INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2022-2024

SG13-TD463/WP1

STUDY GROUP 13

Original: English

Question(s):	6/13	Geneva, 26 July 2023

TD

Source:	Editors
Title:	Draft new Recommendation ITU-T Y.3817 (formerly Y.QKDN-qos-iw-req): “Quantum key distribution networks interworking - Requirements of quality of service assurance” - for consent

Contact:	Jeongyun Kim ETRI Korea (Rep. of)	Tel:+82-42-860-5311 Fax: +82-42-860-6405 Email: jykim@etri.re.kr
Contact:	Taesang Choi ETRI Korea (Rep. of)	Tel:+82-10-2740-5628 Fax: +82-42-860-6405 Email: choits@etri.re.kr
Contact:	Hyungsoo Kim KT corp. Korea (Rep. of)	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 Recommendation ITU-T Y.QKDN-qos-iw-req is revised based on C-63 at Q6/13 meeting and Q6/13 & Q16 joint meeting July 2023, which propose to request consent and clean-up. New text for QoS assurance at Ax in Clause 7.4 is proposed as well in C-64.

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

No.	Title	Source	Discussion
Q6-13-July23-C-063-Y.QKDN-qos-iw-req	Proposal for requesting consent and clean-up of Y.QKDN-qos-iw-req	ETRI	The proposal is accepted with modification. The whole text is carefully reviewed and is well improved according to comments. Based on the draft, Q6/13 decide to request consent at WP1 meeting.
Q6-13-July23-C-064-Y.QKDN-qos-iw-req	Proposed text for Clause 7.4 QoS assurance at Ax of Y.QKDN-qos-iw-req	ETRI	The proposal is accepted with modification. Based on the comment, direction indication for application is removed.

Draft new Recommendation ITU-T Y.3817 (formerly Y.QKDN-qos-iw-req)

Quantum key distribution networks interworking - Requirements of quality of service assurance

Summary

This Recommendation specifies the high-level and functional requirements of quality of service (QoS) assurance for quantum key distribution networks (QKDN) interworking. The functional requirements include QoS information transfer, QoS negotiation, QoS management and QoS routing.

Keywords

QKDN; QKDN interworking; QoS assurance; requirements;

Table of Contents

Draft new Recommendation ITU-T Y.3817 (formerly Y.QKDN-qos-iw-req)

Quantum key distribution networks interworking - Requirements of quality of service assurance

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:

- Introduction to QoS assurance for QKDN interworking (QKDNi)
- High-level requirements of QoS assurance for QKDNi
- Functional requirements of QoS assurance for QKDNi;

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 Y.3801] Recommendation ITU-T Y.3801 (2020), *Functional requirements for quantum key distribution networks*

[ITU-T Y.3806] Recommendation ITU-T Y.3806 (2021), Requirements of QoS assurance for quantum key distribution networks.

[ITU-T Y.3810] Recommendation ITU-T Y.3810 (2022), *Quantum key distribution network interworking – Framework.*

[ITU-T Y.3811] Recommendation ITU-T Y.3811 (2022), *Quantum key distribution networks – Functional architecture for quality of service assurance*.

3. Definitions

3.1 Terms defined elsewhere

3.1.1 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.

3.1.2 quantum key distribution network (QKDN) [b-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.

3.1.3 quality of service (QoS) [b-ITU-T P.10]: The totality of characteristics of a telecommunications service that bear on its ability to satisfy stated and implied needs of the user of the service (see [b-ITU-T E.800]).

3.2 Terms defined in this Recommendation

None.

4. Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ID	Identifier
GWF	Gateway Function
GWN	Gateway Node
IWF	Interworking Function
IWN	Interworking Node
KM	Key Manager
KMA	Key Management Agent
QKD	Quantum Key Distribution
QKDN	Quantum key distribution networks
QKDNi	Quantum key distribution networks interworking
QoS	Quality of Service

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. Introduction to QoS assurance for QKDN interworking

The quantum key distribution networks (QKDN) is expected to be able to provide optimized support for a variety of different QKD services. From a viewpoint of the cryptographic application in the service layer, QKDN services mean the distribution of both quantum keys and relevant information. In order to provide the same level of QKDN services that the application wants, 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 in different QKDN, especially in terms of QoS assurance. In addition, QoS information of QKD nodes such as key life-time, QKD link status, alarm on fault may be exchanged in order to support QoS assurance. The exchange is made in information hiding manner.

