# Current Standardisation Landscape and existing Gaps in the Area of Quantum Key Distribution

Marius Loeffler, Christian Goroncy (DIN - Deutsches Institut für Normung e. V.)
Thomas Länger, Andreas Poppe (Austrian Institute of Technology)
Alexander Neumann (Deutsche Telekom AG),
Matthieu Legré (ID Quantique)
Imran Khan (Max Planck Institute for the Science of Light)
Christopher Chunnilall (National Physical Laboratory)
Diego López (Telefonica)
Marco Lucamarini, Andrew Shields, Elisabetta Spigone, Martin Ward (Toshiba Europe Ltd.)
Vicente Martin (Universidad Politecnica de Madrid)

## European Horizon 2020 Project "OPENQKD"

This document is based on a deliverable of the "Standardisation and Certification Work Package" of the European Horizon 2020 Project "OPENQKD" (grant agreement No 857156, project duration Sept. 2019 - Feb. 2023, online: https://openqkd.eu). The OPENQKD project consortium consists of 38 organisations (12 academia, 7 industry-oriented research institutes, 2 non-profit authorities and national measurement institutes, 5 SMEs, and 12 large enterprises, mostly telecom and datacom network equipment providers).

The mission of the OPENQKD project is the establishment of QKD-based secure communication as a well-accepted, robust and reliable technology instrumental for securing traditional industries and vertical application sectors, and to prepare the deployment of a Europe-wide QKD-based infrastructure in future. To this goal OPENQKD will establish a European, QKD-enabled experimentation platform and demonstrate in up to 39 use cases that QKD can, together with other cryptographic technologies, fill the needs of a secure European communication infrastructure.

The work described in this document has been conducted within the OPENQKD project. This document reflects only the OPENQKD Consortium view and the European Union is not responsible for any use that may be made of the information it contains.

## Legal disclaimer

Version 1 (December 2020)

## Executive Summary

**The Quantum Flagship.** The Quantum Technology FET (Future and Emerging Technologies) Flagship Programme of the European Commission is a €1 bn investment in quantum technology (QT) research and innovation. Its goals include:

- Consolidating and expanding European leadership and excellence in QT research;
- Kick-starting a competitive European QT industry;
- Generating opportunities for innovative businesses and investments in QTs;
- Creating radically improved solutions across many domains (including energy, health, security, and the environment) for the benefit of society and the individual.

**Importance of Standards.** The development of industrial standards is essential for supporting the strategic goals of the Quantum Flagship. Standards promote the interoperability of equipment from different vendors, for example, allowing QT products to be integrated into telecom networks. They foster the creation of a supply chain by defining interfaces and specifications for components and modules within equipment or distributed systems.

Standards and certification safeguard that QT products are fit for purpose and of benefit to the user and society. For example, they can ensure that quantum-based information security products are implemented correctly and are free of design flaws and loopholes. They can allow QT products to be certified “secure” by an independent third-party test laboratories. Standards are driven by product vendors and users, but they also play an important role in shaping the research landscape by highlighting the challenges requiring concerted research and development efforts. Due to the open and transparent processes within standards development, the requests of the user are being properly addressed, preventing wrong investments in research and development without future demands.

**Standards Developing Organisations.** ETSI was the standards developing organisation (SDO) starting QKD standardisation in 2008. The ETSI Industry Specification Group for Quantum Key Distribution (ISG-QKD) was born from the QT community established by the European FP6 project, SECOQC. To date it has produced 14 Group Specifications and Reports in areas such as protocol security, implementation security, component and module characterisation, key delivery, and use cases. The ISG-QKD has also been an important forum in the QT community, helping to shape recent research and innovation projects, such as OPENQKD.

The emergence of commercial-grade products for QKD and Quantum Random Number Generation, and their uptake by early adopters in the past few years has produced a surge in interest in QT standards. Membership of the ETSI ISG has swelled to include equipment vendors, telecom operators, end users, national metrology institutes and leading security researchers and the pace of development has increased. In parallel, and to a large extent in competition, several other SDOs have established initiatives in QT, including CEN/CENELEC, ISO/IEC, IEEE and ITU-T. The activities of these groups and others are discussed in detail in this document.

**Increasing Activity.** The increasing activity in QKD standardisation worldwide (with 22 published standards and 20 documents under development) is an indicator of both increased maturity and a strong interest in the practical application and commercialisation of the technology. QKD standards have been mainly developed in three areas: basic definitions (ontology, use cases), security specifications and evaluation, and interoperability.

**Gaps.** Despite the progress, gaps remain in many fields where standards already exist, or are under development:

- In the field of security certification of QKD modules, dedicated activities covering almost the entire chain from security specification to evaluation methodology is currently under development in ISO and ETSI, with practically applicable standards expected in early 2022. OPENQKD has specific activities to drive and support the establishment of the evaluation and certification processes, including involving commercial evaluation laboratories and national certification authorities to strengthen a positive outlook in this area.

- In addition, guidance for the specification and evaluation of particular QKD components, e.g. QKD transmitter and receiver modules, needs to be provided – this gap is also addressed within the OPENQKD project where project documents will be provided to inform these work items, and respective standardisation activities shall be initiated.
- In the field of QKD networking, gaps exist on two levels: on the level of network interoperability (QKD integration into existing fibre infrastructures, key delivery interfaces, network control, integration of QKD generated keys with cryptographic solutions), and on the level of security certification of networks. Gaps on the networking level are being addressed in ETSI, gaps about the security in networks also have started at ITU-T, but the importance of QKD network standards is widely recognised and further activities by other SDOs can reasonably be expected.
- In the field of satellite modules and networks, early developments are underway but no applicable component and interoperability standards, e.g. for the optical ground receiver, or the satellite optical terminal are available. Standards for the interoperability of space networks and fibre-bound ground networks also still need to be addressed.

**Standardisation Roadmap**. OPENQKD proposes a roadmap, in alignment with the Strategic Research Agenda of the Quantum Flagship[1], to prioritise standards developing activities, as well as supporting activities, addressing the identified gaps according to their urgency.

- In the field of security standards, a further involvement of evaluation laboratories and certification bodies, potentially in the form of a funded project, would support and speed up the achievement of this goal. The development of standards for more QKD components is already addressed on several levels and needs to be supported in the short term. Standards for new quantum protocols, as well as for technologically advanced components, e.g. the quantum repeater, need to be defined in the medium term.
- In fibre network interoperability of QKD systems, further coordination and structured activity are required to achieve the necessary standards for network interoperability. Standards for the full quantum internet need to be defined in the medium term to support the development of the European Quantum Communication Infrastructure (QCI).
- Standards for satellite QKD, specifically for the QKD ground segment and the space segment (component and interoperability standards), as well as interoperability standards between space networks and ground networks need to be defined in the medium term.

**Coordination**. To optimise the positive impact of QT standardisation for research and industry, a dedicated monitoring and coordinating body needs to be set up. Such a body may identify and monitor existing or developing gaps as well as other needs and opportunities in standardisation, and coordinate actions among standards developing organisations. Given the breadth of standards activities in the QT domain, this monitoring body should be independent to be most effective and to be able to co-ordinate activities across the whole spectrum of SDOs.

[1] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=65402

# Table of Contents

# 1. Introduction

The purpose of this document is to provide an overview of the current standardisation landscape in the field of Quantum Key Distribution (QKD) and identify potential gaps that need to be filled by future work in QKD standardisation.

These gaps need to be addressed by various stakeholders. Standard Developing Organisations (SDOs) should harmonise their work on QKD, thus avoiding repetitions or contradictions in standards published by different organisations. Industry entities need to improve their awareness of the ongoing standardisation processes in the field of QKD. Researchers in the field of QKD will gain specific insights from the presented gap analysis to direct their effort to where it is needed most. To strengthen the European role in the QKD world, policy members should proactively address the needs and gaps identified in this report by providing resources, e.g. via harmonized QKD standards. These standards are in then accordance to European values and strengthen the European market and stakeholders. International standards based on European ones provide European stakeholders advantages in the international market and avoid cost for adaption if standards adaption goes in the opposite direction.

This document is structured as follows: A short introduction is followed by an overview of current activities in QKD standardisation on national, European, and international levels (Section 2). Section 3 lists all currently available QKD standards (22 published, 20 under development) and potential standardisation gaps grouped into four main categories. Section 4 points out the strategic importance of quantum technologies standardisation in general, and of a well-conceived and well-executed European quantum standards coordination in particular. It also presents a detailed strategic standardisation roadmap spanning the next decade until 2030. In this roadmap, areas for European research policy to potentially apply leverage in support of the goals of the Quantum Flagship initiative of the European Commission are identified.

