**3GPP TSG-SA3 Meeting #124 draft\_S3-253693-r1\_**

**Wuhan, China, 13 – 17 October 2025 merger of S3-253319 and S3-253334**

**Source: China Mobile**

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

**Document for: Approval**

**Agenda item: 5.2.1**

**Spec: 3GPP TR 33.703**

**Version: 0.1.0**

**Work Item: FS\_CryptoPQC**

**Comments**

1. **Introduction**

This contribution proposes a sub-clause of cryptographic agility.

1. **Reason for Change**

To minimize the impact brought by migration of cryptograhpic algorithms, the 3GPP system is required to have the ability to replace and adapt cryptographic algorithms while preserving security of existing operations.

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

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

## 5.X Cryptographic agility

Cryptographic agility[Y][Z] refers to the capabilities needed to replace and adapt cryptographic algorithms while preserving security and ongoing operations. The 3GPP system need to consider cryptographic agility.

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

# 2 References

[Y] NIST, "Considerations for Achieving Cryptographic Agility: Strategies and Practices," CSWP 39, Jul. 2025. [Online]. Available: [https://csrc.nist.gov/pubs/cswp/39/considerations-for-achieving-cryptographic-agility/2pd](https://csrc.nist.gov/pubs/cswp/39/considerations-for-achieving-cryptographic-agility/2pd" \t "https://chat.deepseek.com/a/chat/s/_blank)

[Z]IETF RFC 7696: “Guidelines for Cryptographic Algorithm Agility and Selecting Mandatory-to-Implement Algorithms”.

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