**3GPP TSG-SA3 Meeting #124 S3-253691-r4**

**Wuhan, China, 13 – 17 October 2025**

**Source: Ericsson, Qualcomm, NCSC, NPL, NTAC, BSI, NIST, US NSA, BT, Vodafone, KDDI, Verizon, Huawei, HiSilicon**

**Title: Pseudo-CR on General Assumptions of the PQC study**

**Document for: Approval**

**Agenda item: 5.2.1**

**Spec: 3GPP TR 33.703**

**Version: 0.1.0**

**Work Item: FS\_CryptoPQC**

**Comments**

This pCR proposes a set of general assumptions.

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

# 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".

[2] 3GPP TR 33.938: "3GPP Cryptographic Inventory".

[3] 3GPP TS 33.180: "Security of the Mission Critical (MC) service".

[4] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[5] IETF Internet-Draft: "Post-Quantum Cryptography for Engineers".

[6] IETF RFC 6509: ''MIKEY-SAKKE: Sakai-Kasahara Key Encryption in Multimedia Internet KEYing (MIKEY)''.

[7] IETF RFC 9794: "Terminology for Post-Quantum Traditional Hybrid Schemes".

[8] NIST IR 8547: "Transition to Post-Quantum Cryptography Standards".

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

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

\* \* \* Next Change \* \* \* \*

## 4.2 General Assumptions

In the present document, PQC is referred to as cryptographic algorithms that are deemed to be secure against attacks from both classical and quantum computing.

All traditional public key cryptographic algorithms used in 3GPP systems need to be migrated to PQC algorithms. If suitable PQC options are not available, then an alternative path needs to be provided and justified, e.g. deprecation, mitigation, and re-architecting.

The PQC options are to be drawn from well-studied standardised primitives and protocols.

Both hybrid and standalone KEM are in the scope of this study. Standalone and hybrid signatures are also in the scope of this study.

Editor’s Note: Further general assumptions are FFS.

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