Welcome to the World of Standards

EUROPEAN TELECOMMUNICATION STANDARDS INSTITUTE (ETSI) TECHNICAL COMMITTEE CYBER WORKING GROUP FOR QUANTUM SAFE CRYPTOGRAPHY (WG-QSC)

CHAIRMAN'S REPORT AND SUMMARY OF WORK ITEMS

Mark Pecen, Chairman, ETSI TC Cyber QSC

ICMC17 16 – 19 May 2017

Agenda

1. About the working group QSC
2. Recent organisational changes
3. Recent technical progress
4. Summary of published work items

Technical Committee Cyber, Working Group Quantum Safe Cryptography (QSC)

- Founded March 2015 as Industry Specification Group (ISG) QSC
- Our focus is on the practical implementation of quantum safe primitives, including performance considerations, implementation capabilities, benchmarking and practical architectural considerations for specific applications
- Our work may feed into other ETSI groups and projects as 3GPP and other standards bodies such as International Telecommunication Union (ITU), e.g. SG-17 or SC27 (now managed in ITU)
- Our objectives DON'T include the development of cryptographic primitives or focus on QKD
  - These are propositions best left to academia and other groups who specialise in the area

Who are the QSC members ?

- Governments
  - Provide us with requirements from public perspective
- Academia
  - Bring the latest, newest basic science
- Industry
  - Focus on how to implement and use technologies

Operations of the QSC

- We currently hold 5 regular meetings each year at ETSI headquarters in Sophia Antipolis, FRANCE
- Over a 2-year period, we've accumulated sufficient participation to justify the development of normative specifications in the ETSI manner of
  - Stage 1 service requirements
  - Stage 2 architecture and engineering requirements
  - Stage 3 Technical Reports (TR) and Technical Specifications (TS)

ISG QSC becomes TC Cyber WG-QSC

- In order to produce normative ETSI specifications, such as Technical Reports (TR) or Technical Specifications (TS), if was necessary to promote the group to become a Working Group (WG) of a ETSI Technical Committee (TC)
- After 2 years of operating as an Industry Specification Group (ISG), the QSC became part of a larger Technical Committee (TC), TC Cyber Working Group for Quantum Safe Cryptography (WG-QSC) in March 2017
- Existing QSC officers were re-elected to continue serving in TC Cyber WG-QSC and maintain its working pace and environment
- TC Cyber WG-QSC chairman regularly reports to TC Cyber
- All WG approved output documents flow into TC Cyber plenary for final approval

Recent publications

- QSC-001 “Quantum-Safe Primitives Assessment”
  http://www.etsi.org/deliver/etsi_gr/QSC/001_099/001/01.01.01_60/gr_QSC001v010101p.pdf
- QSC-003 “Case studies and deployment scenarios”
  http://www.etsi.org/deliver/etsi_gr/QSC/001_099/003/01.01.01_60/gr_QSC003v010101p.pdf
- QSC-004 “Quantum Safe Threat Analysis”
  http://www.etsi.org/deliver/etsi_gr/QSC/001_099/004/01.01.01_60/gr_QSC004v010101p.pdf
- QSC-006 “Limits of Quantum Computing”
  http://www.etsi.org/deliver/etsi_gr/QSC/001_099/006/01.01.01_60/gr_QSC006v010101p.pdf

