**3GPP TSG-SA3 Meeting #124 S3-253690**

**Wuhan, China, 13 – 17 October 2025 (revision of S3-253287-r1)**

**Source: Nokia, US NSA**

**Title: Pseudo-CR on proposed new text for general assumptions**

**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 for the introduction of new text related to assumptions. For the transition to PQC the guidelines and requirements from the different regulatory and governmental agencies must be considered. These inputs to the 3GPP transition to PQC are relevant, because these provide guidance on the preferred PQ security levels and with that implicit refer to the preferred post-quantum algorithms.

The proposal is to collect and summarize any preference related to post-quantum algorithms and with that to prepare the ground for the post-quantum selection process.

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

\* \* \* 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] 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] ANSSI: “ANSSI views on the Post-Quantum Cryptography transition (2023 follow up)”, link

[x2] NCSC: “Timelines for migration to post-quantum cryptography”, [link](https://www.ncsc.gov.uk/guidance/pqc-migration-timelines)

[x3] NSM 10: “Memorandum for the heads of executive departments and agencies”, [link](https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf" \l ":~:text=As%20per%20NSM-10%2C%20%E2%80%9Cthe%20United%20States%20must%20prioritize,the%20quantum%20risk%20as%20is%20feasible%20by%202035.%E2%80%9D)

[x4] NIST SP800-131A: “Transitioning the Use of Cryptographic Algorithms and Key Lengths”, [link](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf)

[x5] NIST IR 8547 ipd: “Transition to Post-Quantum Cryptography Standards”, [link](https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf)

[x6] US NSA: “Commercial National Security Suite 2.0 (CNSA2.0)”, [link](https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/1/CSI_CNSA_2.0_FAQ_.PDF)

[x7] BSI: “Quantum-safe cryptography”, [link](https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.pdf?__blob=publicationFile&v=6)

[x8] BSI: “Cryptographic Mechanisms”, [link](https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html)

[x9] BSI TR 02102-1: “Cryptographic Mechanisms: Recommendations and Key Lengths”

[x10] NCSC: “Next steps in preparing for post-quantum cryptography“, [link](https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography)

[x11] ETSI TC SET, “Technical Report on impacts of the post-quantum cryptography on ETSI TC SET specifications”

[x12] …

\* \* \* 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].

ANSSI Agence Nationale de la Sécurité des Systèmes d'Information

BSI Bundesamt für Sicherheit in der Informationstechnik

DIB Defense Industrial Base

DoD Department of Defense

ECIES Elliptic Curve Integrated Encryption Scheme

ISO International Organization for Standardization

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

NSA National Security Agency

NCSC National Cyber Security Centre

NSM National Security Memorandum

NSS National Security Systems

PKC Public Key Cryptography

PQC Post Quantum Cryptography

SDO Standards Development Organizations

SECG Security Engineering & Consulting Group

SUCI Subscription Concealed Identifier

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

# 4 Overview

## 4.1 Background Information

### 4.1.x Summary of Security Agency Views

Editor’s Note: Timeline information from other organizations.

## ~~4.2 General Assumptions~~

~~Editor's Note: This clause contains overall assumption and/or security assumptions for this study.~~

The security of symmetric cryptography is not significantly impacted by quantum computers, and existing symmetric algorithms with at least 128-bit keys (such as AES) can continue to be used. The security of hash functions such as SHA-256 is also not significantly affected, and secure hash functions can also continue to be used [x10], [x5].

The security of asymmetric cryptography is impacted by quantum computers and potential mitigations are shown below. As part of the PKC, the Public key-based user authentication algorithms are not subject to retroactive attack. This means that classical algorithms could be still used, waiting for significant advances in the area of quantum computing before migrating to post-quantum ones [x12].

**ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information)**

The ANSSI view on the Post-Quantum Cryptography transition is providing recommendations and has been documented by a follow-up paper (2023 follow up) [x1]. The ANSSI still strongly emphasizes the necessity of hybridization wherever post-quantum migration is needed both in short and medium term. The ANSSI encourages to dimension the parameters of symmetric primitives as to ensure conjectured post-quantum security. In practice at least the same security level as AES-256 for block ciphers and at least the same security level as SHA2-384 for hash functions. It is important to avoid modifying the parameters of the standardized instance.

ANSSI does not provide a closed list of recommended NIST algorithms.

If the ML-KEM scheme is selected for being included in products, then it is recommended to use the highest possible NIST security level, preferably Level 5 (ML-KEM-1024) (i.e., equivalent to AES-256) or Level 3 (ML-KEM-768) (i.e., equivalent to AES-192) [x1].

If the ML-DSA scheme is selected for being implemented in products, then it is recommended to use the highest possible NIST security level, preferably Level 5 (ML-DSA-87) (i.e., equivalent to AES-256) or Level 3 (ML-DSA-65) (i.e., equivalent to AES-192) [x1].

If the SLH-DSA scheme is selected for being implemented in products, then it is recommended to use the highest possible NIST security level, preferably Level 5 (SLH-DSA-SHA2/SHAKE-256s/f) (i.e., equivalent to AES-256) or Level 3 (SLH-DSA-SHA2/SHAKE-192s/f) (i.e., equivalent to AES-192) [x1].

