INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2017-2020

SG13-TD100/PLEN

STUDY GROUP 13

Original: English

Question(s): 16/13 Geneva, 13-24 March 2023

TD

Source: Editors

Title: Draft new Supplement 74 to ITU-T Y.3800-series Recommendations (Y.supp.QKDN-roadmap): "Standardization roadmap on Quantum Key Distribution Networks" - for agreement

Contact: Mark McFadden E-mail: mark@internetpolicyadvisors.com
DCMS
UK

Contact: Zhangchao Ma
CAS Quantum Network, Co. Ltd. E-mail: mazhangchao@qtict.com
China

Abstract: This TD contains the draft Supplement ITU-T Y.supp.QKDN-roadmap "Standardization roadmap on Quantum Key Distribution Networks" for agreement at the plenary meeting.

Draft new Supplement 74 to ITU-T Y.3800-series Recommendations (Y.supp.QKDN-roadmap)

Standardization roadmap on Quantum Key Distribution Networks

Summary

Supplement 74 to ITU-T Y.3800-series Recommendations provides the standardization roadmap on quantum key distribution networks. It describes the landscape with related technical areas of trust technologies from an ITU-T perspective and list up related standards and publications developed in standards development organizations (SDOs).

Table of Contents

Page

Draft new Supplement to ITU-T Y-series Recommendations (Y.supp.QKDN-roadmap)

Standardization roadmap on Quantum Key Distribution Networks

1 Scope

This Supplement provides the standardization roadmap on quantum key distribution networks. It addresses the following subjects:

- Landscape and related technical areas of QKDN technologies from an ITU-T perspective;
- The collection of related standards and publications on QKDN technologies in standards development organizations (SDOs).

2 References

[ITU-T Y.3800] Recommendation ITU-T Y.3800 (2019)/Cor.1 (2020), *Overview on networks supporting quantum key distribution*.

[ITU-T Y.3801] Recommendation ITU-T Y.3801 (2020), *Functional requirements for quantum key distribution networks*.

[ITU-T Y.3802] Recommendation ITU-T Y.3802 (2020), *Quantum key distribution networks - Functional architecture.*

[ITU-T Y.3803] Recommendation ITU-T Y.3803 (2020), *Quantum key distribution networks – Key management*.

[ITU-T Y.3804] Recommendation ITU-T Y.3804 (2020), *Quantum Key Distribution Networks - Control and Management*.

[X.STR-SEC-QKD] Technical Report ITU-T X.STR-SEC-QKD (2020), *Security considerations for quantum key distribution network*

[ITU-T X.1710] Recommendation ITU-T X.1710 (2020), *Security framework for quantum key distribution networks.*

[ITU-T X.1712] Recommendation ITU-T X.1712 (2021)/Cor.1 (2022), *Key combination and confidential key supply for quantum key distribution networks.*

[ITU-T X.1714] Recommendation ITU-T X.1714 (2020), *Key combination and confidential key supply for quantum key distribution networks.*

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following term defined elsewhere:

1.1.1. key manager (KM) [ITU-T Y.3800]: A functional module located in a quantum key distribution (QKD) node to perform key management in the key management layer.

1.1.2. key management agent (KMA) [ITU-T Y.3802]**:** A functional element to manage keys generated by one or multiple quantum key distribution (QKD) modules in a QKD node (trusted node).

NOTE - KMA acquires keys from one or multiple QKD modules, synchronizes, resizes, formats, and stores them. It also relays keys through key management agent (KMA) links.

1.1.3. key supply agent (KSA) [ITU-T Y.3802]: A functional element to supply keys to a cryptographic application, being located between a key management agent (KMA) and the cryptographic application.

NOTE - Application interfaces for cryptographic applications are installed into the key supply agent (KSA). The KSA synchronizes keys, and verifies their integrity via a KSA link before supplying them to the cryptographic application.

1.1.4. quantum key distribution (QKD) [b-ETSI GR QKD 007]: Procedure or method for generating and distributing symmetrical cryptographic keys with information theoretical security based on quantum information theory.

1.1.5. quantum key distribution module [ITU-T Y.3800]**:** A set of hardware and software components that implements cryptographic functions and quantum optical processes, including quantum key distribution (QKD) protocols, synchronization, distillation for key generation, and is contained within a defined cryptographic boundary.

NOTE – A QKD module is connected to a QKD link, acting as an endpoint module in which a key is generated. These are two types of QKD modules, namely, the transmitters (QKD-Tx) and the receivers (QKD-Rx).

1.1.6. quantum key distribution network (QKDN) [ITU-T Y.3800]: A network comprised of two or more quantum key distribution (QKD) nodes connected through QKD links.

NOTE – A QKDN allows sharing keys between the QKD nodes by key relay when they are not directly connected by a QKD link.

3.2 Terms defined in this Supplement

None

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

QKD Quantum Key Distribution

QKDN Quantum Key Distribution Network

QoS Quality of Service

SDN Software Defined Network

5 Conventions

None.

6 Standardization Activities on QKDN

QKD and its networking technologies have attracted a lot of interest in multiple SDOs, e.g., ITU-T, ISO/IEC JTC1, IEEE, IETF, ETSI, as shown in Figure 6. The status of QKDN standardization in different SDOs will be summarized in the following sub-clauses.

