QKD Security Certification

Current State of the Activity and Outlook

ITU Workshop on
QKD protocols, security, and certification
Singapore, 8 November 2022

Thomas Länger and Florian Fröwis
ID Quantique Europe GmbH, Vienna, Austria

--v3--

Outline of presentation

- About ID Quantique Europe GmbH
- QKD security certification context
- Necessity and advantages of security certification
- Principal procedure and involved parties
- Problems and open issues
- „Background Documents“ for security evaluation
- Other problem zones
- IDQE‘s approach towards certification

...on 15 slides

IDQ Europe
Est. 2022

QKD developer to secure EU's critical infrastructure with QKD

Vienna, Austria

Activities ramping up

- Certification and standardisation
  - ETSI
  - ASI (Austrian ISO mirror group)
  - CEN/CENELEC
- Quantum Communications solution design, integration and support for customers in Europe
- R&D for EU QKD system
- Manufacturing

QKD security certification context

QKD products (links, networks)

- **Promise highest security levels;**
- Are **intended for security critical applications.**

Owners (users) require

- **confidence that their data is protected**,
- **Minimizing risks** by **sufficient and effective countermeasures.**

Security certification

- Is a **structured process for security assessment;**
- **Delivers assurance for prospective users;**
- **Enables safe deployment** and **observance of due diligence.**

Necessity and advantages of security certification

- **Certified QKD products will be mandatory for actual deployment;**
- Nobody would entrust their secrets to a product that is not certified!

- Certified products constitute a **valuable competitive advantage;**
- **IDQ Europe is committed to create certification framework.**

- **Early involvement** in certification provides **important strategic advantage;**
- Through **acquisition of experience and expertise;**
- **Early involvement** also means potential influence on evolving procedures.

- **→ Goal: certify IDQ's new Clavis XG BB84!**

Principal procedure and involved parties

- Use paradigm of **ISO/EN 15408 “Common Criteria for IT Security Evaluation”** (CC);
- CC established in the late 1990ies, currently Version 3.1, revision 5
  - Standards available online on commoncriteriaportal.org (free of charge).

- **Vendor** provides security specification for a QKD product;
- An **evaluation lab** evaluates the specification (that it is complete, sufficient);
- An **evaluation lab** evaluates the QKD product against the specification;
- A **certification authority** oversees the process and finally issues a certificate;
- A **certificate** is basically a “stamped and signed” text document.

Problems and open issues

On the following slides we identify several **problems and open issues on the way to a successful certification of a QKD product**:

- **Missing “Background Documents” (BGDs) for cryptographic choices;**
- **Missing BGDs for the quantum optical part;**
  - Here especially the “problem zone” QKD protocols and security proofs;
- **Applicability of evaluation methodologies;**
- **“Quantum Security Evaluation Facilities” are not available;**
- **Recognition of security certification to be clarified**

The „form“ of Background Documents (BGDs)

- **BGD: any external document referenced in a Common Criteria security specification**:
  - In a Protection Profile or Security Target;
- **Additional documents, necessary for the actual security evaluation**

- **Background documents are, e.g.:**
  - **Published standards;**
  - Other “**widely accepted publications**”;
  - Peer reviewed **publications, white papers;**
  - **Whatever the ITSEF and EA (evaluation authority) see fit for purpose**.

Required „Background Documents“ for cryptographic choices

- QKD implementations are **highly individual implementations**;
- With security features **using very specific cryptography**;
- **CC are indifferent to cryptographic algorithms and protocols;**
- **CC only address security functional domain**.

- **ITSEFs will not accept “proprietary crypto”**

- Therefore, any choice of a **cryptographic algorithm, protocol, or selection of parameters** needs to be **backed by approved documentation**, i.e., a **Background Document**, for:
  - **Authentication protocols;**
  - **Any “payload encryption”;**
  - **Random Number Generation (RNG).**

Required „Background Documents“ for quantum optical part

- **For the specification of the QKD protocol**
  - Security proof;
  - Parameterisation of components;
  - Implementation guidance.
- **For sources, detectors, and other components** (to some extent available)
  - Parameters, characterisation;
  - Specific evaluation methods.
- **For RNG specification** (available for non-quantum RNGs)
- **Other BGDs:**
  - Catalogue of attack methods;
  - Attack rating methodologies.

Potential Background Documents (ETSI)

- ETSI GS QKD 003 **Components and Internal Interfaces** V2.1.1
- ETSI GS QKD 005 **Security Proofs** (V1.1.1 published 2010-12), (update in preparation: V1.4.2, stable draft 2022-06-17)
- ETSI GS QKD 010 **Implementation security: Protection against Trojan horse attacks** in one-way QKD systems, V.0.4.1
- ETSI GS QKD 011 **Component characterization: characterizing optical components for QKD systems** V1.1.1
- ETSI GS QKD 013 **Characterisation of optical output of QKD transmitter modules**, V0.1.0, Stable draft (2021-09-20)
- ETSI GR QKD 019 **Design of QKD interfaces with Authentication** V0.0.92, Early draft (2022-06-20)

(non-exhaustive list)

Potential Background Documents (other SDOs)

- ETSI GR QSC 001 **Quantum-Safe Cryptography (QSC); Quantum-safe algorithmic framework** V1.1.1
- IEEE P1913 **Software-Defined Quantum Communication** (QN, SB)
- ETSI GS QKD 012 Quantum Key Distribution (QKD); **Device and Communication Channel Parameters for QKD Deployment**, V1.1.1
- ITU-T SG 17 X.cf-QKDN **Use of cryptographic functions on a key generated in Quantum Key Distribution networks**
- ITU-T SG 17 X.sec-QKDN-tn **Security req's for QKD networks -Trusted node**
- IEEE P1913 **Software-Defined Quantum Communication**, Drafting

(non-exhaustive list)

Evaluation methodologies

- **ISO/IEC 23837-2** defines an **entire catalogue of evaluation and testing methods for SFRs**:
  - For QKD protocols;
  - For quantum optical components;
  - And for conventional (network) components of QKD modules.
- **ETSI** has standards for specific component characterisation, e.g.
  - ETSI GS QKD 011 **Component characterization** (136 pages!)
  - ETSI GS QKD 013 **Characterization of optical output of QKD transmitter modules** (draft, 57 p.)

- **Are these methodologies "sufficient"?**
- **Are all required methodologies available?**
- **Who will carry out these evaluations?**

How do we address this challenge?

Implementing an **iterative approach**:

1. Develop a **detailed certification concept**
2. **Make sure it fits to specific implementation**
3. **Accord it with the community, certification authorities and ITSEFS**

   → So that a certification carried out according to that concept will likely be successful.

   (Plan B: partial certification as intermediate goal)

- **IDQE is actively driving QKD standardisation and standards coordination**
  - Thomas is **co-editor of CEN/CENELEC FGQT Standards Roadmap**
  - **Specifically responsible for QKD and QKD security certification standards coordination**
  - **Also for BGD coordination.** (btw. 1st draft release of the roadmap will happen early 2023)
  - **Will likely adress the issue of missing BGDs in a joint activity in the ETSI ISG QKD (with BSI, DT, etc.)**

Thank you for your attention !

florian.froewis
@idquantique.eu

ID Quantique Europe GmbH
Am Europlatz 2
1120 Vienna, Austria

thomas.laenger
@idquantique.eu