ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T Y.3817 (09/2023)

SERIES Y: Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities

Quantum key distribution networks

Quantum key distribution network interworking – Requirements for quality of service assurance

ITU-T Y-SERIES RECOMMENDATIONS

Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities

GLOBAL INFORMATION INFRASTRUCTURE	Y.100-Y.999
General	Y.100-Y.199
Services, applications and middleware	Y.200-Y.299
Network aspects	Y.300-Y.399
Interfaces and protocols	Y.400-Y.499
Numbering, addressing and naming	Y.500-Y.599
Operation, administration and maintenance	Y.600-Y.699
Security	Y.700-Y.799
Performances	Y.800-Y.899
INTERNET PROTOCOL ASPECTS	Y.1000-Y.1999
General	Y.1000-Y.1099
Services and applications	Y.1100-Y.1199
Architecture, access, network capabilities and resource management	Y.1200-Y.1299
Transport	Y.1300-Y.1399
Interworking	Y.1400-Y.1499
Quality of service and network performance	Y.1500-Y.1599
Signalling	Y.1600-Y.1699
Operation, administration and maintenance	Y.1700-Y.1799
Charging	Y.1800-Y.1899
IPTV over NGN	Y.1900-Y.1999
NEXT GENERATION NETWORKS	Y.2000-Y.2999
Frameworks and functional architecture models	Y.2000-Y.2099
Quality of Service and performance	Y.2100-Y.2199
Service aspects: Service capabilities and service architecture	Y.2200-Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250-Y.2299
Enhancements to NGN	Y.2300-Y.2399
Network management	Y.2400-Y.2499
Computing power networks	Y.2500-Y.2599
Packet-based Networks	Y.2600-Y.2699
Security	Y.2700-Y.2799
Generalized mobility	Y.2800-Y.2899
Carrier grade open environment	Y.2900-Y.2999
FUTURE NETWORKS	Y.3000-Y.3499
CLOUD COMPUTING	Y.3500-Y.3599
BIG DATA	Y.3600-Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	**Y.3800-Y.3999**
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	Y.4000-Y.4999
General	Y.4000-Y.4049
Definitions and terminologies	Y.4050-Y.4099
Requirements and use cases	Y.4100-Y.4249
Infrastructure, connectivity and networks	Y.4250-Y.4399
Frameworks, architectures and protocols	Y.4400-Y.4549
Services, applications, computation and data processing	Y.4550-Y.4699
Management, control and performance	Y.4700-Y.4799
Identification and security	Y.4800-Y.4899
Evaluation and assessment	Y.4900-Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.3817

Quantum key distribution network interworking – Requirements for quality of service assurance

Summary

Recommendation ITU-T Y.3817 specifies high-level and functional requirements for quality of service (QoS) assurance for quantum key distribution network interworking. The functional requirements include QoS information transfer, QoS negotiation, QoS management and QoS routing.

History [*]

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T Y.3817	2023-09-29	13	11.1002/1000/15645

Keywords

QKDN, QKDN interworking, QoS assurance, requirements.

[*] To access the Recommendation, type the URL https://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.3817

Quantum key distribution network interworking –
Requirements for quality of service assurance

1 Scope

This Recommendation specifies high-level and functional requirements for quality of service (QoS) assurance for quantum key distribution network (QKDN) interworking. This Recommendation includes the following:

- an introduction to QoS assurance for QKDN interworking (QKDNi);
- high-level requirements for QoS assurance for QKDNi;
- functional requirements for 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 X.1710] Recommendation ITU-T Y.1710 (2020), *Security framework for quantum key distribution networks*.

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

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

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

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

[ITU-T Y.3806] Recommendation ITU-T Y.3806 (2021), *Quantum key distribution networks – Requirements for quality of service assurance*.

