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

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

**Title: Reply-LS on QSC Protocol Inventory**

**Response to: LS S3-240223 on QSC Protocol Inventory from ETSI**

**Release:**

**Work Item:**

**Source: SA WG3**

**To: ETSI TC Cyber**

**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 ETSI TC Cyber for their LS on Quantum Safe Cryptographic (QSC) Protocol Inventory. SA3 would like to provide the following responses to the questions raised:

**Q1: The leading working groups / committees leading on QSC implementation.**

**SA3:** SA working group 3 (SA3).

**Q2: Information relating to any similar current or planned activity underway in your organisation to build a similar protocol list.**

**SA3:** No.

**Q3: A detailed list of all cryptographic algorithms and / or protocol implementations that your organisation is responsible for and the quantum safe cryptographic status of each. This may include the current guidance on algorithm exposure, effective key lengths, potential for hybrid deployment and potential for cryptoagility.**

SA3: 3GPP SA3 has the following relevant technical reports/specifications completed/being developed. They focus more on symmetric 256-bit algorithms.

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)

**Q4: The website address(es) that provide historical QSC information, current development of guidance / standards and future updates (these can include both public and member-only addresses).**

**SA3**: there is no specific website for such information. However, all the technical reports and specifications for security aspects developed or being developed in SA3 are available at <https://www.3gpp.org/dynareport?code=33-series.htm>

**Q5: A summary of the current quantum safe cryptography work status within your organisation.**

**SA3**: SA3 has developed/been developing technical reports and specifications focusing on symmetric 256-bit algorithms. For asymmetric algorithms and protocols, SA3 is monitoring the development efforts being made in other standard bodies, e.g. NIST, IETF, and will consider more studies and specifications in due time.

**Q6: A summary of any anticipated future roadmap.**

**SA3**: not available at the time being.

**Q7: A contact point(s) for clarification.**

**SA3**: 3GPP Liaisons Coordinator, <mailto:3GPPLiaison@etsi.org>

# 2 Actions

**To ETSI TC Cyber**

**ACTION:** SA3 kindly asks TC Cyber 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)