Recommendation [ITU-T Y.3806] specifies the high-level and functional requirements of QoS assurance for quantum key distribution networks (QKDN). The requirements in the Recommendation [ITU-T Y.3806] are described in terms of a single QKDN domain, not multiple QKDN domains. In general, a QKDN is allowed to comprise the QKDN components provided by different vendors, providers, and capabilities. It means that the QKDN components probably support the different QoS and, thus, QoS negotiation is necessary. In addition, the QKDN components are related to multiple 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 know how to provide the QoS translation and negotiation. Figure 1 indicates where QoS translation or negotiation are necessary for QKDN interworking, which is noted by the arrows with circled numbers. End-to-end QoS ranges over multiple QKDNs.

From cryptographic applications perspective, two reference points are identified. The Ak is a reference point connecting a cryptographic application and a key supply function in a Key Management layer. The QoS information about the key is exchanged between two layers and may be expressed differently according to the characteristics of the two layers. The QoS information is necessary to be translated and negotiated, which 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 necessary to be negotiated, which is indicated by the arrow representing number four.

The Kxi is a reference point connecting two KMs in each QKD node such as a Gateway node (GWN). The Kxi' is a reference point connecting two KMs within a QKD node such as an Interworking node (IWN). They are defined in [ITU-T Y.3810]. They are responsible for exchanging QoS information and operations for the key relay, key synchronization, and authentication. QoS information is used for selecting either a GWN or a KM in an IWN, which is indicated by the arrow representing number three. Figure 1 can applied to illustrate QoS assurance for QKDN interworking with GWN, if interworking node IWN is replaced to GWN. From QoS viewpoint, IWN and GWN are considered as the same in terms of interworking mechanism.

On the other hand, the Kq is a reference point connecting a key storage function in a key management layer with a QKD-key supply function in a QKD module. The QoS translation and negotiation may happen between key management layer and Quantum layer, which is indicated by the arrow representing number two.

