ACTIVITIES CONCERNING SECURITY STANDARDS

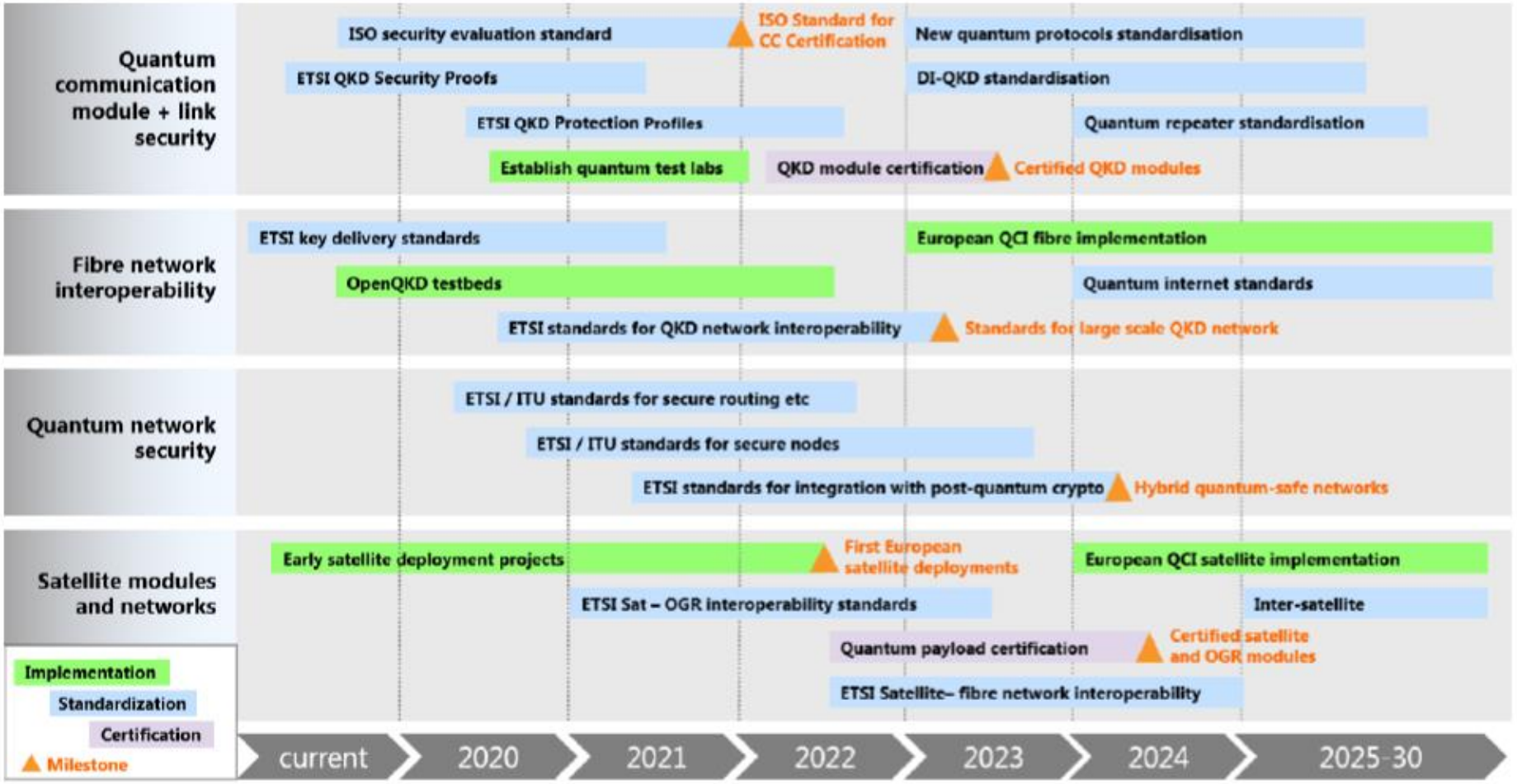
First workshop on “Standardisation and certification of QKD systems and QKD networks”