Figure 1.1: QKDN standardization timeline

6.1 ITU-T

ITU-T was the first SDO to standardize QKD as a network. In July 2018, ITU-T SG13 initiated the first work item (i.e., Y.3800) on QKD and brought in the concept of Quantum Key Distribution Network (QKDN) firstly. Afterwards, there are more than 40 work items conducted by 4 different groups in ITU-T under the umbrella of QKDN, which can be divided into 4 branches as follows:

- Study Group 13 (Q16/13 and Q6/13): focus on network aspects of QKDN
- Study Group 17 (Q15/17, formerly Q4/17): focus on security aspect of QKDN
- Study Group 11 (Q2/11): focus on QKDN high layer protocols and signaling
- Focus Group on Quantum information technology for Networks (FG-QIT4N): to study the implications of QITs for both quantum and ICT network

6.1.1 ITU-T Study Group 13

A landscape diagram for the QKDN standardization work in SG13 is as illustrated in Figure 2. SG13 has the following work items on QKDN as listed in Table 1.

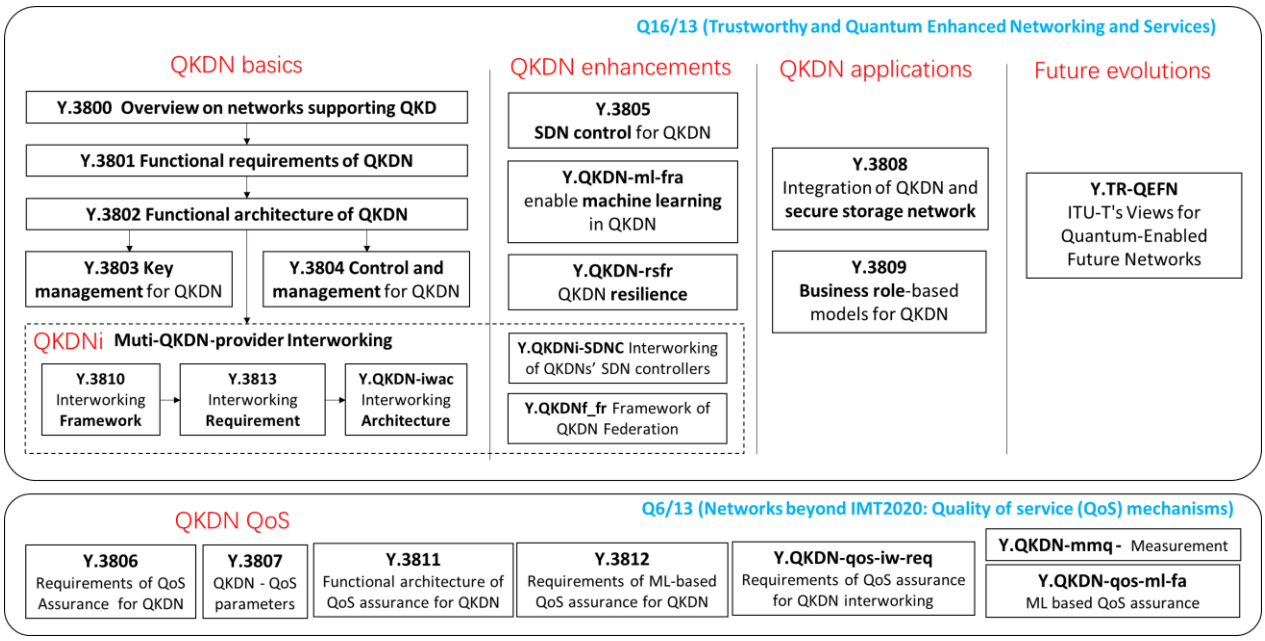

Figure 2: QKDN standardization landscape in ITU-T SG13

Table 1: QKDN related work items in ITU-T SG13

Name	Group	Title	Summary	Status
Y.3800	Q16/13	Overview on networks supporting quantum key distribution	Recommendation ITU-T Y.3800 gives an overview on networks supporting quantum key distribution (QKD). This Recommendation aims to provide support for the design, deployment, operation and maintenance for the implementation of QKD networks (QKDNs), in terms of standardized technologies. The relevant network aspects of conceptual structure, layered model and basic functions are within the scope of the Recommendation to support its implementation.	Approved (10/2019)
Y.3801	Q16/13	Functional requirements for quantum key distribution network	For quantum key distribution networks (QKDN), Recommendation ITU-T Y.3801 specifies functional requirements for quantum layer, key management layer, QKDN control layer and QKDN management layer.	Approved (04/2020)
Y.3802	Q16/13	Quantum key distribution networks - Functional architecture	Recommendation ITU-T Y.3802 specifies the functional architecture model, detailed functional elements and interfaces, architectural configurations and overall operational procedures of the quantum key distribution (QKD) network.	Approved (12/2020)
Y.3803	Q16/13	Quantum key distribution networks - Key management	The objective of this Recommendation is to provide the help for design, deployment, and operation of key management of QKDN. Overall structure and basic functions of QKDN are first reviewed along with Recommendation ITU-T Y.3800, requirements of QKDN are second reviewed along with draft Recommendation ITU-T Y.3801, and then functional elements and procedures of key management are described in this Recommendation.	Approved (12/2020)
Y.3804	Q16/13	Quantum key distribution networks - Control and management	This Recommendation is to specify the control, management, and orchestration for Quantum Key Distribution network.	Approved (09/2020)
Y.3805	Q16/13	Software Defined Networking Control for Quantum Key Distribution Networks	This recommendation specifies the software-defined network control of QKDN. It includes why introducing SDN into QKDN, the function requirements of SDN control for QKDN, SDN-based control architecture for QKDN which include the SDN controller, the programmable controlled components, and the interfaces	Approved (11/2021)