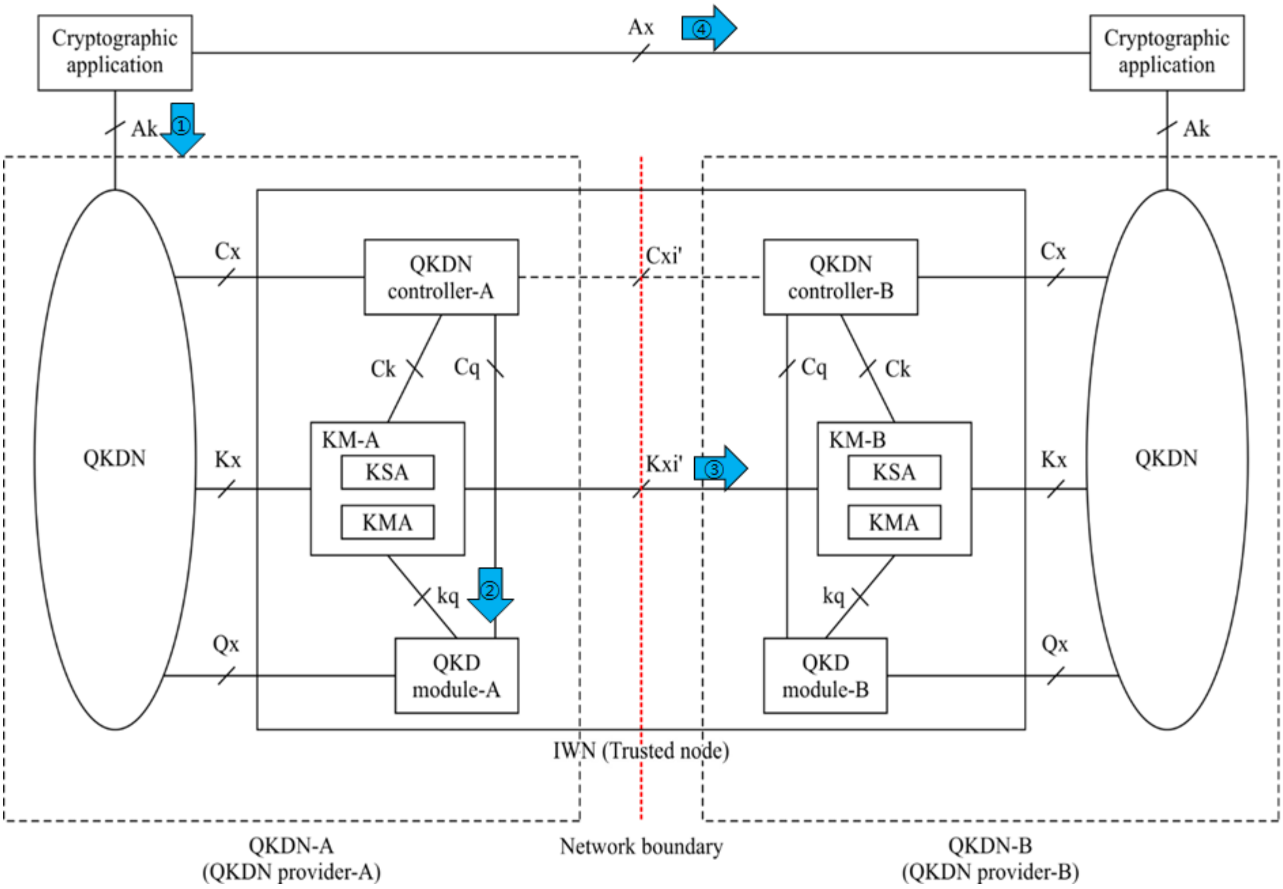

Figure 1 – Portion of the QoS assurance for QKDN interworking with IWN

6.1 QoS assurance at Ak

The Ak is a reference point connecting a cryptographic application and a key supply function in a Key Management layer. The Key Management layer responds to the cryptographic application with a Key response message containing Key(s) and Key ID(s) when receiving a Key request message from the cryptographic application.

The two types of cryptographic applications are banking and cloud computing, for example. They may have a different level of QoS per security policy of their business. Thus, they can request a desirable number of Keys to support multiple QoS levels. In addition, the cryptographic application is able to get multiple Keys either at once by transmitting single Key request message or on several times by transmitting multiple Key request messages.

From the cryptographic application perspective, the amount of data to encrypt, the number of Keys and replacement cycles of Keys, for example, have some relations with the Key length, Key availability and Key generation rate in the Key Management layer, respectively. The Key Management layer can choose as much best Key(s) as possible per cryptographic application. QoS mapping between the cryptographic application and the Key Management layer may be necessary.

There are two types of QoS expressions; implicit and explicit. The former utilizes an application name on requesting Key. QoS information in the Key Management layer can be identified if an application name is notified. The pre-agreement is required for application name notification.

The latter expresses QoS information in the Key request message. The QoS information may include a Key length, a Key availability and a Key generation rate. QoS mapping between the cryptographic application and Key Management layer may be unnecessary for this.

From QoS assurance perspective, the Key Management layer is able to determine as much best Key(s) as possible depending on which type of QoS expression is used.

6.2 QoS assurance at Kq

The Kq is a reference point connecting a key storage function in a Key Management layer with a QKD-key supply function in a QKD module. In the quantum layer, a pair of QKD modules generates a pair of symmetric (identical) random bit strings in its own way based on an IT-secure protocol of QKD. The pair of QKD modules is typically provided from same vendor in a QKDN. Some pairs of QKD modules from different vendors can also be deployed in the QKDN.

The Key Management layer receives QKD-key(s) from a QKD module/QKD modules which is/are located in the same QKD node and to store them securely. The lengths of the acquired QKD-keys may differ from one another. The KMA re-formats (combines or splits) the different length QKD-keys into keys of a prescribed unit length.

Furthermore, the Key Management layer is necessary to support the operations with multiple QKD modules produced by different vendors. The QKD modules may provide different QKD-key lengths depending on their characteristics.

