ETSI TC CYBER Working Group Quantum Safe Cryptography

Matthew Campagna, Amazon

1st International Quantum Communication Conclave

28/03/2023

Agenda

- A brief history of the TC CYBER WG QSC
- Basic information about the working group today
- Completed Technical Recommendations and Specifications
- Current Work Items
- How to participate in ETSI TC CYBER WG QSC

ETSI

European Telecommunication Standards Institute

- Regionalized standards body focused on ITS
  - 29 Technical Committees, 17 Industry Specification Groups, 2 Open Source Groups
- Special role in Europe to produce Harmonized European Standards (CEN, CENELC, ETSI)
- Partners in 3GPP and oneM2M
- Funded through membership and EC, Europe Free Trade Association (EFTA)
- Located in Sophia Antipolis, Provence-Alpes-Côte d'Azur, France
- Director-General: Luis Jorge Romero

ETSI TC CYBER WG QSC

2013 1st ETSI-IQC Quantum Safe Cryptography Workshop

2015 ETSI published the Quantum Safe Cryptography and Security Paper

2015 ETSI Industry Specification Group (ISG) on QSC

2017 QSC becomes a working group of TC CYBER

Meetings are coordinated with CYBER, meet 4 times a year in Sophia-Antipolis

Held in hybrid mode with teleconferencing

ETSI TC CYBER WG QSC

Chair: Matthew Campagna (Amazon)

Vice chairs:

Philip Lafrance (ISARA)

Dan Grundy (NCSC)

Secretary: Anthony Barnett (Thales)

Technical Officer: Laure Pourcin (ETSI)

Healthy participation: 30 – 40 registered participants from corporate/government/academia

Finished TR/TS

CYBER; Quantum-Safe Key Exchanges, ETSI TR 103 507 V1.1.1 (2017-10)

Quantum-Safe Public Key Encryption and Key Encapsulation, ETSI TR 103 832 V1.1.2 (2021-09)

CYBER; Quantum-Safe Signatures, ETSI TR 103 616 V1.1.1 (2021-09)

CYBER; Quantum-Safe Virtual Private Networks, ETSI TR 103 617 V1.1.1 (2018-09)

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

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

State Management for stateful authentication mechanisms, ETSI TR 103 692 V1.1.1 (2021-11)

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

Current Work Items

CYBER; Migration to QSC for ITS, DTR/CYBER-QSC-0018 (TR)

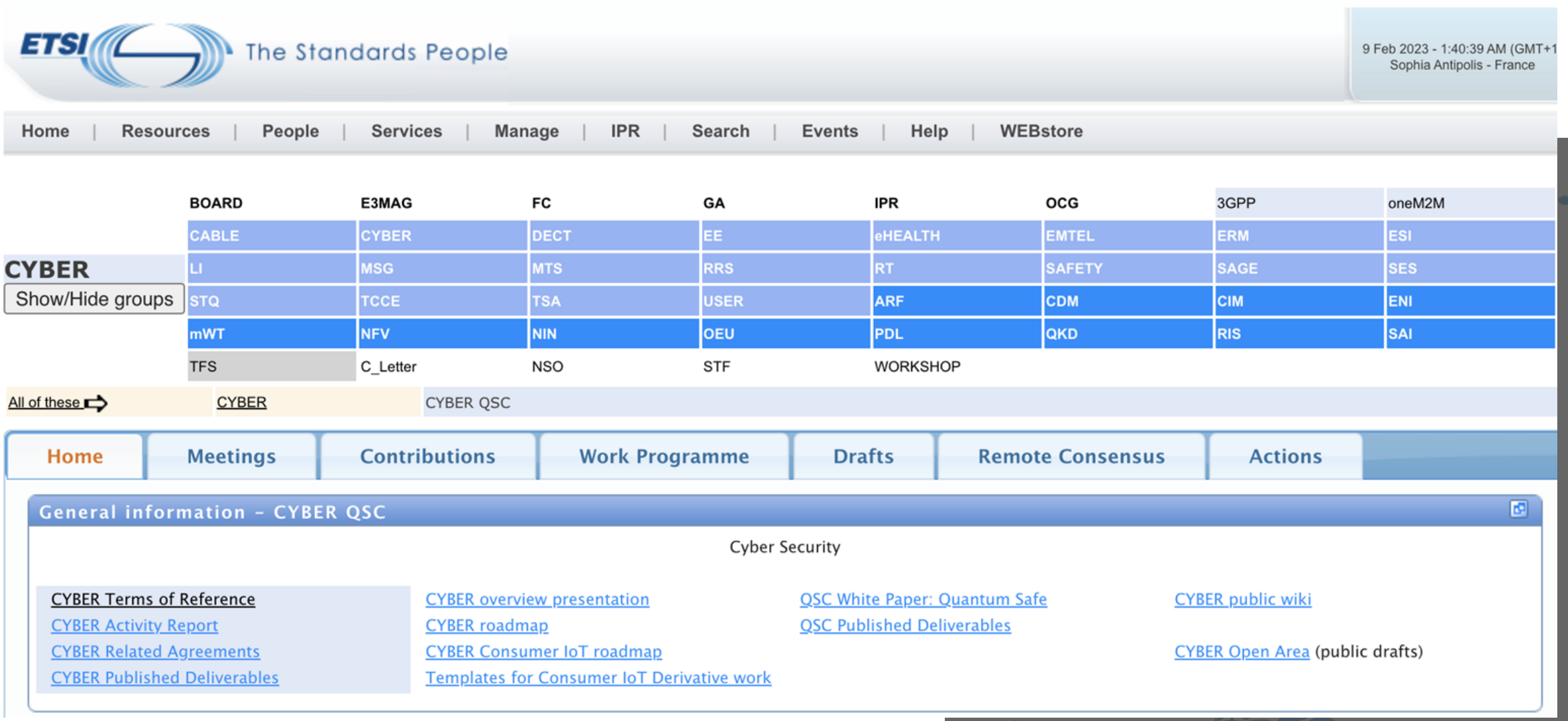
CYBER; Deployment Considerations for Hybrid Schemes, DTR/CYBER-QSC-0021(TR)