			of SDN controller in QKDN, hierarchical SDN controller for multi-domain QKDN, procedures of different SDN control functions, applications scenarios for SDN controlled QKDN, and security considerations.	
Y.3806	Q6/13	General Aspects of QoS on the Quantum Key Distribution Network	This Recommendation is to specify General Aspects of QoS on the Quantum Key Distribution Network as follows: - Descriptions of QoS (Quality of Service) and NP (network performance) on QKD network - Illustration of how the QoS and the NP concepts are applied in QKD network - Identification of the features of, and the relationship between these concepts - Classification of performance concerns for which parameters may be needed	Approved (9/2021)
Y.3807	Q16/13	Quantum key distribution networks – Quality of service parameters	Recommendation ITU-T Y.3800 specifies an overview on networks supporting quantum key distribution (QKD). For the purpose of design, deployment, operation and maintenance to support QKD network (QKDN) implementation, the required quality level of quantum key distribution service should be identified and quantified.	Approved (2/2022)
Y.3808	Q16/13	Framework for integration of quantum key distribution network and secure storage network	This Recommendation describes framework for integrating quantum key distribution network (QKDN) and secure storage network (SSN). In particular, the scope of this Recommendation includes: - overview of SSN; - functional requirements for SSN; - functional architecture model of SSN; - reference points; - operational procedures.	Approved (2/2022)
Y.3809	Q16/13	Business role-based models in Quantum Key Distribution Network	Draft Recommendation ITU-T Y.QKDN_BM describes business roles, business role-based models, and service scenarios in Quantum Key Distribution Network (QKDN) from different deployment and operation perspectives with existing user networks for supporting secure communications in various application sectors. This draft Recommendation can be used as a guideline for applying QKDN from business point of views as well as for deployment and operation of QKDN from telecom operators' point of views.	Approved (2/2022)

Y.3810	Q16/13	Quantum Key Distribution Networks – Internetworking Framework	Quantum key distribution network (QKDN) is a cryptographic infrastructure to provide secure symmetric keys to cryptographic applications in user networks. Constructing a large scale QKDN which covers wide area, it may consist of multiple QKDNs and they are interworking each other. The functional requirements and architecture of single QKDN are specified based on the functional requirements of QKDN in [ITU-T Y.3801], functional architecture and operational procedures of QKDN in [ITU-T Y.3802]. This recommendation is to specify a framework for interworking QKDNs. Security considerations are mentioned when it is directly related to the security of keys. This Recommendation will consider the following aspects for interworking QKDNs. 1) Interworking between QKDNs supported by different QKDN providers. NOTE - QKDN provider is specified in [draft ITU-T Y.QKDN_BM]. 2) Interworking between QKDNs with different technologies. Different technologies can be used in QKDNs such as: - Key relay encryption methods (i.e. OTP, AES etc.) - Key relay schemes (i.e. case 1 and case 2 which are specified in [ITU-T Y.3800]) - Key relay alternatives (i.e. XORs uniformly processed at destination node etc. which are specified in [ITU-T Y.3803]) - Configurations of QKDN controller (i.e. centralized QKDN or distributed QKDN which are specified in [ITU-T Y.3802] - Protocols in the key management layer, the QKDN control layer and the QKDN management layer. NOTE - Details of protocols is outside the scope of this Recommendation.	Approved (9/2022)
Y.QKDN-qos-iw-req	Q6/13	Requirements of QoS assurance for QKDN interworking	This draft Recommendation specifies the high-level and functional requirements of QoS assurance for quantum key distribution networks (QKDN) interworking, and the scope of this recommendation is as follows: Overview of QoS assurance for QKDN interworking High-level requirements of QoS assurance for QKDN interworking Functional requirements of QoS assurance for QKDN interworking;	Draft
Y.3811	Q6/13	Quantum key distribution networks - Functional architecture for quality of service assurance	This Recommendation specifies a functional architecture of QoS assurance for the quantum key distribution networks (QKDN). This recommendation first provides an overview of the functional architecture of QoS assurance for the QKDN. It then describes the functional architecture of QoS assurance which includes functional entities such as QoS data collection, data processing, data storage, data analytics, QoS anomaly detection and prediction, QoS policy decision making, and enforcement and reporting. Based on the functional entities described in the functional architecture, this Recommendation specifies a basic operational procedure of QoS assurance for the QKDN.	Approved (9/2022)
Y.3812	Q6/13	Quantum key distribution networks - Requirements for machine learning based quality of service assurance	This Recommendation specifies high-level and functional requirements of machine learning (ML) based QoS assurance for the quantum key distribution networks (QKDN). This recommendation first provides an overview of requirements of ML based QoS assurance for the QKDN. It describes a functional model of ML based QoS assurance and followed by associated high level and functional requirements of ML based QoS assurance. And some use cases are described.	Consented (7/2022)

Y.3813	Q16/13	Quantum key distribution networks interworking – functional requirements	For quantum key distribution networks (QKDN), Recommendation ITU-T Y.QKDN_iwrq specifies functional requirements for QKDNi. This Recommendation describes the general requirements, the functional requirements for QKDNi with GWNs and the functional requirements for QKDNi with IWNs.	Draft
Y.3814	Q16/13	Quantum key distribution networks - functional requirements and architecture for machine learning	For quantum key distribution networks (QKDN), Recommendation ITU-T Y.QKDN_iwrq specifies functional requirements for QKDNi. This Recommendation describes the general requirements, the functional requirements for QKDN is expected to be able to maintain stable operations and meet the requirements of various cryptographic applications efficiently. Due to the advantages of machine learning (ML) related to autonomous learning, ML can help to overcome the challenges of QKDN in terms of quantum layer performances, key management layer performances and QKDN control and management efficiency. Based on the functional requirements and architecture of QKDN in [ITU-T Y.3801] and [ITU-T Y.3802], this recommendation is to specify a framework for ML-enabled QKDN (QKDNml), including the role of ML in QKDN, the functional requirements, architecture and operational procedures of QKDNml.QKDNi with GWNs and the functional requirements for QKDNi with IWNs.	Draft
Y.QKDN-rsfr	Q16/13	Quantum key distribution networks - resilience framework	For quantum key distribution network (QKDN), Y.QKDN-rsfr specifies framework of QKDN resilience. This recommendation describes the overview of QKDN resilience, scenarios and requirements of QKDN protection and recovery. It also includes different use cases of QKDN resilience in the appendix.	Draft
Y.QKDN-iwac	Q16/13	Quantum key distribution networks interworking – architecture	This Recommendation specifies functional architecture for QKDNi. In particular, the scope of this Recommendation includes the following aspects for QKDNi: - Functional architecture for QKDNi; - Functional elements for QKDNi; Basic operational procedures for QKDNi.	Draft
Y.QKDNi-SDNC	Q16/13	Quantum Key Distribution Network Interworking – Software Defined Networking Control	The recommendation specifies the Software Defined Network (SDN) control for the interworking between QKDN providers focusing on the requirements for SDN controller in QKDN control layer and functional architecture for SDN control in QKDNi when SDN is used to provision the services for QKDNi. For SDN control of QKDNi, the reference points and the hierarchy of SDN controllers will be specified.	Draft

