A.1 justification for proposed draft new ITU-T Y.QKDN-nq-rf, "Quantum key distribution networks – Requirements and framework for end-to-end QKDN and non-quantum cryptographies services"

Question:	Q16/13	**Proposed new ITU-T Recommendation**	Geneva, 23 Oct - 3 Nov 2023
Reference and title:	ITU-T Y.QKDN-nq-rf, "Quantum key distribution networks – Requirements and framework for end-to-end QKDN and non-quantum cryptography services"		
Base text:	TD411/WP3	**Timing:**	2025, March
Editor(s):	Taesang Choi, ETRI; Jeongyun Kim; ETRI; Hyeongsoo Kim, KT; Gyumyung Lee, KAIST; Qingcheng Zhu, BUPT; Yongli Zhao, BUPT; Guosheng Zhu, Wuhan Rayton Network Technology	**Approval process:**	AAP

Scope (defines the intent or object of the Recommendation and the aspects covered, thereby indicating the limits of its applicability):

This draft Recommendation specifies use cases, architectural models, high-level, functional requirements, and a framework for end-to-end quantum key distribution network (QKDN) and non-quantum cryptography (NQC) services. In particular, the scope of this Recommendation includes:

- Introduction of end-to-end QKDN and NQC services;
- Use cases of QoS assurance for end-to-end QKDN and NQC services;
- Architectural models for end-to-end QKDN and NQC services;
- High-level requirements of end-to-end QKDN and NQC services;
- Functional requirements of end-to-end QKDN and NQC services.

Summary (provides a brief overview of the purpose and contents of the Recommendation, thus permitting readers to judge its usefulness for their work):

In order to support QKD service to IMT-2020 users including mobile objects (i.e., autonomous car, mobile phone, etc.), it is challenging to establish and maintain a quantum channel stably with them and supporting KSA-keys. TR-QKDN-nq addresses these issues and describes several use cases to deliver KSA-keys generated from QKD networks to the IMT-2020 user applications by means of modern cryptography (e.g., PKI technology) with PQC algorithms. It also identifies various issues to be addressed for standardization. Implications include end-to-end three use cases related issues, control and management, and QoS aspect.

This draft Recommendation specifies use cases, architectural models, high-level and functional requirements for end-to-end QKDN and non-quantum cryptography (NQC) services.

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

ITU-T Y.3804 "Quantum Key Distribution Networks - Control and Management"

ITU-T Y.3805 "Quantum Key Distribution Networks – Software defined networks control"

ITU-T Y.3814 "Quantum Key Distribution Networks – functional requirements and architecture for machine learning enablement"

ITU-T X.1714 "Key combination and confidential key supply for quantum key distribution networks"

ITU-T X.509 (2019) "The Directory; Public-key and attribute certificate frameworks"

ITU-T TR-QKDN-nq "ITU-T's Views for Quantum-Enabled Future Networks"

ITU-T TR.hyb_qsafe "Overview of key management of hybrid approaches for quantum-safe communications"

Liaisons with other study groups or with other standards bodies:

ITU-T SG17, ETSI ISG-QKD, IETF

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

ETRI, KT corp., KAIST, Korea Univ., and Korea (Rep. of), BUPT, Wuhan Rayton Network Technology

Annex B: Proposed initial draft of Y.QKDN-qos-nq-rf

Initial draft Recommendation ITU-T Y.QKDN-qos-nq-rf

Requirements and framework for end-to-end QKDN and non-quantum cryptography services

Summary

In order to support QKD service to IMT-2020 users including mobile objects (i.e., autonomous car, mobile phone, etc.), it is challenging to establish and maintain a quantum channel stably with them and supporting KSA-keys. TR-QKDN-nq addresses these issues and describes several use cases to deliver KSA-keys generated from QKD networks to the IMT-2020 user applications by means of modern cryptography (e.g., PKI technology) with PQC algorithms. It also identifies various issues to be addressed for standardization. One of them is an implication on the end-to-end QoS assurance.

This draft Recommendation specifies use cases, architectural models, high-level and functional requirements for end-to-end QKDN and non-quantum cryptographies (NQC) services.

Keywords

end-to-end QKDN and NQC services, QKD (quantum key distribution), QKDN (QKD network), quality of service assurance.

Table of Contents

Initial draft Recommendation ITU-T Y.QKDN-qos-nq-rf

Requirements and framework for end-to-end QKDN and non-quantum cryptography services

Scope

This draft Recommendation specifies use cases, architectural models, high-level, functional requirements, and a framework for end-to-end quantum key distribution network (QKDN) and non-quantum cryptography (NQC) services. In particular, the scope of this Recommendation includes:

- Introduction of end-to-end QKDN and NQC services;
- Use cases for end-to-end QKDN and NQC services;
- Architectural models for end-to-end QKDN and NQC services;
- High-level requirements for end-to-end QKDN and NQC services;
- Functional requirements for end-to-end QKDN and NQC services.

