INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2022-2024

SG13-TD339/WP1

STUDY GROUP 13

Original: English

Question(s):	6/13	Geneva, 13 - 24 March 2023

TD

Source:	Editors
Title:	Draft new Recommendation ITU-T Y.QKDN-qos-iw-req: “Requirements of QoS assurance for QKDN interworking”

Contact:	Jeongyun Kim ETRI Editors	Tel:+82-42-860-5311 Fax: +82-42-860-6405 Email: jykim@etri.re.kr
Contact:	Taesang Choi ETRI Editors	Tel:+82-10-2740-5628 Fax: +82-42-860-6405 Email: choits@etri.re.kr
Contact:	Hyungsoo Kim KT corp. Editors	Tel:+82-10-6808-5199 Fax: +82-2-526-6306 Email: hans9@kt.com
Contact:	Chun-Seok YOON KT corp. Korea (Rep. of)	Tel: +82-10-9383-6351 Fax: +82-2-526-6306 E-mail: chuck.yoon@kt.com

Abstract: This draft new Recommendation ITU-T Y.QKDN-qos-iw-req is revised based on C-466 at SG13 meeting March 2023, which propose high-level and functional requirements of QoS routing.

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

No.	Title	Source	Discussion
C-466	Y.QKDN-qos-iw-req: update of requirements	ETRI	Accepted with minor modification - Latency is changed to KKRD (KSA-key Response Delay) - Two QKD nodes are replaced to Sending and receiving QKD nodes - Regarding terms about path and route, Editor's Note is added

Draft new Recommendation ITU-T Y.QKDN-qos-iw-req

Requirements of QoS assurance for QKDN interworking

Summary

This draft recommendation specifies the high-level and functional requirements of QoS assurance for quantum key distribution networks (QKDN) interworking.

Keywords

QKDN interworking; QoS assurance, requirements;

Table of Contents

Draft new Recommendation ITU-T Y.QKDN-qos-iw-req

Requirements of QoS assurance for QKDN interworking

1. Scope

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;

Editor’s Note: This draft Recommendation plans to work on the requirements first, and if possible, whether to start work on the framework will be depend on the work progress of architecture for QKDN interworking in Q16/13.

2. References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T E.417] Recommendation ITU-T E.417 (2005), *Framework for the network management of IP-based networks*.

[ITU-T P.10] Recommendation ITU-T P.10/G.100 (2017), *Vocabulary for performance and quality of service*.

[ITU-T Q.1741.9] Recommendation ITU-T Q.1741.9 (2015), *IMT-2000 references to Release 11 of GSM evolved UMTS core network.*

[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.QKDN_Arch] Draft Recommendation ITU-T Y.QKDN_Arch (2020), *Functional architecture of quantum key distribution networks*.

[ITU-T Y.QKDN_KM] Draft Recommendation ITU-T Y.QKDN_KM (2020), Key management for quantum key distribution networks.

[ITU-T Y.QKDN_CM] Draft Recommendation ITU-T Y.QKDN_CM (2020), Control and management for quantum key distribution networks.

[ITU-T Y.QKDN_qos_gen] Draft Recommendation ITU-T Y.QKDN_QOS_GEN (2020), General aspects of QoS on quantum key distribution networks.

[ITU-T Y.QKDN_qos_req] Draft Recommendation ITU-T Y.QKDN_QOS_REQ (2020), Requirements of QoS assurance for quantum key distribution networks.

3. Definitions

3.1 Terms defined elsewhere

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

3.1.2 network performance [ITU-T E.417]: The performance of a portion of a telecommunications network that is measured between a pair of network-user or network-network interfaces using objectively defined and observed performance parameters.

3.1.3 quality of experience [ITU-T P.10]: The degree of delight or annoyance of the user of an application or service. [b-Qualinet2013]

NOTE – Recognizing on-going research on this topic, this is a working definition which is expected to evolve for some time. (This note is not part of the definition.)

3.1.4 quality of service [ITU-T Q.1741] : The collective effect of service performances, which determine the degree of satisfaction of a user of a service. It is characterized by the combined aspects of performance factors applicable to all services, such as: service operability performance; service accessibility performance; service retainability performance; service integrity performance; and other factors specific to service.

3.2 Terms defined in this Recommendation

None.

4. Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

QoE	Quality of Experience
QoS	Quality of Service
QKDN	Quantum key distribution networks

5. 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 Recommendation 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.

