INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2022-2024

SG13-TD311/WP3

STUDY GROUP 13

Original: English

Question(s): 16/13

Geneva, 26 July 2023

TD

Source: Editor

Title: Draft Technical Report ITU-T TR.QKDN-nq:“Overview for integration of quantum key distribution network with non-quantum cryptographies” (output of interim meeting, 17-21 July 2023)

Contact: Hyungsoo KIM
KT corp.
Korea

Tel: +82-10-6808-5199
E-mail: hans9@kt.com

Abstract: This document describes the revised output of Draft Technical Report ITU-T TR-QKDN-nq:“Overview for integration of quantum key distribution network with non-quantum cryptographies” in July interim meeting of Q.16.

This document is based on this meeting's discussion and results on the following contributions:

No.	Title	Source
TD271/WP3	Output of Draft Technical Report ITU-T TR.QKDN-nq: "Overview for integration of quantum key distribution network with non-quantum cryptographies" (output of Q16/13 meeting, Seoul, 7-12 June 2023)	Editor
C-138	Proposed revision of Draft Technical Report ITU-T TR.QKDN-nq: “Overview for integration of quantum key distribution network with non-quantum cryptographies”	KT corp.
C-139	Proposed revision of Clause 8 of Draft Technical Report ITU-T TR.QKDN-nq: “Overview for integration of quantum key distribution network with non-quantum cryptographies”	ETRI, KT corp.
C-140	Proposed text for QoS implications of TR.QKDN-nq	ETRI
C-141	Proposal of supplementing clauses 6 and 8.2 for the integration with non-quantum cryptography on TR.QKDN_nq “Overview for integration of quantum key distribution network with non-quantum cryptographies”	BUPT

Annex

Draft new Technical Report TR.QKDN-nq

Overview for integration of quantum key distribution network with non-quantum cryptographies

[Editor's Note] Terminologies; PKI & Classical should be carefully introduced for their implications.

Summary

Based on ITU-T Recommendation Y.3800, many study items are successfully developed and developing so far. However, in case that mobile objects (i.e., autonomous car, mobile phone, etc.) are to be supplied QKD service, there is a difficulty to establish and maintain a quantum channel stably with them. KSA-keys are not able to be supported on this situation.

For the purpose of delivery of KSA-keys generated from QKD network into the mobile objects, the keys can be delivered through user network using PKI technology (especially key exchange protocol) with PQC algorithm.

Therefore, the integration of QKD network with non-quantum cryptography will enable the QKD network/service providers, bringing its cryptography service to a much wider range of business opportunity.

For this purpose, the relationship between QKDN and E2E cryptography service will be introduced. Then, relative ~~examples~~ use cases for the integration of QKD network with non-quantum cryptography will be described. Finally, based on the analysis of the detailed attributes of examples, implications in terms of further study issue will be identified.

- QKDN's relation to end-to-end cryptography service
- ~~Examples~~ Use Cases for the integration with non-quantum cryptography (e.g., PKI architecture)
- Implications for standardization activity on Study Group 13

Keywords

Quantum Key Distribution; QKD network; PKI architecture, ~~Service Scenario~~, Use Case.

Table of Contents

Page

Draft new Technical Report TR.QKDN-nq

Overview for integration of quantum key distribution network with non-quantum cryptographies

1 Scope

This Recommendation provides the overview for integration of quantum key distribution network with non-quantum cryptographies under three categories as follows:

- QKDN's relation to end-to-end cryptography service
- ~~Examples~~ Use Cases for the integration with non-quantum cryptography (e.g., PKI architecture)
- Implications for standardization activity on Study Group 13

2 References

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

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

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

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 key supply agent-key (KSA-key) [ITU-T Y.3803]: Key data stored and processed in a key supply agent (KSA), and securely shared between a KSA and a matching KSA.

3.1.2 public-key infrastructure (PKI) [ITU-T X.509]: The infrastructure able to support the management of public keys able to support authentication, encryption, integrity or non-repudiation services.