1 References

[ITU-T Y.3804] Recommendation ITU-T Y.3804 “Quantum Key Distribution Networks - Control and Management”

[ITU-T Y.3805] Recommendation ITU-T Y.3805 “Quantum Key Distribution Networks – Software defined networks control”

[ITU-T Y.3814] Recommendation ITU-T Y.3814 “Quantum Key Distribution Networks – functional requirements and architecture for machine learning enablement”

[ITU-T X.1714] Recommendation ITU-T X.1714 “Key combination and confidential key supply for quantum key distribution networks”

[ITU-T X.509] Recommendation ITU-T X.509 (2019) “The Directory; Public-key and attribute certificate frameworks”

2 Definitions

2.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 **assurance** [b-ITU-T X.1500]: The degree of confidence that the process or deliverable meets defined characteristics or objectives.

3.1.2 **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.

3.1.3 **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.

2.2 Terms defined in this Recommendation

None.

3 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

QKD	Quantum Key Distribution
QKDN	QKD Network

4 Conventions

In this Recommendation:

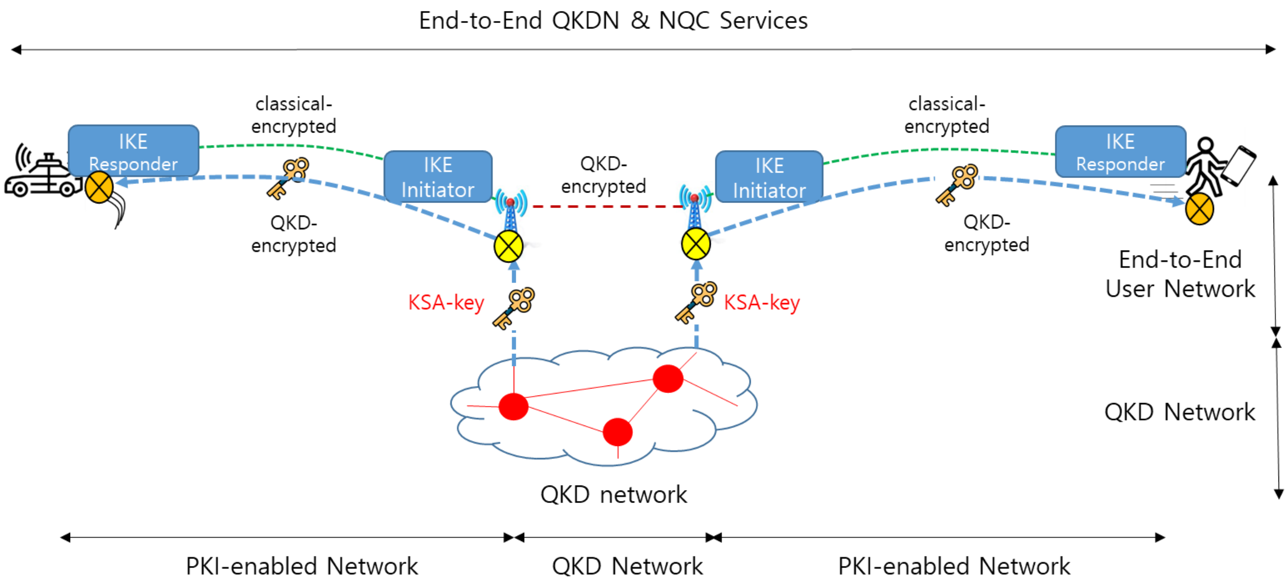
The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

5 Introduction

In order to support QKD service to IMT-2020 users including mobile objects (i.e., autonomous car, mobile phone, etc.), it is challenging to establish and maintain a quantum channel stably with them and supporting KSA-keys. TR-QKDN-nq addresses these issues and describes several use cases to deliver KSA-keys generated from QKD networks to the IMT-2020 user applications by means of modern cryptography (e.g., PKI technology) with PQC algorithms. It also identifies various issues to be addressed for standardization. Implications include end-to-end three use cases related issues, control and management, and QoS aspect.

This draft Recommendation specifies use cases, architectural models, high-level and functional requirements for end-to-end QKDN and non-quantum cryptographies (NQC) services. Figure 1 illustrates end-to-end QKDN and NQC services.



<Figure 1. End-to-end Integrated QoS assurance of QKND and NQC>

6 Use cases for end-to-end QKDN and NQC services

7 Architectural models for end-to-end QKDN and NQC services

8 High-level requirements for end-to-end QKDN and NQC services

9 Functional requirements for end-to-end QKDN and NQC services;

10 Security Consideration