INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2022-2024

SG13-TD22/WP3

STUDY GROUP 13

English only

Question(s): 16/13 Geneva, 4 - 15 July 2022

TD

Source: Editors

Title: Draft new Supplement ITU-T Y.supp.QKDN-roadmap: "Standardization roadmap on Quantum Key Distribution Networks" (output of e-meeting, 7-9 June 2022)

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

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

Keywords: Supplement, QKDN, roadmap

Abstract: This TD updates the status of work program of SG17 and FG-QIT4N related deliverables in the draft Supplement ITU-T Y.supp.QKDN-roadmap "Standardization roadmap on Quantum Key Distribution Networks".

The attached text is the output of Y.supp.QKDN-roadmap, based on the Q16/13 interim meeting, Incheon, 7-9 June 2022.

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

Standardization roadmap on Quantum Key Distribution Networks

Summary

Supplement Y.supp.QKDN-roadmap to ITU-T Y-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

1 Scope ... 3

2 References ... 3

3 Definitions ... 3

3.1 Terms defined elsewhere ... 3

3.2 Terms defined in this Supplement ... 4

4 Abbreviations and acronyms ... 4

5 Conventions ... 4

6 Quantum Key Distribution Networks ... 4

Appendix I Potential Work Items for Standardization on Quantum Key Distribution Networks ... 11

Bibliography ... 11

Draft new Supplement XX to ITU-T Y-series Recommendations

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

5 Conventions

None.

6 Quantum Key Distribution Networks

ITU-T

ITU-T SG13 has been developing core Recommendations on quantum key distribution networks as shown in Figure 7.1.

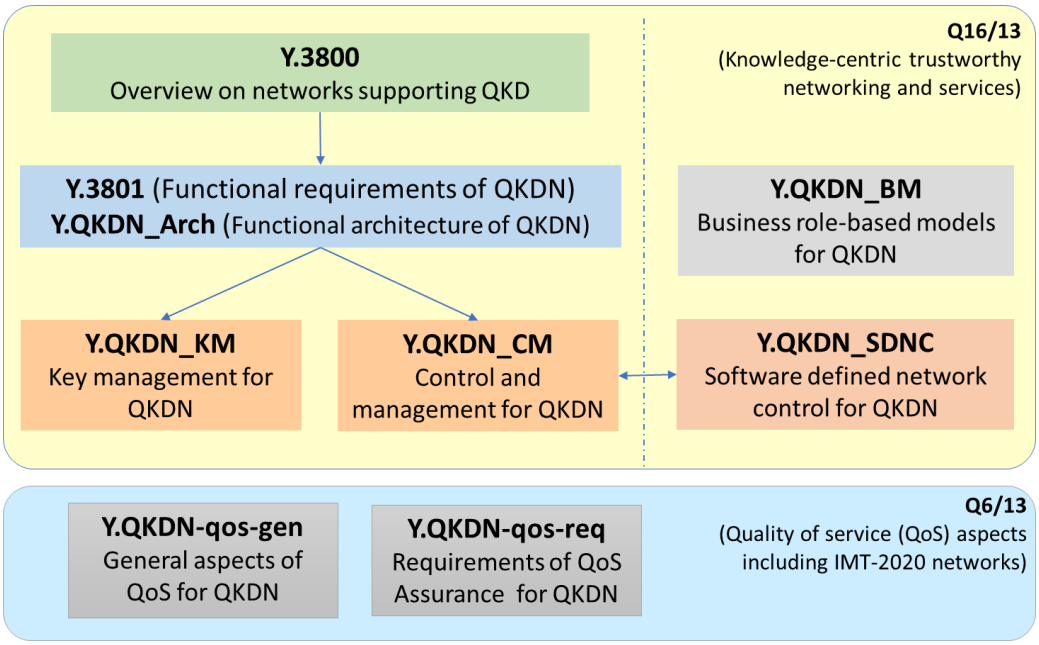

Figure 6.1 ITU-T (draft) Recommendations on quantum key distribution networks in SG13

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.QKDN-SDNC (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 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.	Consented 2021-07-16
Y.QKDN_BM	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.	Draft
Y.QKDN-qos-gen	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	Draft
Y.QKDN-iwfr	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.	Draft

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.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.1714	Q15/17	Key combination and confidential key supplyfor 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~~sec~~-qkd~~n~~	Q15/17	Overview of hybrid ~~security~~ approaches for key exchange ~~applicable to~~with 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.	~~Draft~~ 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.)	~~Draft~~Approved (05/2022)
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.	~~Draft~~Agreed (11/2021)
Technical report ITU-T FG QIT4N D2.1	FG QIT4N	QIT4N Terminology Part 2: Quantum Key Distribution Networks	-	~~Draft~~ 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.	~~Draft~~ 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.	~~Draft~~ 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.	~~Draft~~ 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.	~~Draft~~ 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.	~~Draft~~ 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	~~Draft~~ Agreed (11/2021)

Appendix I

Potential Work Items for Standardization on Quantum Key Distribution Networks

(Editors' note) This appendix should be updated based on the QKDN related activities.

1. Standardization roadmap and challenges

Bibliography

TBD

_____