Standarization needs for a QKD startup

1st Workshop : Standardisation and certification of QKD systems and QKD networks

Sep 28th, 2021

Sebastian Etcheverry, CTO

LUXQUANTA

LuxQuanta

Spin-off from ICFO focused on developing quantum key distribution systems and technology

Continuous variable quantum key distribution

- Based on telecommunication components.
- Ideal for network integration.
- High performance at metro distances.
- Cost-effective.

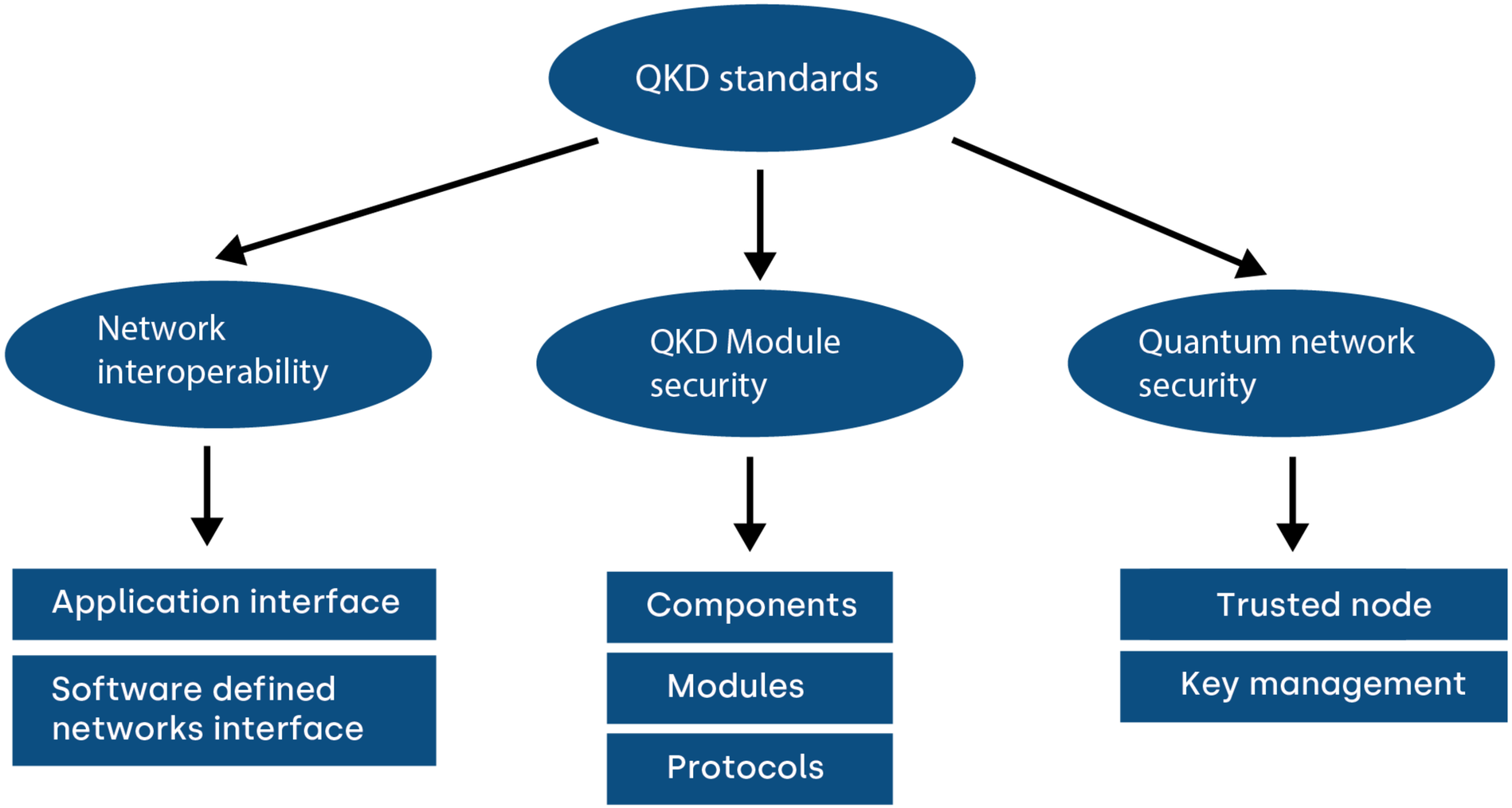
ICFO- The Institute of Photonic Sciences - Barcelona

QKD standardization

Definition of standards will help QKD manufacturers start-ups to

- Define and focus technical developments (software interfaces, components, etc)
- Reduce time-to-market
- Speed-up deployment and field validation in relevant use-cases
- Develop products that can be part of a network security ecosystem
- Provide products with high security standards considering practical implementation
- Provide flexibility to the customers and facilitate the adoption of QKD technology

