**3GPP TSG-SA3 Meeting #123 S3-252978-r2**

**Goteborg, Sweden, 25 – 29 August 2025** merger of 2638, 2758, 2791

**Source: Huawei, HiSilicon, Samsung, China Mobile**

**Title: Pseudo-CR on description of PQC security levels**

**Document for: Approval**

**Agenda item: 5.2.1**

**Spec: 3GPP TR 33.703**

**Version: 0.0.0**

**Work Item: FS\_CryptoPQC**

**Comments**

This contribution proposes text on PQC security levels.

\* \* \* 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*.

[x1] IETF Internet-Draft: “Post-Quantum Cryptography for Engineers”.

[x2] NIST IR 8547: “Transition to Post-Quantum Cryptography Standards”.

[x3] IETF RFC 9794: “Terminology for Post-Quantum Traditional Hybrid Schemes”.

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

# 5 Principles and attributes of PQC to use in 3GPP procedures

Editor’s Note: This clause contains impact of using hybrid and standalone PQC algorithms in 3GPP procedures, impact to 3GPP procedures due to larger length of PQC key, signature, and message compared to the length of those in traditional cryptography, security levels (I-V) required to align with existing 3GPP procedures level of assurance, suitability of classes of post-quantum signature algorithms (e.g., lattice-based, hash-based) to 3GPP procedures.

### 6.1 PQC security level

Both IETF and NIST use the concept of security levels/security strength categories to group algorithms, keys, and protocols related to PQC. The security is defined as a function of resources required to break AES and SHA2/SHA3 algorithms, i.e., exhaustive key recovery for AES and optimal collision search for SHA2/SHA3. The security strength is broadly grouped into the following 5 levels [x1][x2]:

Level 1: at least as hard as breaking AES-128 (exhaustive key recovery)

Level 2: At least as hard as breaking SHA-256/SHA3-256 (collision search)

Level 3: At least as hard as breaking AES-192 (exhaustive key recovery)

Level 4: At least as hard as breaking SHA-384/SHA3-384 (collision search

Level 5: At least as hard as breaking AES-256 (exhaustive key recovery)

### 6.2 Hybrid and standalone schemes

Post-Quantum Traditional (PQT) hybrid scheme as defined in RFC 9794 [x3], is a multi-algorithm scheme where at least one component algorithm is a post-quantum algorithm and at least one is a traditional algorithm. Both the PQT hybrid scheme and the standalone PQC scheme are considered in the present document.

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