6. Overview

The QKDN is expected to be able to provide optimized support for a variety of different QKD services. From a viewpoint of the application in the service layer, sending quantum keys and relevant information will be called as QKDN services. In order to provide QKDN services as same as applications want, the end-to-end QoS assurance and interoperability between transmitting and receiving QKD nodes (including QKD module and QKD link) are provided.

Security level and key supply service policy can be different between transmitting and receiving QKD nodes, especially in terms of QoS assurance. Different information of Quantum key can be applied to transmitting and receiving QKD nodes. In addition, status information of QKD nodes such as QBER, key rate, QKD link status, alarm on fault should be exchanged in order to support QoS assurance.

The one of the challenges of the QKDN is to assure the network performance [ITU-T E.417] and different quality of service (QoS) [ITU-T Q.1741]/quality of experience (QoE) [ITU-T P.10] requirements of different application scenarios.

Draft Recommendation ITU-T Y.QKDN-iwfr "Quantum key distribution networks - interworking framework" introduced two conceptual models for QKDN interworking. The conceptual models are classified to two, Gateway Functions and with IWF. In the GF model, the QKDN interworking is performed between different KMs and QKD modules in each QKD node. The IWF is used for connecting QKDNs and is installed in a trusted node other than inside of the QKDN which interworks.

The work on QKDN interworking is progressing in Q16/13. Based on this work, this draft Recommendation specifies the high-level and functional requirements of QoS assurance for quantum key distribution networks (QKDN) interworking.

7. QoS assurance for QKDN interworking

Recommendation ITU-T Y.3806 specifies the high-level and functional requirements of QoS assurance for quantum key distribution networks (QKDN). The requirements in this Recommendation are described in terms of a single QKDN domain, not multiple domains. Furthermore, the requirements are derived from assuming that the QKDN components are provided by a single vendor or have same capability.

In general, a QKDN is allowed to comprise the QKDN components providing by different vendors or different domains and they even have a bit of different capabilities. It means that the QKDN components probably support the different QoS. Therefore, QoS negotiation is necessary within a certain range. In addition, the QKDN components are at different layers, for example application layer, key management layer and quantum layer. The expressions of QoS information may be different for the QKDN components at different layers. In this context, QoS information is translated between different layers and between same layer at different domains.

For the end-to-end QoS assurance of the QKDN interworking, it is essential to how to provide the QoS translation and the QoS negotiation in association with QKDN. Figure 1 illustrates the portion that QoS translation or negotiation are necessary for QKDN interworking, which is slightly modified from Recommendation ITU-T Y.3806. The portions are indicated by the arrows with circled number in Figure 1. End-to-end QoS consists of several sub-QKDNs: ingress and egress QKDN access network (QAN) and QKDN backbone network (QBN).

From an application perspective, two reference points are identified. The Ak is a reference point connecting a cryptographic application and a key supply function in a KM layer. The QoS information about the key is exchanged between them and may be expressed differently according to each layer. The QoS information is probably translated and negotiated where is indicated by the arrow representing number one.

The Ax is a reference point connecting two cryptographic applications in a user network. It is responsible for the two cryptographic applications to exchange their QoS information. The QoS information is probably negotiated where is indicated by the arrow representing number four.

The Kxi is a reference point connecting two key management (KM) layers within a QKD node such as access node and relay node, which is newly defined here. It is responsible for exchanging QoS information and operations required for the key relay, key synchronization and authentication. The QoS information is probably negotiated where is indicated by the arrow representing number three.

On the other hand, the Kq is a reference point connecting a key storage function in a KM layer with a QKD-key supply function in a QKD module. The QoS translation and negotiation may happen between KM layer and Quantum layer, where is indicated by the arrow representing number two. The Kx is a reference point connecting two key management (KM) layers in each QKD node via a KM link.

