ETSI Cyber TC Quantum-Safe Cryptography Working Group

Presented by: Matthew Campagna (Amazon)

For: IETF PQUIP

2025-11-06

Agenda

- ETSI
- ETSI TC CYBER QSC Working Group
- Recently finished Recommendations and Specifications
- New work items
- Upcoming ETSI events

© ETSI 2025. All rights reserved.

European Telecommunication Standards Institute

Founded in 1988 as a non-profit Europeans Standards Organization.

One of three ESO that produce European Harmonized Standards for E.U. regulation and legislation.

Director General: Jan Ellsberger.

Membership: 900+ member organizations, 60+ countries.

Structure: 30 Technical Committees, 16 Industry Specification Groups.

Location: Sophia Antipolis, France.

Partnerships: 3GPP and oneM2M.

Funding: Membership, European Commission, and Partnerships like 3GPP.

© ETSI 2025. All rights reserved.

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.

2018 QSC became a working group of the Technical Committee CYBER.

© ETSI 2025. All rights reserved.

Highlights from the past

ETSI White Paper No. 8

Quantum Safe Cryptography and Security

An introduction, benefits, enablers and challenges

June 2015

ISBN No. 979-10-92620-03-0

ETSI (European Telecommunications Standards Institute)
06921 Sophia Antipolis CEDEX, France
Tel +33 4 92 94 42 00
info@etsi.org
www.etsi.org

Challenges identified:

- Confidence in new post-quantum algorithms.
- Rigidity of existing protocols to accommodate these algorithms.
- A sense of urgency about adoption.

Recommendations:

- Adoption using hybrid key establishment.
- Call for greater algorithm agility in protocols.
- Two stage approach to adoption:
    - Confidentiality (key establishment).
    - Authentication (digital signatures).

© ETSI 2025. All rights reserved.

ETSI TC CYBER WG QSC

Chair: Matthew Campagna (Amazon)

Vice chairs: Mark Pecen (Beyond Affinity)

James Howe (Sandbox AQ)

Peter C (NCSC)

Secretary: Anthony Barnett (Thales)

Technical Officer: Kim Nordström (ETSI)

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

Held in hybrid mode with teleconferencing.

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

© ETSI 2025. All rights reserved.

Recent Recommendations & Specifications

Impact of Quantum Computing on Symmetric Cryptography, TR 103 967 V1.1.1 (2025-01). Impact of Quantum Computing on Cryptographic Security Proofs, TR 103 965 V1.1.1 (2024-10).	Analysis
A Repeatable Framework for Quantum-Safe Migrations, TR 104 016 V1.1.1 (2024-10). Deployment Considerations for Hybrid Schemes, TR 103 966 V1.1.1 (2024-10). State management for stateful authentication mechanisms, TR 103 692 V1.1.1 (2021-11).	Migration Plans & Recommendations
Efficient Quantum-Safe Hybrid Key Exchanges with Hidden Access Policies, TS 104 105 V1.1.1 (2025-02). Quantum-Safe Hybrid Key Establishment, TS 103 744 V1.2.1 (2025-03).	Standards

© ETSI 2025. All rights reserved.

ETSI-FORGE

github.com/etsi-forge

Platform Solutions Resources Open Source Enterprise Pricing Search or jump to... Sign in Sign up

etsi-forge / cyber.103744_QHKEX Public

Notifications Fork 0 Star 1

Code Issues 1 Pull requests Actions Projects Security Insights

kats_v1.2.x 4 Branches 0 Tags Go to file Code

This branch is up to date with `master`.

mattcampagna Merge branch 'update_rand_derand' into 'master' 41caf04 · 3 months ago 12 Commits

LICENSE	Updated LICENSE and README.md file	5 years ago
Makefile	Add all tests for derandomized qhkex	5 months ago
README.md	Update README file	5 months ago
crypto.c	Add all tests for randomized qhkex	5 months ago
crypto.h	Add all tests for randomized qhkex	5 months ago
main.c	Add all tests for randomized qhkex	5 months ago
qshkex.c	Comments Updates	4 months ago
qshkex.h	Add all tests for derandomized qhkex	5 months ago

README License

TS 103 744 Quantum-safe Hybrid Key Exchanges

About

Informative reference implementation as reported in Annex C of ETSI TS 103 744, "CYBER; Quantum-safe Hybrid Key Exchanges. The code is not intended for production use. It is intended to be a reference implementation for test. - READ ONLY - Contribute at https://forge.etsi.org/rep/cyber/103744_QHKEX

Readme
BSD-3-Clause license
Activity
Custom properties
1 star
0 watching
0 forks
Report repository

Releases

No releases published

Packages

© ETSI 2025. All rights reserved.

