**3GPP TSG-SA3 Meeting #123 S3-252977-r2**

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

**Source: Ericsson**

**Title: Pseudo-CR on assumptions of the PQC study**

**Document for: Approval**

**Agenda item: 5.2.1**

**Spec: 3GPP TR 33.703**

**Version: 0.0.0**

**Work Item: FS\_CryptoPQC**

**Comments**

This document proposes some content for the assumptions clause of the TR 33.703.

\* \* \* First 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".

[X1] IETF Statement on Quantum Safe Cryptographic Protocol Inventory, https://datatracker.ietf.org/liaison/1942/

[X2] 3GPP S3--244307: "3GPP Statement on PQC Migration", https://www.3gpp.org/ftp/tsg\_sa/WG3\_Security/TSGS3\_118\_Hyderabad/docs/S3-244307.zip

[X3] Sam Jaques, Quantum Attacks on AES, https://www.youtube.com/watch?v=eB4po9Br1YY&t=3227s

[X4] NIST, Transition to Post-Quantum Cryptography Standards, https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf

[X5] NCSC, Next steps in preparing for post-quantum cryptography, https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography

[X6] EU, Roadmap for the Transition to Post-Quantum Cryptography  
<https://digital-strategy.ec.europa.eu/en/news/eu-reinforces-its-cybersecurity-post-quantum-cryptography>

[X7] UK NCSC, Timelines for migration to post-quantum cryptography  
<https://www.ncsc.gov.uk/guidance/pqc-migration-timelines>

[X8] NIST IR 8547: "Transition to Post-Quantum Cryptography Standards"  
<https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf>

[X9] 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>

[X10] ANSSI, Guide des Mécanismes cryptoraphiques  
<https://cyber.gouv.fr/sites/default/files/2021/03/anssi-guide-mecanismes_crypto-2.04.pdf>

[X11] ASD, Guidelines for cryptography  
<https://cyber.gouv.fr/sites/default/files/2021/03/anssi-guide-mecanismes_crypto-2.04.pdf>

[X12] 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>

[X13] Swedish NCSC, Kvantsäker kryptografi  
<https://www.ncsc.se/sv/aktuellt/kvantsaker-kryptografi/>

[X14] NSM Cryptographic Recommendations  
<https://nsm.no/getfile.php/1314334-1742808614/NSM/Filer/Dokumenter/Veiledere/NSM%20Cryptographic%20Recommendations%202025.pdf>

[X15] 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>

[X16] NIST FIPS 203: "Module-Lattice-Based Key-Encapsulation Mechanism Standard"  
<https://doi.org/10.6028/NIST.FIPS.203>

[X17] NIST FIPS 204: "Module-Lattice-Based Digital Signature Standard"  
<https://doi.org/10.6028/NIST.FIPS.204>

[X18] NIST FIPS 205: "Stateless Hash-Based Digital Signature Standard"  
<https://doi.org/10.6028/NIST.FIPS.205>

[X19] ANSSI views on the Post-Quantum Cryptography Transition (2023 follow up) <https://cyber.gouv.fr/sites/default/files/document/follow_up_position_paper_on_post_quantum_cryptography.pdf>

[X20] ENISA EUCC Guidelines on Cryptography

<https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en>

[X21] 3GPP S3-242378: "Reply-LS on PQC Migration"

<https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_116_Jeju/docs/S3-242378.zip>

[X22] 3GPP S3-242377: " 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 Assumptions

## 4.1 General

This clause contains overall assumption and/or security assumptions for this study

## 4.2 Overview

The security protocols that use symmetric and/or asymmetric cryptography in 3GPP systems are listed in TR 33.938 [x1]. It is assumed that all the security protocols using asymmetric algorithms are potentially undermined by quantum computation. 3GPP specifications employ public-key cryptography in the TLS 1.2 and TLS 1.3 handshakes, IKEv2, PKI (including X.509 certificates, CMP, CRL, and OCSP), JOSE, COSE, SUCI Protection, and MIKEY-SAKKE. The TLS 1.3 handshake is used in DTLS 1.3, QUIC, and TLS-based EAP methods such as EAP-TLS 1.3. TLS 1.2 handshake is used in DTLS 1.2 and EAP-TLS 1.2. The DTLS handshake is also applied in DTLS-SRTP and DTLS over SCTP. COSE is used for SEAL CWT tokens. JOSE is used in PRINS and for JWT tokens in OAuth and OpenID.

