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

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

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

**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>.

[X1] 3GPP LS: "3GPP Statement on PQC Migration", <https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_118_Hyderabad/docs/S3-244307.zip>

[X2] 3GPP LS: "LS reply to GSMA on PQC", <https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_116_Jeju/docs/S3-242378.zip>

[X3] 3GPP LS: "LS on Quantum Safe Cryptographic Protocol Inventory", <https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_116_Jeju/docs/S3-242377.zip>

\* \* \* 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. Alternatives include, but are not limited to, deprecation, mitigation, and re-architecting.

PQC algorithms and traditional algorithms co-exist until transition is completed.

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.

The availability of interoperable implementations of standards is an important factor for 3GPP standardization, as it enables cost-effective, reliable, and interoperable deployments.

For protocols like TLS 1.3 and IKEv2, which support negotiation of cryptographic parameters, PQC algorithms can be deployed as soon as the relevant IETF specifications and well-tested implementations are available.

For protocols such as SUCI calculation, which are defined by 3GPP and require explicit 3GPP specification for UE and core network interoperability, 3GPP should start the specification work as soon as possible by first identifying suitable standardized PQC algorithms.

NOTE X: The conclusions of previous work in 3GPP on symmetric cryptography still stand — the widely accepted position is that 128-bit symmetric algorithms will remain secure for decades [X1, X2, X3]. In many cases 3GPP specifications already have an option to use larger key sizes. For other cases, 3GPP is working on specifying the usage of the 256-bit algorithms to complement the 128-bit symmetric algorithms.

NOTE Y: When a 3GPP crypto profile does not explicitly forbid a cryptographic algorithm, it means that the cryptographic algorithm is optional to use. Since the 3GPP profiles for TLS 1.3 and IKEv2 do not currently list any PQC algorithms (i.e., do not forbid any PQC algorithms either), ML-KEM, ML-DSA, and SLH-DSA are effectively optional to use, and can be implemented by vendors. Nodes supporting PQC algorithms can still interoperate with legacy nodes that do not support PQC algorithms, provided both sides are standards compliant.

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