**3GPP TSG-SA3 Meeting #124 S3-253692-r1**

**Wuhan, China, 13 – 17 October 2025 (revision of S3-253288)**

**Source: Nokia**

**Title: Pseudo-CR on proposed new text for PQC level description**

**Document for: Approval**

**Agenda item: 5.2.1**

**Spec: 3GPP TR 33.703**

**Version: 0.1.0**

**Work Item: FS\_CryptoPQC**

**Comments**

This pCR is on the PQC security level description and is basically adding for every PQ security level its corresponding traditional and post-quantum algorithm. The main reason for this is that a PQ security level is implicit referring to a post-quantum algorithm that must be considered for the transition to PQC.

[1] TR 33.703, “Study on Transitioning to Post Quantum Cryptography (PQC) in 3GPP”

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

\* \* \* 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".

[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] PQUIP draft-ietf-pquip-pqc-engineers: “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] FIPS 203: “Module-Lattice-Based Key-Encapsulation Mechanism Standard”

[x2] FIPS 204: “Module-Lattice-Based Digital Signature Standard”

[x3] FIPS 205: “Stateless Hash-Based Digital Signature Standard”

[x4] FN-DSA: Falcon is a cryptographic signature algorithm submitted to NIST, Refer to [https://falcon-sign.info/falcon.pdf](https://falcon-sign.info/falcon.pdf%22%20%5Co%20%22https%3A//falcon-sign.info/falcon.pdf%22%20%5Ct%20%22_blank)

[x5] NIST: “Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process “,
<https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf>

[x6] …

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

### 5.1 PQC security level

The NIST use the concept of security levels/security strength categories to group algorithms, keys, and protocols related to PQC [x5]. Security is defined as a function of resources comparable to or greater than those required to break AES and SHA2/SHA3 algorithms, i.e., key search on block cipher for AES and collision search on a 256-bit hash function for SHA2/SHA3. The security strength is broadly grouped into the following 5 levels [2] and to each of the PQ security levels, the corresponding traditional and post-quantum algorithm can be mapped:

Level 1: At least as hard as breaking AES-128 (key search on block cipher), PQC-Algorithm: ML-KEM-512 [x1], FN-DSA-512 [x4], SLH-DSA-SHA2/SHAKE-128f/s [x3]

Level 2: At least as hard as breaking SHA-256/SHA3-256 (collision search on a 256-bit hash function), PQC-Algorithm: ML-DSA-44 [x2]

Level 3: At least as hard as breaking AES-192 (key search on block cipher), PQC-Algorithm: ML-KEM-768 [x1], ML-DSA-65 [x2], SLH-DSA-SHA2/SHAKE-192f/s [x3]

Level 4: At least as hard as breaking SHA-384/SHA3-384 (collision search on a 256-bit hash function), PQC-Algorithm: No algorithm tested at this level

Level 5: At least as hard as breaking AES-256 (key search on block cipher), PQC-Algorithm: ML-KEM-1024 [x1], FN-DSA-1024 [x4], ML-DSA-87 [x2], SLH-DSA-SHA2/SHAKE-256f/s [x3]

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