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

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

CYBER; Impact of Quantum Computing on Symmetric Cryptography, DTR/CYBER-QSC-0022(TR)

How to participate

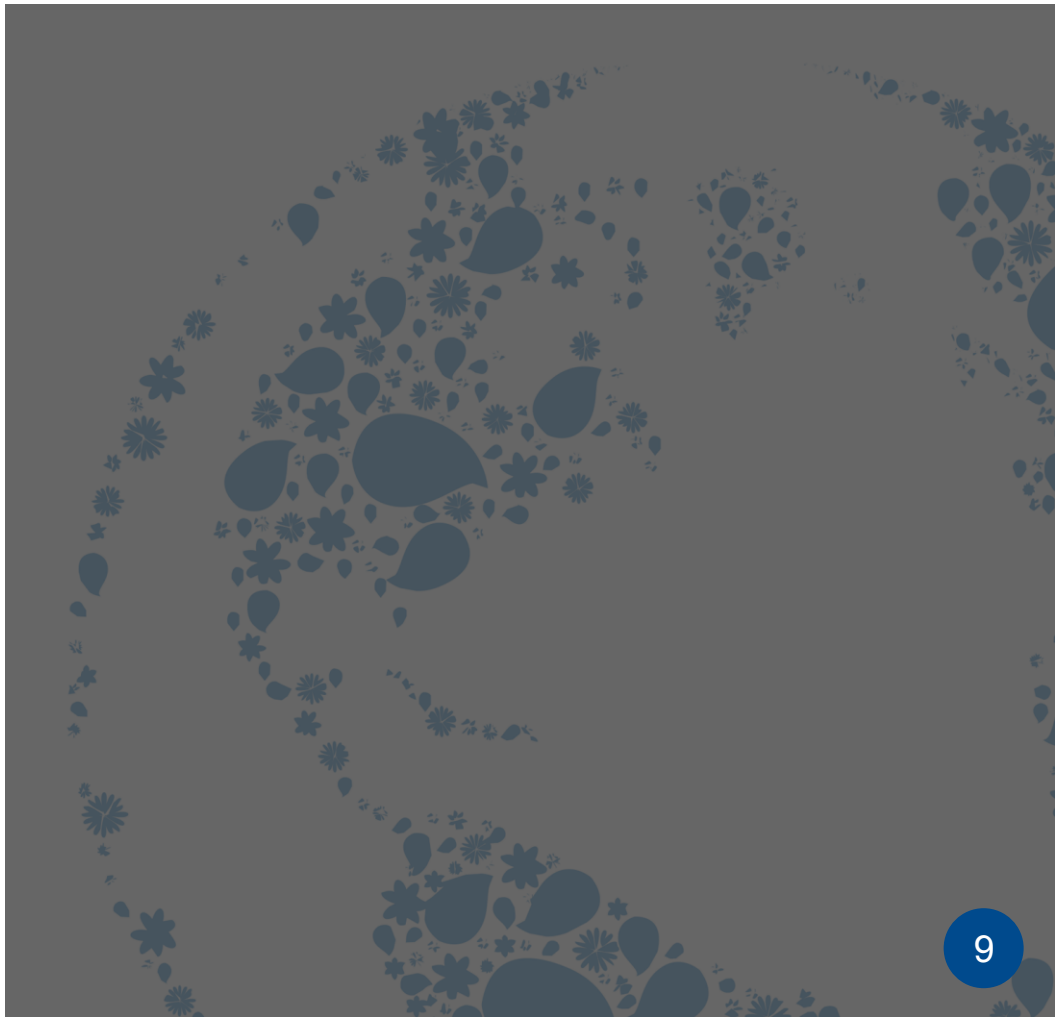


How to participate

23 May – CYBER QSC#30 (Sophia Antipolis, FR)

19 September – CYBER QSC#31 (Sophia Antipolis, FR)

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



Thank you for your attention

Matthew Campagna

campagna@amazon.com