**3GPP TSG-SA3 Meeting #116 *S3-242377-r2***

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

**Title: LS on Quantum Safe Cryptographic Protocol Inventory**

**Response to: LS S3-241763/CYBERQSC(23)032007r2 on Quantum Safe Cryptographic Protocol Inventory from ETSI TC CYBER QSC WG (ETSI QSC)**

**Source: Ericsson, to be 3GPP SA3**

**To: ETSI TC CYBER QSC WG (ETSI QSC)**

**Cc:**

**Contact person: Mohsin Khan**

 **mohsin(dot)a(dot)khan(at)ericsson(dot)com**

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

**Attachments:** **None**

# 1 Overall description

3GPP SA3 would like to thank ETSI CYBER QSC for their LS making 3GPP SA3 aware of “ETSI TR 103 619 V1.1.1 (2020-07) Migration strategies” and the new work item to develop a protocol inventory. SA3 would like to provide the following responses to the questions raised in the LS:

**Question 1: The leading working groups / committees leading on QSC implementation.**

**Answer:** 3GPP SA3 will lead the work to introduce Post-Quantum Cryptography in 3GPP specifications.

**Question 2: Information relating to any similar current or planned activity underway in your organisation to build a similar protocol list.**

**Answer:**

In 2018 SA3 completed a study that includes an evaluation of the impact a Cryptographically Relevant Quantum Computers (CRQCs) will have on the security of 3GPP systems. The outcome is captured in 3GPP TR 33.841: Release 16. This work was conducted before mature guidance existed for quantum resistant symmetric key crypto systems.

SA3 continues to actively monitor the status and development of relevant PQC algorithms and quantum-resistant protocols in other SDOs such as IETF.

**Question 3: 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.**

**Answer:**

SA3 is confident that the symmetric algorithms (AES-128, SNOW 5G, ZUC, MILENAGE, TUAK, SHA-256, etc.) used in 4G and 5G are quantum-resistant and will continue to be considered secure and remain in use.

The public-key cryptography used in 3GPP systems is primarily found in the security protocols standards that 3GPP leverages. These protocols specifications are maintained by other SDOs, but SA3 is tracking their update to a quantum resistant version. 3GPP specifications rely on the following IETF security specifications that use public-key cryptography.

*IKEv2, X.509, PKCS #10, CMP, CRL* ***,*** *OCSP, TLS, DTLS* ***,*** *QUIC****,*** *JOSE****,*** *COSE****,*** *EAP, MIKEY-SAKKE*

3GPP maintains profiles for the protocols, such as TLS and IKEv2, to ensure the secure usage of these protocols. For the symmetric algorithms, the 128-bit algorithms currently in use in 5G systems are considered secure against Cryptographically Relevant Quantum Computers (CRQCs).

3GPP’s procedure for encryption of SUPI into SUCI [2] uses ECIES, which is standardized by SECG [3] with P-256 and Curve25519. SA3 is aware that it will need to update its specifications to provide a profile option that is quantum resistant.

3GPP SA3 has been closely following of the ongoing work of NIST’s post quantum cryptography process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms [1]. SA3 is aware that final standards for these new algorithms are expected later this year.

Regarding the effective key length, 3GPP SA3 has not discussed security levels and hybrid modes.

**Question 4: 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).**

**Answer:**

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

**Question 5: A summary of the current quantum safe cryptography work status within your organisation.**

**Answer:**

SA3 continues to actively monitor the status and development of relevant PQC algorithms and quantum-resistant protocols in other SDOs such as IETF.

**Question 6: A summary of any anticipated future roadmap.**

**Answer:**

3GPP SA3 plans to start the work to introduce PQC in 3GPP specifications as soon as corresponding IETF security protocol standards are updated with PQC-resistant algorithms.

**Question 7: A contact point(s) for clarification.**

**Answer:** 3GPP Liaisons Coordinator, mailto:3GPPLiaison@etsi.org

.3GPP SA3 asks ETSI CYBER QSC to take this information into account.

References:

[1] NIST, “Comments Requested on Three Draft FIPS for Post-Quantum Cryptography”
<https://csrc.nist.gov/news/2023/three-draft-fips-for-post-quantum-cryptography>

[2] 3GPP TS 33.501, “Security architecture and procedures for 5G System”
<https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169>

[3] SECG, “Standards for Efficient Cryptography Group”
<https://www.secg.org/>

#  2 Actions

**To ETSI TC CYBER QSC WG (ETSI QSC)**

**ACTION:** 3GPP SA3 asks ETSI CYBER QSC to take this 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)