Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Certification of QKD-Devices

Workshop: Standardisation and certification of QKD systems and QKD networks

Dr. Manfred Lochter, BSI

28. September 2021

BSI

as the federal cyber security authority

shapes information security in digitization

through prevention, detection and reaction

for

government, business and society.

Overview

Introduction
The ETSI/BSI-PP
What is missing?
A Certification Ecosystem
Approval

Introduction

The participating member states Plan to work together to establish a cooperation framework – EuroQCI – for exploring within the next 12 months, the possibility of developing and deploying in the Union, within the next 10 years, a ***certified*** *secure end-to-end quantum communication infrastructure (QCI) composed of space-based and terrestrial-based solutions, enabling information and data to be transmitted and stored* ***ultra-securely*** *and capable of linking critical public communication assets all over the Union.*

(QCI Declaration)

The absence of certified and authorised devices and certification criteria, and the fact that early commercial products were compromised quite quickly, means that we are still in the phase of experimentation rather than application in concrete use-cases. The fact that no QKD solutions have received a security accreditation is an evidence of the low maturity of QKD implementation robustness.
Rebuttal: this is the subject of ongoing work by ETSI and BSI. The QCI project will be a driver for this.

(European Quantum Communication Infrastructure - JRC Report 3.7)

IT-Sicherheit durch Quantentechnologie gewährleisten

Woran lassen wir uns messen?
Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

Im Bereich des Quantencomputing stehen bis 2025 Rechner mit mindestens 100 Qubits auf der Basis souveräner Technologie aus Deutschland und Europa bereit und stehen für Anwendungsuntersuchungen aus dem Sicherheitsbereich zur Verfügung.

Im Hochsicherheitsbereich hat der Wechsel zu quantensicherer Kryptografie begonnen.

In Staat, Wirtschaft und Gesellschaft ist die Dringlichkeit des Wechsels zu quantensichererer Kryptografie akzeptiert und in kritischen Bereichen eingeleitet. Pilot-Infrastrukturen binden Partner aus den verschiedenen Bereichen ein.

Technologien und Lösungen der Quantenkommunikation von Anbietern aus Deutschland und Europa stehen für Staat, Wirtschaft und Gesellschaft zur Verfügung.

Die Studie zur Realisierbarkeit von Quantencomputern wird fortgeführt und aktualisiert.

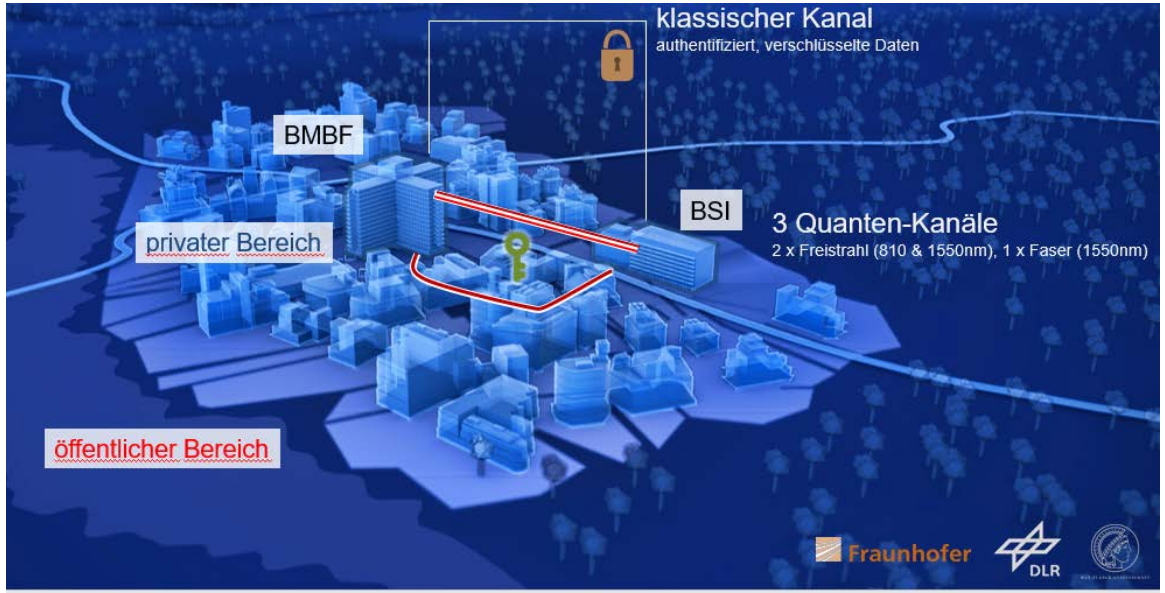
IT-Sicherheit durch Quantentechnologie gewährleisten