New Work Items

Secure Implementation Guidance for Key Encapsulation Mechanisms and Digital Signature Schemes;

- Part 1: General.
- Part 2: ML-KEM.
- Part 3: ML-DSA.
- Part 4: SLH-DSA.

Cryptographic Agility in Software Quantum-Safe Cryptography Migration.

QSC Extended Roadmap.

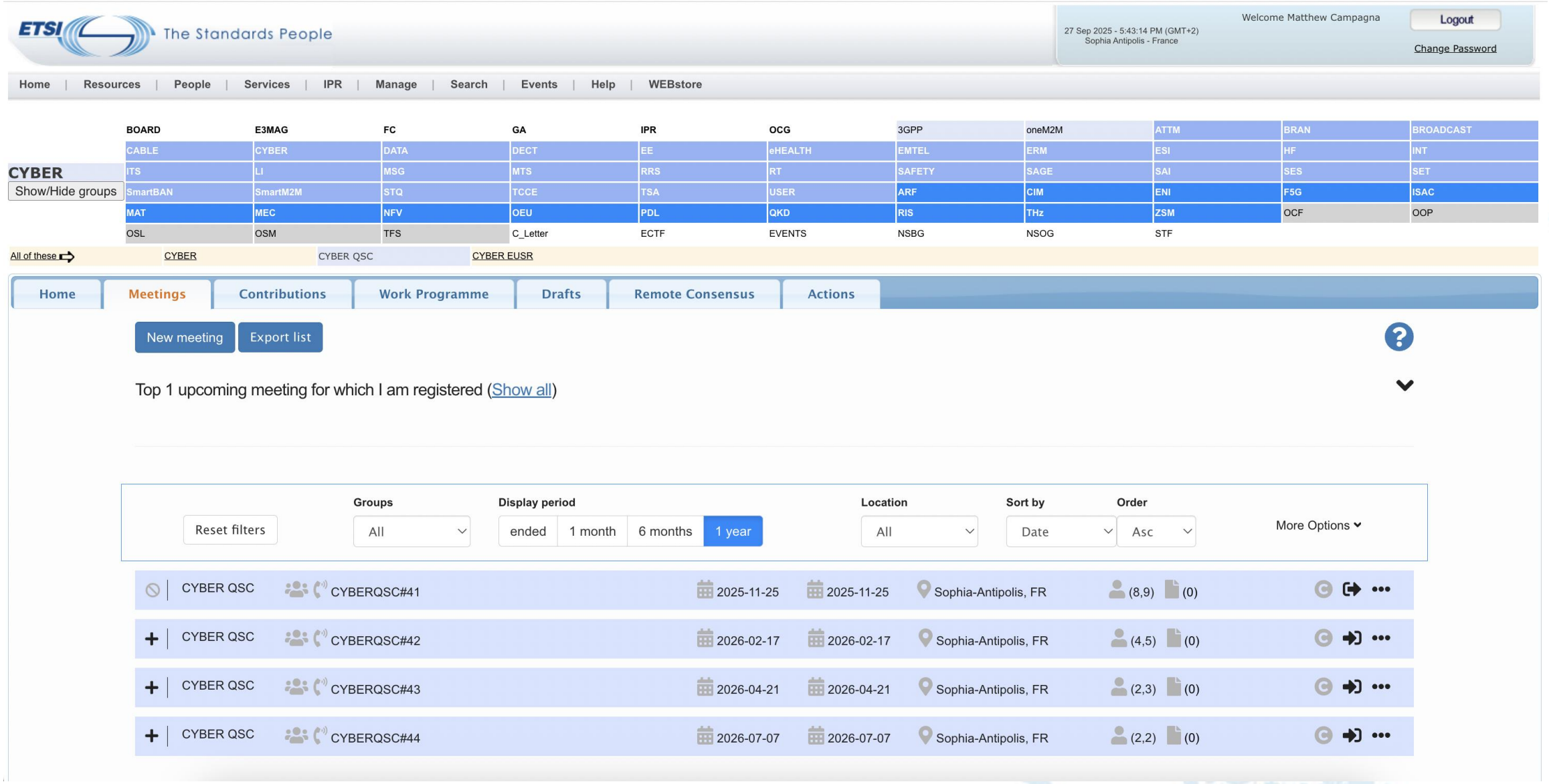
Migration Plans & Recommendations

Authenticated Quantum-Safe Hybrid Key Establishment (AQSHKE), ETSI TS.

Standards

© ETSI 2025. All rights reserved.

How to participate



© ETSI 2025. All rights reserved.

Next QSC Conference

© ETSI 2025. All rights reserved.

Thank you for your attention

Follow us on:

© ETSI 2025. All rights reserved.