**3GPP TSG-SA3 Meeting #124 S3-253694 (Merged S3-253548)**

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

**Source: Ericsson, Qualcomm, Huawei**

**Title: Pseudo-CR on updating skeleton of clause 6**

**Document for: Approval**

**Agenda item: 5.2.1**

**Spec: 3GPP TR 33.703**

**Version: 0.1.0**

**Work Item: FS\_CryptoPQC**

**Comments**

This document proposes to update the skeleton for clause 6 of the TR 33.703.

\* \* \* First Change \* \* \* \*

# 6 Protocols expected to be updated for PQC by other SDOs

Editor’s Note: This clause contains the expected timeline for when security protocols defined by other SDOs will include PQC algorithms and be available for inclusion into 3GPP procedures. The timeline includes the availability of stable protocols.

## 6.1 General

Editor’s Note: This subclause states e.g. that protocols in TR 33.938 that are to be updated in other SDO and their profiles to be used in 3GPP are described here.

The present document discusses several IETF documents that are at different levels of maturity in the overall IETF standardization process [x1], and categorizes them as follows:

- IETF Individual Draft: A document that has been submitted to IETF and has not been adopted by one of the working groups in IETF. On the IETF Datatracker website, such documents have type “Active Internet-Draft (individual)”.

- IETF WG Draft: A document that has been reviewed and adopted by one of the working groups in IETF. On the IETF Datatracker website, such documents have type “Active Internet-Draft (xyz WG)”, where xyz is the name of the working group that adopted the document, e.g., tls.

- IETF RFC: A document that has gone through the whole IETF standardization process.

## 6.X Protocol #X

### 6.X.1 General

Editor’s Note: This clause includes background information about protocol #X (e.g., introductory information, relevant summary, if any, from the existing 3GPP profile of the protocol, useful references to specification documents etc.).

### 6.X.2 Current Work in IETF

Editor’s Note: This clause includes current status of PQC migration of protocol X in IETF — published RFCs, if any, and different drafts and their status. If Protocol X is specified by any other SDO than IETF, then the title of this clause will use the name of the appropriate SDO instead of IETF.

#### 6.X.2.1 Overview

#### 6.X.2.2 IETF RFCs

#### 6.X.2.3 IETF WG Drafts

#### 6.X.2.4 IETF Individual Drafts

### 6.X.3 3GPP Considerations

Editor’s Note: This clause includes potential alternative options on PQC migration that 3GPP SA3 could consider. For example, for TLS 1.2, the following alternative options may be considered by 3GPP: (1) state in its profile that TLS 1.2 is expected to already have been fully phased out in 5G systems by XXXX date. (ii) add a NOTE in its profile explicitly stating that TLS 1.2 is vulnerable to quantum attacks and is strongly recommended not to be used.

Editor’s Note: This clause does not include any conclusions.

\* \* \* Next 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] IETF: “About RFCs”. Available at https://www.ietf.org/process/rfcs/.

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