Wichtige Voraussetzung für den Einsatz von Quantum Key Distribution(QKD)in hochsicheren Netzen ist die zertifizierbare Sicherheit von Produkten. Hierzu entwickelt die Bundesregierung ein Protection Profile gemäß Common Criteria, begleitet die Erstellung zusätzlich benötigter technischer Angaben durch Studien und erforscht **quantitative und qualitative Aspekte der vorliegenden Sicherheitsbeweise.**

Der mögliche Sicherheitsgewinn durch QKD wird nicht nur in Forschungsprototypen, sondern auch im realen Einsatz demonstriert, um die Praxistauglichkeit zu demonstrieren

Cybersicherheitsstrategie für Deutschland 2021

QuNET-Demonstration



MAX PLANCK INSTITUTE
FOR THE SCIENCE OF LIGHT

NEWS & EVENTS DIVISIONS RESEARCH AT M

HOME | NEWS & EVENTS | NEWS FROM THE INSTITUTE | **NEWS-DETAIL**

First quantum-secured video conference between two federal agencies

10.08.2021

Initiative QuNET demonstrates highly secure and practical quantum communication

Photo: BMBF

Photo: Fraunhofer IOF

Today, two German federal authorities communicated via video for the first time in a quantum-secure manner. The QuNET project, an initiative funded by the German Federal Ministry of Education and Research (BMBF) to develop highly secure communication systems, is thus demonstrating how data sovereignty can be guaranteed in the future. This technology will not only be important for governments and public authorities but also to protect everyday data.

It was a foretaste of the communication of the future - or rather, the "data security" of the future. Because when Federal Research Minister Anja Karliczek invited members of the Federal Office for Information Security (BSI) to a video conference today, everything looked the same, at least for outsiders. Together with Andreas Könen, Head of Department CI "Cyber and IT Security" at the Federal Ministry of the Interior, Building and Community (BMI) and BSI Vice President Dr. Gerhard Schabhüser, the minister talked via video stream.

The ETSI/BSI-Protection Profile

- Limited Scope: P&M QKD; Point-to-Point
- Goal: EAL4+AVA_VAN_5+ALC_DVS.2

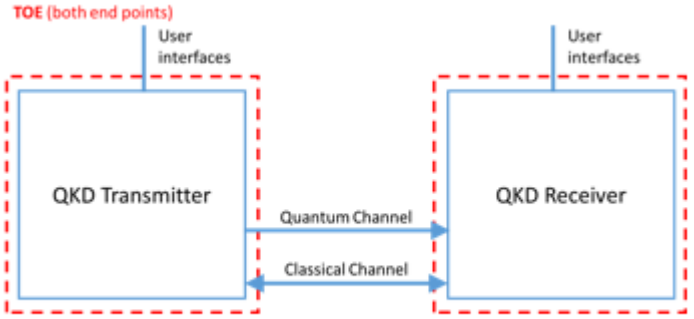


Figure 1: The TOE-boundary, i.e. the two QKD modules

- PP should be complete this autumn
- Very good industry participation
- Help from NICT
- Discussions helped to create a better understanding between communities
- Introduces packages
- Options to address national policies, e.g. on randomisation, or environment
- Goal: Internationally recommended PP
- Parallel activities by ISO
- **PP needs to be certified**

Central Part: FCS_QKD

Security in Quantum Cryptography

Christopher Portmann*

Department of Computer Science,
ETH Zurich, 8092 Zurich,
Switzerland

Renato Renner†

Institute for Theoretical Physics,
ETH Zurich, 8093 Zurich,
Switzerland

(Dated: February 2, 2021)

Quantum cryptography exploits principles of quantum physics for the secure processing of information. A prominent example is secure communication, i.e., the task of transmitting confidential messages from one location to another. The cryptographic requirement here is that the transmitted messages remain inaccessible to anyone other than the designated recipients, even if the communication channel is untrusted. In classical cryptography, this can usually only be guaranteed under computational hardness assumptions, e.g., that factoring large integers is infeasible. In contrast, the security of quantum cryptography relies entirely on the laws of quantum mechanics. Here we review this physical notion of security, focusing on quantum key distribution and secure communication.

Scientific review needed!

5 Extended component definition

5.1 Quantum Key Distribution (FCS_QKD)

This section describes the security functional requirements for the generation of QKD keys, which may be used as secrets for cryptographic purposes. The IT security functional requirements for a TOE are defined in an additional family Quantum Key Distribution (FCS_QKD) of the Class FCS (Cryptographic support).

