**3GPP TSG-SA3 Meeting #124 S3-253834-r1**

Wuhan, China, 13 – 17 October 2025

**Title: LS on PQC transition for RFC 6509**

**Response to:**

**Release: Release 20**

**Work Item: FS\_CryptoPQC**

**Source: 3GPP SA3**

**To: IETF SEC Area**

**Cc:**

**Contact person: Zander Lei**

 **lei.zhongding@huawei.com**

**Send any reply LS to: 3GPP Liaisons Coordinator,** **mailto:3GPPLiaison@etsi.org**

**Attachments:**

# 1 Overall description

3GPP SA3 has started a study on “Transitioning to Post Quantum Cryptography (PQC) in 3GPP”. This is to prepare the PQC transition for security protocols used in 3GPP systems. 3GPP SA3 has identified that the MIKEY-SAKKE protocol, which is used in 3GPP systems to transport cryptographic keys securely for Mission Critical Services, is specified in the IETF RFC 6509. Since it employs asymmetric cryptography for key distribution and may be vulnerable to quantum computing, SA3 would like to know whether there is any plan for IETF to update the RFC 6509 using PQC. If yes, SA3 appreciate if IETF can provide estimated timeline for the protocol update.

# 2 Actions

**To IETF IESG, IETF SEC Area**

**ACTION:** SA3 kindly requestIETF to provide feedback on the question above.

# 3 Dates of next TSG SA WG 3 meetings

SA3#125 17 – 21 November 2025 Dallas, US

SA3#126 9 – 13 February 2026 India (TBD)