# 2. Overview of activities in QKD standardisation

## 2.1. General

In order to provide an overview of existing standards and identify existing gaps in the QKD standardisation landscape, current national, European and international standardisation activities need to be considered.

Generally speaking, a standard is a consensus-based document, which is approved by a recognised standardisation body or standards developing organisation (SDO). A standard may provide rules, guidelines, or characteristics of activities or their results, reflecting a current state-of-the-art. A standard should be based on the consolidated results of science, technology and experience, aiming at the promotion of the optimum benefits of the whole community.

## 2.2. Standardisation landscape

### 2.2.1. National standardisation

At the national level, each country has its own national standardisation bodie(s). Examples of national standardisation bodies are the British Standards Institute (BSI), the German Institute for Standardization (DIN), Royal Netherlands Standardization Institute (NEN), and the French Standardisation Association (AFNOR). Each National Standardisation Body in Europe develops national standards as long as there is no existing European standard (EN) on a particular scope.

There are also specific cybersecurity authorities at the national level in Europe like in Germany, the Bundesamt für Sicherheit in der Informationstechnik (BSI, Federal Office for Information Security). The BSI is in charge of providing IT and communication security for the German government, as well as consulting services for small- and medium-sized enterprises (SME). The BSI is also Germany's certification authority for security certifications, and responsible for the accreditation of security test laboratories. BSI is also aware of the relevance of (post) quantum cryptography (e.g. explained within the report BSI TR 021012, *Cryptographic methods: Recommendations and key lengths*[2]).

The US standardisation landscape differs from the European approach, but should be considered in the context of security standardisation. Different standardisation organisations promote the development of standards in the US. The most relevant one is ANSI, the American National Standards Institute, which oversees the development of voluntary consensus standards in the US and coordinates the international standardisation work of the USA. It works as a kind of umbrella organisation by coordinating 270 standards developing organisations, such as Un-

[2] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile&v=10

derwriter Laboratories (UL), the American Society of Mechanical Engineers (ASME), the International Institute of Electrical and Electronics Engineers Standards Association (IEEE SA), or the American Society for Testing and Material (ASTM). In addition, NIST, the National Institute of Standards and Technology, a physical sciences laboratory and a non-regulatory agency of the United States Department of Commerce, contributes to American standardisation. NIST's Federal Information Processing Standards (FIPS) s are widely used beyond their intended use for US American government agencies, and even inspired an ETSI standard for the security of QKD modules. The **NIST Cryptographic Technology (CT) Group**[3] conducts research, develops, engineers, and produces guidelines, recommendations and best practices for cryptographic algorithms, methods, and protocols. It is active in the field of cryptographic mechanisms, addressing topics such as hash algorithms, symmetric and asymmetric cryptographic techniques, cryptographic key management, authentication, and random number generation. Users can take advantage of the availability of secure applications in the marketplace made possible by the appropriate use of standardised, high quality cryptography.

In Japan, the **Cryptographic Research and Evaluation Committee (CRYPTREC)** evaluates and recommends cryptographic algorithms for use in government and industry and will thus be responsible for the assessment of QKD. Governmental and other future users request guidelines, national standards, and certifications from such organizations before a rollout of QKD technology. CRYPTREC will be supported by the Japanese **National Institute of Information and Communications Technology (NICT)**, specifically its **Quantum ICT Advanced Development Center**. NICT has a leading role in international standardisation and working in the ITU-T study group 13 “Future Networks” for standardisation of QKD network structure and architecture and ITU-T study group 17 “Security” where standardisation of QKD network with its security aspects are ongoing. NICT is also working in the ITU-T focus group on Quantum Information Technology for Networks (FG-QIT4N) for general discussions on quantum information technology, and in ISO/IEC JTC (Joint Technical Group) 1/SC27 “Information security, cybersecurity and privacy protection” for security requirements, test and evaluation methods of QKD.

### 2.2.2. European standardisation

European standardisation is a widely accepted tool to lower trade barriers. It provides harmonised standards that are reliable indicators of conformity with relevant EU legislation. In this context, the “New Approach” (explained below) based on an EU Council resolution was introduced in 1985 to fulfil the technical harmonisation and standardisation needs and since then, it changed the European standardisation landscape. As a result, nowadays about 80 % of the published standards have European or international origin.

At the European level, following an European Commission (EC) information directive, standardisation work is carried out by the European Committee for Standardisation (CEN),[4] the European Committee for Electrotechnical Standardisation (CENELEC)[5] and ETSI[6], which is rec-

[3] https://csrc.nist.gov/Groups/Computer-Security-Division/Cryptographic-Technology

[4] www.cen.eu

[5] www.cenelec.eu/

ognised as an European Standards Organisation dealing with telecommunication, broadcasting and other electronic communication networks and services. The European standardisation organisations CEN and CENELEC are liable under Belgian law, while ETSI is organised according to French law.

Members of CEN and CENELEC are the national standards organisations of EU and EFTA member states, and the national standards organisations of other countries intending to become members of the EU or EFTA. In August 1982, CEN and CENELEC released a cooperation agreement where they declared themselves joint European standardisation organisations. Their main responsibility lies in the harmonisation of existing European standards. CEN/CENELEC organs such as the General Assembly, Administrative and Technical Boards and Technical Committees are open to all members, and include national delegations presenting agreed positions. A **CEN-CENELEC Focus Group on Quantum Technologies (FGQT)**[7] has been established with more than 150 participants from all over Europe. Its objective is to gather relevant stakeholders interested in standardization in the field of Quantum Technologies (QT), ensure interaction among them, map ongoing activities, define needs and opportunities and recommend further action to ensure that standards support the deployment of QT in industry. This group has relevant contributions from the European Quantum Flagship initiative.

The vast majority of more than 800 members of ETSI is affiliated to companies, research institutions and telecom service providers as well as other organisations from Europe and other parts of the world. In 1987, ETSI was created from the standardisation activities of the European Conference of Postal and Telecommunications Administrations and its members are international stakeholders from industry, organisations and government. The **ETSI ISG-QKD**[8] (Industry Specification Group on Quantum Key Distribution for Users) shall bring together the important European actors from science, industry, and commence to address standardisation issues in quantum cryptography, and quantum technology in general including many of the OPENQKD partners, who are active contributors. Nevertheless, the ISG-QKD has members from all over the world (e.g. Japanese NICT). The **ETSI TC CYBER WG QSC**[9] (Technical Committee Cyber Security Working Group for Quantum-Safe Cryptography), former ETSI ISG QSC (Industry Specification Group on Quantum-Safe Cryptography), aims to assess and make recommendations for quantum-safe cryptographic primitives and protocols, taking into consideration both the current state of academic cryptology and quantum algorithm research, as well as industrial requirements for real-world deployment. The ETSI ISG QSC sought to standardise the relevant algorithms, primitives, and risk management practices as needed to seamlessly preserve our global information security infrastructure.

At the European level, different types of standardisation documents are available – each one of these is representing a different level of consensus. The European Standard (EN) aims at developing a normative specification reflecting the current state of a technology and/or

[6] www.etsi.org/

[7] www.cencenelec.eu/standards/Topics/QuantumTechnologies/Pages/default.aspx

[8] https://www.etsi.org/technologies/quantum-key-distribution

[9] https://www.etsi.org/technologies/quantum-safe-cryptography

knowledge. If a national standard is in conflict with, or a duplicate of an EN standard, it shall be withdrawn. One special type of EN is the mandated (harmonised) EN, which is applied in the context of the New Legislative Framework (a.k.a. New Approach) and developed on the basis of a mandate from the European Commission to set out the essential requirements for the product or service that are specified in an EC Directive. These essential requirements deal in particular with health and safety of users, as well as other fundamental matters. A Conformité Européenne (CE) marking is placed on products that comply with essential requirements of EU directives on those products. Each user of a marked product can assume that essential requirements (requested by public regulation) are fulfilled.

Other products of European standardisation include:

- European Technical Specifications (CEN/TS, CENELEC/TS or ETSI TS), which aim to aid market development and growth for products or methods still under development and/or in trial phase;
- European Technical Reports (CEN/TR, CENELEC/TR or ETSI TR) are informative documents providing recommendations, explanations, and/or information on the technical content of standardisation work. TRs may be prepared when it is considered urgent or advisable to provide additional information to CEN-CENELEC members, the European Commission, the EFTA Secretariat, or other governmental agencies or outside bodies.