Family Behaviour

Quantum Key Distribution relates to two or more end points (modules) establishing a confidential, shared, random bit string. It uses a communication channel carrying quantum states, which by quantum physical principles cannot be eavesdropped on without introducing anomalies with high probability. The establishment is achieved using a protocol that limits the joint probability that the protocol does not abort and that

- any entity outside the modules has gained knowledge about the bit strings, or
- the shared bit strings are not identical in both modules, or
- the distribution of bit strings has statistical properties different from uniform distribution

to a well defined value. This value is called the security parameter of the quantum key distribution protocol.

Component levelling:

FCS_QKD: Quantum Key Distribution	1

FCS_QKD.1 Prepare and Measure Quantum Key Distribution requires quantum key distribution in between two modules to be established using a Prepare and Measure protocol including information reconciliation and privacy amplification. The actual protocols and the algorithms for their application shall be chosen in accordance with the underlying security proof to support the claimed value of the security parameter. The SFR depends on local random numbers to choose physical and cryptographic protocol parameters, and to randomly partition measurement data into private and public data. The SFR furthermore depends on an authenticated classical communication channel.

Management: FCS_QKD.1

There are no management activities foreseen.

What‘s missing? The Ecosytem!

- A Technical Domain: Impact of the CSA?
- CSA-Level „High“
- Industry Working Groups necessary
- Accompanying documentation (e.g. on Sidechannels)
- Security proofs (study planned)
- Standards for Protocols/Interfaces
- Standards for the use of QKD keys
- Distribution of authentication keys (PQ-PKI?)
- OTP or AES?
- Which networks?

For assurance level ‘substantial’, the evaluation, in addition to the requirements for assurance level ‘basic’, should be guided at least by the verification of the compliance of the security functionalities of the ICT product, ICT service or ICT process with its technical documentation.

for assurance level ‘high’, the evaluation, in addition to the requirements for assurance level ‘substantial’, should be guided at least by an efficiency testing which assesses the resistance of the security functionalities of ICT product, ICT service or ICT process against elaborate cyberattacks performed by persons who have significant skills and resources.

Use of QKD?

BSI‘s position: QKD only in hybrid solutions as optional additional input. Hybrid solutions support End-to-End security
Encryption: AES (Additional use of the OTP possible)
Management of Authentication Keys has to be solved? PKI and ITS?
Availability of certified Products?
Integration in existing infrastructures?

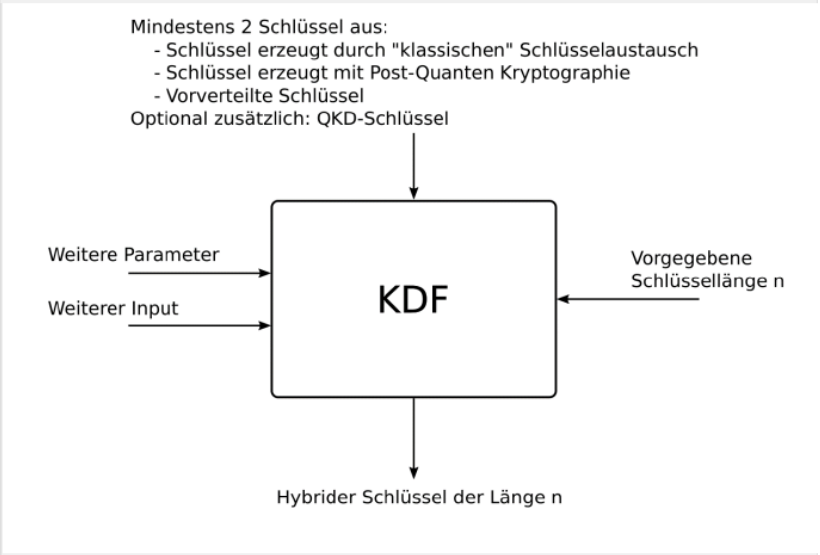


Abbildung: Schematische Darstellung der hybriden Schlüsseleinigung mittels einer Key Derivation Funktion (KDF)

For government use Certification is often not sufficient. There may be additional requirements, not only on the product itself, but also on its lifecycle and origin.

Protection of Classified Data and next steps

- For the protection of classified data additional requirements hold
- Evaluation according to EU Rules necessary
- Origin of products; Lifecycle
- Evaluations with the goal to approve a product can be based on CC evaluations
- The EU Council should be involved in an early stage of EuroQCI
- Additional requirements may hold, e.g. the use of hybrid modes

Next steps?

- Additional packages?
- Entanglement based QKD
- Security proofs
- Protocol Standards
- KMGT
- **Urgency** if timeline shall be met
- **Funding** of the certification of the PP