International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3806

(09/2021)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Quantum key distribution networks

Quantum key distribution networks – Requirements for quality of service assurance

Recommendation ITU-T Y.3806

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
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	
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	
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	
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.3806

Quantum key distribution networks – Requirements for quality of service assurance

Summary

Recommendation ITU-T Y.3806 specifies the high-level and functional requirements of quality of service (QoS) assurance for quantum key distribution networks (QKDN). The functional requirements include QoS planning, QoS monitoring, QoS optimization, QoS provisioning, QoS protection and recovery.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3806	2021-09-13	13	11.1002/1000/14777

Keywords

High-level and functional requirements, QoS assurance, quantum key distribution network.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

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

		Page
1	Scope	1
2	References	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Recommendation	1
4	Abbreviations and acronyms	2
5	Conventions	2
6	Introduction	2
7	High-level requirements of QoS assurance for QKDN	3
8	Functional requirements of QoS assurance for QKDN	4
	8.1 Quality of service planning requirements for QKDN	5
	8.2 Quality of service monitoring requirements for QKDN	5
	8.3 Quality of service optimization requirements for QKDN	5
	8.4 Quality of service provisioning requirements for QKDN	6
	8.5 Quality of service protection/recovery requirements for QKDN	6
9	Security considerations	6
Bibliography		7

Recommendation ITU-T Y.3806

Quantum key distribution networks – Requirements for quality of service assurance

1 Scope

This Recommendation specifies the high-level and functional requirements of QoS assurance for quantum key distribution networks (QKDN). This Recommendation covers:

– Introduction of QoS assurance for quantum key distribution network.

– High-level requirements of QoS assurance for quantum key distribution network.

– Functional requirements of QoS assurance for quantum key distribution network.

NOTE 1 – Some requirements in this Recommendation refer to QoS information (i.e., key length, key amount, node pair names or IDs, etc.) provided by entities within a quantum key distribution network (QKDN) for QoS assurance purposes. The information provided under a requirement will depend on the use case and/or the implementation. How to specify the information included is outside the scope of this Recommendation and the selection made in the implementation will not prevent a claim of conformance with this Recommendation.

NOTE 2 – Requirements in this Recommendation are limited to a single QKDN.

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.*

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

This Recommendation defines the following terms:

3.2.1 KSA key response delay: The time measured at KSA, (t2 – t1) between the occurrence of two corresponding events, key request message at time1 and replied KSA key at time2 over a reference point between a cryptographic application and KML in QKDNs, where (t2 > t1).

3.2.2 KSA key delivery error ratio (KKDER): The ratio of the number of KSA keys corrupted in transit between a KSA and a cryptographic application to the total number of KSA keys successfully transferred.

3.2.3 KSA key delivery loss ratio (KKDLR): The ratio of the number of KSA keys not received by a cryptographic application to the total number of KSA keys sent to it by a KSA.

3.2.4 key request session recovery ratio: The ratio of the numbers of recovered key request sessions to the total number of failed key request sessions.

3.2.5 wavelength reservation ratio: The ratio of the reserved wavelength resources for recovery to the total of the allocated wavelength resources.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

E2E	End to End
ID	Identifier
KKDER	KSA Key Delivery Error Ratio
KKDLR	KSA Key Delivery Loss Ratio
KM	Key Management
NP	Network Performance
QAN	Quantum Access Network
QBER	Quantum Bit Error Rate
QBN	Quantum Backbone Network
QKD	Quantum Key Distribution
QKDN	Quantum Key Distribution Network
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

For the end-to-end QoS assurance of the QKDN, it is essential to define the scope of the QoS in association with QKDN. Figure 1 illustrates the relationship between an end-to-end QKDN QoS and its associated network performance (NP) of the underlying QKDN. End-to-end QoS consists of several network performances of different 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. The QoS information may include key length, key amount, node pair names or identifiers (IDs), etc. 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.

Two reference points are identified with respect to a user node. The Kx is a reference point connecting two key management (KM) layers in each QKD node via a KM link. It is responsible for exchanging information and operations required for the key relay, key synchronization and authentication. 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. It is responsible for transferring QKD-keys generated by a QKD module to the KM layer. The QoS information of the QKD-key such as size, volume, may be transferred as well.

From a QKDN controller perspective, one reference point is identified. The Ck is a reference point connecting the QKDN controller control and management function in a QKDN controller and a KM control and management function in a KM layer. It is responsible for the QKDN controller to communicate control information with a KM layer. The QKDN controller is able to deliver QoS requests on behalf of the cryptographic applications.