From QoS assurance perspective, the Key Management layer is able to support QoS transformation, for example change in Key length from the quantum layer to Key Management layer. The operation of QoS mapping is also performed in terms of cryptographic applications. For example, the Keys in Key Management layer are able to have a variety of Key length with respect to a number of cryptographic applications.

6.3 QoS assurance at Kxi’

In general, a pair of QKD modules (transmitter 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 QKD 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 2, the QKDN controller performs QKDN interworking and the details refer to Interworking of QKDNs with different control schemes in [ITU-T Y.3810].

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

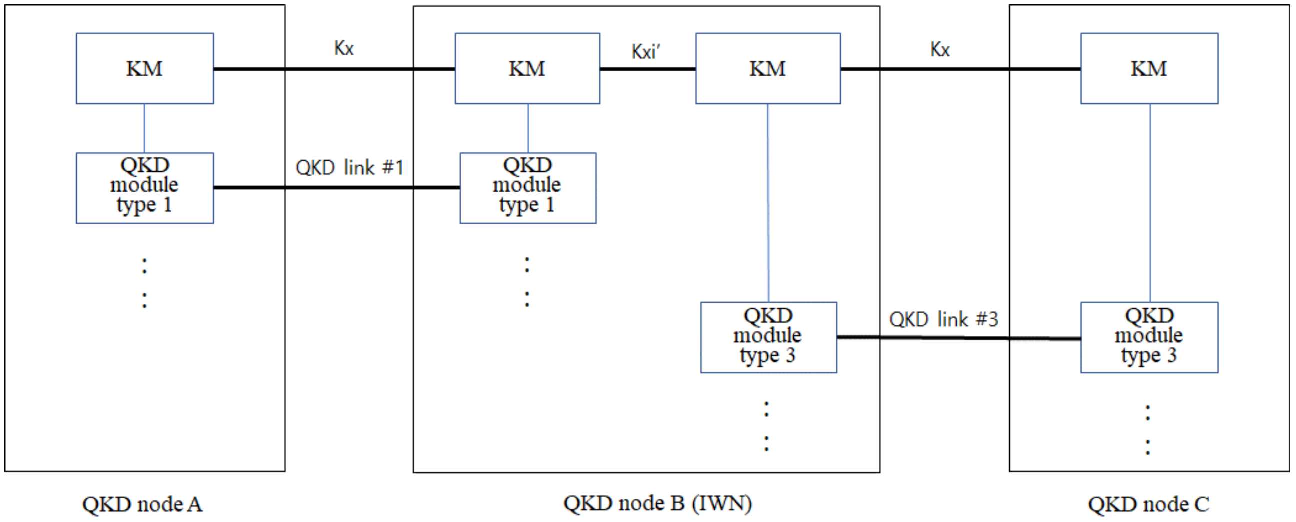

Figure 2 – QKDN interworking in the QKD modules with different QoS characteristics

6.4 QoS assurance at Ax

This clause introduces a brief description of the Ax, which is a reference point connecting two cryptographic applications in a user network. The applications may exchange QoS information either when delivering a Key ID or when having a separate operation. Then applications are able to learn the Key characteristics directly. The Key life-time and Key generation rate are examples for QoS information. It is useful for applications to anticipate the usage pattern of the Key, unless pre-configuration is made.

From QoS assurance perspective, the cryptographic application is able to understand and anticipate how long the Key is effective and when new Key is needed, if QoS information is available.

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

According to [ITU-T Y.3806] and [ITU-T Y.3811], 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 has a direction to extend functional components for end-to-end QoS assurance and interoperability in an interworking QKD node (e.g., IWN).

It is assumed that a QKD 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.

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 (or route), 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.

