**3GPP TSG-SA3 Meeting #123 S3-252982-r1**

**Goteborg, Sweden, 25 – 29 August 2025**

**Source: Huawei, HiSilicon**

**Title: PQC migration for PKI certificates**

**Document for: Approval**

**Agenda item: 5.2.1**

**Spec: 3GPP TR 33.703**

**Version: 0.0.0**

**Work Item: FS\_CryptoPQC**

**Comments**

It is proposed to study the PQC migration scheme of the PKI certificates 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".

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

## 6.X Protocol #X：PKI certificates

The IETF is specifying PQC migration for PKI certificates to support various security mechanisms. In this clause, how to employ PKI certificates using PQC in 3GPP is studied.

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