\*

### 7.1 Threats

### 7.1.1 General

Most of security protocols used in 3GPP systems are specified in other standards development organizations (SDOs). In case that these protocols are not updated to use PQC in other SDOs, the 3GPP system may be vulnerable to attacks based on quantum computation. The clause 7.2 contains all of these protocols identified and potential solutions to address the issues.

### 7.1.2 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.

As per TS 33.501 [4] and Table 4.3.2-1 of 3GPP Cryptographic inventory 3GPP TR 33.938 [2], the SUCI calculation is done based on ECIES scheme. The ECIES is specified in the SECG version 2 [9] and [10].

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.

\*\*\* Start of 2nd 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.

### 7.2.1 Solutions to Protocol 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 SUCI calculation

##### 7.2.1.Y.1 Introduction

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

##### 7.2.1.Y.3 Evaluation

### 7.2.2 Solutions to Protocol MIKEY-SAKKE key exchange

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.

#### 7.2.2.Y Solution #Y to Protocol MIKEY-SAKKE key exchange

##### 7.2.2.Y.1 Introduction

##### 7.2.2.Y.2 Solution details

##### 7.2.2.Y.3 Evaluation

\*\*\* End of 2nd Change \*\*\*