Certain specifications, which are developed with the rapid consensus of expert stakeholders (no full consensus is needed), can be found in CEN/CENELEC Workshop Agreements (CWA), ETSI Group Specifications (GS) and Group Reports (GR). The latter two being regular products of ETSI Industry Specification Groups, like e.g. the ETSI ISG-QKD (ETSI Industry Specification Group on Quantum Key Distribution). All document types differ in their development procedures and binding forces.

### 2.2.3. International standardisation

The International Organization for Standardization (ISO)[10] as well as the International Electrotechnical Commission (IEC)[11] are standardisation organisations operating at a global level. When describing the international standardisation landscape, the Vienna and Dresden Agreements need to be detailed. Those agreements between CEN and ISO (Vienna agreement) as well as between CENELEC and IEC (Dresden agreement), aim at carrying out specialist work at one level of standardisation, and use parallel voting procedures to achieve simultaneous adoption of international standards (ISO/IEC) on European level (EN standards) and vice versa.

ISO members are national standardisation organisations from all over the world that set up their national mirror committees of the ISO committees they attend. Each participating national body has one vote in a specific ISO committee, but the goal is to reach a unanimous consensus in all decisions related to standardisation. The national bodies commit themselves to adopt

[10] www.iso.org

[11] www.iec.ch

ISO standards unchanged as national standards and to develop deviating standards only when there are no suitable ISO Standards that can be adopted nationally. In the case of IEC, similar agreements apply. **ISO/IEC JTC 1/SC 27**[12] "IT Security" is the Sub-Committee 27 of the Joint Technical Committee 1 of ISO and IEC. The SC 27 develops standards for IT security, cybersecurity and privacy protection. The QKD work items are part of working group WG3 "Security evaluation, testing and specification", which also develops and maintains the ISO/IEC 15408 *Common Criteria for Information Technology Security Evaluation* (CC) standard itself. The two QKD security evaluation standards currently being developed in WG3, ISO/IEC 23837-1 and 2 both are "applications" of the Common Criteria paradigm to QKD.

The United Nations specialised agency in terms of information and telecommunication technologies is the International Telecommunications Union (ITU). **ITU-T/SG 13**[13] "Future Networks" dealing with next-generation networks and their evolution, while focusing on future networks and network aspects of mobile telecommunications and their QKD related work items prefixed with "ITU-T Y.QKDN". **ITU-T/SG 17**[14] "Security" coordinates security-related work across all ITU-T Study Groups and their QKD related work items prefixed with "ITU-T TR" and "ITU-T X". **ITU-T FG-QIT4N**[15] (Focus Group on Quantum Information Technology for Networks) was established in September 2019 to tackle pre-standardisation issues of quantum information technology for networks. Partners from OPENQKD have taken a leading role in the FG-QIT4N, including the coordination of a work package and being lead editors of D2.2 "Technical report on the QIT4N use case part 2: Quantum Key Distribution Network". ISO, IEC and ITU established the WSC - The World Standards Cooperation[16] in 2001, in order to strengthen and advance their voluntary consensus-based international standards systems.

The Internet Engineering Task Force (IETF)[17] and the Internet Research Task Force (IRTF)[18] play another important role. The IRTF focuses on longer term research issues related to the Internet, while the parallel organisation, the IETF, focuses on the medium term issues of engineering and standards making. The IETF is a non-profit organisation, in which mostly industry consortia are organised. It develops and promotes non-mandatory standards and all work is carried out voluntarily. The **Quantum Internet Research Group (QIRG)**[19] has focused on general architecture principles for a future Quantum Internet and it is generating high interest within the IETF/IRTF community. The **Crypto Forum Research Group (CFRG)**[20] within IRTF is a general forum for discussing and reviewing uses of cryptographic mechanisms, both for

[12] www.iso.org/committee/45306.html

[13] https://www.itu.int/en/ITU-T/about/groups/Pages/sg13.aspx

[14] https://www.itu.int/en/ITU-T/about/groups/Pages/sg17.aspx

[15] https://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/default.aspx

[16] https://www.worldstandardscooperation.org

[17] https://www.ietf.org

[18] https://irtf.org

[19] https://irtf.org/qirg

[20] https://irtf.org/cfrg

network security in general and for the IETF in particular. They are aware of, but not focused on, QKD at present.

In addition, the US based standards organisation IEEE SA established the international group **IEEE SA QuantumComm** – Software-Defined Quantum Communication (P1913)[21] in March 2016 with activities up to December 2020 with the purpose to define a classical interface to quantum communication devices that permits these devices to be reconfigured to implement a variety of protocols and measurements.

The GSMA (Groupe Speciale Mobile Association) represents the interests of the more than 750 mobile operators and almost 400 companies worldwide in the broader mobile ecosystem, including device makers and handset as well as software companies, equipment providers, internet companies and adjacent industry sectors. The **GSMA Internet Group**[22] has started an activity on the analysis of threats, challenges and business opportunities brought by quantum technologies on telecommunication networks and service infrastructures. While the GSMA is not strictly speaking as a standardisation group, its influence as pre-standardisation forum in the telco industry is extremely relevant.

[21] https://standards.ieee.org/project/1913.html

[22] https://www.gsma.com/aboutus/workinggroups/internet-group-3

# 3. Overview of the standardisation landscape in QKD: existing standards, ongoing activities and gaps in QKD

Despite the fact that QKD is a very innovative topic and still a lot of work is done in research, several standardisation documents exist already, addressing different areas of QKD. The following part will provide an overview of existing standards, standards under development and potential gaps. In the beginning of each part an overview of existing standards in that area is given, where existing standards are reported in black and draft standards in grey. The complete list of the documents can be found in the annex. For the identification of gaps and the presentation of a strategic roadmap towards filling these gaps, QKD standards and related specifications are put in categories according to topical similarities: "Quantum communications module security", "Fibre network interoperability", "Quantum network security", and a fourth group "Other standards". The strategic roadmap for QKD standardisation (see next section) introduces the additional category "Satellite modules and networks". Currently, there are no standards available for satellite QKD – and only very rudimentary activities to develop such standards.

## 3.1. Quantum communications module security

In the following subsections, standardisation documents related to QKD components and modules are discussed, gaps identified, and actions proposed.

### 3.1.1. Overview of standards in quantum communications module security

Table 1 provides an overview of existing standards and standards under development in the area of in quantum communications module security.

**Table 1: Standards in quantum communications module security**

| SDO | Document number | Document title | Version | publ. date |
|---|---|---|---|---|
| ETSI | GR QKD 003 | Quantum Key Distribution (QKD); Components and Internal Interfaces | V2.1.1 | 2018-03 |
| ETSI | GR QSC 004 | Quantum-Safe Cryptography; Quantum-Safe threat assessment | V1.1.1 | 2017-03 |
| ETSI | GS QKD 005 | Quantum Key Distribution (QKD); Security Proofs | V1.1.1 | 2010-12 |
| ETSI | GS QKD 005 | Quantum Key Distribution (QKD); Security Proofs | V2.1.1 | *Drafting* |
| ETSI | GS QKD 008 | Quantum Key Distribution (QKD); QKD Module Security Specification | V1.1.1 | 2010-12 |
| ETSI | GS QKD 010 | Quantum Key Distribution (QKD); Implementation security: Protection against trojan horse attacks in one-way QKD systems | V.1.1.1 | *Drafting* |

| | | | | |
|---|---|---|---|---|
| ETSI | GS QKD 011 | Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems | V1.1.1 | 2016-05 |
| ETSI | GS QKD 012 | Quantum Key Distribution (QKD); Device and Communication Channel Parameters for QKD Deployment | V1.1.1 | 2019-02 |
| ETSI | GS QKD 013 | Quantum Key Distribution (QKD); Characterisation of optical output of QKD transmitter modules | V1.1.1 | *Drafting* |
| ETSI | GS QKD 016 | Quantum Key Distribution (QKD); Protection Profile (PP) | V.1.1.1 | *Drafting* |
| ETSI | GR QKD 019 | Quantum Key Distribution (QKD); Design of QKD interfaces with Authentication | | *Drafting* |
| ISO/IEC | 23837-1 | Information security – Security requirements, test and evaluation methods for quantum key distribution – Part 1: requirements | | *Drafting* |
| ISO/IEC | 23837-2 | Information security – Security requirements, test and evaluation methods for quantum key distribution – Part 2: test and evaluation methods | | *Drafting* |

### 3.1.2. Gaps in QKD protocols

In general, current hardware-focused documents address prepare-and-measure phase-encoded fibre BB84 systems as well as CV-QKD systems. BB84 is a QKD protocol developed by Charles Bennet and Gilles Brassard in 1984, while one of the main protocols for CV-QKD was introduced by Grosshans and Grangier in 2020. Many systems will use the COW (Coherent One-Way QKD) protocol and some next-generation ones employ the CV-QKD QPSK protocol. ETSI GR QKD 003 *Quantum Key Distribution (QKD); Components and Internal Interfaces* describes this and other protocols. The COW protocol requires revisions or supplements to a few existing standards.