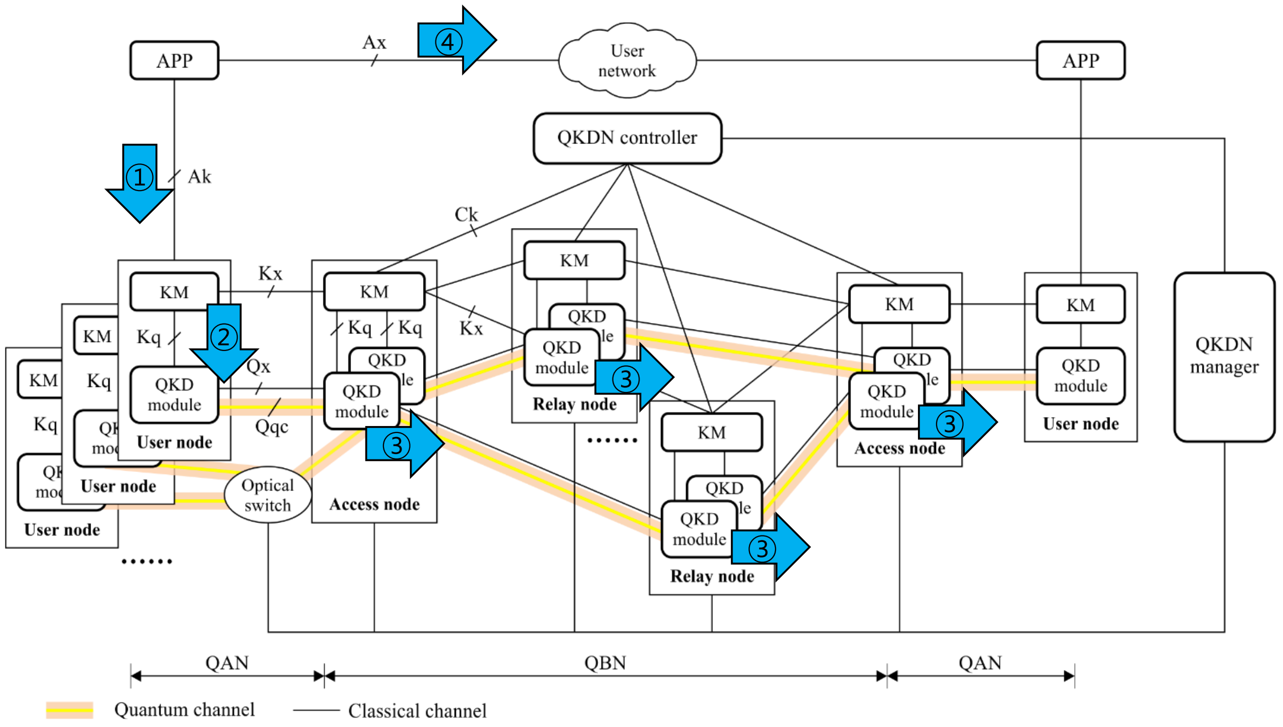

Figure 1 – Portion of the QoS assurance for QKDN interworking

7.1 QoS assurance at Ak

TBD

7.2 QoS assurance at Kq

TBD

7.3 QoS assurance at Kxi

In general, a pair of QKD modules (sender and receiver) works with single technology (such as a QKD protocol, restriction of hardware, strict security requirements etc.). For example, two QKD module type 1 at QKD node A and QKD node B are connected a QKD link type 1. On the other hand, two QKD module type 3 at QKD node B and QKD node C are connected a QKD link type 3. When the KMs at QKD node A, QKD node B and QKD node C have same operations such Key relay encryption methods and etc., no more processing is performed among them and they look like single KM. Furthermore, QKD module type 1 and QKD module type 3 at QKD node B are able to support same capability such as QoS and so on, no further modification is necessary.

The QKD link type 1 and the QKD link type 3 have different characteristics in transporting quantum bits if QKD module type 1 and QKD module type 3 support different QoS. It allows the QKDN node B to perform QKDN interworking, especially in QoS aspect. In that sense, some interworking between QKD module type 1 and QKD module type 3 from KM perspective happens by the KM in QKD node B.

Even a QKDN controller is skipped in Figure 1, the QKDN controller performs QKDN interworking and the details refer to Interworking of QKDNs with different control schemes in Y.QKDN-iwfr.

From QKDN provider's interworking perspective, the QKD node B is to be an IWN.

