Security Conference

Post Quantum - Network Standards Ecosystem Update

Michael Salmon Verizon

14.10.2023

Introduction

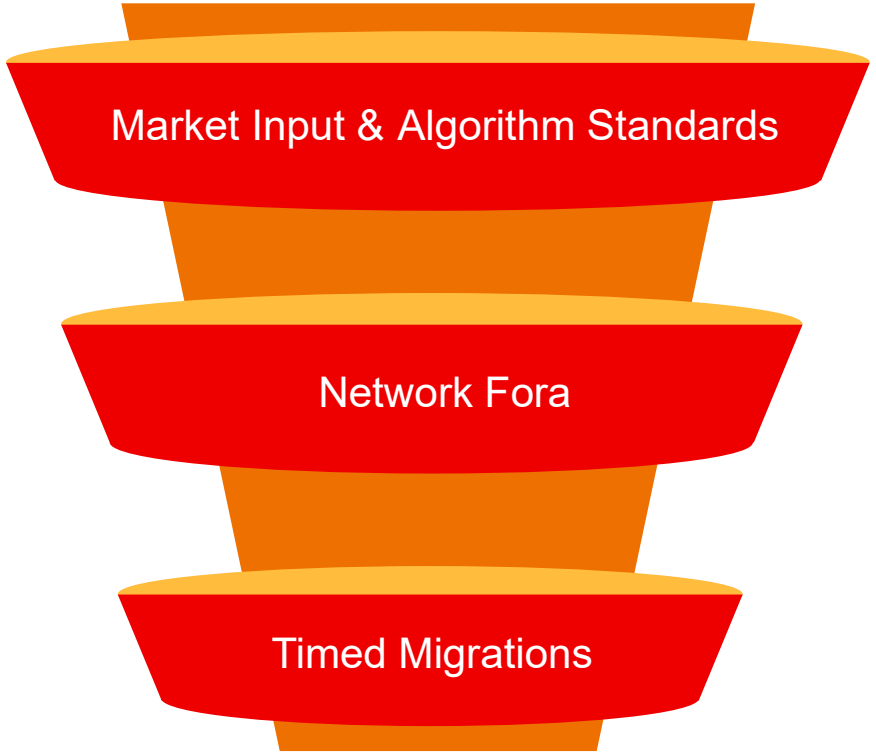
Presentation Focus

- Ecosystem Overview
- Network Fora Highlights

  ETSI, IETF, GSMA, ATIS, CSCC

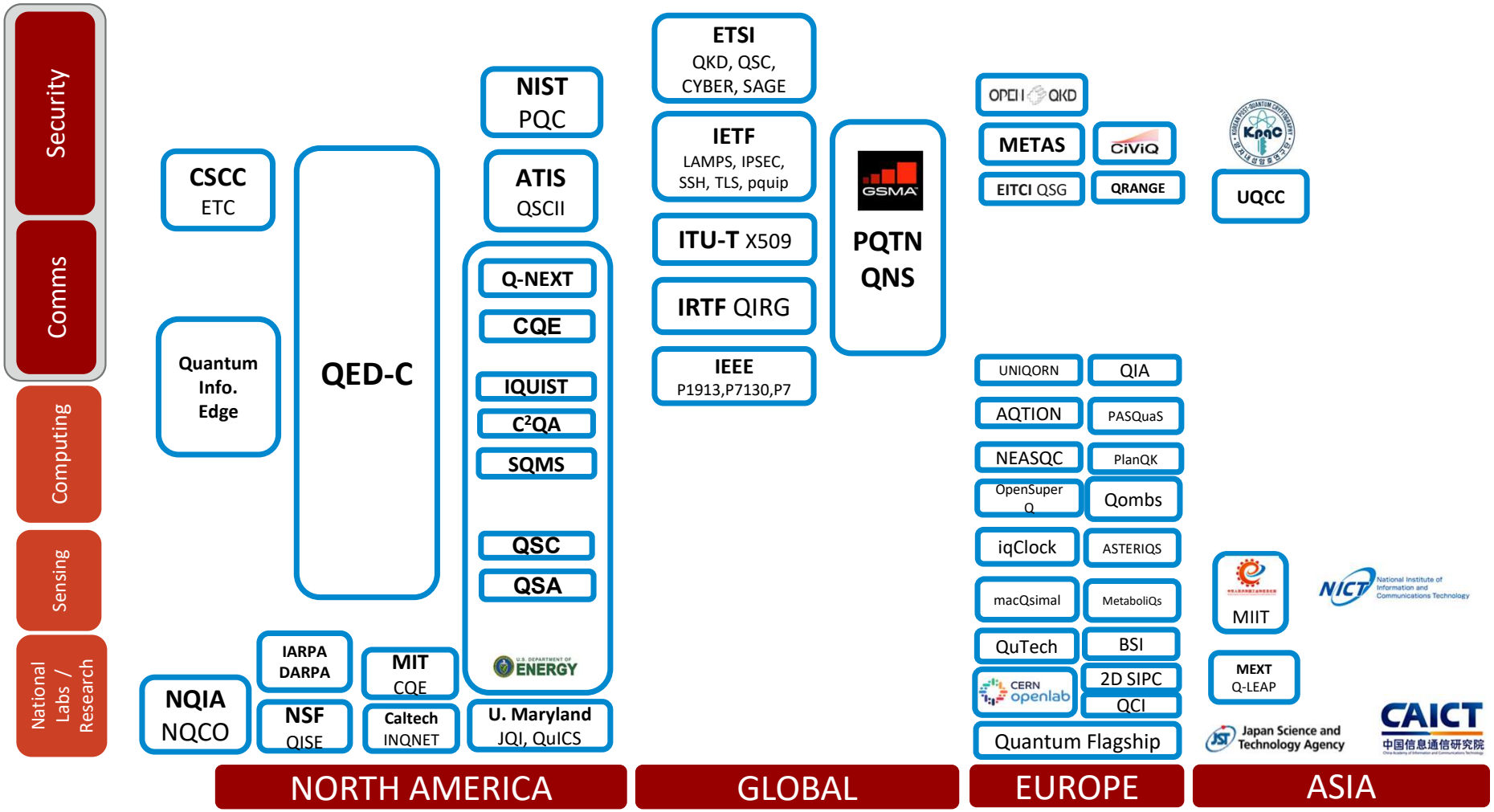
Notable

- NIST: SP 1800-38, RMF
- ITU-T SG 13-SG17 (X.1811)
- ISO
- ANSI X9



Quantum-Safe Networks

Ecosystem Overview



European Telecommunications Standards Institute

CYBER/QSC

- WG-QSC make assessments and recommendations from industry and academia on real-world deployments of quantum-safe crypto, incl. practical and security properties, and appropriately applying QSC primitives to application domains

Leadership
Matt Campagna (AWS)
Philip Lafrance (ISARA)
Dan Grundy (NCSC)
Anthony Barnettt (Thales)
Laure Pourcin (ETSI)

Key Deliverables

"Quantum Safe Cryptography and Security [Introduction]" (WP No.8)

"Quantum-safe algorithmic framework" (QSC 001)

"Case Studies and Deployment Scenarios" (QSC 003)

"Quantum-Safe threat assessment" (QSC 004),

"Limits to Quantum Computing applied to symmetric key sizes" (QSC 006)

"Quantum-Safe Key Exchanges" (TR 103 570) / "QS-Hybrid Key Exchanges" (TS 103 744)

"Critical Security Controls for Effective Cyber Defence" (TR 103 305)

"Migration strategies and recommendations to Quantum Safe schemes" (TR 103 619)

"Migration to QSC for ITS" (TR 103 949)

Internet Engineering Task Force

Pre-’23, IETF WGs began revising protocols: LAMPS, TLS, IPSECME, COSE

Leadership (pquip)
Paul Hoffman (ICANN)
Sofia Celi (BRAVE)

Q1 ‘23 - Post-Quantum Use In Protocols (pquip) WG founded

- Acts as central across all IETF PQC activities