Matthieu LEGRE, ID Quantique

07/10/2021

OPENQKD STANDARDIZATION ROADMAP (2020)

Figure 2. QKD standards roadmap



- Link to the OpenQKD document

Quantum communication module + link security (1)

- Security requirements for QKD modules
  - ETSI GS QKD 008 V1.1.1 (2010-12); Quantum Key Distribution (QKD); QKD Module Security Specification
  - ETSI DGS/QKD-016-PP (GS); Quantum Key Distribution (QKD): Protection Profile [early draft]
    - Conformity with CC framework
    - Written by security experts with the support of QKD experts
    - Opportunity: point of view of final user
    - Risk: partial incompatibility with some QKD principles or practical aspects
  - ISO JTC1/SC27 WG3; Information security—Security requirements, test and evaluation methods for quantum key distribution—Part 1:Requirements [CD2]
    - Conformity with CC framework
    - Written by QKD experts and CC methodology experts
    - Opportunity: CC evaluation of QKD modules
    - Risk: security problem addresses user needs partially

Quantum communication module + link security (2)

- Tests and evaluation methods for QKD protocols
  - ETSI GS QKD 005 V1.1.1 (2010-12); Quantum Key Distribution (QKD); Security Proofs
  - ETSI RGS/QKD-0005ed2_SecProofs (GS QKD 005); QKD Sec Proofs Rev [stable draft]
- Tests and evaluation methods for QKD modules
  - ETSI GS QKD 011 V1.1.1 (2016-05); Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems
  - ETSI DGS/QKD-0013_TransModChar (GS QKD 013); Quantum Key Distribution (QKD); Component characterization: Transmitter module characterization [stable draft]
  - ISO JTC1/SC27 WG3; Information security—Security requirements, test and evaluation methods for quantum key distribution—Part 2: Test and evaluation methods [CD2]
    - Strength of this document
- Best practices
  - DGS/QKD-0010_ISTrojan (GS QKD 010); Implementation security against Trojan horse [stable draft]

QUANTUM NETWORK SECURITY (1)

- Secure key routing over a QKD network
  - ITU-T X.1710 (10/2020): Security framework for quantum key distribution networks
  - ITU-T draft X.1712 (ex X.sec_QKDN_km): Security requirements and measures for QKD networks - key management [consented draft]
  - ITU-T X.sec_QKDN_CM: Security requirements and measures for quantum key distribution networks - control and management [draft]
  - ITU-T X.sec_QKDN_A&A: Authentication and authorization in QKDN using quantum safe cryptography [draft]

- Secure nodes
  - ITU-T X.sec_QKDN_tn: Security requirements and designs for quantum key distribution networks - trusted node [draft]

QUANTUM NETWORK SECURITY (1)

- Integration of QKD in security ecosystem
  - ITU-T X.sec_QKDN_intrq: Security requirements and measures for integration of QKDN and secure storage network [draft]
    - Security requirements apply to secure storage network and not to QKD
  - ITU-T TR.hybsec-qkdn: Technical Report on overview of hybrid security approaches applicable to QKD networks [draft]
    - Landscape of quantum-safe hybrid approaches
    - Checking with the compatibility with QKD technology

- Integration of Quantum-safe technologies in security ecosystem
  - ETSI TR 103 619 V1.1.1 (2020-07); CYBER; Migration strategies and recommendations to Quantum Safe schemes
  - ETSI TS 103 744 V1.1.1 (2020-12); CYBER; Quantum-safe Hybrid Key Exchanges
  - IETF RFC 8784; Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security, June 2020

ID Quantique

20 YEARS QUANTUM INNOVATION

Quantum.
Trust enabled for the future

Thank you for your attention!

Subscribe to our newsletter

Watch our webinars

info@idquantique.com | www.idquantique.com

ID Quantique

Founded in 2001

3 Product lines:

1. Quantum Random Number Generation
2. Quantum-Safe Security
3. Quantum Sensing

High-quality engineering

Best-in-class performance

Trust

Operational simplicity