**3GPP TSG-SA3 Meeting #124 S3-253287-r1**

**Wuhan, China, 13 – 17 October 2025**

**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

[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

[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] NIST, 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] …

\* \* \* 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

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

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

### 4.1.1 Transition Timeline

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 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 has functions. It is important to avoid modifying the parameters of the standardized instance.

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).

The NCSC guidance 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 [x2].

~~The US NSA is providing reference to the NSM 10, “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], [x6].~~

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 Commerical National Security Algorithm Suite 2.0 (CNSA 2.0) [x6].

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) BSI: ML-KEM-768, ML-KEM-1024NCSC: ML-KEM-768NSA: ML-KEM-1024 |
| ML-DSA  | NIST  | ANSSI: Preferred Level 5 (ML-DSA-87) or Level 3 (ML-DSA-65) BSI: ML-DSA-65, ML-DSA-87NCSC UK: ML-DSA-65NSA: ML-DSA-87 |
| SLH-DSA  | NIST  | ANSSI: Level 5BSI: Level 5NCSC UK: Not preferred~~NSA: Level 5~~ |
| FN-DSA  | NIST  | ANSSI: Preferred Level 5  |
| FrodoKEM  | ISO  | BSI: FrodoKEM-976 and FrodoKEM-1344  |
| McEliece  | ISO  | BSI: mceliece460896, mceliece6688128 and mceliece8192128 and mceliece460896f, mceliece6688128f and mceliece8192128f (faster variants)  |

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