[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

This Recommendation uses the following 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:

GWN	Gateway Node
ID	Identifier
IWN	Interworking Node
KM	Key Manager
KMA	Key Management Agent
KML	Key Management Layer
QKD	Quantum Key Distribution
QKDN	Quantum Key Distribution Network
QKDNi	Quantum Key Distribution Network interworking
QL	Quantum Layer
QoS	Quality of Service

5 Conventions

In this Recommendation:

The phrase "is required" indicates a requirement that must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

The phrase "is recommended" indicates a requirement that 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

QKDNs are expected to provide optimized support for a variety of different QKD services. From the viewpoint of a 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, 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 differ between transmitting and receiving QKD nodes in different QKDNs, especially in terms of QoS assurance. In addition, QoS information of QKD nodes such as key lifetime, QKD link status and alarm on fault may be exchanged in order to support QoS assurance. The exchange is made in information hiding manner.

[ITU-T Y.3806] specifies high-level and functional requirements for QoS assurance for QKDNs. The requirements of [ITU-T Y.3806] are described in terms of a single, not multiple, QKDN domain. In general, a QKDN is allowed to comprise the QKDN components provided by different vendors, providers and capabilities. This means that QKDN components probably support different QoS and, thus, QoS negotiation is necessary. In addition, QKDN components are related to multiple layers, e.g., application layer, key management layer (KML) and quantum layer (QL). The expressions of QoS information may differ for QKDN components at different layers. In this context, QoS information is translated between different layers and between the same layer in different domains.

For end-to-end QoS assurance of QKDNi, it is essential to know how to provide QoS translation and negotiation. Figure 1 indicates where QoS translation or negotiation are necessary for QKDNi, indicated by the arrows with circled numbers. End-to-end QoS ranges over multiple QKDNs.

From the cryptographic applications perspective, two reference points are identified. Ak is a reference point connecting a cryptographic application and a key supply function in a KML. QoS information about the key is exchanged between two layers and may be expressed differently according to their characteristics. Translation and negotiation of QoS information is necessary, which is indicated by the arrow labelled 1.

Ax is a reference point connecting two cryptographic applications in a user network. Ax enables two cryptographic applications to exchange their QoS information. Negotiation of QoS information is necessary, which is indicated by the arrow labelled 4.

Kxi is a reference point connecting two key managers (KMs) in each QKD node such as a gateway node (GWN). Kxi' is a reference point connecting two KMs within a QKD node such as an interworking node (IWN). These reference points are specified in [ITU-T Y.3810]. Kxi and Kxi' enable exchange of QoS information and operations for key relay, key synchronization and authentication. QoS information is used to select either a GWN or a KM in an IWN, which is indicated by the arrow labelled 3. Figure 1 can applied to illustrate QoS assurance for QKDNi with a GWN, if an IWN is replaced by a GWN. From the QoS viewpoint, an IWN and GWN are considered as the same in terms of interworking mechanism.

On the other hand, Kq is a reference point that connects a key storage function in a KML with a QKD-key supply function in a QKD module. QoS translation and negotiation may happen between the KML and QL, which is indicated by the arrow labelled 2.