Given the wide variation in requirements, specifications, technical capabilities, and implementation maturity across protocols, this study is organized by security protocol. Each major protocol, MIKEY-SAKKE, SUCI Protection, TLS 1.2 Handshake, TLS 1.3 Handshake, IKEv2, JOSE, and COSE, is covered in a separate clause. Technical evidence suggests that symmetric cryptography is not practically affected by quantum computers[X1–X5,X21, X22]. However, we need to further investigate this aspect in this study as some governmental agencies such as ANSSI and ENISA still encourage using larger key sizes [X19, X20]. This study does not focus on any particular generation of mobile networks and analyses various aspects that will be useful for PQC migration.

All 3GPP implementations using a security protocol need to comply with the corresponding 3GPP profile. If a specification does not explicitly reference the applicable profile, the reference needs to be added, with exceptions where appropriate.

In the present document, Post-quantum cryptography (PQC) is referred to as cryptographic algorithms that are deemed secure against attacks from both classical and quantum computation. Considering that the current PQC algorithms lack long-term validation in reality, the 3GPP system is assumed to support the capabilities to replace a PQC algorithm and/or add a new PQC algorithm wherever needed in an agile and smooth way to avoid potential security breaches.

## 4.3 Other organisations recommendations on PQC, deployments, and implications for 3GPP

Countries and agencies around the world are generally aligned on the need to migrate to post-quantum cryptography (PQC) as soon as possible. The common recommendation is to complete migration for prioritized systems by around 2030 and for all systems by approximately 2035. Examples of government-issued PQC migration timelines can be found in [X6–X15]. While definitions of "prioritized systems" vary between governments, they typically include systems protecting confidentiality, firmware and software updates, and critical infrastructure.

It is important to note that these government requirements apply to deployments. To enable full PQC adoption in deployed systems, standards need to be updated and implementations need to be available well in advance. Although the migration of signature-based authentication in protocols such as TLS and IPsec is typically not prioritized for completion until 2035, transitioning public key infrastructures (PKI) often takes a decade or more, making it critical to begin the development process immediately.

Since 3GPP Rel-21 is expected to enter deployment around 2030, all normative work related to PQC migration for prioritized systems needs to be finalized in Rel-20. Furthermore, to meet more aggressive government targets aiming for 100% PQC in deployment by 2030–2031, completing normative work early in Rel-20, rather than at the end, is strongly preferred.

Most governments require use of standardized or conservative PQC algorithms, such as the already standardized ML-KEM (FIPS 203), ML-DSA (FIPS 204), and SLH-DSA (FIPS 205) [X16–X18]. These are global standards designed by cryptographers from all over the world

A point of disagreement among governments is the use of hybrids. Some agencies require standalone ML-KEM and ML-DSA, while others mandate that, for now, ML-KEM and ML-DSA be hybridized with, for example, ECC. No government requires SLH-DSA to be hybridized. While the IETF and real-world deployments have embraced hybrid KEMs, hybrid signatures have not seen the same adoption.

With the publication of ML-KEM, ML-DSA, and SLH-DSA, Post-Quantum Cryptography (PQC) has quickly moved from research to implementation and deployment. In TLS, X25519MLKEM in has already seen massive implementation support and is the default in OpenSSL, Firefox, Chrome, Edge, Go, etc. Cloudflare reports that over 40% of all HTTPS client requests use PQC. OpenSSL 3.5 LTS supports ML-KEM, ML-DSA, and SLH-DSA. OpenSSH is now using mlkem768x25519 as the default key exchange, Many IKEv2 implementations support ML-KEM. IKEv2 always uses ML-KEM in hybrid with (EC)DHE. The availability of well-tested and interoperable implementations is an important factor for 3GPP standardization, as it enables cost-effective, reliable, and interoperable deployments.

5G relies on IETF protocols, such as IKEv2, TLS 1.3, DTLS, JOSE, the Internet X.509 profile, CMP, CRL, OCSP, EAP-TLS, and EAP-AKA-FS, for almost all uses of public-key cryptography. The IETF is therefore critical to the migration of 5G to PQC. 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 implementations are available. Since the 3GPP TLS 1.3 and IKEv2 profiles do not currently list any PQC algorithms, ML-KEM, ML-DSA, and SLH-DSA are optional and can be implemented by vendors. Nodes supporting PQC algorithms can still interoperate with legacy nodes that do not, provided both sides are standards-compliant. The most urgent profiles to update are those for protocols such as SUCI protection, which are defined by 3GPP and require explicit 3GPP specification for UE and core network interoperability.

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