- Does not update/define protocols, define crypto
- Has published Internet Drafts
- Will document operational and design guidance for PQC transitions

https://datatracker.ietf.org/wg/pquip/about/

https://github.com/ietf-wg-pquip/state-of-protocols-and-pqc

GSM Association

GSMA Post Quantum Telco Network Task Force (PQTN)

- Focuses on uniting telcos to prepare telcos for the quantum era. The task force has gained significant momentum and now includes more than 50 companies and over 20 major operators.
- Influences: 3GPP, O-RAN

Leadership
Lory Thorpe (IBM)
Luke Ibbetson (Vodafone)

Key Activity

Published Feb'23 - Post Quantum Telco Network Impact Assessment Whitepaper

Published Sept'23 – Guidelines for Quantum Risk Management for Telco

Planned PQC Best practices - Q1'24

Alliance for Telecommunication Industry Solutions

Quantum-Safe Communication and Information Initiative

OQS Test Framework (proposed project)

- Open Quantum Safe -Test Framework (OQS-TF), is designed to rigorously assess the reliability of quantum-resistant cryptographic algorithms. Aims to establish consistent performance standards across various hardware, operating systems, virtualized infrastructures, and device platforms.

Communications Sector Coordinating Council

Emerging Technologies Committee

- Focuses on the impact of the new and developing technologies (e.g. AI/ML, PQC) on products, and services of the communications sector.

Leadership
Vaibhav Garb, Co-Chair (Comcast)
Taylor Hartley, Co-Chair (Ericsson)
Justin Perkins, Co-Chair (CTIA)

Key Activity

"The Engineer Who Cried Quantum", July 2023,
https://www.comms-scc.org/wp-content/uploads/2023/07/The-Engineer-Who-Cried-Quantum.pdf