3.1.~~1~~3 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.

3.2 Terms defined in this Technical Report

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

E2E End To End

IKE Internet Key Exchange

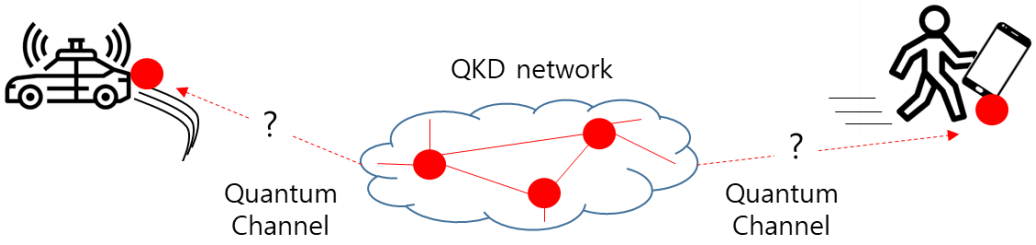
IT-secured Information Theoretically-secured

KpqC	Korean Post Quantum Cryptography
KSA-key	Key Supply Agent-key
NIST	National Institute of Standards and Technology
PAT	Pointing, Acquisition and Tracking
PKI	Public Key Infrastructure
PQC	Post Quantum Cryptography
QKD	Quantum Key Distribution
QKDN	Quantum Key Distribution Network
TLS	Transport Layer Security

5 Introduction

Based on ITU-T Recommendation Y.3800, many study items are successfully developed and developing so far. However, in case that mobile objects (i.e., autonomous car, mobile phone, etc.) are to be supplied QKD service, there is a difficulty to establish and maintain a quantum channel stably with them, for the purpose of KSA-keys delivery.

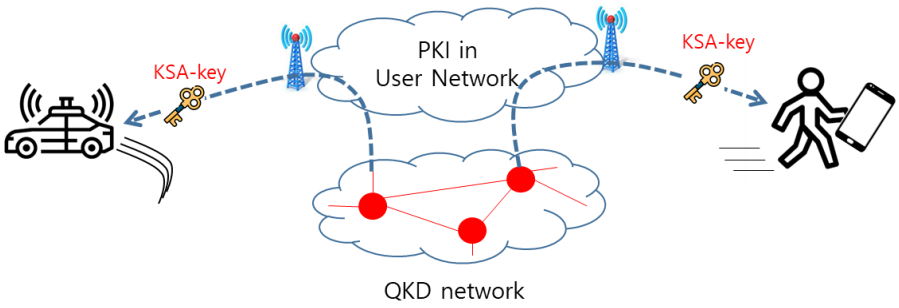
Even though PAT (Pointing, Acquisition and Tracking) technology are combined with QKD modules, it is expected that the required accuracy for the quantum channel is not able to be achieved, due to the unpredictability of the movement and corresponding position of the mobile objects. It means that QKD network cannot support standalone the end-to-end cryptography service between the car and the mobile phone on this situation.



<Figure 1. An example of QKD network in the mobile object environment >

PKI in user network is considered as a market-oriented security aspect for the extension of QKD service. The combination between key generation/distribution of QKD network and other PKI (Public-key Infrastructure)-related functions are essential in user network.

In order to overcome the difficulty for the mobile objects, some additional functions for existing cryptography architecture can be used. For the purpose of delivery of KSA-keys generated from QKD network into the mobile objects, the keys can be delivered through user network with PKI technology (especially key exchange protocol), instead of the extension of quantum channel.



<Figure 2. KSA-key delivery through PKI in user network>

However, this approach makes a problem against quantum computer's attack, since cryptographic algorithms in existing PKI architecture are known as non-quantum safe. To address Quantum-safe, overhauling existing PKI architecture is required as existing algorithms become obsolete.

Fortunately, some ongoing standardisation projects such NIST PQC (Post Quantum Cryptography) and KpqC (Korean PQC) are currently aimed to standardise a set of post-quantum secure encryption/key exchange algorithms and digital signature algorithms.