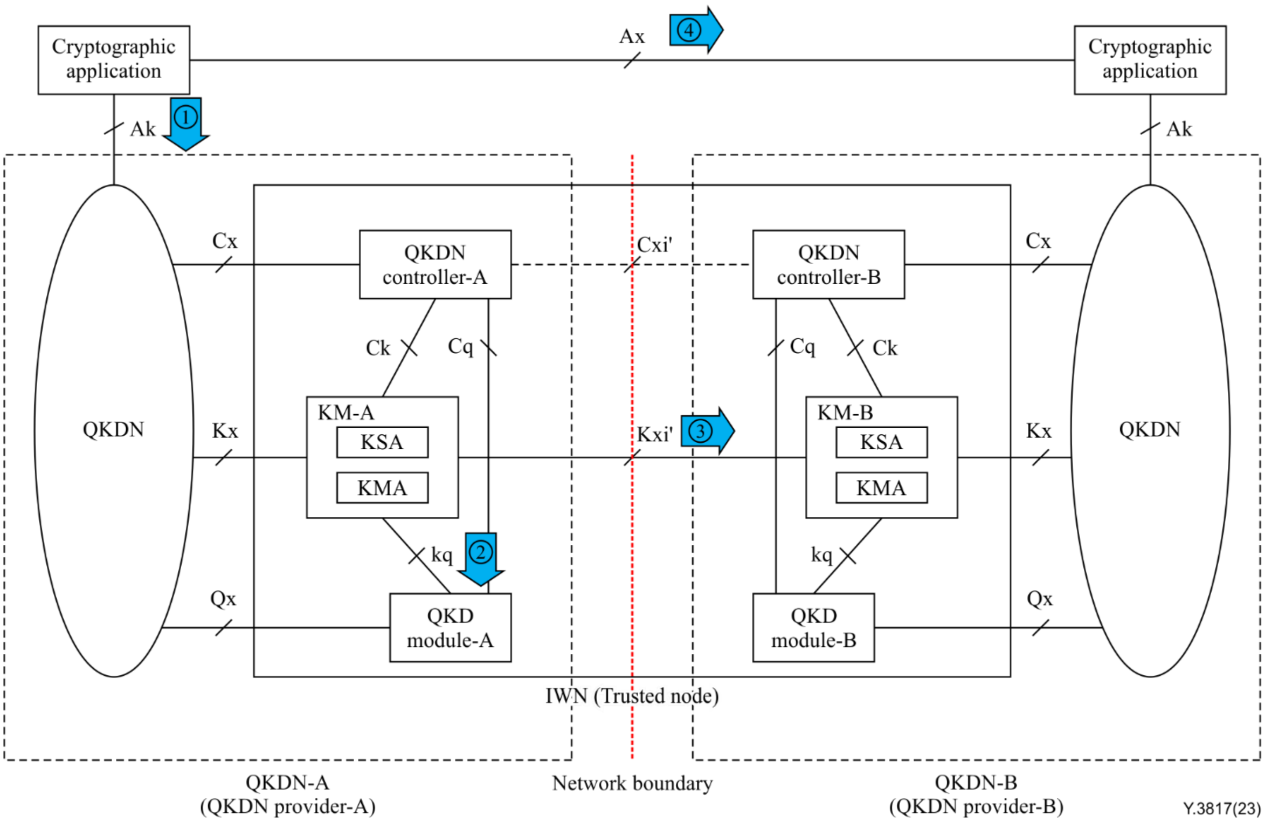

Figure 1 – Portion of the QoS assurance for QKDN interworking with IWN

6.1 QoS assurance at Ak

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

Examples of two types of cryptographic application are banking and cloud computing. They may have a different level of QoS according to the 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 simultaneously by transmitting a single key request message or at different 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 key length, key availability and key generation rate in the KML, respectively. The KML can choose as many best key(s) as possible per cryptographic application. QoS mapping between the cryptographic application and the KML may be necessary.

There are two types of QoS expression, implicit and explicit.

The former utilizes an application name on requesting a key. QoS information in the KML can be identified if an application name is notified. Pre-agreement is required for application name notification.

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

From the QoS assurance perspective, the KML is able to determine as many best key(s) as possible depending on which type of QoS expression is used.

6.2 QoS assurance at Kq

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

The KML receives QKD-key(s) from one or more QKD modules that are located in the same QKD node and stores them securely. The lengths of the acquired QKD-keys may differ. The key management agent (KMA) re-formats (combines or splits) QKD-keys of different lengths into keys of a prescribed unit length.

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

From the QoS assurance perspective, the KML is able to support QoS transformation, e.g., change in key length from the QL to KML. The operation of QoS mapping is also performed in terms of cryptographic applications. For example, keys in the KML are able to have a variety of key lengths 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 a single technology (such as a QKD protocol, restriction of hardware or strict security requirements). For example, two QKD modules of type 1 at QKD node A and QKD node B are connected by a QKD link type 1. On the other hand, two QKD modules of type 3 at QKD node B and QKD node C are connected by a QKD link type 3. When the KMs at QKD node A, QKD node B and QKD node C have the same operations, such as the same key relay encryption methods, no more processing is performed among them, and they can be considered as single KMs. Furthermore, QKD module type 1 and QKD module type 3 at QKD node B are able to support the same capability such as QoS, and 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. This situation allows the QKD node B to perform QKDNi, especially on the QoS aspect. In that sense, KM interworking for QKD module type 1 and QKD module type 3 happens in QKD node B.