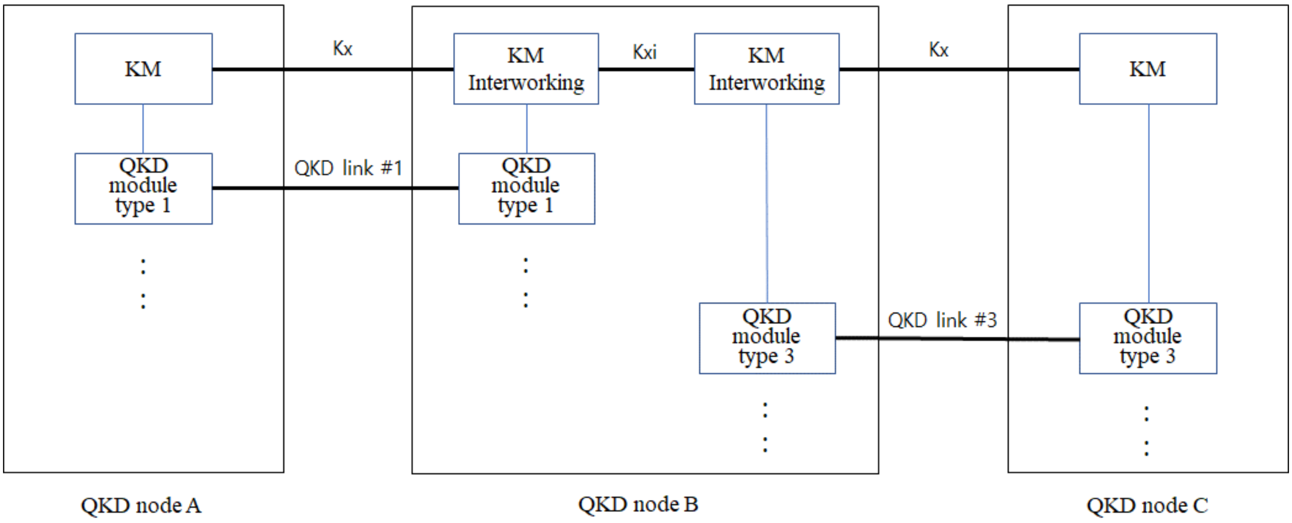

Figure 2 – QKDN interworking in the QKD modules with different QoS characteristics

7.4 QoS assurance at Ax

TBD

8. High-level requirements of QoS assurance for QKDN interworking

According to [ITU-T Y.3806] and [ITU-T Y.QKDN-qos-fa], the QKDN layered functional architecture and the associated functional components are defined. Basically, the high-level requirements for QoS assurance in [ITU-T Y.3806] should be applied to QKDNi as well. Several high-level requirements of Y.3806 are extracted to emphasize their importance.

This Recommendation extends functional components required for end-to-end QoS assurance and interoperability between transmitting and receiving QKD nodes.

It is assumed that a QKDN node (e.g. IWN) includes several QKD modules which may have different capabilities such as QoS. Each QKD module is associated with the corresponding KM.

[Editor's Note: If End-to-end QoS assurance functional element is added in QKD control layer, key management layer and quantum layer. Each element is interacting with each layer's control and management function to fulfil the QoS KPIs. This lead to produce extended requirements.]

Editor' Note – Q6 will try to ensure consistency with Q16 about requirements for QKDN Interworking.

A QKDN topology with two relay QKDNs is illustrated in Figure 3. Cryptographic applications in user network are connected to each QKDN A and QKDN D respectively. A Quantum key is relayed between QKDN A and QKDN D through QKDN B or QKDN C.

QKDN A is to choose an appropriate path, for example toward QKDN B or toward QKDN C, for relaying the Key to the application connecting to QKDN D. If the availability of QKDN B is low but that of QKDN C is high, then QKDN A lead to choose the path toward QKDN C for successfully completing relay.

[Editor's Note] Decision on the terms, "path or route" will be decided in the future meeting, contributions are solicited.

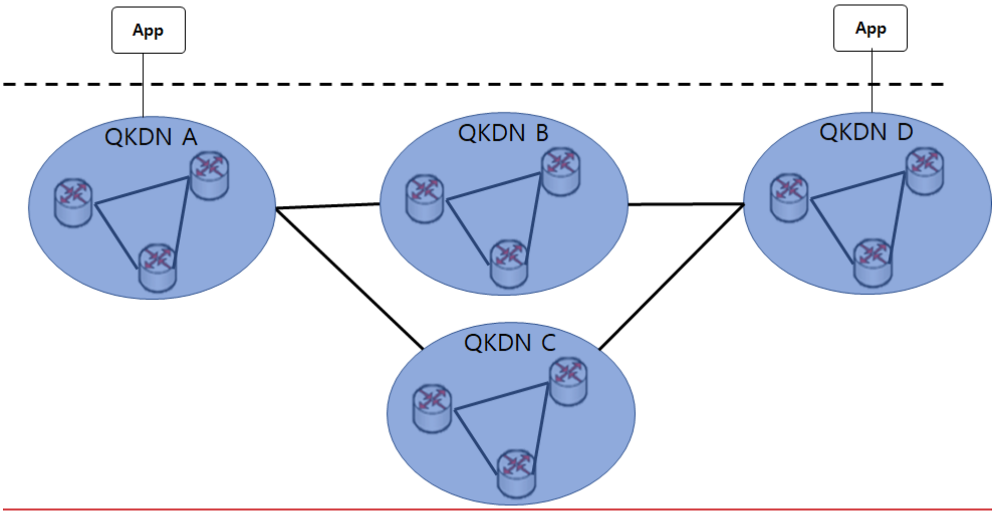

Figure 3 – QKDN topology with two relay QKDNs

It is required that QoS be considered at the level of the overall QKDNi, as well as at the system level.