Other protocols, for which complete security proofs may potentially be achieved, are currently subject of research. These will generate additional requirements once they have become industrially significant. It is not possible to define a set of approved protocols and at the same time keep the door open to include new developments.

### 3.1.3. Gaps in QKD components

An existing document specifying standardised measurement procedures for characterising QKD components is ETSI GS QKD 011 *Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems*. This standard needs to be revised or supplemented to address some of the newer components identified in ETSI GR QKD 003 *Quantum Key Distribution (QKD); Components and Internal Interfaces*. Newer components are expected in relation to other QKD protocols and their implementation in several areas, for instance fibre, satellite, entanglement, or general free-space QKD. Additionally, as the technology moves from implementations that use bulk optics and electronics to integrated photonics and electronics chips, components developed for telecom will be re-used for QKD with a variety of possible side-channels. There will be plenty of novel components with different realisations requiring standardised measurement procedures.

### 3.1.4. Gaps in QKD modules

Further gaps are identified with the ongoing efforts to standardise the methodology to assess and certify the implementation security of QKD modules. Both ISO and ETSI have ongoing activities in this area.

In ISO, the documents ISO/IEC 23837 Part 1 *Security requirements* and Part 2 *Test and evaluation methods* will be standards to facilitate the specification and evaluation of Common Criteria described in ISO/IEC 15408 *Protection Profiles and Security Targets.* Part 1 lists important aspects for the security specification of QKD modules and provides a set of standardised security functional requirements. Part 2 provides a specific evaluation method, including supplementary activities, for the evaluation of QKD module Protection Profiles (implementation independent specifications of specific types of QKD modules), as well as for the evaluation of actual module implementations against QKD module security targets. Once published, the ISO/IEC 23837 series will enable the evaluation and certification of QKD modules with recognition within the scope of the current Common Criteria Recognition Agreement (CCRA) and potentially also beyond[23].

The ETSI GS QKD 016 *Quantum Key Distribution (QKD); Protection Profile (PP*), will be an actual Protection Profile within the Common Criteria framework providing an implementation-independent specification of a QKD module, established by a commercial Common Criteria evaluation labarotory and thus very near to actual real-world evaluation and certification. It is reasonable to expect that the ETSI PP will make use of the preparatory documents from ISO described above. Additional requirements for the PP may be extracted from other supplementary documents describing the correct measurement procedures to be applied to QKD systems for the evaluation of their practical security.

The currently drafted ETSI GS QKD 013 *Quantum Key Distribution (QKD); Characterisation of optical output of QKD transmitter modules* intends to specify measurement procedures for characterising specific properties of the optical output of QKD transmitter modules, without having access to the internal components of the modules, while draft ETSI GS QKD 010 intends to describe protection for QKD systems against Trojan horse attacks launched against

[23] The amended CCRA from 2014 (https://www.commoncriteriaportal.org/files/CCRA - July 2, 2014 – Ratified September 8 2014.pdf, online: 1.3.2020) assures automatic recognition among its 26 signatories only for Evaluation Assurance Level 2 (EAL2). Recognition for higher EALs, as they likely will be provided for QKD modules, will be specifically addressed by local regulatory authorities, which may require additional assurance.

the components that encode or decode bit values and/or basis values and/or the intensities of signal, decoy and vacuum states on the quantum channel.

OPENQKD D9.3 and D9.4 are concerned with testing QKD transmitter modules, and they can inform the work of the above-mentioned ETSI Work Items. Furthermore, they will also identify which additional properties of the transmitted quantum states should be measured, as well as which additional countermeasures to hacking attacks should be tested. Therefore, work in OPENQKD is likely to both identify, and provide the expertise for drafting additional metrology and security standards.

A clear gap exists for an equivalent document to GS QKD 013, but addressing the properties of QKD receiver modules. OPENQKD D9.3 and D9.5 are concerned with testing QKD receiver modules, and this work will not only inform the drafting of the receiver equivalent to GS QKD 013, but is also likely to identify, and provide the expertise for drafting additional security and metrology standards, e.g. those concerned with testing countermeasures to specific hacking attacks on receiver modules.

## 3.2. Standards dealing with fibre network interoperability

Fibre network interoperability is about how the modules are used in the fibre network. It includes interoperability and many other aspects like routing and management of quantum keys.

### 3.2.1. Overview of standards in the area of fibre network interoperability

Table 2 provides an overview of existing standards and standards under development in the area of fibre network interoperability.

**Table 2: Standards in the area of fibre network interoperability**

| SDO | Document number | Document title | Version | publ. date |
|---|---|---|---|---|
| ETSI | GS QKD 004 | Quantum Key Distribution (QKD); Application Interface | V2.1.1 | 2020-08 |
| ETSI | GS QKD 014 | Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API | V1.1.1 | 2019-02 |
| ETSI | GS QKD 015 | Quantum Key Distribution (QKD); Quantum Key Distribution control interface for software defined Networks | (publication pending) | 2020-12 approved |
| ETSI | GS QKD 017 | Quantum Key Distribution (QKD); Network architectures | | *Drafting* |
| ETSI | GS QKD 018 | Quantum Key Distribution (QKD); Orchestration Interface of Software Defined Networks | | *Drafting* |
| ITU-T SG 13 | Y.3800<br>(ex Y.QKDN_FR, Corrigendum 1) | Overview on networks supporting quantum key distribution | | 2020-04 |
| ITU-T SG 13 | Y.3801<br>(ex Y.QKDN-req) | Functional requirements for quantum key distribution networks | | 2020-04 |

| | | | | |
|---|---|---|---|---|
| ITU-T SG 13 | Y.3802<br>(ex Y.QKDN_Arch) | Quantum key distribution networks – Functional architecture | | Approved |
| ITU-T SG 13 | Y.3803<br>(ex Y.QKDN_KM) | Quantum key distribution networks – Key management | | Approved |
| ITU-T SG 13 | Y.3804<br>(ex Y.QKDN_CM) | Quantum key distribution networks – Control and management | | Approved |
| ITU-T SG 13 | Y.QKDN_SDNC | Software Defined Network Control for Quantum Key Distribution Networks | | *Drafting* |
| ITU-T SG 13 | Y.QKDN_BM | Business role-based models in Quantum Key Distribution Network | | *Drafting* |
| ITU-T SG 13 | Y.QKDN_frint | Framework for integration of QKDN and secure network infrastructures | | *Drafting* |
| ITU-T SG 13 | Y.QKDN-qos-gen | General Aspects of QoS on the Quantum Key Distribution Network | | *Drafting* |
| ITU-T SG 13 | Y.QKDN-qos-req | Requirements for QoS Assurance of the Quantum Key Distribution Network | | *Drafting* |
| ITU-T SG 13 | Y.QKDN-qos-arc | Functional architecture of QoS assurance for quantum key distribution networks | | *Drafting* |
| ITU-T SG 13 | Y.QKDN-qos-ml-req | Requirements of machine learning based QoS assurance for quantum key distribution networks | | *Drafting* |

### 3.2.2. Gaps related to the performance

In the area of standards related to performance, there is need for a classification of the performance of QKD modules, which addresses, for instance, the budget loss, as it is currently assessed for Small Form Factor Pluggable Transceiver (SFP) modules. Depending on the channels used, whether optical fibres or free space, and on the conditions of the link, its noise and loss levels, the performance of QKD modules dramatically changes. Figures are needed to compare QKD modules from different manufacturers on a fair and common standardised basis.

### 3.2.3. Gaps regarding key delivery

Currently existing standards for key delivery interfaces (ETSI GS QKD 004 *Quantum Key Distribution (QKD); Application Interface* and ETSI GS QKD 014 *Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API)* will likely not be able to cover all the requirements e.g. security requirements on the Application Programming Interfaces (API) of existing and future applications in a QKD network. Therefore, gaps for new interfaces will likely open up in the future. In general, the requirements for key delivery APIs need to be defined for different use cases and at different layers of the network architectures. Moreover, standards in this area need to be benchmarked against these API requirements. If gaps are identified in the benchmarking process, additional key delivery APIs will require a modification of existing standards. In the case of major extensions, the new APIs need to be defined in a new standard.