QKD standardization

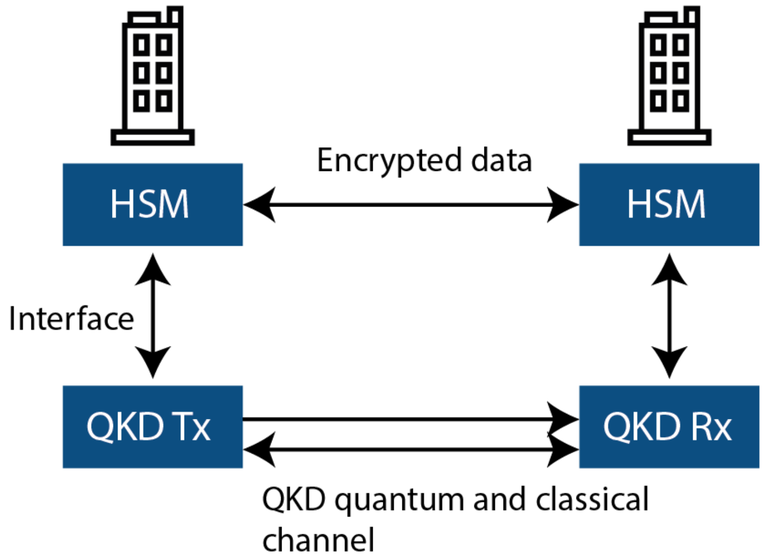


Network interoperability

Interface between QKD and application
Example: using QKD with commercial hardware security modules

ETSI GS QKD 004
Quality of service, flexible, multiple sessions, network metadata, **implementation agnostic**

ETSI GS QKD 014
Rest-API, single-key request, simple implementation.



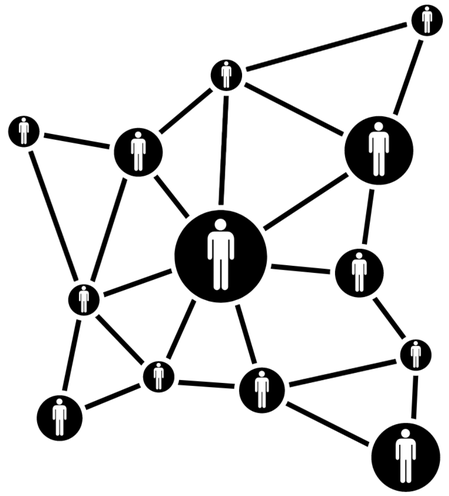
Network interoperability

Software define network interfaces (SDN)

SDN-QKD would facilitate the deployment of QKD in telecommunication networks (zero-touch integration) and reduce costs (avoid building networks exclusively for QKD).

Standards such as the ETSI QKD 015 (drafting) are needed

- QKD integrated at the physical level and connected to the network controller.
- Architectural design based on a YANG model to orchestrate the QKD resources
- Direct and virtual (multi-hop) links



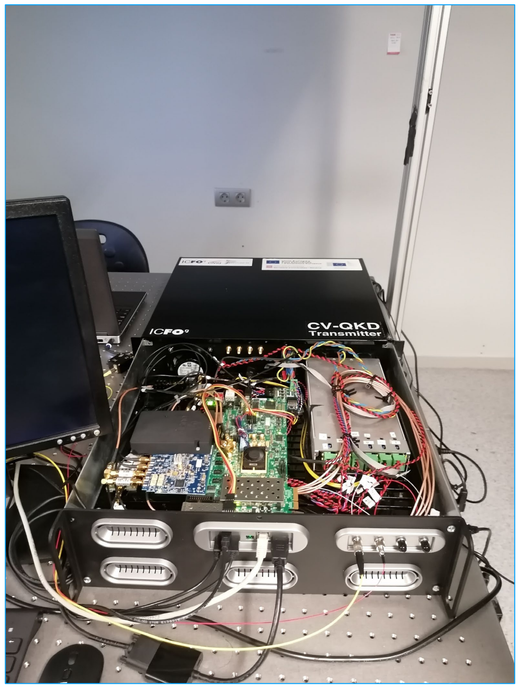
Start-ups/QKD manufactures targeting telecommunication industry as main customer are expected to follow/participate on SDN-QKD developments and implement defined standards

QKD module security

Modules and components

Standards are needed for selection of components and internal module design.

- Characterization procedure for critical components (i.e. modulators, detectors)
- Characterization of new components (i. e. QRNG) to meet regulatory requirements.
- Analysis of practical implementations of QKD protocols (control electronics, digital signal processing methods, auxiliary signals, etc)
- Side-channel attacks and countermeasures
- Characterization procedures for output signals (i.e. ETSI QKD 016, drafting)



Some available standards; ETSI GS QKD 011, ETSI GR QKD 003

Drafting ISO/IEC 23837, ETSI GS QKD 016 protection profile – aiming at certification of QKD

QKD module security

Protocols and security proofs

Standards needed for selection of QKD protocol and implementation of data processing

- Approved protocols for DV-QKD and CV-QKD based on the maturity of security proof and practical implementation.
- Evaluation procedure for parameter estimation and reconciliation (error correction codes, privacy amplification).
- Authentication procedure (pre-stored keys, PQC)

Some available standards
ETSI QKD 005 (drafting), ETSI GR 003

QKD network security

Trusted nodes and key management

Standards needed for developing interfaces for network operation

- Software define network, network architectures, and framework for integration of QKD in networks.
- Trusted relay implementation (i. e. data processing, bitwise XOR)
- Defense-in-depth (combination with PCQ or traditional methods)
- Authentication and key management in network environments
- Interoperability of QKD from different vendors
- Denial-of-service countermeasures
- Additional requirements for certification; MTBF

Some available standards; ITU-T 3800, ITU SG17 XSTR-SEC-QKD, ETSI GS QKD 003

Conclusions

- Definition of standards will facilitate the deployment of QKD and its adoption by telecommunication industry

- Standards will provide solutions to critical aspects of QKD such as side-channel attacks, authentication, and denial-of-service.

Start-ups developing QKD system would highly benefit by early definition of standards to focus technical development, and allow for field validation in large networks and relevant use-cases

Thank you

sebastian.etcheverry@luxquanta.com

LUXQUANTA