Even if a QKDN controller is skipped in Figure 2, the QKDN controller performs QKDNi and the details refer to Interworking of QKDNs with different control schemes in [ITU-T Y.3810].

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

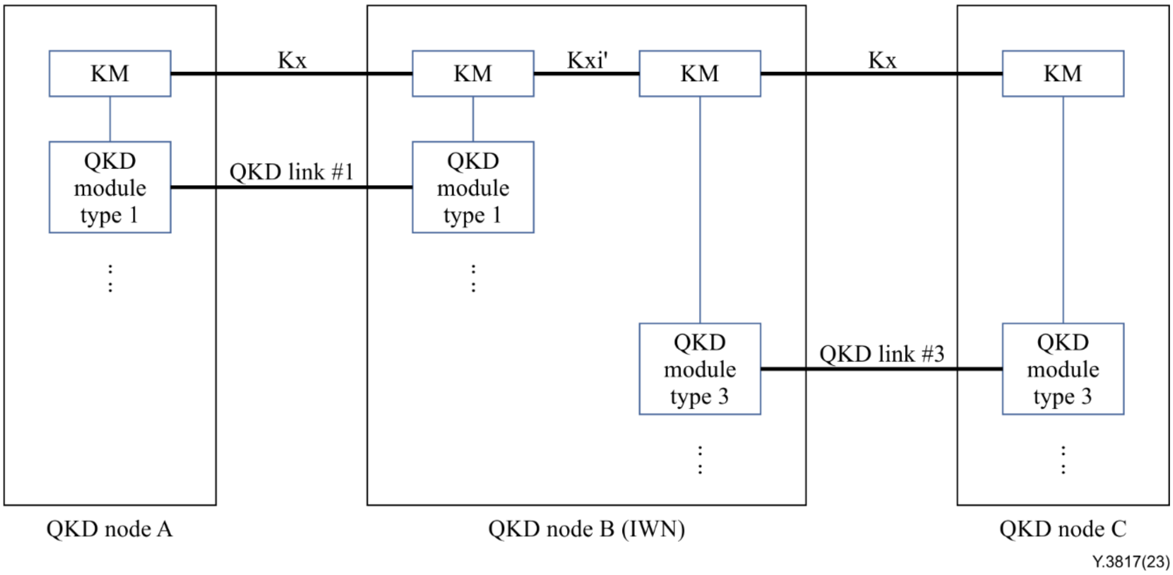

Figure 2 – QKDN interworking in the QKD modules with different QoS characteristics

6.4 QoS assurance at Ax

This clause introduces a brief description of 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 operating separately. Applications are then able to learn key characteristics directly. The key lifetime and key generation rate are examples for QoS information. It is useful for applications to anticipate the usage pattern of the key, unless it is pre-configured.

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

7 High-level requirements of QoS assurance for QKDN interworking

The QKDN layered functional architecture and the associated functional components are specified according to [ITU-T Y.3806] and [ITU-T Y.3811]. Basically, the high-level requirements for QoS assurance in [ITU-T Y.3806] should also be applied to QKDNi. Several high-level requirements of [ITU-T Y.3806] are mentioned ed here to emphasize their importance.

This Recommendation aims to extend functional components for end-to-end QoS assurance and interoperability in an interworking QKD node (e.g., an IWN).

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

A QKDN topology with two relay QKDNs is illustrated in Figure 3. Cryptographic applications in a user network are connected to each QKDN A and QKDN D. 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), e.g., toward QKDN B or toward QKDN C, to relay 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 tends to choose the path toward QKDN C for successful completion of the relay.

