**3GPP TSG-SA3 Meeting #124 S3-253695**

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

**Source: Huawei, HiSilicon**

**Title: General description for clause 6.1**

**Document for: Approval**

**Agenda item: 5.2.1**

**Spec: 3GPP TR 33.703**

**Version: 0.1.0**

**Work Item: FS\_CryptoPQC**

**Comments**

This contribution proposes general text for clause 6.1 for protocols that are updated by other SDOs to use PQC.

\* \* \* 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".

[x] 3GPP TR 33.938: "3GPP Cryptographic Inventory".

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

### 6.1 General

According to the inventory in TR 33.938[x], many security protocols and algorithms used in 3GPP (e.g. (D)TLS, IKEv2, JWE, JWS, etc.) are specified in other standard organizations (e.g. IETF). They are expected to be updated using PQC in the corresponding organizations.

In this clause, the progress of the post-quantum migration of these protocols are reported. Mature specifications developed by related SDOs will be given priority consideration. In addition, whether the relevant solutions can be directly applied to specific 3GPP scenarios is evaluated.

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