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

Standardization roadmap on Quantum Key Distribution Networks

Summary

Supplement XX 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

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 trust technologies from an ITU-T perspective;

− The collection of related standards and publications on trust technologies in standards development organizations (SDOs).

2 References

TBD

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following term defined elsewhere:

3.1.1 **<Term 1>** [Reference]: <optional quoted definition>.

3.1.2 **<Term 2>** [Reference]: <optional quoted definition>.

TBD

3.2 Terms defined in this Supplement

None.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

TBD

5 Conventions

None.

6 Overview to trust technologies

6.1 Landscape of trust technologies from an ITU-T perspective

TBD

6.2 Related technical areas

7 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.

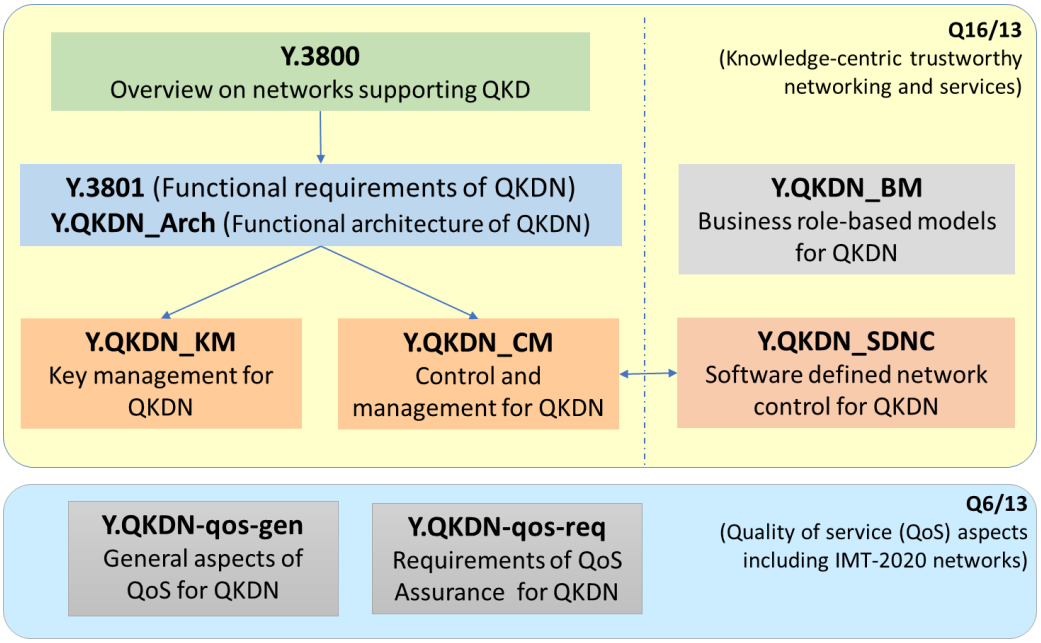

Figure 7.1 ITU-T (draft) Recommendations on quantum key distribution networks in SG13

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	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.	Draft
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

Technical Report TR.sec-qkd	Q4/17	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	Q4/17	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.sec-QKDN-km	Q4/17	Security requirements for quantum key distribution networks - key management	Recommendation ITU-T X.sec_QKDN_km 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.	Draft

X.1714	Q4/17	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	Q4/17	Security requirements 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
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
Technical report ITU-T FG QIT4N D2.1	FG QIT4N	QIT4N Terminology Part 2: Quantum Key Distribution Networks	-	Draft
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

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
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
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
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
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

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

_____

A.13 justification for new Y_supp-QKDN- roadmap "Standardization roadmap on Quantum Key Distribution Networks"

Question:	Q16/13	**Proposed new ITU-T Supplement**	Virtual, 5-16 July 2021	
Reference and title:	Y_supp-QKDN- roadmap "Standardization roadmap on Quantum Key Distribution Networks"			
Base text:	TD609/WP3		**Target date:**	2023-12
Editor(s):	Mark McFadden, DCMS, UK Zhangchao MA, CAS Quantum Network Co. Ltd, China		**Approval process:**	Agreement

Purpose and scope (defines what issue this non-normative document will address, thus permitting readers to judge its usefulness for their work; also defines the intent or objective of the non-normative document and the aspects covered, thereby indicating the limits of its applicability):

This draft Supplement includes the following items:

– A comprehensive list of activities related to QKDN within ITU-T;

– An overview of the relationship of the activities, including their status.

Summary (provides a brief overview of the proposal):

This supplement presents a comprehensive list of activities (work items) within the ITU-T associated with QKDN. The scope of the list includes both study groups and Focus groups. The list will reflect the status of the work item, as well as the date of approval.

This document will be updated periodically.

Relations to ITU-T Recommendations or other documents (approved or under development):

Liaisons with other study groups or with other standards bodies:

SG17, SG11, FG-QIT4N, ETSI ISG QKD, ISO/IEC JTC1/SC27, IRTF QIRG, CEN-CENELEC FG QT

Supporting members that are committing to contributing actively to the work item:

UK, Canada, Korea (Republic of), KT, Kaist, SK Telecom, QuantumCTek Co., Ltd., CAS Quantum Network Co., Ltd.

_____