**3GPP TSG-SA3 Meeting #116 *S3-24xxxx***

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 their LS on 3GPP studies for migration to Post-Quantum Cryptography (PQC). 3GPP SA3 has the following relevant technical reports/specifications completed/being developed:

1. **TR 33.841**: Study on the support of **256-bit algorithms** for 5G (Release 16).

2. **TS 35.240/ TS 35.241/TS 35.242**: Specification of the **Snow 5G** based 256-bits algorithm set (Release 18)

3. **TS 35.243/ TS 35.244/TS 35.245**: Specification of the **AES** based 256-bits algorithm set (Release 18)

4. **TS 35.246/ TS 35.247/TS 35.248**: Specification of the **ZUC** based 256-bits algorithm set (Release 18)

5. **TS 35.234/TS 35.235/TS 35.236/TS 35.237**: Specification of the **MILENAGE-256** algorithm set (Release 19, ongoing)

6. **TR 33.700-41**: Study on cryptographic algorithm transition to 256 bits (Release 19, ongoing)

SA3 would like to provide the following responses to the questions raised for SA3:

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

**[SA3**]: The study reports and specifications completed/being developed in SA3 are shown above. They focus more on symmetric 256-bit algorithms. For asymmetric algorithms and protocols, SA3 is monitoring the development efforts being made in other standard bodies, e.g. ETSI SAGE, IETF etc, and will consider more studies and specifications in due time.

* **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 not made any decisions on whether a legacy system, e.g. 4G or 3G, is required to be involved in PQC migration. It is noted that the symmetric 128 algorithms are secure at the time being and considered secure in foreseeable life time of the legacy systems even if quantum computers arrive. They will be reviewed from time to time when any potential risks arise.

# 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 TBD (India)