Y.QKDNf_fr	Q16/13	Framework of Quantum Key Distribution Network Federation	Despite the fact that the interworking aspects between different QKD providers and possibly between two different QKDN operators, this is very start of the large scale of QKDN networks to provide the end to end QKD service to cover the large areas to the end users and to provide the QKD service when the end user is not in the area of home network etc. Therefore, the federation of QKDNs to share the resources and capabilities of many QKDN providers shall be considered to create the industry ecosystem including operators, vendors, OEMS and service providers which could lead to eventually a platform to develop additional services in the future. Federation refers to the interaction and coordination between QKDN providers and QKDNs, supporting multi-operator, -network, - vendor environment to provide the seamless QKDN service to the end users. If the end user wishes to have the same level of security which QKDN provides when the end user moves to the region of other QKDN provider, then the end user needs to find the service capability in that region. The relevant QKDN service discovery, network capability discovery, resource allocation and negotiation and the subsequent service provisioning need to be performed. As QKD technology is being deployed around the world, however, still limited coverage exists from QKDN perspective as only some operators deploy them in part of their networks. Therefore, it is good to have the mechanisms to have the same level of security service in the different regions where possible and to combine resources among multiple operators. Furthermore, the QKDN sharing could be also considered where one operator does not have QKDN coverage in certain regions in a certain country.	Draft
TR-QEFN	Q16/13	ITU-T's Views for Quantum-Enabled Future Networks	The scope of this Technical Report is to describing ITU-T's Views for Quantum-Enabled Future Networks for the future networks study to act as a document to help SG13 to study the future network evolution towards Quantum era.	Draft
Supplement 70 to ITU-T Y.3800-series (ex Y.supp.QKDN-mla)	Q16/13	Quantum Key Distribution Networks - Applications of Machine Learning	For quantum key distribution networks (QKDN), the supplement presents the applications of machine learning (ML) in the quantum layer, the key management layer and the management and control layers of QKDN including the use case background, issue, role of ML in QKDN, use case analysis and, benefits and impact.	Approved (7/2021)
Y.QKDN-qos-mmq	Q6/13	Quantum key distribution Networks - Measurement methodology for QoS parameters	To evaluate QoS for QKD network, ITU-T Rec. Y.3807 'Quantum key distribution networks - Quality of service parameters' was developed and approved in December, 2021. The QoS parameters in ITU-T Rec. Y.3807 should be quantitatively measured and utilized for the design, deployment, operation and maintenance to support QKDN implementation. For this purpose, a method for measuring those parameters are required. There are two possible methods of measuring QoS parameters; in-service and out-of-service. In-service measurement is performed when testing the quality delivered by a network to a user connection. In the in-service measurement mode, the live traffic of a connection i s monitored directly. The out-of-service measurement mode makes use of particular test tools, for estimating accurately QoS parameters.	Draft

Y.QKDN-qos-ml-fa	Q6/13	Quantum key distribution networks - Functional architecture enhancement for machine-learning based quality of service assurance	This Recommendation specifies functional architecture enhancement of machine learning based QoS assurance for the quantum key distribution networks (QKDN). This Recommendation first provides an overview of functional architecture enhancement of machine learning based QoS assurance for the QKDN. It then describes a functional architecture enhancement of QoS assurance which includes functional components such as QoS data collection, data processing, data storage, data analytics, QoS anomaly detection and prediction, QoS policy decision making, enforcement and reporting. Based on the capabilities described in the functional architecture enhancement, this recommendation specifies operational procedures of QoS assurance for the QKDN.	Draft
TR.QN-UC	Q16/13	Use cases of quantum networks beyond QKDN	Based on the deliverable (D1.2) of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N), this Technical Report sorts and analyses use cases of quantum networks beyond QKDNcollected from FG QIT4N in the context of networking technologies as the mandate of ITU-T SG13. The uses cases which are only applied by quantum networks beyond QKDN are collected, investigated and summarized; all use cases are analysed by current bottlenecks, application scenarios, technical requirements and solutions. This Supplement also provides analyses for future applications and potential standardization requirements.	Draft
Y.Supp.QKDN-UC	Q16/13	Use cases of quantum key distribution networks	Based on the deliverable (D2.2) of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N), this Supplement consolidates the QKDN use cases collected from the ITU-T FG QIT4N in the context of networking technologies as the mandate of ITU-T SG13. Through a comprehensive analysis, the QKDN uses cases are classified into several classes and this Supplement highlights the competitive advantage of the use cases brought by QKDN and provides suggestions for future standardization efforts in ITU-T SG13.	Draft
Y.supp.QKDN-roadmap	Q16/13	Standardization roadmap on Quantum Key Distribution Networks	This Supplement provides the standardization roadmap on quantum key distribution networks. It addresses the following subjects: - Landscape and related technical areas of QKDN technologies from an ITU-T perspective; - The collection of related standards and publications on QKDN technologies in standards development organizations (SDOs).	Draft
Y.QKDN_SSNarch	Q16/13	Functional requirements for integration of quantum key distribution network and secure storage network	In several countries, proof-of-concept demonstrations of QKDNs for commercialization are becoming active. In order to widen applications and market of QKDNs, it is important to study how to integrate QKDNs and the other security infrastructures in the user networks. Secure storage network is one of applications of QKDN to protect critical data for a long-term. This draft Recommendation will study on functional architecture and reference points for secure storage network (SSN). It includes detailed description of each function and reference point of SSN based on functional architecture model defined in Y.3808.	Draft

