**3GPP TSG-SA3 Meeting #123 S3-252983-r1**

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

**Source: Huawei, HiSilicon**

**Title: Pseudo-CR on General description for protocols not updated for PQC by other SDOs**

**Document for: Approval**

**Agenda item: 5.2.1**

**Spec: 3GPP TR 33.703**

**Version: 0.0.0**

**Work Item: FS\_CryptoPQC**

**Comments**

This contribution proposes general text for clause 7.1 for protocols that are not expected to be updated by other SDOs to use PQC.

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

## 7.1 Threats

Most of security protocols used in 3GPP systems are specified in other standards development organizations (SDOs). In case that these protocols are not updated to use PQC in other SDOs, the 3GPP system may be vulnerable to attacks based on quantum computation. The clause 7.2 contains all of these protocols identified and potential solutions to address the issues.

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