**3GPP TSG-SA3 Meeting #123 draft\_S3-252980-r2**

**Goteborg, Sweden, 25 – 29 August 2025 is revision of S3-252793**

**Source: China Mobile**

**Title: Pseudo-CR on Crypto Agility**

**Document for: Approval**

**Agenda item: 5.2.1**

**Spec: 3GPP TR 33.703**

**Version: 0.0.0**

**Work Item: FS\_CryptoPQC**

**Comments**

1. **Introduction**

This contribution proposes a sub-clause of cryptographic agility.

1. **Reason for Change**

The 6G system has been foreseen to face the threat of quantum computing attacks, thus the cryptographic system of the 6G network need to be quantum-resistant. To minimize the impact brought by rounds of migration of cryptograhpic algorithms, the 6G system is requiring the ability to flexibly evolve and dynamically adjust, including agile negotiation of algorithms/protocols, real-time updates of algorithms/protocols, and agile scheduling of cryptographic algorithms.

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

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

## 5.X Cryptographic agility

A major cryptographic transition is expected in the near future to mitigate against the threat of quantum computers. Cryptographic algorithms will need to be updated to mitigate against these threats. Mobile communication systems need an efficient and cost-effective way to transition existing cryptographic algorithms.

Cryptographic agility [X] is the ability to replace and adapt cryptographic algorithms while preserving security of existing operations. In 3GPP protocols, an important attribute of crypto agility is the ability to maintain interoperability when introducing new cryptographic algorithms while preventing the use of weak algorithms.

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

# 2 References

[X] NIST Cybersecurity White Paper NIST CSWP 39ipd Considerations for Achieving Crypto Agility.

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