**3GPP TSG-SA3 Meeting #123 S3-252979-r1**

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

**Source: Huawei, HiSilicon**

**Title: PQC Migration of different functionalities in authenticated key exchange protocols (e.g. IKEv2, TLS)**

**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 consider the urgency of PQC migrating for different functionalities of the authenticated key exchange protocols in 3GPP.

\* \* \* First 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].

CRQC Cryptanalytically Relevant Quantum Computer

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

# 5 Principles and attributes of PQC to use in 3GPP procedures

Editor’s Note: This clause contains impact of using hybrid and standalone PQC algorithms in 3GPP procedures, impact to 3GPP procedures due to larger length of PQC key, signature, and message compared to the length of those in traditional cryptography, security levels (I-V) required to align with existing 3GPP procedures level of assurance, suitability of classes of post-quantum signature algorithms (e.g., lattice-based, hash-based) to 3GPP procedures. 5.1 General

While the CRQC that can compromise classical cryptography is not yet available, the preparation for post-quantum transition can be arranged according to risks posed by CRQC. For example, the “Harvest Now, Decrypt Later” attack poses risks for data even before CRQC arrival. Therefore, the functionalities, e.g., key exchange, signature, and certificate management, that mitigating such attacks should be transited to have the quantum-resistant capability.

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