Standardization and Certification of QKD-Devices and QKD-Networks

Oliver Maurhart, Thomas Länger, Andreas Poppe, Christoph Pacher, Martin Stierle, Helmut Leopold

AIT Austrian Institute of Technology GmbH, Center for Digital Safety & Security, 1210 Vienna, Austria.

Contact: oliver.maurhart@ait.ac.at, martin.stierle@ait.ac.at

Introduction

The transition of Quantum Technologies (QT) being no longer pure basic research but touching applied fields with emerging products is companied by requests for standardization and certification. The call of the markets [1] requesting products based on QT will require alignment of QT products to match not only the need for standards but also the proof to fulfil certification procedures. In addition, most operators will ask for a multi-vendor strategy.

In the context of the European Quantum Communication Infrastructure we intended to ask if a broader roll-out of QKD in a market economy is well prepared with respect to standardzation and certification. We try to answer the main two question:

- **Can a larger network be built and operated with equipment that is certified and tested according to existing standards?**
- **Are all interfaces standardised so that a multi-vendor strategy can be implemented?**

QKD Interfaces inspired by the ISO/OSI Network model

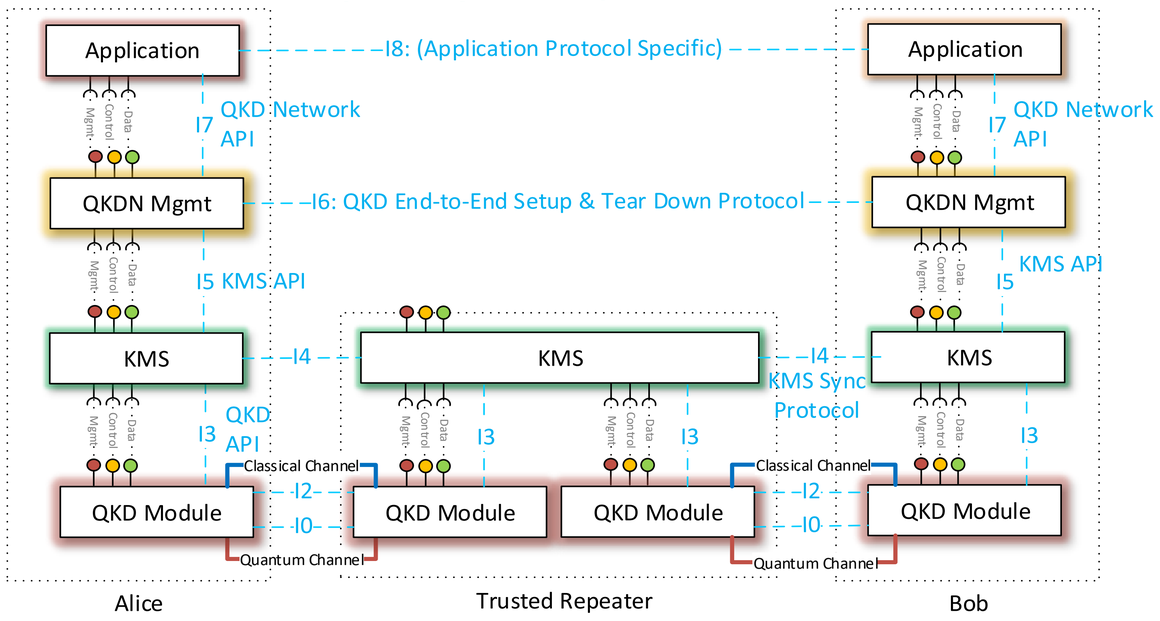

Fig. 1: Deployment scenarios of an application receiving secret keys over a QKD network built from QKD links.

