LIAISON STATEMENT

Title: Quantum Safe Cryptographic Protocol Inventory

Date: 12/12/2023

From (source): ETSI TC CYBER QSC WG (ETSI QSC)

Contact(s): Matt Campagna Chair of TC CYBER QSC WG (campagna@amazon.com)
*Cyber*Support@etsi.org

To: 3GPP SA3, 3GPP SA3-LI, CEN/CENELEC JTC22, CEN/CENELEC FGQT, ENISA, ETSI ISG QKD, ETSI ISG ZSM, ETSI SC SAGE, GlobalPlatform: Crypto Sub-Task Force , GSMA PQTN, IEC JTC 2 Quantum Technologies, IEC SEG 14, IEEE P1943, IETF IPSECME, IETF LAMPS, IETF PQUIP, IETF TLS, IRTF CFRG, ISO SC27 WG2, ITU-T SG11, ITU-T SG13, ITU-T SG17, JRC, Linux Foundation Post Quantum Cryptography Alliance, MITRE, NIST NCCoE, OASIS, O-RAN Alliance WG11, Wifi Alliance

Copy to:

Response to: *Cyber*Support@etsi.org
(if applicable)

Attachments: NA
(if applicable)

1. Overall description:

ETSI Technical Committee CYBER Working Group on Quantum Safe Cryptography, hereafter referred to as ETSI QSC, has already developed Quantum Safe Cryptography migration documentation, notably in the form of ETSI TR 103 619 V1.1.1 (2020-07) *Migration strategies and recommendations to Quantum Safe schemes*. This document outlines a 3-stage process for migration:

Stage 1 - Inventory compilation

Stage 2 - Preparation of the migration plan

Stage 3 - Migration execution

ETSI TR 103 619 contains some high-level guidance on inventory compilation. However, an in-depth analysis of cryptographic protocol usage will assist an entity in building a deeper understanding of their inventory within deployed, complex, inter-connected networks containing both legacy and more modern systems.

At QSC#31, ETSI QSC agreed a new work item to develop a protocol inventory that, when complete, aims to significantly assist in the development of Step 2 & 3 (above) by providing a centralised source describing the QSC status of each identified inventory item. Once an inventory of protocol usage is built, it will be important to diagnose the likely QSC implications of each entry. To that end, building a protocol list that contains reference information on the deployed crypto algorithm, current key length(s), potential for cryptoagility would be valuable in building an effective migration plan. This plan may involve multiple steps

from classical cryptographic algorithms through hybrid arrangements (combinations of classical quantum-vulnerable and quantum-resistant public-key algorithms) before a full QSC state is reached.

ETSI QSC note some national work activity[1] that develops this concept and illustrates a start to developing this concept.

To build this centralised source, ETSI are seeking additional information on your respective cryptographic algorithms and protocol implementations (including key lengths) describing:

- The leading working groups / committees leading on QSC implementation.
- Information relating to any similar current or planned activity underway in your organisation to build a similar protocol list.
- 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.
- 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).
- A summary of the current quantum safe cryptography work status within your organisation.
- A summary of any anticipated future roadmap.
- A contact point(s) for clarification.

ETSI QSC therefore looks forward to feedback on the above information.

2. Actions: Reply to ETSI TC CYBER QSC WG with the requested information.

3. Date of next meetings of the originator:

QSC#33	20th February 2024	ETSI (Hybrid)

[1] EG Annex G of the recent CFDIR Update to v3 of Canadian National Quantum-Readiness, BEST PRACTICES AND GUIDELINES