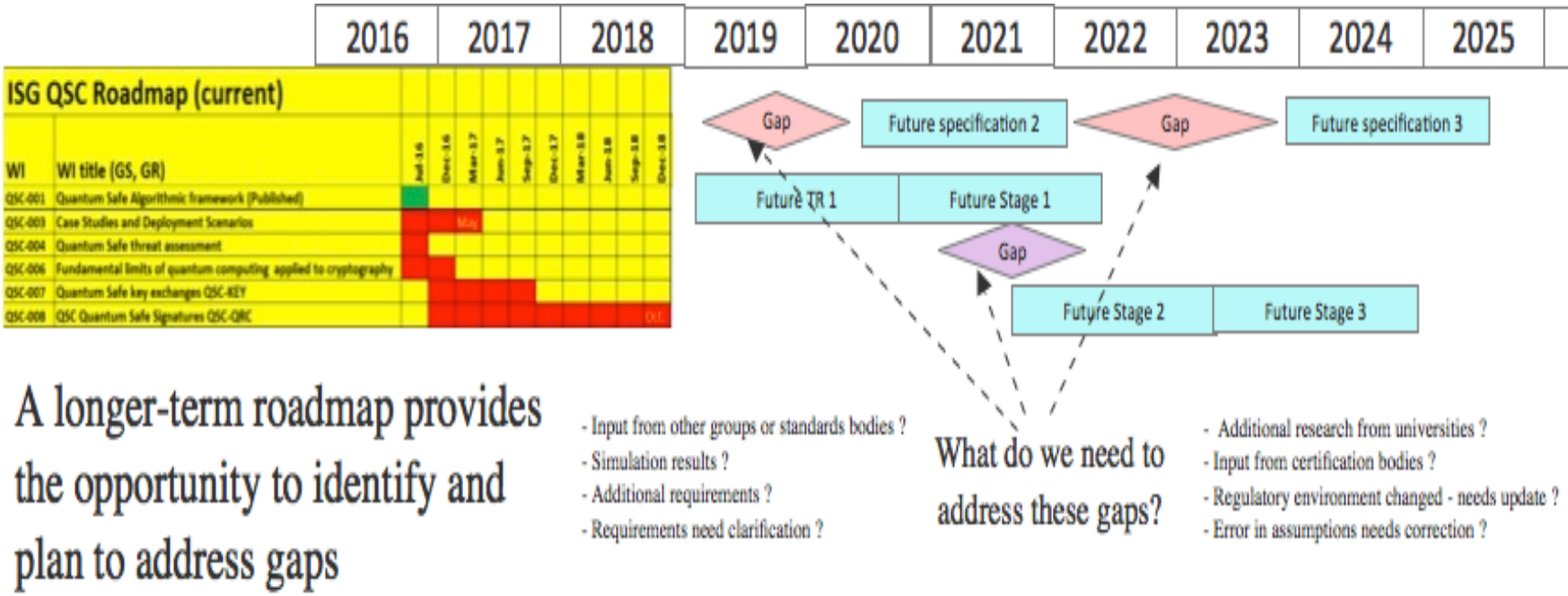
Three new work items created recently

- Created Two New Work Items of major interest at QSC#7, September 2016
  - QSC-007: Quantum-Safe Key Exchanges: proposed by CESG, supported by Phillips International, ISARA Corp., CESG, Thales U.K. and Queens University Belfast proposed in QSC#7, September 2016
  - QSC-008: Quantum-Safe Cryptographic Signature assessment: proposed by INRIA, supported by Phillips International, Thales U.K. limited, CESG, Queens University Belfast and Security Innovation Inc., Belfast proposed in QSC#7, September 2016

- New Work Item created at QSC#1, March 2017 (Note the numbering scheme starts at #1 again after promoting the group to a TC)
  - QSC-009: Quantum Safe Virtual Private Network (VPN): proposed by ISARA Corporation, supported by NCSC, Phillips, Amazon, Qunion PIDS, Thales UK Ltd.