### 3.2.4. Gaps regarding control network and management

In the area of control and management, software-defined networks (SDNs) will require the definition of a set of minimal information and control mechanisms that are made available to the network in order to steer the QKD modules present in a node (southbound interface of the SDN controller). ETSI GS QKD 015 *Quantum Key Distribution (QKD); Quantum Key Distribution control interface for software defined Networks* has been recently approved and ETSI GS QKD 018 *Quantum Key Distribution (QKD); Orchestration Interface of Software Defined Networks*, early draft stage, deals with these issues, but more will be needed. A similar interface would need to be devised for the connection of the controller to the local Key Management System (KMS), either through a local agent in the node (SDN agent) or directly to the SDN controller. Moreover, in the same area, but for traditional networks, a standard for a minimum set of control and management commands for QKD modules and KMSs is not available and needs to be developed. A comparable standard should describe a minimum set of log messages generated by the same entities. Finally, to address the multi domain/vendor cases, appropriate northbound interfaces of the SDN controller also need to be defined.

### 3.2.5. Gaps covering the interfaces

Part of the standardisation work is defining the different components that constitute the general architecture of a QKD network (e.g. GS QKD 017 *Quantum Key Distribution (QKD); Network architecture*s). Once these components are identified and their functionality clearly defined, the flow of information between them can be described and the corresponding interfaces can be specified. This is a crucial point as the interoperability of the different components (hardware and software) of a QKD network depend on it. In addition, a proper functional decomposition would allow for disaggregation, opening the market for an ecosystem of different providers that can be seamlessly integrated using open interfaces and protocols.

## 3.3. Standards dealing with quantum network security

### 3.3.1. Overview of standards in quantum network security

Standardisation in quantum networks security has only recently started, mainly by ITU-T, as it is shown in Table 3. However, this is a vast and rapidly evolving field and a large number of standards are expected in this area.

**Table 3: Standards in quantum network security**

| SDO | Document number | Document title | Version | publ. date |
|---|---|---|---|---|
| ETSI | GS QSC 003 | Quantum Safe Cryptography; Case Studies and Deployment Scenarios | V1.1.1 | 2017-02 |
| ITU-T SG 17 | XSTR-SEC-QKD | Security considerations for quantum key distribution networks | | 2020-03 |

| | | | | |
|---|---|---|---|---|
| ITU-T SG 17 | X.1710<br>(ex X.sec-QKDN-ov) | Security framework for quantum key distribution networks | | Approved |
| ITU-T SG 17 | X.1714<br>(ex X.cf-QKDN) | Key combination and confidential key supply for quantum key distribution networks | | Approved |
| ITU-T SG 17 | X.sec-QKDN-km | Security requirements for quantum key distribution networks - Key management | | *Drafting* |
| ITU-T SG 17 | X.sec-QKDN-tn | Security requirements for quantum key distribution networks -Trusted node | | *Drafting* |
| ITU-T SG 17 | X.sec_QKDN_intrq | Security requirements for integration of QKDN and secure network infrastructures | | *Drafting* |

The OPENQKD project intends to demonstrate up to 39 use-cases related to quantum networks and the EU is planning to deploy an entire quantum communication infrastructure in the near future (see Section 4.1). Standards are needed to establish secure key exchange at the nodes of the network and the key management rules within a node. More demand for standards can be expected when quantum networks will be deployed in the field.

### 3.3.2. Gaps in QKD networks security

A set of ITU SG17 recommendations is under development. Those recommendations, in particular ITU-T X.sec-QKDN-km *Security requirements for quantum key distribution networks - key management*, will describe the security of QKD networks in generic terms. The Common Criteria certification of key management systems based on ITS (Information Theoretic Security) cryptographic algorithms such as One Time Pad or Wegman-Carter authentication is not yet covered by a standard or a current project of a standards developing organisation.

### 3.3.3. Gaps dealing with the integration of QKD generated keys

The current vision to make the future IT infrastructure secure against attacks using quantum computers identifies QKD as key distribution primitive with information theoretic security, and Post Quantum Cryptography (PQC) algorithms for the actual cryptographic tasks as e.g. encryption and authentication. The main idea is to achieve both the peculiar security benefits of QKD and PQC algorithms.

However, there are many possible ways to implement this plan and utmost diligence is required for the integration of QKD with the different cryptographic methods to avoid mistakes that could easily compromise the overall security of the network. Due to the complexity of the subject, standards are needed to agree on a common set of protocols and rules to protect the networks from external attacks. The standard X.1714 (ex X.cf-QKDN) *Key combination and confidential key supply for quantum key distribution networks* has been approved and addresses the combination of QKD keys with common cryptographic algorithms. Going in a similar direction, the draft standard DTS/CYBER-QSC-0015 (TS 103 744) from the technical committee CYBER QSC is one proposed set of designs for quantum-safe hybrid key exchanges that can support QKD. More standards are needed to allow a smooth migration of the current

IT infrastructure to the new paradigm, capable of guaranteeing long term security, while being practical and cost effective.

## 3.4. Other standards and documents in the area of QKD

### 3.4.1. Overview of other standards in the area of QKD

Table 4 provides an overview of other existing standards and standards under development in the area of QKD.

**Table 4: Other standards related to QKD**

| SDO | Document number | Document title | Version | publ. date |
|---|---|---|---|---|
| ETSI | GR QSC 001 | Quantum-Safe Cryptography (QSC); Quan-tum-safe algorithmic framework | V1.1.1 | 2016-07 |
| ETSI | GR QSC 006 | Quantum-Safe Cryptography (QSC); Limits to Quantum Computing applied to symmetric key sizes | V1.1.1 | 2017-02 |
| ETSI | GR QKD 007 | Quantum Key Distribution (QKD); Vocabulary | V1.1.1 | 2018-12 |
| ETSI | TR 103570 | CYBER; Quantum-Safe Key Exchanges | V1.1.1 | 2017-10 |
| *IEEE* | *P1913* | *Software-Defined Quantum Communication* | | *Drafting* |

The technical report ETSI TR 103570 *CYBER; Quantum-Safe Key Exchanges* compares a selection of proposals for quantum-safe key exchanges taken from the academic literature and gives an overview of each key exchange, lists proposed parameters and gives software performance estimates on a range of processors. The draft standard IEEE P1913 intends to define the Software-Defined Quantum Communication (SDQC) protocol that enables configuration of quantum endpoints in a communication network in order to dynamically create, modify, or remove quantum protocols or applications.

### 3.4.2. Gaps in vocabulary

Regarding general vocabulary and definitions of various terms, the content of the existing report ETSI GR QKD 007 *Quantum Key Distribution (QKD); Vocabulary* is currently under revision to meet the current needs of the QKD community. It is important to ensure that all the new terms are included in the document to guarantee harmonisation of the language. It is common and desirable that terms established in the vocabulary of a certain SDO are adopted by other SDOs working on related items. This simplifies the standardisation work, creates a common set of definitions, which are broadly agreed and understood, and harmonises the work of different SDOs leading to common standards easily adoptable by the quantum communications industry.

### 3.4.3. Further relevant documents

**ETSI White Paper No. 27: Implementation Security of Quantum Cryptography. Introduction, challenges, solutions.**

The ETSI White Paper No. 27 (published 2018) summarises the current status of quantum cryptography implementation security and outlines the current understanding of the best practice related to it. It illustrates the discussion with Quantum Key Distribution (QKD), although many of the arguments also apply to the other quantum cryptographic primitives. It is beyond the scope of this document to analyse the security of all QKD protocols.

**GSMA Q_004 Quantum Computing, Networking and Security (under development)**

The scope of the document GSMA Q_004 will provide an overview of the state-of-the-art of the quantum technologies and their related levels of maturity in terms of the indicator Technology Readiness Level (TRL), with particular reference to: quantum security (QKD, QNRG and the provisioning of quantum security as a service), quantum computing, quantum networking and communications, and quantum metrology. The whitepaper will perform an analysis of the ongoing experimental Proof-of-Concepts (PoC) and of use cases experimenting with the above mentioned technologies, and will provide the main requirements for a seamless integration of quantum nodes/systems/devices in the network infrastructures without service disruption and large additional investment costs.

## 3.5. Overview of ongoing QKD standardisation activities and connections to OPENQKD

In Table 5 (Colour code: red (ISO); blue (ETSI); violet (ITU-T); orange (OPENQKD, tasks and deliverables)) ongoing standardisation activities and potential inputs from the OPENQKD project are shown. Table 5 extends over a period of 3 years, whereas longer-term prospects for standards in quantum communications are discussed in Section 4.