Note - The study of PQC is out of scope of this document.

From this point of view, it is recommended that the integration of QKD network and PKI with PQC algorithm should be studied for the extension of QKD service availability and market penetration for QKD service provider. Considering this study is just one of possibilities, other possible approaches should be studied as well. In addition to those approaches, architecture and functional requirements can be further studied.

As a conclusion, the integration of QKD network with non-quantum cryptography will enable the QKD network/service providers, bringing its cryptography service to a much wider range of business opportunity.

6 QKDN's relation to end-to-end cryptography service

~~<TBD>~~

Figure 3 shows the QKDN's relation to end-to-end cryptography service. The end-to-end cryptography service requires cryptographic keys for the end-to-end encryption of messages between two end users. QKDN provides a secure way of establishing symmetric keys between two users for end-to-end data encryption. E2E encryption which helps prevent data breaches and cyber attacks is important for data security and privacy, especially for sensitive and confidential information, such as business documents, financial details and medical conditions. Figure 3 shows the QKDN's relation to end-to-end cryptography service. The end-to-end encryption can be realized between the cryptographic applications in the user network by applying QKDN or applying the integration of QKDN and non-quantum cryptographies.

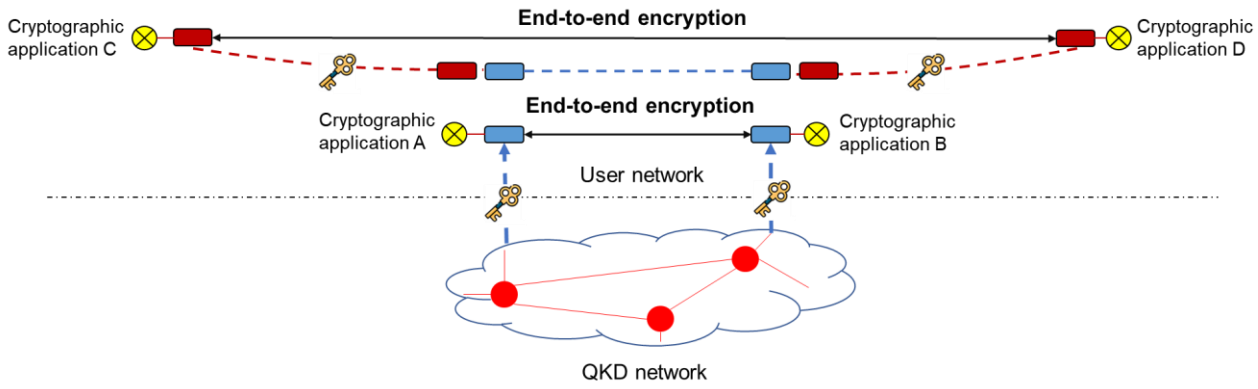


Figure 3. QKDN's relation to end-to-end cryptography service.

Figure 3 of ITU-T Recommendation Y.3800 shows a relation between 3 layers in QKDN and a service layer in User Network. The service for QKD technology in service layer is a cryptography service which is encrypted and decrypted by symmetric KSA-keys from QKDN; QKD-encrypted. On the other hand, PKI architecture can be introduced in service layer as well. The service is encrypted and decrypted with classical asymmetric cryptographic keys from modern cryptographic module; ~~PKI~~ Classical-encrypted.

Note: How to generate and distribute cryptographic keys is out of scope in this Technical Report.

From modern cryptographic technology's perspective, 3 types of cryptographic service are possible. They are E2E QKD-encrypted, E2E ~~PKI~~ Classical-encrypted and Integrated QKD- & PKI-encrypted. In the type of E2E QKD-encrypted, QKDN should covers whole coverage of cryptographic service in User Network and this example is the basic assumption of ITU-T Recommendation Y.3800-series. And the other type, E2E ~~PKI~~ Classical-encrypted, has been specified in many modern cryptographic technology-related ITU Recommendations and other SDOs standards including ITU-T Recommendation X.509.