Y.QKDN_SSNreq	Q16/13	Functional requirements for integration of quantum key distribution network and secure storage network	In several countries, proof-of-concept demonstrations of QKDNs for commercialization are becoming active. In order to widen applications and market of QKDNs, it is important to study how to integrate QKDNs and the other security infrastructures in the user networks. Secure storage network is one of applications of QKDN to protect critical data for a long-term. This draft Recommendation will study on functional requirements for secure storage network (SSN). It includes detailed description of each layer of SSN based on functional architecture model defined in Y.3808.	Draft
Y.QKDN-amc	Q16/13	Quantum key distribution networks - Requirements and architectural model for autonomic management and control	Autonomic Management and Control (AMC) is about Decision-making-Elements (DEs) as autonomic functions (i.e. control-loops) with cognition introduced in the management layer as well as in the control layer. Cognition in DEs, enhances DE logic and enables DEs to manage and handle even the unforeseen situations and events detected in the environment around the DE(s). As the number and diversity of devices that make up the individual QKDNs continue to grow, automating QKDN control and management tasks becomes ever-more important to improve the quality of services (QoS). To cope with the challenges of QKDN control and management, while minimizing human intervention towards full automation of QKDN, this draft Recommendation specifies the requirements and architectural model for AMC in QKDNs including the overview, requirements, consideration for cognition process and architectural model.	Draft

6.1.2 ITU-T Study Group 17

A landscape diagram for the QKDN standardization work in SG17 is illustrated in Figure 3. SG17 has the following work items on QKDN as listed in Table 2.