In order to develop useful and thus successful standards, **it is in general necessary to deploy the technology first, learn the lessons from the field, and then translate the experience into standards**. This is one of the declared goals of OPENQKD, whose QKD deliverables are expected to translate the experience gathered from the use cases into new work items for standardisation of QKD. Additional funded projects should be promoted to start these activities as soon as 2021. Also new areas, such as quantum communications transmitted by satellite, are missing in Table 5. Satellite QKD is an area of increasing activity and will warrant the development of standards in the near future.

Table 5: Ongoing standardisation work in QKD and potential input from the OPENQKD-project

| Topic | Ongoing activity | 2020 | | | | 2021 | | | | 2022 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Quantum communicaitons module security | QKD implementation security requirements, test and evaluation mehtods | 🟥 23837-1,2 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | | | |
| | QKD protection profile | 🟦 GS QKD 016 | 🟦 | 🟦 | 🟦 | 🟦 | | | | | | | |
| | QKD security proofs | 🟦 GS QKD 005 rev | 🟦 | 🟦 | 🟦 | | | | | | | | |
| | QKD security against the Trojan-horse attack | 🟦 QKD 010 | 🟦 | 🟦 | 🟦 | | | | | | | | |
| | Characterisation of QKD transmitter | 🟦 QKD 013 | 🟦 | 🟦 | 🟦 | | | | | | | | |
| | Design of QKD interfaces with authentication | | | 🟦 GR QKD 019 | 🟦 | 🟦 | 🟦 | | | | | | |
| | Measurement methology QKD systems | 🟨 | 🟨 | 🟨 | | | | | | | | | |
| | TX security | | | 🟨 | 🟨 | 🟨 | | | | | | | |
| | RX security | | | | 🟨 | 🟨 | 🟨 | 🟨 | | | | | |
| | Interface security | | | | | 🟨 | 🟨 | 🟨 | 🟨 | 🟨 | | | |
| | Security evaluation and certification process | | | | | | | 🟨 | 🟨 | 🟨 | 🟨 | 🟨 | |
| Fibre network interoperability | Quantum networks and interoperability | 🟪 Y.QKDN (SG13) | 🟪 | 🟪 | 🟪 | 🟪 | | | | | | | |
| | APIs for different use cases and architectures | 🟨 | 🟨 | 🟨 | | | | | | | | | |
| | QKD control interface for software-defined networks (SDNs) | 🟦 GS QKD 015 | 🟦 | | | | | | | | | | |
| | Agent-module exchange within node in SDN | | | 🟨 | 🟨 | 🟨 | 🟨 | 🟨 | | | | | |
| | Network architectures | 🟦 GS QKD 017 | 🟦 | 🟦 | | | | | | | | | |
| | Orchestration Interface of Software Defined Networks | | | | 🟦 GS QKD 018 | 🟦 | 🟦 | | | | | | |
| Quantum network security | Quantum network security | 🟪 Y.sec (SG17) | 🟪 | 🟪 | 🟪 | 🟪 | | | | | | | |
| | Cryptographic functions for QKD networks | 🟪 X.cf-QKDN | 🟪 | | | | | | | | | | |
| other | Quantum threat to asymmetric cryptography | 🟦 GS 004 | 🟦 | | | | | | | | | | |
| | Vocabulary for QKD | 🟦 GR QKD 007 | 🟦 | | | | | | | | | | |
| | Supportive document on standardization | 🟨 | | | | | | | | | | | |

🟦 ETSI

🟥 ISO/IEC

🟪 ITU-T

🟨 OPENQKD

# 4. Coordination and roadmap for QKD standardisation

It is apparent from Table 5 that standardisation in quantum communications has recently gained momentum and has involved international and European standard developing organisations (SDOs) in several areas of the QKD technology. However, the resulting standardisation process is often fragmented and uncoordinated. This can lead to contradictory standards, which would likely not be adopted by the quantum communications industry. Co-ordination of standards development is required to avoid this potential scenario.

## 4.1. Strategic importance of QT standardisation

In autumn 2018, the European Commission launched its long term and large-scale research and innovation initiative, the Quantum Flagship[24] (Quantum Technologies FET Flagship Programme of the European Commission). Within a period of 10 years, research and innovation projects in the field of quantum technologies shall be funded at the cumulative extent of up to €1bn. The explicit goals of the QT flagship, as stated in the "Quantum Manifesto"[25], are:

- "*Kick-start a European quantum industry to position Europe as a leader in quantum technologies" and thus to "create a competitive industry for long-term prosperity and security*";
- Consolidation and expansion of European leadership and excellence in the research area of Quantum Technologies;
- "*Make Europe a dynamic and attractive region for innovative business and investments in quantum technologies*";
- Benefit from quantum technologies "*to provide better solutions (…) in such fields as energy, health, security, and the environment*".

Furthermore, the manifesto suggests "Key activities" – several of these activities can directly be implemented or facilitated by standardisation activities. It has to be noted that the current report only regards standardisation as far as it is relevant for QKD and quantum communication, as well as adjoining fields based upon QKD (e.g. secure communication applications):

- "Support growth in scientific activities linked to quantum technologies": QKD standardisation can act as incentive for scientific research that is needed for specific standards (e.g. standards for the qualification of QKD components, such as photon transmitters and receivers).
- "Facilitate a new level of coordination between academia and industry to move advances in quantum technologies from the laboratory to industry": Currently active QKD standardisation groups have (actually without exception) members from academia, other research institutions, certification laboratories, as well as producers of QKD components and systems and thus facilitate coordination and knowledge transfer.

[24] https://ec.europa.eu/digital-single-market/en/quantum-technologies

[25] https://qt.eu/app/uploads/2018/04/93056_Quantum-Manifesto_WEB.pdf

- “Promote the involvement of member regions that do not currently have a strong quantum technologies research programme”: This is directly supported by the open access policies of standardisation groups: e.g. ISO enables access through national bodies at no cost, granting voting rights on a national basis; ETSI asks only for moderate fees for the participation of academic and other research organisations.

Other key activities, which can at least be supported by standardisation activities, include:

- “Coordinate public investments and strategies in quantum technologies at the European level”: Funded research projects can easily either directly participate in standards groups, like in ETSI, or through national bodies in ISO, or have formal liaisons with QKD standardisation groups. Thus, most research projects in the field of QKD have their own standardisation activities (in the form of work packages, e.g. the OPENQKD project’s WP9 to which this report belongs) and produce strategic assessment and advice, which can be fed back to the respective funding bodies.
- “Create a new generation of quantum technology professionals in Europe through focused education at the intersection of science, engineering and business (…)”: This strategic key activity is a supported by the heterogeneous composition of QKD standards groups, facilitating knowledge transfer across domains.
- “Create a favourable ecosystem of innovation and business creation for quantum technologies”: Standards developing organisations have through their composition and activities a share in the creation of a favourable ecosystem in the field of QT.

## 4.2. QKD and QT standardisation coordination

The previous subsection 4.1 has established the impact and importance of quantum key distribution standardisation (and generally quantum technologies standardisation) to support the general goals of the current Quantum Flagship initiative. However, for maximum impact, and to avoid certain pitfalls, a centralised coordination for supporting and steering standardisation activities is advisable.

The flagship program implements (or plans to implement) specific cooperation and coordination activities[26] to “coordinate national strategies and activities”, promote collaboration, “form an industry leadership group”, set up advisory boards. With regard to standardisation, the Quantum Manifesto mentions to “integrate national metrological institutes in developing quantum-based standards for the most mature quantum technologies (e.g. quantum key distribution)”.

In support of quantum standardisation coordination, the CEN/CENELEC Focus Group Quantum Technology (FGQT) was established in 2020. The FGQT will monitor developments in quantum technologies standardisation and identify relevant standardisation needs and opportunities for all types of quantum technologies at a European level. The FGQT will promote interaction between all relevant European stakeholders in the quantum technologies area and propose further actions in standardisation. It will encourage European stakeholders to delegate experts to standardisation committees on a European and worldwide level (e.g. to ISO/IEC

[26] https://qt.eu/app/uploads/2018/04/93056_Quantum-Manifesto_WEB.pdf; p. 14

and ITU-T technical committees) and make recommendations to standards developing organisations technical bodies. While the FGQT itself will, according to its terms of reference, not be developing standards, it intends to make recommendations to SDOs, including CEN/CENELEC itself. Here the FGQT needs to be aware of, and consequently avoid, a potential conflict of interest when recommendations for producing standards are given to SDOs, including CEN/CENELEC. **Ideally, standardisation coordination would be facilitated on a level above that of a single SDO.**

Indeed, one pitfall should be avoided: SDOs should not enter into competition and develop standards in parallel – thus wasting a particular scarce resource, i.e. the expertise of quantum technology professionals. ITU-T recently established a QT Focus Group with very similar goals to those stated by CEN/CENELEC. This comes on top of the other initiatives already running in ETSI, ISO/IEC, ITU-T SG13, ITU-T SG17, IEEE etc. Given the large number of ongoing or planned SDO initiatives, it remains to be seen which of these will be able to make an impact. Ultimately, QT vendors and end users will decide to which of these competing initiatives they can commit their limited resources.