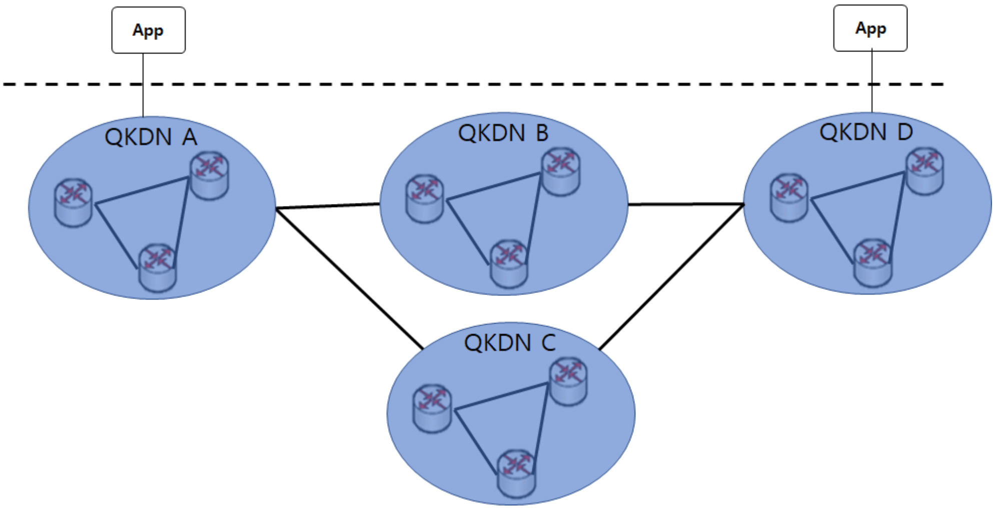

Figure 3 – QKDN topology with two relay QKDNs

QoS is required to be considered across QKDNs that interwork to serve a cryptographic application, as well as within individual QKDN.

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

NOTE – QoS model and QoS profile is described in [ITU-T Y.3806].

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

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

QKDN is required to support transformation of QoS information in interworking QKD nodes.

QKDN is required to support end-to-end QoS assurance in interworking QKD nodes.

KM is required to exchange the QoS information in interworking QKD nodes.

NOTE – A KM resides in an interworking QKD node (e.g., IWN).

KM is required to exposure the QoS information to other function (e.g. QDKN controller) in interworking QKD nodes.

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

QKDN controller is required to select a KM based on QoS requirement from cryptographic application.

8. Functional requirements of QoS assurance for QKDN interworking

Functional requirements of QoS assurance for QKDNi are extension from that for a single QKDN. Therefore [ITU-T Y.3806] is applied to QKDNi as well. The following requirements are specific to QoS assurance for QKDNi.

NOTE – A KM resides in an interworking QKD node (e.g., IWN).

8.1 QoS information transfer

A KM submitting key relay requests to a KM in another QKDN through QKDNi is recommended to include QoS information in Key relay requests, including acceptable ranges for QoS values.

8.2 QoS negotiation

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

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

NOTE – A part of QoS information is exchanged.

8.3 QoS management

KM is required to be aware of a part of QoS information of corresponding KMs.

Transmitting KM is recommended to select an receiving KM by help of QKDN controller, in interworking QKD node (e.g., IWN),

8.4 QoS routing

A QKDN controller is required to consider QoS requirements from cryptographic applications along with policies of the QKDN it resides within and policies agree between interworking QKDNs when deciding QKDNi routes.

NOTE –QoS requirement relates to values of key consumption rate and key availability of QKD nodes.

9. Security considerations

This Recommendation describes the high-level and functional requirements of QoS assurance for quantum key distribution networks (QKDN) interworking, therefore, security requirements described in [b-ITU T X.1710], [ITU-T Y.3801] and [b-ITU-T Y.3802] and general network security requirements and mechanisms in IP-based networks described in [b-ITU-T Y.2701] and [b-ITU T Y.3101] should be applied. Details are outside the scope of this Recommendation.

Bibliography

[b-ITU-T E.800] Recommendation ITU-T E.800 (2008), *Definitions of terms related to quality of service.*

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

[b-ITU-T X.1710] Recommendation ITU-T Y.1710 (2020), *Security framework for quantum key distribution networks.*

[b-ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

[b-ITU-T Y.3101] Recommendation ITU-T Y.3101 (2018), *Requirements of the IMT-2020 network.*

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

[b-ITU-T Y.3802] Recommendation ITU-T Y.3802 (2020), *Quantum key distribution networks – Functional architecture.*

[b-ETSI GR QKD 007] ETSI GR QKD 007 V1.1.1 (2018), *Quantum Key Distribution (QKD); Vocabulary*.
https://www.etsi.org/deliver/etsi_gr/QKD/001_099/007/01.01.01_60/gr_qkd007v010101p.pdf

____