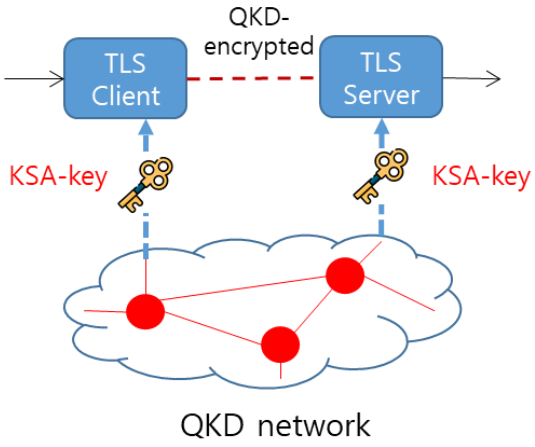
However, the type of Integrated QKD- & ~~PKI~~ Classical-encrypted is not specified in terms of how to design, deploy, operate and maintain. The relevant aspects for use cases and implications for further standardization activity are within the scope of this Technical Report to support its implementation.

7 ~~Examples~~ ~~Use Cases~~ for the integration with non-quantum cryptography

~~Editor's note – Two terminologies, QKD-encrypted and PKI-encrypted, should be identified.~~

7.1 Vertical integration; E2E QKD-encrypted model

In this ~~example~~ use case, KSA-keys generated from QKD network supply to TLS (Transport Layer Security) client and server symmetrically. TLS communication between client and server can be encrypted and decrypted thorough the keys. Therefore a public-key exchange procedure may not be required, during the initiation process, so called TLS handshake.



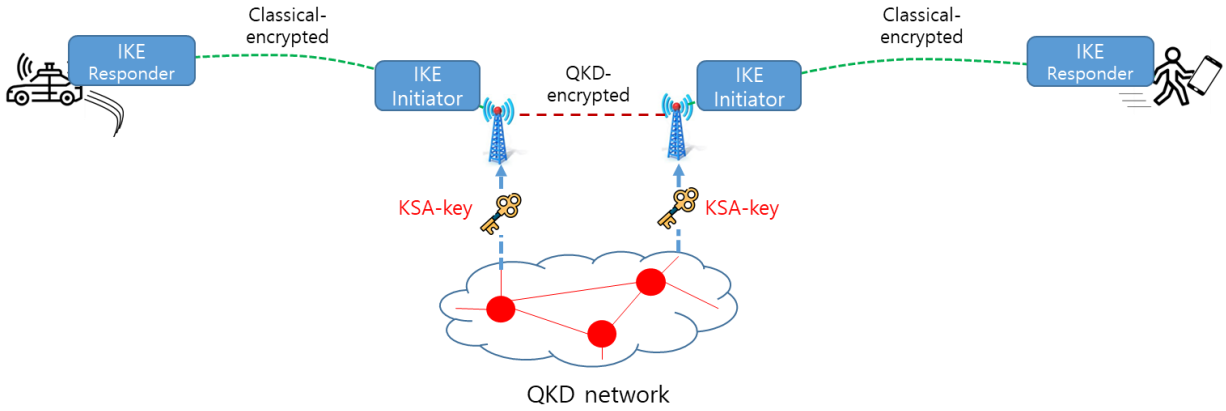
<Figure 3. ~~Example~~ Use case of integration between QKDN and TLS protocol>

NOTE 1 – It is assumed that TLS client/server and QKD module/key manger are located in the same trusted node together. Based on this assumption, the delivery connectivity from QKDN to TLS functions is considered to be IT-secured.

NOTE 2 – Figure 3 of ITU-T Recommendation Y.3800 specifies illustration of the conceptual structures of a QKDN and a Use Network. But, in this figure, cryptographic application is not a part of Trusted Node in align with QKD network.