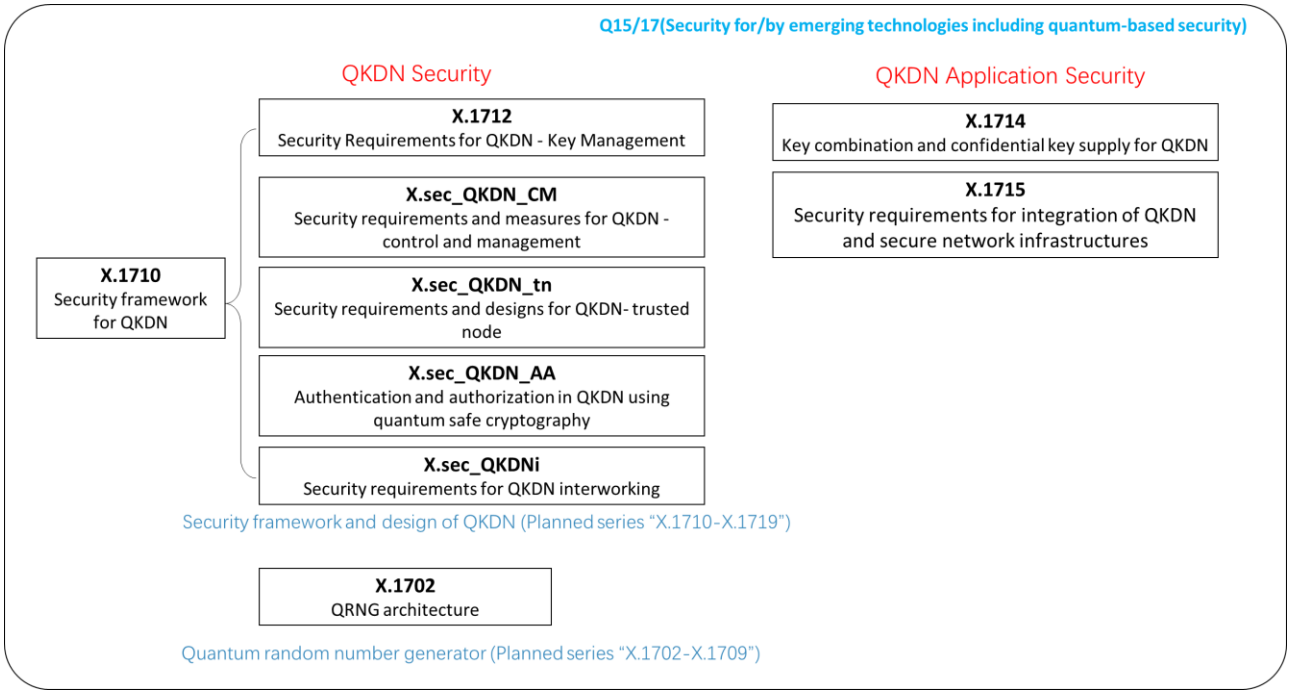

Figure 3: QKDN standardization work items in SG17

Table 2: QKDN related work items in ITU-T SG17

Name	Group	Title	Summary	Status
X.1710	Q15/17	Security framework for quantum key distribution networks	Recommendation ITU-T X.1710 specifies a framework of security threats, security requirements and security services for quantum key distribution networks (QKDNs). In this Recommendation, a simplified general structure of QKDN and the relevant security threats are specified. Then, on this basis, general security requirements and corresponding security capabilities and security functions are specified.	Approved (10/2020)
X.1712 Cor.1	Q15/17	Security requirements for quantum key distribution networks - key management	Recommendation ITU-T X.1712 specifies security requirements for key management in quantum key distribution networks (QKDNs). This Recommendation provides support for design, implementation, and operation of key management of QKDN with approved security. In this Recommendation, security objectives, security threats, security requirements for key management in the QKDN are identities and then it specifies methods and technical specifications of key management to meet the security requirements.	Approved (02/2022)
X.STR-SEC-QKD	Q15/17	Security considerations for quantum key distribution network	As a result of quantum computers threat, quantum safe cryptography is becoming increasingly important. Quantum key distribution (QKD) is a technology using quantum physics to secure the distribution of symmetric encryption keys which solves the problem of key distribution by allowing the exchange of a cryptographic key between two remote parties with information-theoretic security, guaranteed by the fundamental laws of physics. This key can then be used securely with conventional cryptographic algorithms. Post-quantum cryptography (PQC) refers to cryptographic algorithms which are resilient to attacks by the quantum computer. Some 'post-quantum' cryptographies, such as lattice-, code- or hash-based cryptosystems, are currently believed to be quantum-safe until proven otherwise. These two technologies, i.e., QKD and PQC are two pillars complementary to each other for quantum safe cryptography. QKD can be used as a key establishment alternative and QKD deployment is used to secure operators' backbone communications. PQC is a collection of cryptographic algorithms considered to be secure against quantum computer for end-point security. This Technical Report only studies the perspective of QKD. Although QKD technologies have been developed for several decades, there is a need to develop a QKD framework to satisfy requirements from the telecom network's perspective.	Agreed (03/2020)
X.1714	Q15/17	Key combination and confidential key supply for quantum key distribution networks	The present recommendation aims at specifying configurations of cryptographic functions used on a key generated in Quantum Key Distribution Networks for hybrid key exchange and confidential key supply.	Approved (10/2020)

X.sec-QKDN-tn	Q15/17	Security requirements and designs for quantum key distribution networks – trusted node	Quantum key distribution (QKD) enables two remote parties to share a common random binary key that is unknown to a potential eavesdropper. QKD network based on trusted nodes have been widely adopted to enlarge the key distribution distance and enrich QKD-based applications. The trustworthy concept of trusted node is a fundamental element to ensure the overall security in QKD network. The objective of this Recommendation is to provide the guide for implementation and operation securely of trusted nodes in QKD network. This Recommendation will identify the security threats and provide security requirements of trusted node, as well as specific techniques to meet the requirements.	Draft
TR.hyb-qkd	Q15/17	Overview of hybrid approaches for key exchangewith QKD	This Technical Report provides a landscape of the standardization activities on hybrid approaches for migration towards quantum-safe algorithms or protocols within international, regional and national organizations. The hybrid approaches that are covered by this technical report are for key exchange and authentication. Firstly, most of these standardization activities are envisioned and performed by experts in post-quantum cryptography. However, the compatibility of those published or under study standards with QKD has not been verified presently despite the fact that QKD protocols are also key exchange protocols. Nevertheless, the proposed hybrid approaches for key exchange might not be directly applicable to QKD based on existing standards. This Technical Report presents the possible way forward to accommodate QKD protocols in the context of the hybrid approaches for key exchange. This compatibility is studied for generic hybrid key exchange and hybrid key exchange specific to certain communication protocols. Secondly, QKD protocols need to exploit authentication mechanisms. In turn, hybrid approaches for authentication could allow the integration in QKD protocols of an authentication mechanism that is compatible with QKD security proofs and is recognized by security certification bodies. Finally, this Technical Report identifies the gaps in existing or on-going standardization works on hybrid approaches to make them usable with or useful for QKD protocols.	Agreed (05/2022)
X.sec_QKDN_AA	Q15/17	Authentication and authorization in QKDN using quantum safe cryptography	This Recommendation aims to study on authentication and authorization for QKDN. It also studies IDs and public key certifications in QKDN because they are essential elements for authentication and authorization. This new work item aims to study the following areas. IDs and their management in QKDN; Public key certification supported by PKI; Authentication and authorization in QKDN; This work item will fill the missing area of study on security of QKDN	Draft
X.sec_QKDN_CM	Q15/17	Security requirements and measures for quantum key distribution networks – control and management	This Recommendation specifies use cases, security threats in the context of quantum computing, security requirements and security measures for controllers and managers of QKDN. This draft Recommendation will refer the existing Recommendations and on-going draft Recommendations in SG13 and SG17 covering QKDN.	Draft
X.1715 (X.sec_QKDN_intrq)	Q15/17	Security requirements for integration of QKDN and secure network infrastructures	For quantum key distribution networks (QKDN), Recommendation ITU-T X.sec_QKDN_intrq specifies security requirements for integration of QKDN with various user networks (e.g., storage, cloud, sensor, content, etc.)	Approved (05/2022)

X.sec_QKDNi	Q15/17	Security requirements for Quantum Key Distribution Network interworking (QKDNi)	This Recommendation specifies the security requirements for QKDN interworking (QKDNi). In particular, the scope of this Recommendation includes: Security threats for QKDN Interworking (QKDNi); Security requirements for QKDNi including authentication and authorization aspects;	Draft

6.1.1 ITU-T Study Group 11

SG11 has the following work items on QKDN protocols, as listed in Table 1.