Standardization I

- Standards are **driven by network operators, product vendors and users**, but they also play an important role in shaping the research landscape by highlighting the challenges requiring concerted R&D effort.
- Standardization **prevents wrong investments** in research and development without future user demands. Figure 1 depicts the current situation in QT concerning trusted repeater end-to-end QKD.
- To **guarantee trust and confidence** in QKD commonly understood, scrutinized and security checked network protocols (I0, I2, I4, I6 and I8) have to be defined.
- At the moment no standardization activities can be found, focusing on the Interfaces I4 and I6.
- Thus, QKD networks with different Key Management Systems cannot be set-up.
- This will be relevant in the context of the **QCI initiative of the European Commission**, if different operators (European telecommunication companies) in different countries get involved, which cannot be forced to opt for the same vendor.

Standardization II

- Alongside the process **APIs** (I3, I5, I7) have to be created too, which allow accessing the functionality in **between layers of this architecture** and which provide the final keys, stored in Key Management Systems (KMS), in a standard manner for arbitrary applications.
- To each of these, solutions and concepts do exist and some are already **discussed in several SDOs**.
- However, **only a few are currently accepted as standards**.
- The main questions for a bigger roll-out are the missing **interface for connecting the QKD network with SDN management** of telecommunication networks and how to build **a secure trusted repeater with QKD modules from different vendors.**

Certification

- Certification is about an **approval by an independent ”third-party” certification authority** that the product **manufacturer follows the respective standards**.
- Two main aspect are relevant for certification of QKD Networks:
- First is the topic of **implementation security** of the QKD module itself and how counter measures against potential side-channel attacks are implemented which are shown in the ETSI White paper [2].
- Second, the QKD modules, KMS and the control of QKD Networks is basically implemented as software which runs on normal computers. Therefore, certification typically will follow a **Common Criteria Framework** safeguard that QT products **are fit for purpose and of benefit to the user** to ensure that quantum-based information security products are implemented correctly with respect to potential cyber security attacks.
- The **ETSI GS QKD 016 Quantum Key Distribution (QKD) Protection Profile** (PP) will within the CC framework provide an implementation-independent specification of a QKD module.

Conclusions

- **Q**: Can a larger network be built and operated with equipment that is certified and tested according to existing standards?
- **A**: Not yet.
  The « cyber security **standards » based on common criteria are not yet published.** In addition, we will see, if the ETSI GS QKD 016 will only focus on the QKD module or also include the KMS and the QKD Network Management.
- **Q**: Are all interfaces standardised so that a multi-vendor strategy can be implemented?
- **A**: Not yet.
  Even if a roll out will be based on the KMS from one vendor it will be **difficult to certify** a trusted repeater network based on **QKD modules from different vendors** and the option to have **KMS from different vendors** in one network is not yet foreseen in an standardization activity.

Relevant International Standardization Organizations (SDO)

- **ETSI (ISG QKD)**
  SDO with the longest history focused on QKD, components, the link-layer and interfaces to networks. Different group specifications have been released and first steps towards certification already done.
- **ITU-T (Study groups SG 13, SG 17 and Focus group FG-QIT4N)**
  The security and architecture of networks for QKD and the possibility to include other quantum technology building blocks are discussed at different groups.
- **EU accelerated initiative CEN-CENELEC (FGQT Focus Group on Quantum Techn.)**
  Started very recently (June 2020) with the aim to kick-start standardization to fields beyond quantum communications
- **Other activities: ISO/IEC (JTC1, SC27), IEEE (P1913), IETF/IRTF (QIRG), GSMA**

Acknowledgements

We acknowledge the support of

- the EU QKD testbed initiative OpenQKD (grant agreement number 857156),
- the EU Flagship project CiViQ (grant agreement number 820466), and
- the EU Flagship project UNIQORN (grant agreement number 820474).

References

[1] T. Länger and G. Lenhart, “Standardization of quantum key distribution and the ETSI standardization initiative ISG-QKD,” New J. Phys. 11(5), 055051 (2009).

[2] M. Lucamarini, et. al, “Implementation Security of Quantum Cryptography Introduction, challenges, solutions”. ETSI White Paper No. 27, July 2018. ISBN No. 979-10-92620-21-4