If the FN-DSA scheme is selected for being implemented in products, then it is recommended to use the highest possible NIST security level, preferably Level 5 (FN-DSA-1024) (i.e., equivalent to AES-256) [x1].

**BSI (Bundesamt für Sicherheit in der Informationstechnik)**

The German BSI has developed technical guidelines for different PQC issue, i.e., recommendations on key lengths (BSI TR-02102-1), use of TLS (BSI TR-02102-2), use of IKEv2 (BSI TR-02102-3), use of secure shell (BSI TR-02102-4).

If the ML-KEM scheme is selected for being included in products, then it is recommended to use NIST security level, preferably Level 5 (ML-KEM-1024) (i.e., equivalent to AES-256) or Level 3 (ML-KEM-768) (i.e., equivalent to AES-192) [x9].

If the ML-DSA scheme is selected for being implemented in products, then it is recommended to use NIST security level, preferably Level 5 (ML-DSA-87) (i.e., equivalent to AES-256) or Level 3 (ML-DSA-65) (i.e., equivalent to AES-192). The ML-DSA schemes to be used in the ‘hedged’ variant [x9].

If the SLH-DSA scheme is selected for being implemented in products, then it is recommended to use NIST security level, preferably Level 5 (SLH-DSA-SHA2/SHAKE-256s/f) (i.e., equivalent to AES-256) or Level 3 (SLH-DSA-SHA2/SHAKE-192s/f) (i.e., equivalent to AES-192). The SLH-DSA schemes to be used in the ‘hedged’ variant. The ‘pure’ version of SLH-DSA is preferred and for special applications, the ‘pre-hash’ version of SLH-DSA can also be used in accordance with the remarks in FIPS-205 [x9].

The FN-DSA schemes are not considered.

**US NSA (US National Security Agency)**

The NSM 10 states that, the United States must prioritize the timely and equitable transition of cryptographic systems to quantum-resistant cryptography, with the goal of mitigating as much of the quantum risk as is feasible by 2035."[x3]. For traditional cryptographic algorithms, the document (SP 800-131A) is intended to provide more detail about the transitions associated with the use of cryptography by Federal Government agencies for the protection of sensitive, but unclassified information [x4]. For the transition to PQC, the NIST IR 8547 provides timelines [x5]. The transition to PQC for classified National Security Systems (NSS) is set out by US NSA in the Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) [x6] and is therefore not particularly well-suited for the transition to PQC for telecommunications systems.

**NCSC (National Cyber Security Centre)**The NCSC guidance [x2] sets out the necessary steps towards PQC migration, describes how preparatory work might vary across different sectors, and provides advice on timescales for key activities on the long journey to PQC.

The NCSC guidance on ‘Next steps in preparing for post-quantum cryptography’ helps system and risk owners in commercial enterprises, public sector organizations and critical national infrastructure to think about how to best prepare for the migration to post-quantum cryptography [x10].

If the ML-KEM scheme is selected for being included in products, then it is recommended to use NIST security Level 3 (ML-KEM-768) (i.e., equivalent to AES-192) [x10].

If the ML-DSA scheme is selected for being implemented in products, then it is recommended to use NIST security Level 3 (ML-DSA-65) (i.e., equivalent to AES-192) [x10].

The SLH-DSA signatures are seen to be **not** suitable for general purpose use cases as the signatures are large and the algorithms are much slower than ML-DSA.

The FN-DSA schemes are not considered.

~~Table 4.2-1: Government Body & Algorithm Suites Preferred~~

|  |  |  |
| --- | --- | --- |
| **~~Algorithm~~** | **~~SDO~~** | **~~Government Body & Algorithm Suites Preferred~~** |
| ~~ML-KEM~~ | ~~NIST~~ | ~~ANSSI: Preferred Level 5 (ML-KEM-1024) or Level 3 (ML-KEM-768) [x1]~~  ~~BSI: ML-KEM-768, ML-KEM-1024 [x7], [x8]~~  ~~NCSC UK: ML-KEM-768 [x2]~~  ~~NSA: ML-KEM-1024 [x6]~~ |
| ~~ML-DSA~~ | ~~NIST~~ | ~~ANSSI: Preferred Level 5 (ML-DSA-87) or Level 3 (ML-DSA-65) [x1]~~  ~~BSI: ML-DSA-65, ML-DSA-87 [x7], [x8]~~  ~~NCSC UK: ML-DSA-65 [x2]~~  ~~NSA: ML-DSA-87 [x6]~~ |
| ~~SLH-DSA~~ | ~~NIST~~ | ~~ANSSI: Level 5 [x1]~~  ~~BSI: Level 5 [x7], [x8]~~  ~~NCSC UK: Not preferred [x2]~~  ~~NSA: Level 5~~ |
| ~~FN-DSA~~ | ~~NIST~~ | ~~ANSSI: Preferred Level 5 [x1]~~ |
| ~~FrodoKEM~~ | ~~ISO~~ | ~~BSI: FrodoKEM-976 and FrodoKEM-1344 [x7], [x8]~~ |
| ~~McEliece~~ | ~~ISO~~ | ~~BSI: mceliece460896, mceliece6688128 and mceliece8192128 and mceliece460896f, mceliece6688128f and mceliece8192128f (faster variants) [x7], [x8]~~ |

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