There is a considerable risk that competing SDOs will develop conflicting standards, thus leading to incompatible products in the marketplace – a development that could stifle the growth of the QT industry. In the field of cloud computing, this sort of competition has led to the paradoxical situation of virtually hundreds of competing cloud standards developed by dozens of SDOs – while closed-source proprietary commercial offerings, like Amazon with its Amazon Web Services, sets the market dominant de facto standards.

It is essential that national metrology institutes (NMIs) bring their expertise to bear upon the development of testing standards. Some NMIs, e.g. OPENQKD partner NPL (National Physical Laboratory, UK), INRIM (Istituto Nazionale di Ricerca Metrologica, Italy) and PTB (Physikalisch-Technische Bundesanstalt, Germany) already participate in SDOs activities. This can be strengthened through engagement with the European Metrology Network for Quantum Technologies (EMN-Q)[27]. The EMN-Q was recently set up to ensure coherent engagement between NMIs and stakeholders (including industry, the flagship and national QT programmes) so that NMIs make efficient use of their finite resources to best support quantum technologies in developing measurement services and contributing to globally accepted standards. NMIs should therefore also be supportive of avoiding parallel standardisation activity.

## 4.3. Strategic standardisation roadmap

In order to materialise the advantages that standardisation can potentially deliver for the advancement of quantum technologies and the transformation into practical applications, the identified gaps need to be addressed. The missing standards and supplementary documentation and activities need to be prioritised according to their urgency to reach defined milestones. The QKD standards roadmap (see Figure 1) presents a structured time plan to this approach.

[27] https://www.euramet.org/european-metrology-networks/quantum-technologies/

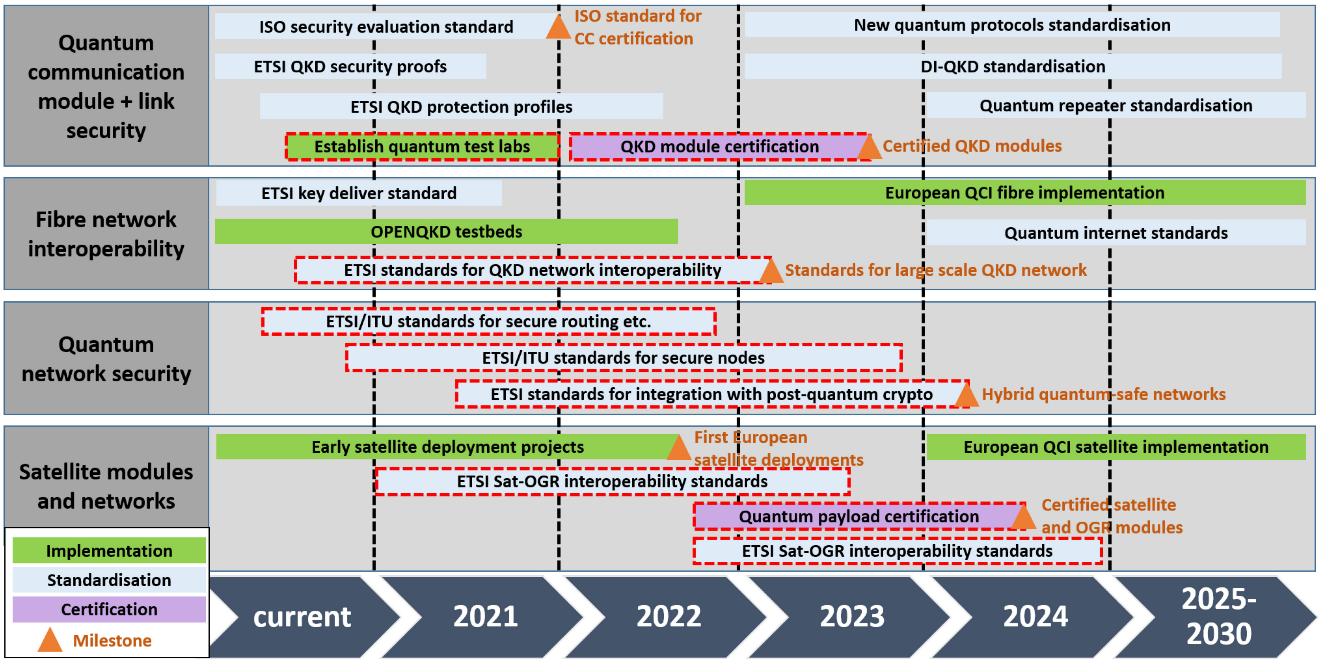
Quantum communication module + link security
ISO security evaluation standard
ISO standard for CC certification
New quantum protocols standardisation
ETSI QKD security proofs
DI-QKD standardisation
ETSI QKD protection profiles
Quantum repeater standardisation
Establish quantum test labs
QKD module certification
Certified QKD modules
Fibre network interoperability
ETSI key deliver standard
European QCI fibre implementation
OPENQKD testbeds
Quantum internet standards
ETSI standards for QKD network interoperability
Standards for large scale QKD network
Quantum network security
ETSI/ITU standards for secure routing etc.
ETSI/ITU standards for secure nodes
ETSI standards for integration with post-quantum crypto
Hybrid quantum-safe networks
Satellite modules and networks
Early satellite deployment projects
First European satellite deployments
European QCI satellite implementation
ETSI Sat-OGR interoperability standards
Quantum payload certification
Certified satellite and OGR modules
ETSI Sat-OGR interoperability standards
Implementation
Standardisation
Certification
Milestone
current
2021
2022
2023
2024
2025-2030

Figure 1. QKD standards roadmap

### Quantum communication module and link security

In the field of security standards for the quantum communications module, significant effort is already underway, as has been shown in section 3.1. Both the ISO and the ETSI initiatives have been kicked-off, are on track, and the teams in charge have the required expertise and potential that a positive outcome can reasonably be expected. The ISO initiative is located within ISO/JTC1 SC27 WG3, which develops and revises the ISO/IEC 15408 Common Criteria standard itself, while the ETSI ISG-QKD has recently started its ETSI GS QKD 016 *Quantum Key Distribution (QKD); Protection Profile (PP)*. The German BSI is also currently active in this field: It has contracted an evaluation laboratory with the development of a Common Criteria Protection Profile for the QKD link, and information exchange is planned between these different activities. Required side documents, as e.g. component standards, are to some extent available, but need to be provided for a greater variety of components – activities in this direction are already under way.

The ETSI ISG plans to engage a Common Criteria test laboratory in the writing of a QKD Protection Profile. To our knowledge, this is the only involvement of a commercial test laboratory so far. However, to secure wide recognition of security evaluations, it would be beneficial to involve evaluation laboratories in different countries, and to develop the expertise in these laboratories for evaluating Protection Profiles and products against Security Targets. This would stimulate the flow of expertise in both directions, making standards more suitable for actual evaluations and certifications in different (national) certification schemes.

The security standards currently in preparation focus on prepare and measure type QKD protocols. Once a successful certification will have been demonstrated, standards for alternative QKD protocols will be required in the medium term. Device independent QKD (DI-QKD), and its many variants, such as measurement device independent QKD and Twin-Field QKD, have great potential to resolve in a fundamental way substantial security problems that today require significant effort to tackle and mitigate in current security standards. Standardisation for DI-QKD needs to be started in the medium term, to further stimulate progress in research and to have standards ready when practical solutions become available. Moreover, in the medium term, standardisation work should begin for more exotic quantum components that will be needed for the future quantum internet, e.g. quantum repeaters.

**Fibre network interoperability**

In the field of fibre network interoperability, the OPENQKD project will be providing several metropolitan-area networks with different topologies, as well as some long range links (direct links and sequences of links), as testbeds for QKD systems and top-level applications. OPENQKD project results shall support and enable the practical installation of the European Quantum Communication Infrastructure (QCI) starting around 2023. A particular additional requirement for a large-scale deployment is to define interfaces on all layers for components and QKD links of different vendors. The ETSI ISG-QKD has scheduled a relevant activity on large-scale network standards for publication in 2023.

