**3GPP TSG-SA3 Meeting #116 *S3-242378-r3***

Jeju, South Korea, 20th - 24th May 2024

**Title: Reply-LS on PQC Migration**

**Response to: LS S3-240692 on 3GPP studies for PQC Migration from GSMA**

**Release:**

**Work Item:**

**Source: SA WG3**

**To: GSMA PQTN**

**Cc:**

**Contact person: lei.zhongding@huawei.com**

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

**Attachments:**

# 1 Overall description

SA3 thanks GSMA for the LS on 3GPP studies for migration to Post-Quantum Cryptography (PQC). SA3 would like to provide the following responses to the raised questions:

* **Q1: Timeline of the study, specifications and migration for both symmetric algorithms and asymmetric algorithms, cryptographic primitives, and relevant protocols**

**[SA3**]: SA3 completed one study on impact of quantum computing to 3GPP systems back in 2018. The outcomes were captured in the report TR 33.841: Study on the support of 256-bit algorithms for 5G (Release 16). In general, SA3 has the following understanding on the PQC issues:

* Quantum computing will weaken the security of all asymmetric algorithms in common use today, including those used in the profiles and protocols in the 5G systems, e.g. ECIES for SUPI encryption, IPsec, TLS, DTLS, JWS, X.509 certificates, CRL, CMP etc. It is notable that all these asymmetric algorithms and protocols are developed in other standards bodies. They are assessed by SA3 before being adopted or adapted into 3GPP systems. SA3 will update the use of twithmade by the respective standards bodies
* As far as the symmetric algorithms are of concern, SA3 considers that all the 128-bit algorithms currently used in 5G systems can be considered as secure against attacks from both classical and quantum computing. Besides, a number of 256-bit algorithms have been specified to offer higher security options, e.g. TS 35.240-248for Snow 5G/AES/ZUC algorithms (Release 18).
* **Q2: Are the legacy systems i.e., 4G, 3G etc., considered for PQC migration? If so, then what is the timeline for the migration of legacy systems**

**[SA3]:** SA3 has discussed the issue on the following aspects:

* Symmetric algorithms (128 bit): they are used for subscriber authentication and to secure the air interface as well as traffic within/between networks, e.g. traffic protection in IPsec. Currenlty, SA3 is of the opinion that these symmetric algorithms can beconsidered as secure against attacks from both classical and quantum computing in foreseeable life time of the legacy systems.
* Asymmetric algorithms/protocols (e.g. IPsec, TLS): they are mostly used for 3GPP network domain security and SA3 maintain 3GPP profiles of these protocols. Profiles of these protocols apply to 4G and 3G too. SA3 will update the 3GPP profiles of these protocols with quantum-resistant algorithms.

In the meantime, SA3 is actively monitoring the status of quantum computing and development of PQC algorithms / protocols in other SDOs.

# 2 Actions

**To GSMA**

**ACTION:** SA3 kindly asks GSMA to take above information into account.

# 3 Dates of next TSG SA WG 3 meetings

SA3#117 19 - 23 August 2024 Maastricht (Netherlands)

SA3#118 14 - 18 October 2024 Hyderabad (India)