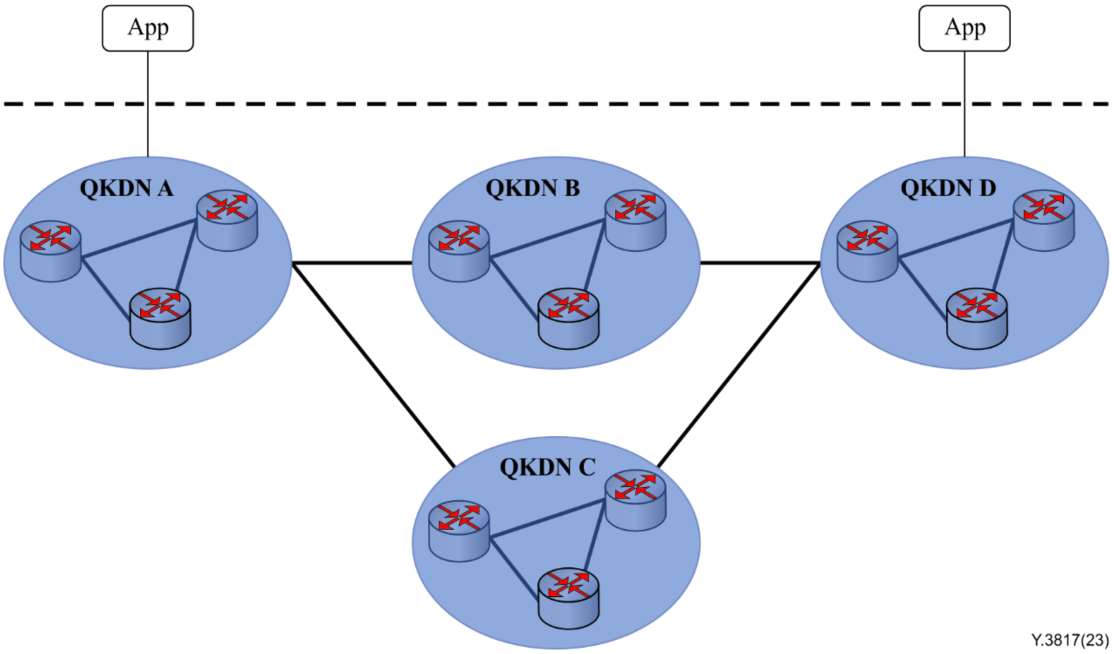

Figure 3 – QKDN topology with two relay QKDNs

Consideration of QoS is required across QKDNs that interwork to serve a cryptographic application, as well as within individual QKDNs.

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

NOTE 1 – A QoS model and QoS profile are described in [ITU-T Y.3806].

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

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

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

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

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

NOTE 2 – A KM resides in an interworking QKD node (e.g., an IWN).

A KM is required to expose QoS information to other functions (e.g., QDKN controller) in interworking QKD nodes.

A KM may optionally expose QoS information to a cryptographic application.

The QKDN controller is required to select a KM based on QoS requirements from the cryptographic application.

8 Functional requirements of QoS assurance for QKDN interworking

Functional requirements of QoS assurance for QKDNi are extensions from those for a single QKDN. Therefore, [ITU-T Y.3806] is also applied to QKDNi. The requirements in clauses 8.1 to 8.4 are specific to QoS assurance for QKDNi.

NOTE – A KM resides in an interworking QKD node (e.g., an 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 them, including acceptable ranges for QoS values.

8.2 QoS negotiation

The receiving KM is required to reject key relay requests 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

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

A transmitting KM is recommended to select a receiving KM with the help of a QKDN controller, in an interworking QKD node (e.g., an IWN).

8.4 QoS routing

A QKDN controller is required to consider QoS requirements from cryptographic applications along with policies of the QKDN in which it resides and ensure that 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 high-level and functional requirements of QoS assurance for QKDN interworking, therefore, security requirements described in [ITU T X.1710], [ITU-T Y.3801] and [ITU-T Y.3802] and general network security requirements and mechanisms in IP-based networks described in [ITU-T Y.2701] and [ITU T Y.3101] should be applied. Details lie 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 Y.3800] Recommendation ITU-T Y.3800 (2019), *Overview on networks supporting quantum key distribution*.

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

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Published in Switzerland
Geneva, 2023