7.2 Horizontal integration; Concatenated combination of QKD-encrypted and ~~PKI~~ Classical-encrypted model

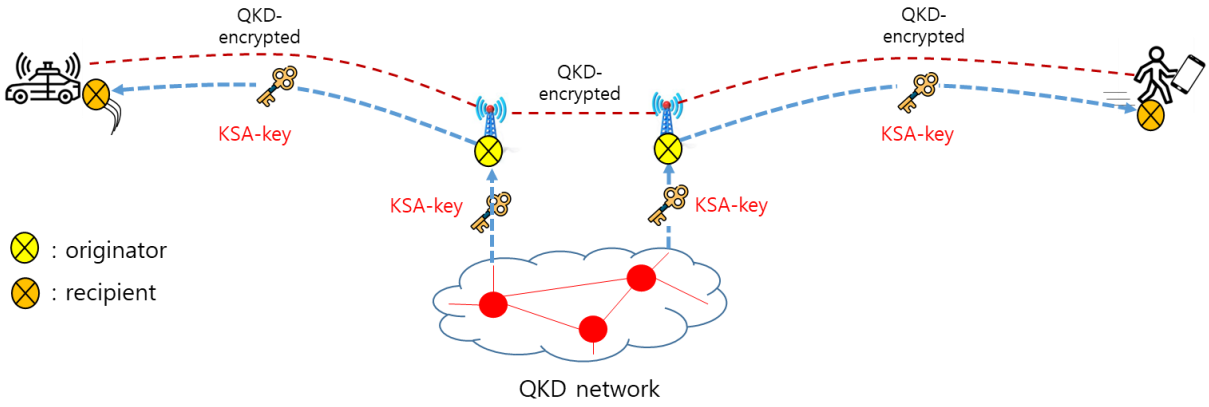
In this ~~example~~ use case, KSA-keys generated from QKD network supply only to the corresponding portion for QKD-encrypted. The other end portions are encrypted by the cryptographic keys derived from ~~PKI~~ Classical cryptography, IKE protocol.



<Figure 4. ~~Example~~ Use case of concatenation of QKDN and PKI>

7.3 Horizontal integration; E2E QKD-encrypted model

In this ~~example~~ use case, KSA-keys generated from QKD network supply to the corresponding portion. Then the keys delivers to the both ends of connectivity through key exchange function of ~~PKI~~ Classical cryptography. The communication between both ends can be QKD-encrypted by the received KSA-keys.



NOTE – The terminology of originator and recipient are derived from ITU-T Recommendation X.509 (2019)

<Figure 5. ~~Example~~ Use case of concatenation of QKDN and PKI>

8 Implications for standardization activity on Study Group 13

8.1 General Implications for standardization activity

8.1.1 Vertical integration-related

If the TSL client/server and QKD module/Key Manager are not located in the same Trusted Node together, the connectivity from QKD network to TLS functions (e.g. Ak interface for QKDN in ITU-T draft Recommendation Q.QKDN_Ak and ETSI GS QKD 014 interface) should be secured. It is required to be applied PKI cryptography with PQC algorithm against quantum computing attack.

Also Public key generation and exchange procedure in TLS protocol can be removed, but new interface and procedure for receiving KSA-keys from QKD network are required.

NOTE – TLS is just one of non-quantum cryptography protocols integrated with QKD network in this clause. IKE is also taken into account for this purpose. But, details of those further study are out of scope of this document.