Extended roadmapping: 10+ years

- Gaps are difficult to identify in the longer term…
- Unless we search together



We have begun roadmapping activities in QSC#9 and plan roadmapping workshops for future QSC meetings

Summary GROUP REPORT (GR) QSC-001 "Quantum-Safe Primitives Assessment"

- **Provides an overview and best practices by industry and academia for assessing cryptographic primitives** that have been proposed for key establishment and authentication applications, and which may be suitable for standardization by ETSI and subsequent use by industry to develop quantum-safe solutions for real-world applications
- **Primitive families** under consideration
  - **Lattice-based** primitives where the security depends on the difficulty of solving a short or close vector problem in a lattice
  - **Multivariate** primitives where the security depends on the difficulty of solving a system of multivariate polynomial equations
  - **Code-based** primitives where the security depends on the difficulty of solving a decoding problem in a linear code
  - **Hash-based** primitives where the security depends on the difficulty of finding collisions or preimages in cryptographic hash functions
  - **Isogeny-based** key primitives where the security depends on the difficulty of finding an unknown isogeny between a pair of supersingular elliptic curves

Summary GROUP REPORT (GR) QSC-003 "Case studies and deployment scenarios"

- **Examines a number of real-world uses cases** for the deployment of quantum-safe cryptography (QSC)
  - **Typical applications** where cryptographic primitives are deployed today
  - **Identifies some of the consequences** of adapting services and applications to quantum safe equivalents, along with features that may need change to accommodate quantum-safe cryptography
  - **Options for upgrading** public-key primitives for key establishment and authentication, although several alternative, non public-key options are also discussed
- **Cases include**
  - **Network security services**, including TLS, where design choices such as drop-in replacement, hybrid approaches and re-engineering are considered
  - **Potential integration issues** for deploying quantum safe equivalents into existing protocol stacks, including the handling of large key sizes
  - **Offline services**, such as e-mail, and credentials for offline services
  - **Internet of Things (IoT)** aspects, including processor, bandwidth, power consumption and size limitations and impact on cryptosystems
  - **Satellite communications**, and associated limitations
  - **Also** key distribution centres, authentication and certain exotic applications for cryptosystems

Summary GROUP REPORT (GR) QSC-004 "Quantum Safe Threat Analysis"

- **Simplified threat assessment** following the guidelines of ETSI Technical Specification (TS) 102 165-1 for a number of use cases
- **Identification of required capabilities** for certain algorithms
  - Grover's algorithm
  - Shor's algorithm
  - Further implications
- **Threat assessment** for various aspects of security
  - Symmetric key algorithms
  - Public key algorithms
  - Random number generation
  - Security protocols like TLS, IPSec, IKE, SMIME and PKI
- **Industry-specific issues** are identified
  - Banking and e-commerce
  - Intelligent transportation systems
  - eHealth

Summary GROUP REPORT (GR) QSC-006 "Limits of Quantum Computing"

- **Analysis of quantum computing capabilities** is presented within the context of solving symmetric key cryptographic problems
- **Evolution of quantum computing** is discussed
  - Learning curves, such as Moore's law
  - Commercial quantum computers
  - "worst-case" quantum computing
  - Upper-bounds to quantum computing
- **Assumptions** regarding keys and parameter sizes, symmetric keys and output lengths
- **Some conclusions** are made − although speculative, this analysis suggests that symmetric key crypto AES-256 may still be used in the year 2050 based on the assumed power of future quantum computers

QSC work used by other standards groups

- ETSI CTO Adrian Scrase speaks with 3GPP SA Chairman about quantum safe assumption for 5G wireless systems

Important dates for QSC activities

QSC#2	30 - 31 May 2017	Sophia Antipolis (2)
TC Cyber	1 - 2 June 2017	Sophia Antipolis
Security week:	12 - 16 June 2017	Sophia Antipolis
QSC#3	11 - 12 Sep 2017	London, UK
IQC-ETSI QSC workshop	13 - 15 Sep 2017	London, UK (1)
QSC#4	6 - 7 December 2017	Sophia Antipolis

Note (1): Qcrypt also in London, UK 18–22 Sep 2017

Note (2): QSC has already met for 10 meetings, but when the group was promoted from ISG to TC, the numbering of meetings started again at #1

Pictures: from the labs of Institute for Quantum Computing, CANADA

Contact Details:
Mark PECEN, Chairman ISG QSC
mpecen@approachinfinity.ca