

Security Conference

ETSITC CYBER QSC

Presented by: Matthew Campagna

campagna@amazon.com

Amazon Web Services





17/10/2023

Outline



Structure of TC CYBER QSC and how to participate

Completed work items

Current work items

New work items

ETSI-IQC Quantum-Safe Cryptography Workshop



A brief history

- 2000s Development of quantum-resistant schemes (NTRU)
- 2006 PQ Crypto Conference
- 2013 ETSI/IQC 1st Quantum Safe Cryptography Workshop
- 2015 ETSI's Quantum Safe Cryptography ISG (now a TC).
- 2016 NIST PQC Standardization Process
- 2022: NIST Selection for PQC Standardization
- 2024+: NIST Post-Quantum Cryptography Standards

Individual

Academic Community

Industry Community

Standardization & Prototyping

Migration & Adoption



ETSI TC CYBER QSC



Chair: Matthew Campagna (Amazon)

Vice chairs

Philip Lafrance (ISARA)

Dan G (NCSC)

Secretary: Anthony Barnett (Thales)

Technical Officer: Laure Pourcin (ETSI)





ETSI TC CYBER QSC

We meet concurrently with TC CYBER

Most recent meeting

19 September 2023Kourou, French Guiana39 Participants, and 21 contributions

Next meeting

5 December 2023 Sophia-Antipolis, France





Finished TR/TS



QSC Migration; ITS and C-ITS migration study, ETSI TR 103 949 (2023-05)

State Management for Stateful Authentication Mechanisms, ETSI TR 103 692 (2021-11)

Quantum-safe Hybrid Key Exchanges, ETSI TS 103 744 V1.1.1 (2020-12)

Migration strategies for Quantum Safe schemes, ETSI TR 103 619 V1.1.1 (2020-07)

Quantum-Safe Identity-Based Encryption, ETSI TR 103 618 V1.1.1 (2019-12)

Quantum-Safe Virtual Private Networks, <u>ETSI TR 103 617 V1.1.1 (2018-09)</u>

Current Work Items



Quantum-Safe Hybrid Key Exchanges, RTS/CYBER-QSC-0019 (TS 103 744)

Impact of Quantum Computing on Cryptographic Security Proofs, DTR/CYBER-QSC-0020

Deployment Considerations for Hybrid Schemes, DTR/CYBER-QSC-0021

Impact of Quantum Computing on Symmetric Cryptography, DTR/CYBER-QSC-0022



New Work Items



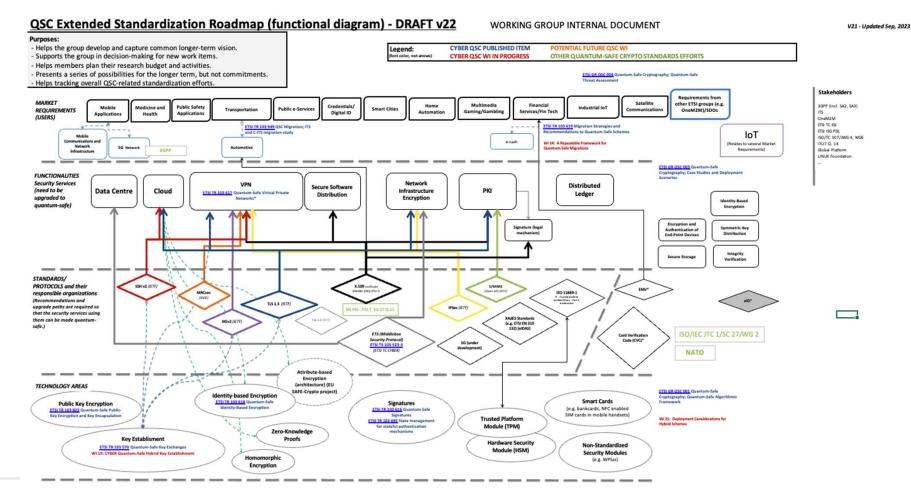
Efficient Quantum-Safe Hybrid Key Exchanges with Hidden Access Policies, DTR/CYBER-QSC-0023

A Repeatable Framework for Quantum-Safe Migrations, DTR/CYBER-QSC-0024

QSC Protocol Inventory, DTR/CYBER-QSC-0025



Roadmap





How to participate



ETSI members can attend the meetings – portal.etsi.org

5 December – CYBER QSC#32 (Sophia Antipolis, FR)

20 February – CYBER QSC#33 (Sophia Antipolis, FR)



10th ETSI-IQC Quantum-Safe Cryptography Workshop

Date: 14 – 16 May 2024



Location: Center for Quantum Technologies, National University

Information:

https://www.etsi.org/events/2284-10th-etsi-iqc-quantum-safe-cryptography-event

Call for presentations:

https://www.etsi.org/events/2284-10th-etsi-iqc-quantum-safe-cryptography-event#pane-6/





Thank you!