Table 1: QKDN related work items in ITU-T SG11

Name	Group	Title	Summary	Status
Q.QKDN_profr	Q2/11	Quantum key distribution networks – Protocol framework	Recommendation ITU-T Q.QKDN_profr specifies a framework for signalling requirements and protocols for quantum key distribution networks (QKDN).	Draft
Q.QKDN_Ak	Q2/11	Protocols for Ak interface for QKDN	Recommendation ITU-T Q.QKDN_Ak specifies protocols for Ak interface in quantum key distribution networks (QKDN).	Draft
Q.QKDN_Ck	Q2/11	Protocols for Ck interface for QKDN	Recommendation ITU-T Q.QKDN_Ck specifies protocols for Ck interface in quantum key distribution networks (QKDN).	Draft
Q.QKDN_Kq-1	Q2/11	Protocols for Kq-1 interface for QKDN	Recommendation ITU-T Q.QKDN_Kq-1 specifies protocols for Kq-1 interface in quantum key distribution networks (QKDN).	Draft
Q.QKDN_Kx	Q2/11	Protocols for Kx interface for QKDN	Recommendation ITU-T Q.QKDN_Kx specifies protocols for Kx interface in quantum key distribution networks (QKDN).	Draft

6.1.3 ITU-T Study Group 11

A landscape diagram for the QKDN standardization work in SG11 is illustrated in Figure 4. SG11 has the following work items on QKDN protocols, as listed in Table 3.

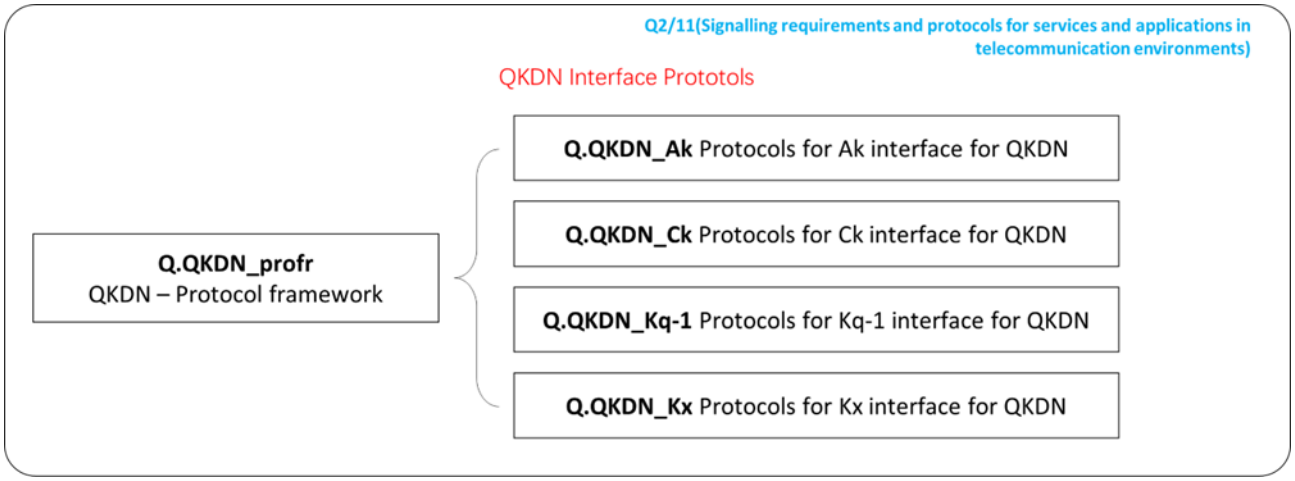

Figure 4: QKDN standardization work items in SG11

Table 3: QKDN related work items in ITU-T SG11

Name	Group	Title	Summary	Status

Q.QKDN_profr	Q2/11	Quantum key distribution networks – Protocol framework	Recommendation ITU-T Q.QKDN_profr specifies a framework for signalling requirements and protocols for quantum key distribution networks (QKDN).	Draft
Q.QKDN_Ak	Q2/11	Protocols for Ak interface for QKDN	Recommendation ITU-T Q.QKDN_Ak specifies protocols for Ak interface in quantum key distribution networks (QKDN).	Draft
Q.QKDN_Ck	Q2/11	Protocols for Ck interface for QKDN	Recommendation ITU-T Q.QKDN_Ck specifies protocols for Ck interface in quantum key distribution networks (QKDN).	Draft
Q.QKDN_Kq-1	Q2/11	Protocols for Kq-1 interface for QKDN	Recommendation ITU-T Q.QKDN_Kq-1 specifies protocols for Kq-1 interface in quantum key distribution networks (QKDN).	Draft
Q.QKDN_Kx	Q2/11	Protocols for Kx interface for QKDN	Recommendation ITU-T Q.QKDN_Kx specifies protocols for Kx interface in quantum key distribution networks (QKDN).	Draft

6.1.4 ITU-T FG-QIT4N

FG-QIT4N has the following work items on QKDN as listed in Table 4.

Table 2 QKDN related work items in ITU-T FG-QIT4N

Name	Group	Title	Summary	Status
Technical report on the ITU-T FG QIT4N D1.1	FG QIT4N	QIT4N terminology part 1: Network aspects of quantum information technology	This document studies the terminology on network aspects of quantum information technology during the lifetime of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N). This document mainly focuses on the survey of terminology. It will research the existing work about network aspects of quantum information technology related terminology from different Standards Development Organizations (SDOs), and study the overlap and divergence among those work, and summarize the terms that are needed but not yet defined. Efforts to fully prepare for the future input documents about relative terminology will be made according to this survey.	Agreed (11/2021)
Technical report ITU-T FG QIT4N D2.1	FG QIT4N	QIT4N Terminology Part 2: Quantum Key Distribution Networks	This document provides a survey on existing terminology lists relevant to QKDN that exist or are in preparatory phases, with identification of any gaps or opportunities that other efforts may have been overlooked.	Agreed (11/2021)
Technical report ITU-T FG QIT4N D1.2	FG QIT4N	QIT4N use case part 1: Network aspects of quantum information technology	This technical report sorts and analyses QIT for network use cases gathered during the lifetime of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N). The uses cases which are only applied by QIT are collected, investigated and summarized. All use cases will be analysed current bottleneck, application scenario, technical requirement and solution. This technical report will provide the analyses and suggestion for future application and potential standardization requirement.	Agreed (11/2021)

