**3GPP TSG-SA3 Meeting #124 S3-253688-r1**

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

**Source: Ericsson, Qualcomm, NCSC, NPL, NTAC, BSI, NIST, US NSA, BT, Vodafone, KDDI, Verizon, Cisco, Deutche Telekom, Telecom Italia, Nokia, Thales**

**Title: Pseudo-CR on Transition timeline 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**

<Proposals, reason for change, abstract, comments if necessary (optional)>

\* \* \* 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] EU, Roadmap for the Transition to Post-Quantum Cryptography
<https://digital-strategy.ec.europa.eu/en/news/eu-reinforces-its-cybersecurity-post-quantum-cryptography>[X2] UK NCSC, Timelines for migration to post-quantum cryptography
<https://www.ncsc.gov.uk/guidance/pqc-migration-timelines>

[X3] NSA, Commercial National Security Algorithm Suite 2.0
<https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF>

[X4] ANSSI, Guide des Mécanismes cryptoraphiques
<https://cyber.gouv.fr/sites/default/files/2021/03/anssi-guide-mecanismes_crypto-2.04.pdf>

[X5] ASD, Guidelines for cryptography
https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism/cybersecurity-guidelines/guidelines-for-cryptography

[X6] Canadian Centre for Cyber Security, Roadmap for the migration to post-quantum cryptography
<https://www.cyber.gc.ca/en/guidance/roadmap-migration-post-quantum-cryptography-government-canada-itsm40001>

[X7] Swedish NCSC, Kvantsäker kryptografi
<https://www.ncsc.se/sv/aktuellt/kvantsaker-kryptografi/>

[X8] NSM Cryptographic Recommendations
<https://nsm.no/getfile.php/1314334-1742808614/NSM/Filer/Dokumenter/Veiledere/NSM%20Cryptographic%20Recommendations%202025.pdf>

[X9] AIVD, The PQC Migration Handbook
[https://english.aivd.nl/binaries/aivd-en/documenten/publications/2024/12/3/the-pqc-migration-handbook/The+PQC+Migration+Handbook+.pdf](https://english.aivd.nl/binaries/aivd-en/documenten/publications/2024/12/3/the-pqc-migration-handbook/The%2BPQC%2BMigration%2BHandbook%2B.pdf)

[X10] 3GPP, Release Timeline
<https://www.3gpp.org/specifications-technologies/releases/release-20>

\* \* \* 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

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

PKI Public Key Infrastructure

PQC Post-Quantum Cryptography

SDO Standards Development Organizations

SECG Security Engineering & Consulting Group

SUCI Subscription Concealed Identifier

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

### 4.1.1 Transition Timeline

Editor’s Note: More timeline information from other organizations is ffs.

Countries and agencies around the world are generally aligned on the need to migrate to Post-Quantum Cryptography (PQC). The common recommendation is to complete migration for high priority systems by around 2030 and for all systems by approximately 2035. Examples of government-issued PQC migration timelines can be found in [8, X1–X9]. Whether a system is high priority or not is determined by a variety of factors such as how long the data needs to remain confidentiality protected and what level of risk is the data owner willing to bear. Some parts of telecommunications systems may be assessed by the network operator to be of high priority.

Although the migration of signature-based authentication in protocols such as TLS and IPsec is typically not prioritized for transition until 2035, transitioning Public Key Infrastructures (PKI), which are necessary to support signature-based authentication, often takes a decade or more, making it critical to begin their transition almost immediately.

Furthermore, it is important to note that the above timelines apply to deployments. For full PQC adoption in deployed systems, it is essential that standards are updated, and stable implementations are made available well in advance of those deployment milestones. The timelines for different stakeholders in the ecosystem, such as standards development organizations (SDO), equipment vendors, and operators deploying the systems are inherently different. Standards bodies need to finalize specifications early, vendors need sufficient lead time to implement, test, and certify solutions, and only then can large-scale deployments take place.

3GPP Rel-20 specification is expected to be frozen in the mid-2027 [X10]. Rel-21 specification can be expected to be completed in the beginning of 2029 at the earliest. So, normative work on PQC migration in Rel-20 would be aligned with vendors and operators trying to meet the above described 2030 migration timeline for high priority systems.

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