**Quantum network security**

Quantum network security has several standardisation activities on track for marrying QKD capabilities with state-of-the-art quantum-safe cryptographic algorithms. Results are expected within the next three years, so that by the middle of the decade practical hybrid quantum safe networks (i.e. networks for confidential and authentic communication secured against quantum computer attacks) will be available. Standards for a future full quantum internet, connecting quantum computers and facilitating the direct transmission of quantum information in a quantum network (including quantum repeaters) are likely to be tackled later, i.e. probably sometime around 2025.

**Satellite modules and networks**

The inherent distance limitations of quantum communication in fibres (without a quantum repeater) led to designs involving optical links between satellites and ground stations. In this way, metropolitan area quantum networks can be interconnected. A first experimental space mission was launched in 2016 with quantum optics experiments carried out in a co-operation of the Chinese Academy of Sciences, the University of Vienna and the Austrian Academy of Sciences. Standardisation activities for optical ground receiver interoperability and interoperability between space quantum networks and terrestrial fibre-based networks need to be started in the short to medium term.

## 4.4. Potential for new EU projects

In this section, funding opportunities in the framework of the Quantum Flagship (see highlighted red framed boxes in Figure 1) are proposed. Such funded projects could address identified gaps and carry out projected activities of the roadmap and thus be in line with the strategic goals of the Quantum Flagship.

**Quantum communication module and link security**

In the field of security certification of QKD systems, several activities have started and considerable effort is already scheduled for the development of the required standards. As mentioned in the previous section, an early involvement by several (maybe five or more) evaluation and testing laboratories and national certification bodies would certainly be beneficial for supporting and securing the envisioned actual certification of QKD equipment. In order to achieve this goal, a funded project could bring together evaluation and testing laboratories from different European countries (and potentially also the certification authorities of the respective national schemes) with corporations (QKD components and QKD link producers) and research organisations in the field of QKD. Such a project may use available testbed facilities (e.g. the OPENQKD testbeds) to determine if these infrastructures are sufficient and adequate for carrying out the required tests for actual evaluations, or if different testing infrastructures would be necessary. Test evaluations could be carried out for existing and hypothetical components using the existing standards, and assessments could be made whether the standards would be sufficient for successful real-world evaluations and approval by certification authorities. Such a project would provide valuable (early) feedback for standards developing organisations, optimally when adjustments in the standards under development are still possible without major revision.

**Fibre network interoperability**

In fibre network interoperability of QKD systems, further coordination and structured activity is required to achieve the necessary standards for network interoperability. Standards for the full quantum internet need to be addressed in the medium term, to support the development of the European Quantum Communication Infrastructure (QCI).

**Quantum network security**

The development of standards for QKD network interoperability, and the development of the security standards required for evaluation and certification would both benefit from support through funded projects. Specifically targeted funding in dedicated projects, or as subprojects in other QKD network projects, will potentially speed up the development process and increase the probability of producing practical and useable standards. Proper guidelines must prevent the overall security from being compromised at network level in order to maintain the high security of QKD-devices working perfectly at lower levels.

### Satellite modules and networks

In December 2019, during the Space19+ event in Seville (Spain),[28] ESA together with European ministers in charge of space activities decided on a boost of space science in Europe. ESA launched the design and development of the space-based SAGA (Secure And cryptoGrAphic) component of the European quantum communication infrastructure to reach in-orbit testing and validation at the end of the project. On the side of the EU and its member states, the future QCI space segment needs to be connected to the fibre-based QCI to form the overall QCI network infrastructure. Both ESA and the EU will proceed towards high practicability for future users by investigating detailed user requirements and defining related QCI use cases. Standardisation and certification will ensure the development of suitable system requirements for the benefit of the future QCI end users.

[28] https://www.esa.int/About_Us/Corporate_news/Record_funding_for_European_space_investments_in_Seville

# Annex

## ETSI Standards

| Document number | Document title |
|---|---|
| ETSI GR QKD 003<br>Read Specification here | Quantum Key Distribution (QKD); Components and Internal Interfaces |
| ETSI GR QKD 007<br>Read Specification here | Quantum Key Distribution (QKD); Vocabulary |
| ETSI GR QSC 001<br>Read Specification here | Quantum-Safe Cryptography (QSC); Quantum-safe algorithmic framework |
| ETSI GR QSC 003<br>Read Specification here | Quantum Safe Cryptography; Case Studies and Deployment Scenarios |
| ETSI GR QSC 004<br>Read Specification here | Quantum-Safe Cryptography; Quantum-Safe threat assessment |
| ETSI GR QSC 006<br>Read Specification here | Quantum-Safe Cryptography (QSC); Limits to Quantum Computing applied to symmetric key sizes |
| ETSI GS QKD 002<br>Read Specification here | Quantum Key Distribution (QKD); Use Cases |
| ETSI GS QKD 004<br>Read Specification here | Quantum Key Distribution (QKD); Application Interface |
| ETSI GS QKD 005<br>Read Specification here | Quantum Key Distribution (QKD); Security Proofs |
| ETSI GS QKD 008<br>Read Specification here | Quantum Key Distribution (QKD); QKD Module Security Specification |
| ETSI GS QKD 010 | Quantum Key Distribution (QKD); Implementation security: Protection against trojan horse attacks in one-way QKD systems |
| ETSI GS QKD 011<br>Read Specification here | Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems |
| ETSI GS QKD 012<br>Read Specification here | Quantum Key Distribution (QKD); Device and Communication Channel Parameters for QKD Deployment |
| ETSI GS QKD 013 | Quantum Key Distribution (QKD); Characterisation of optical output of QKD transmitter modules |
| ETSI GS QKD 014<br>Read specification here | Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API |
| ETSI GS QKD 015<br>Read specification here | Quantum Key Distribution (QKD); Quantum Key Distribution control interface for software defined Networks |
| ETSI GS QKD 016 | Quantum Key Distribution (QKD); Protection Profile (PP) |

| | |
|---|---|
| ETSI GS QKD 017 | Quantum Key Distribution (QKD); Network architectures |
| ETSI GS QKD 018 | Quantum Key Distribution (QKD); Orchestration Interface of Software Defined Networks |
| ETSI GR QKD 019 | Quantum Key Distribution (QKD); Design of QKD interfaces with Authentication |
| ETSI TR 103570<br>*Read report here* | CYBER - Quantum-Safe Key Exchanges |

## ISO/IEC Standards

| Document number | Document title |
|---|---|
| ISO/IEC 23837-1 | Security requirements, test and evaluation methods for quantum key distribution Part 1: requirements |
| ISO/IEC 23837-2 | Security requirements, test and evaluation methods for quantum key distribution Part 2: test and evaluation methods |

## ITU-T Standards

| Document number | Document title |
|---|---|
| X.1710<br>(ex X.sec-QKDN-ov)<br>*Read Specification here* | Security framework for quantum key distribution networks |
| X.1714<br>(ex X.cf-QKDN)<br>*Read Specification here* | Key combination and confidential key supply for quantum key distribution networks |
| X.sec_QKDN_intrq | Security requirements for integration of QKDN and secure network infrastructures |
| X.sec-QKDN-km | Security requirements for quantum key distribution networks - Key management |
| X.sec-QKDN-tn | Security requirements for quantum key distribution networks -Trusted node |
| XSTR-SEC-QKD<br>*Read Report here* | Security considerations for quantum key distribution networks |
| Y.3800<br>(ex Y.QKDN_FR, Corrigendum 1)<br>*Read Specification here* | Overview on networks supporting quantum key distribution |

| | |
|---|---|
| Y.3801<br>(ex Y.QKDN-req)<br>*Read Specification here* | Functional requirements for quantum key distribution networks |
| Y.3802<br>(ex Y.QKDN_Arch)<br>*Read Specification here* | Quantum key distribution networks – Functional architecture |
| Y.3803<br>(ex Y.QKDN_KM)<br>*Read Specification here* | Quantum key distribution networks – Key management |
| Y.3804<br>(ex Y.QKDN_CM)<br>*Read Specification here* | Quantum key distribution networks – Control and management |
| Y.QKDN_BM | Business role-based models in Quantum Key Distribution Network |
| Y.QKDN_frint | Framework for integration of QKDN and secure network infrastructures |
| Y.QKDN-qos-arc | Functional architecture of QoS assurance for quantum key distribution networks |
| Y.QKDN-qos-gen | General Aspects of QoS on the Quantum Key Distribution Network |
| Y.QKDN-qos-ml-req | Requirements of machine learning based QoS assurance for quantum key distribution networks |
| Y.QKDN-qos-req | Requirements for QoS Assurance of the Quantum Key Distribution Network |
| Y.QKDN_SDNC | Software Defined Network Control for Quantum Key Distribution Networks |

## other standards

| **Document number** | **Document title** |
|---|---|
| *IEEE P1913* | Software-Defined Quantum Communication |