Technical report ITU-T FG QIT4N D2.2	FG QIT4N	QIT4N use case part 2: Quantum Key Distribution Network	This document consolidates the real-world QKDN use cases gathered during the lifetime of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N). The QKDN uses cases are classified into vertical and horizontal domains. And it also highlights the competitive advantage of use cases brought by QKDN, the main barriers to QKDN adoption, and the benefits and needs for future standardization efforts.	Agreed (11/2021)
Technical Report ITU-T FG QIT4N D2.3 part1	FG QIT4N	Quantum key distribution network (QKDN) protocols part 1: Quantum layer	This technical report studies and reviews protocols in the quantum layer of the quantum key distribution network (QKDN). This report mainly focuses on quantum key distribution (QKD) protocols in the quantum layer, where QKD is an essential part of the QKDN and is an emerging technology expected to strengthen the security of the current communication network. This technical report endeavours to give an overall review of the QKD protocols, including different types of QKD protocols, their workflows, protocol features, parameters, commercialization status, security proofs, potentials to be integrated in the future network etc. and discussions & suggestions on future plans.	Agreed (11/2021)
Technical Report ITU-T FG QIT4N D2.3 part2	FG QIT4N	Quantum key distribution network (QKDN) protocols part 2: Key management layer, QKDN control layer, and QKDN management layer	This technical report studies classical communication protocols in the quantum key distribution network (QKDN) which include protocols in the key management layer, QKDN control layer, and QKDN management layer. The QKDN protocols are classified into different layers according to main functions of each layer. Each protocol is discussed by giving necessary workflow or parameters.	Agreed (11/2021)
Technical report ITU-T FG QIT4N D2.4	FG QIT4N	QKDN transport technologies	This document discusses the typical scenarios of the co-fiber transmission of quantum key distribution and classic optical communication systems. Analysis about the impact of the classic optical light on the quantum signals is given. Furthermore, some co-fiber schemes are shown in the document, both for DV-QKD system and CV-QKD.	Agreed (11/2021)
Technical Report FG QIT4N D2.5	FG QIT4N	QIT4N standardization outlook and technology maturity part 2: quantum key distribution network	This technical report studies standardization outlook and technology maturity of the Quantum Key Distribution (QKD) network. In particular, the scope of this draft technical report includes: - Overview of QKDN technologies and industry development - Assessment of QKDN technologies maturity - QKDN standardization landscape and gap analysis - Outlook of QKDN standardization	Agreed (11/2021)

6.2 ETSI ISG-QKD

ETSI initiated the industry specification group (ISG) on QKD in 2008. ETSI ISG-QKD had published 9 specifications on QKD by 2019 and have several ongoing work items as listed in Table 5.

Table 3: QKD related work items in ETSI

Reference	Title	Status
GS QKD 002	Quantum Key Distribution (QKD); Use Cases	Published (2010-06)
GR QKD 003	Quantum Key Distribution (QKD); Components and Internal Interfaces	Published (2018-03)
GS QKD 004 V1	Quantum Key Distribution (QKD); Application Interface	Published (2010-12)
GS QKD 004 V2	Quantum Key Distribution (QKD); Application Interface	Published (2020-08)
GS QKD 005	Quantum Key Distribution (QKD); Security Proofs NOTE – Revision in progress	Published (2010-12)
GR QKD 007	Quantum Key Distribution (QKD); Vocabulary NOTE – Revision in progress	Published (2018-12)
GS QKD 008	Quantum Key Distribution (QKD); QKD Module Security Specification	Published (2010-12)
GS QKD 011	Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems	Published (2016-05)
GS QKD 012	Quantum Key Distribution (QKD); Device and Communication Channel Parameters for QKD Deployment	Published (2019-02)
GS QKD 014	Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API	Published (2019-02)
GS QKD 015	Quantum Key Distribution (QKD); Control Interface for Software Defined Networks Note: Revision in preparation ref. RGS/QKD-015ed2_ContIntSDN	Published (2021-03)
DGS/QKD-0010_ISTrojan	Quantum Key Distribution (QKD); Implementation security: protection against Trojan horse attacks in one-way QKD systems	Under development
DGS/QKD-0013_TransModChar	Quantum Key Distribution (QKD); Characterisation of Optical Output of QKD transmitter modules	Under development
DGS/QKD-016-PP	Quantum Key Distribution (QKD); Common Criteria Protection Profile for QKD	Under development
DGR/QKD-017NwkArch	Quantum Key Distribution (QKD); Network architectures	Under development
DGS/QKD-018OrchIntSDN	Quantum Key Distribution (QKD); Orchestration Interface of Software Defined Networks	Under development
DGS/QKD-020_InteropKMS	Quantum Key Distribution (QKD); Protocol and data format of REST-based Interoperable Key Management System API	Under development
DGR/QKD-019_AUTH	Quantum Key Distribution (QKD); Design of QKD interfaces with Authentication	Under development

6.3 ISO/IEC JTC 1/SC 27

ISO/IEC JTC 1/SC 27 initiated the study period "Security requirements, test and evaluation methods for quantum key distribution" in 2017.

In 2019, the study period was completed, and a new work item ISO/IEC 23837 (Part 1&2) was established as listed in Table 21.

Table 4: QKD related works items in ISO/IEC JTC1

Reference	Title	Status
ISO/IEC 23837-1	Security requirements, test and evaluation methods for quantum key distribution Part 1: requirements	Under development
ISO/IEC 23837-2	Security requirements, test and evaluation methods for quantum key distribution Part 2: test and evaluation methods	Under development

_____