8.1.2 Horizontal integration-related

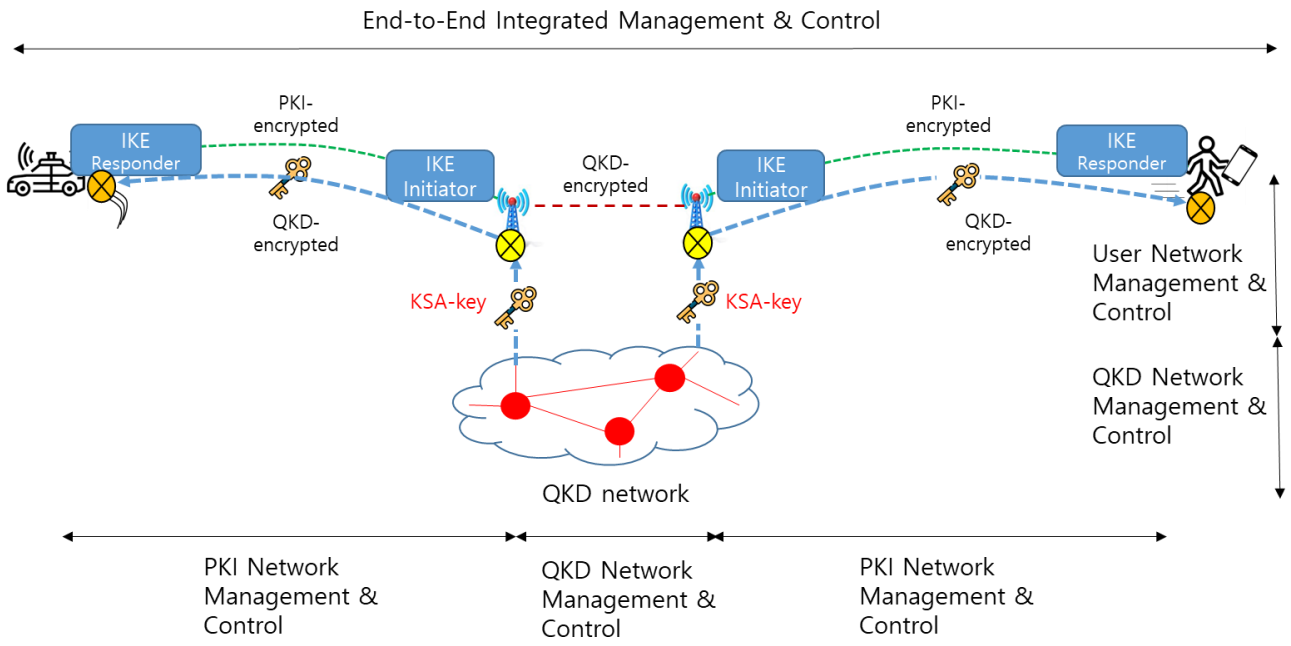
In case of concatenated combination model, there is no specific technical consideration points. But the security threat into physical concatenation between QKD- and ~~PKI~~ Classical -encrypted connectivity might be further studied.

In case of E2E QKD-encrypted model, ~~PKI~~ Classical cryptography should take into account KSA-keys as one of keys to be exchanged between originator and recipient. Relative additional interface and procedure between QKD network and ~~PKI~~ Classical cryptography could be required.

In order to seamless procedure, the originator can be implemented in a part of QKD network, especially in KM layer. Then E2E QKD-encrypted communication can be achieved between both ends without additional interface and procedure.

8.1.3 Management and control implications of vertical and horizontal Integration

The integration of QKD network and PKI with PQC algorithms introduces some management and control implications. QKDN management and control architecture defines QKDN related management and control capabilities and PKI also provides its own management and control functionality. In order to guarantee the quality of key delivery across the integrated environment, cooperation of management and control capabilities needs to be supported. The specific capabilities and reference point extensions for the optimal integration need to be further studied. Figure 6 illustrates the boundary and role of management and control in the integrated environment.



<Figure 6. The boundary and role of management and control in the integrated environment>

8.1.4 QoS aspect

From the QKDN QoS perspective, [ITU-T Y.3806] specifies the requirements including QoS planning, QoS monitoring, QoS optimization, QoS provisioning, QoS protection and recovery. In addition, [ITU-T Y.3807] describes QoS and network performance (NP) on QKDN and specifies the associated relative parameters for QoS and their definitions. Finally, [ITU-T Y.3811] specifies the functional architecture of QoS assurance and basic operational procedures for QKDNs. With these Recommendation, the QKDN QoS is well addressed in terms of only QKDN, not considering user networks and end-devices. The cryptographic applications can be end-devices.

