**3GPP TSG-SA3 Meeting #123 S3-252977-r3**

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

**Source: Ericsson, Huawei, Nokia**

**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] 3GPP TR 33.938: "3GPP Cryptographic Inventory".

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

# 4 Assumptions

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.

Given the wide variation in requirements, specifications, technical capabilities, and implementation maturity across protocols, this study is organized by security protocol. Each major protocol is covered in a separate clause. 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.

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, transitioning public key infrastructures (PKI) often takes a decade or more, making it critical to begin the development process immediately.

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

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