QKDN is required to support a QoS model and its associated QoS profile in terms of QKDNi.

QKDN is required to support QoS negotiation in terms of QKDNi.

QKDN is required for the KM layer to provide an appropriate key to cryptographic applications according to the QoS information in terms of QKDNi.

Editor's Note – It is further study how to associate with QKDN from QKDNi perspective.

The QKDN is required to support transformation of QKD QoS information between QKD nodes having different capabilities and belonging to different providers.

The QKDN is required to support end-to-end QoS assurance between QKD nodes having different capabilities and belonging to different providers.

Editor' Note – Definition of end-to-end needs to be addressed.

The QKDN is required to support negotiation capability for QoS interworking between QKD nodes having different capabilities and belonging to different providers.

Editor' Note – Functional entities involved in negotiation needs to be addressed.

The KM is required to configure and manage the QoS profile of the QKD modules associated with itself.

The KM is required to exchange the QoS profile information between QKD modules.

The KM is required to exposure the QoS profile information to other function (e.g. QDKN controller) in the QKDN node.

The KM is optional to exposure the QoS profile information to cryptographic application.

The QKDN controller is required to select the KM and QKD module based on QoS requirement from cryptographic application.

The KM is required to be aware of the distance (i.e., KKRD) between sending and receiving Quantum nodes, which are connected to a cryptographic application ~~involving key distribution~~.

The KM is required to be aware of the key consumption rate of sending and receiving Quantum nodes, which are connected to a cryptographic application ~~involving key distribution~~.

The KM is required to be aware of the key availability of sending and receiving Quantum nodes, which are connected to a cryptographic application~~involving key distribution~~.

~~[Editor's Note] More information about routing and topology among different QKDNs, particularly different KMs will be provided in terms of QKDNi at May 2023 meeting.~~

9. Functional requirements of QoS assurance for QKDN interworking

[Editor's Note: During the lifecycle of the QKDN services, the QoS lifecycle management ensures that the QoS is also involved in the functional requirements for QKDN services. The QoS assurance functional requirements can be classified into five interdependent categories: QKDN QoS planning, QoS monitoring, QoS optimization, QoS provisioning, and QoS protection/recovery. The functional requirements are planned to extend QKDN interworking aspects.]

[Editor's Note: It will be verified whether the QBER should be included in Key relay request message. It will be identified whether Key information and/or KM information are carried and handled in Quantum layer, Key Management layer or other layers.]

9.1 QoS information transfer

The transmitting KM is required to send Key relay request including QoS information with Key length, QBER in order for the receiving KM to select an appropriate QKD module.

The transmitting KM is recommended to send Key relay request including QoS information with acceptable QoS range values in order to help the receiving KM to select an appropriate QKD module based on the acceptable range values.

9.2 QoS negotiation

The receiving KM is required to reject Key relay request including QoS information if the information is not acceptable.

The receiving KM is recommended to send acceptable QoS information to the transmitting KM if the Key relay request is rejected.

9.3 QoS management

The KM is required to manage KM information including QoS about single or more QKD modules.

The transmitting KM is required to select an appropriate receiving KM based on the KM information if multiple KMs are available.

The receiving KM is recommended to exposure a part of KM information in order for the transmitting KM to get an appropriate choice based on the information.

9.4 QoS routing

The QKDN controller is required to choose ~~determine~~ an appropriate ~~the~~ path between sending and receiving Quantum nodes, which are connected to a cryptographic application,~~considering~~ for guaranteeing the QoS requirement ~~by requested by user network~~.

NOTE – The QoS requirement relates to values of distance (i.e., KKRD), key consumption rate and key availability of QKDN nodes.

~~[Editor's Note] More information about routing and topology among different QKDNs, particularly different KMs will be provided in terms of QKDNi at May 2023 meeting.~~

10. Security considerations

TBD

____