**3GPP TSG-SA3 Meeting #123 S3-252976-r1**

**Goteborg, Sweden, 25 – 29 August 2025**

**Source: Huawei, HiSilicon, LG Electronics**

**Title: Pseudo-CR on Scope of TR 33.703**

**Document for: Approval**

**Agenda item: 5.2.1**

**Spec: 3GPP TR 33.703**

**Version: 0.0.0**

**Work Item: FS\_CryptoPQC**

**Comments**

This contribution provides scope of the study.

\* \* \* First Change \* \* \* \*

The present document studies the complexities involved with the introduction of standalone and/or hybrid Post Quantum Cryptography (PQC) algorithms in existing security protocols used by 5G specifications. These security protocols and their associated algorithms have been listed in TR 33.938 [x] “3GPP Cryptographic Inventory”. Specifically,

* Studies principles and attributes of PQC relevant to use in 3GPP procedures.

- Studies the impact of using hybrid and standalone PQC algorithms in 3GPP procedures

- impact to 3GPP procedures due to larger length of PQC key, signature, and message compared to the length of those in traditional cryptography.

- Determines security levels (I-V) required to align with existing 3GPP procedures level of assurance.

- Studies the suitability of classes of post-quantum signature algorithms (e.g., lattice-based, hash-based) to 3GPP procedures.

* Identifies the protocols with asymmetric cryptography listed in TR 33.938 [x] that are not expected to be updated by other Standards Development Organizations (SDOs) in a near future to use PQC, e.g., MIKEY-SAKKE and SUCI calculation
* Studies security threats and alternative solutions for the 3GPP procedures if they are not updated to use PQC.
* Documents the expected timeline for when security protocols defined by other SDOs will include PQC algorithms and be available for inclusion into 3GPP procedures. The timeline includes the availability of stable protocols.
* Studies 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.

This present document is Generation agnostic.

\* \* \* Next 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".

[x] 3GPP TR 33.938: "3GPP Cryptographic Inventory".

\* \* \* 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].

MIKEY-SAKKE Multimedia Internet KEYing – Sakai-Kasahara Key Encryption

PQC Post Quantum Cryptography

SDO Standards Development Organizations

SUCI Subscription Concealed Identifier

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