On the other hand, there are several types of use network, which means non-quantum network, and the Recommendations for user network QoS are addressed. For example, [ITU-T Y.1540] defines the parameters that may be used in specifying and assessing the performance of speed, accuracy, dependability and availability of IP packet transfer of IP data communication services. [ITU-T Y.3106] specifies the QoS requirements for the IMT- 2020 network.

When ~~the Quantum~~ KSA-key is delivered between two cryptographic applications, it passes through both QKDN and user network. Otherwise, the encrypted data goes through the user network. Figure 7 shows end-to-end QoS domain for cryptographic applications. In order to support end-to-end QoS, two types of QoS are considered in choosing a path between the cryptographic applications. Therefore, the QoS coordination and mapping are necessary between QKDN and user network.

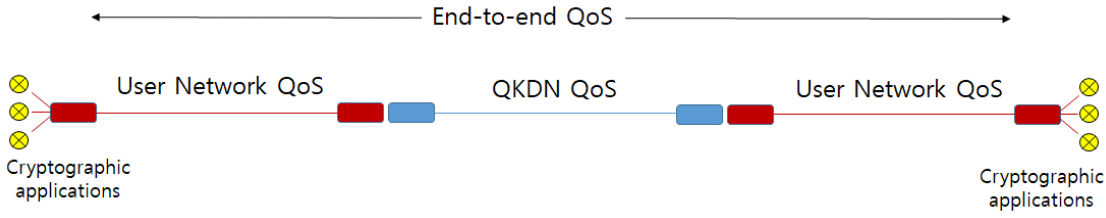


Figure 7. End-to-end QoS domain for cryptographic applications

8.2 Implications for Study Group 13

~~*TBD*~~

8.2.1 Secure delivery of KSA-keys from QKDN to User Network

The trusted node in each ends of Figure 3/Y.3800 should be extended covering cryptographic applications in User Network. Otherwise, it should be informed with other ITU-T SGs and SDOs that Ak interface between QKDN and User Network should be secured (i.e., ~~PKI~~ Classical cryptography with PQC algorithm-based).

8.2.2 Hybrid management and control capabilities between QKDN and User Network

Management and control capabilities associated with safe and reliable end-to-end key delivery need to be studied in Q.16 and Q.6 of SG13. Since Q.16 is responsible for QKDN control and management, the integrated management and control can be under its responsibility. And QoS control and management for integrated end-to-end QKD can be studied in Q.6. Management and control in the integrated environment may need support of the PKI management.

8.2.3 Quality of service for the integration of QKDN and non-quantum cryptographies.

From end-to-end QoS assurance, it is considered how the QoS coordination and mapping are performed and what the impact to existing Recommendations are. ~~Therefore, further study on QoS issues is necessary.~~

~~QoS assurance aspects are important in QKDNs.~~ Due to the different QoS assurance ways of QKDN and non-quantum cryptographies, as well as the various cryptography services, it is challenging to assure the end-to-end QoS for the QKD-encrypted and classical-encrypted services under the integration of QKDN and non-quantum cryptographies. Q6 in SG13 focuses on the QoS aspects related to QKDNs. It is suitable to study the end-to-end QoS assurance for the integration of QKDN and non-quantum cryptographies, such as the overview, QoS assurance requirements, QoS parameters and QoS assurance architecture.

Bibliography

~~*TBD*~~

[b-ETSI GR QKD 007] ETSI Group Report QKD 007 V1.1.1 (2018), *Quantum key distribution (QKD); Vocabulary*

[b-IETF RFC 8446] IETF RFC 8446 (2018), *The Transport Layer Security (TLS) Protocol Version 1.3*

[b-IETF RFC 4306] IETF RFC 4306 (2005), *Internet Key Exchange (Kev2) Protocol*

_____