The Qx is a reference point connecting two quantum layers through a quantum channel in the QKD link. It is responsible for exchanging QoS information about the key including QKD-key bit rate, etc.

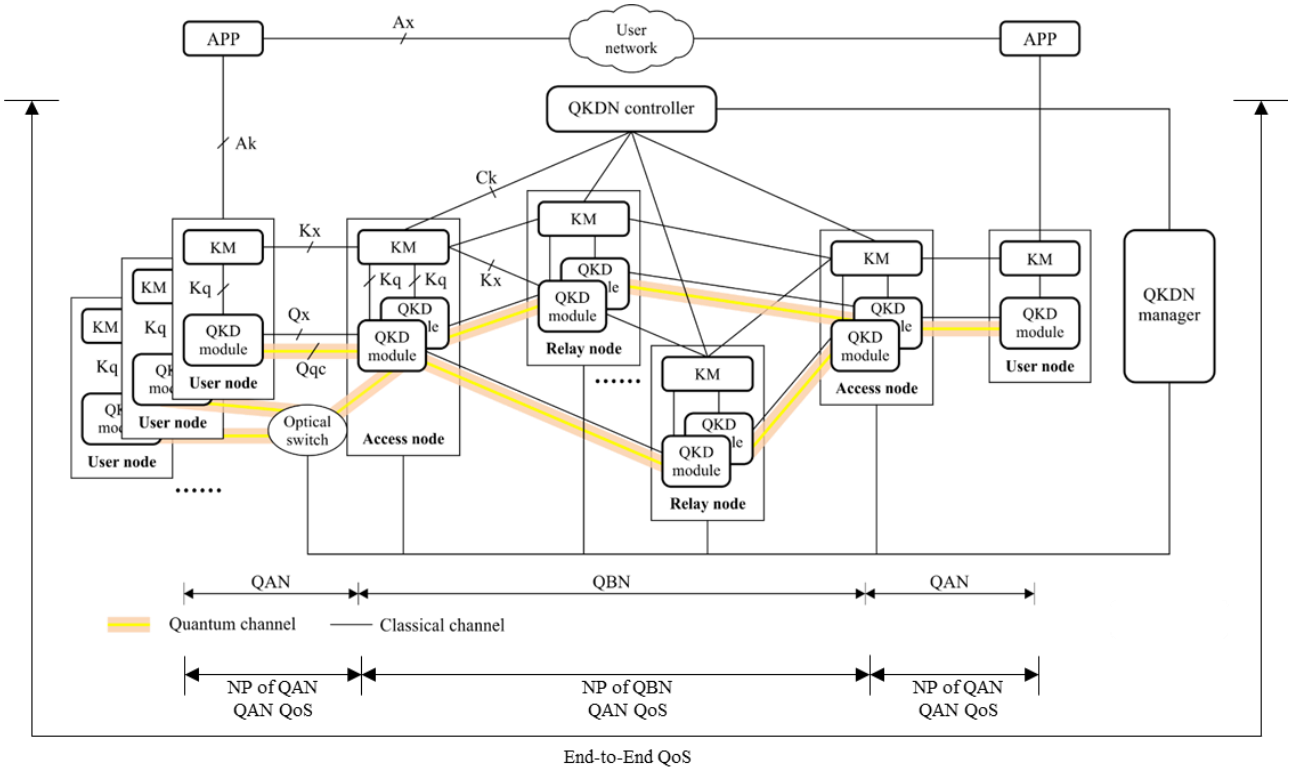

Figure 1 – Scope of the QKDN QoS and relationship with network performance

7 High-level requirements of QoS assurance for QKDN

As described in Figure 1, an end-to-end QKDN QoS can consist of a combination of quantum access network (QAN) QoS and quantum backbone network (QBN) QoS. It indicates a QKDN QoS from the QKD link perspective. On the other hand, the QKDN QoS can also be considered from a viewpoint of applications. Applications should be able to negotiate a required QoS by either pre-provisioning or on-demand basis. QAN can enhance the scalability of QKDN by interconnecting

multiple user nodes. It is responsible for aggregating multiple quantum links and delivering the quantum keys to QBN. QBN is able to relay the quantum keys to remote QAN.

A QKDN QoS profile is necessary to efficiently support the QKDN QoS negotiation. The QKDN QoS profile may include some attributes such as quantum bit error rate (QBER), KSA key delivery loss ratio (KKDLR), maximum secure distance, operating frequency, required security level, etc.

For simplicity of QKDN QoS negotiation, the QKDN QoS profile can further include a QKDN QoS class, specifically representing a range of values about the attributes of the QKDN QoS profile.

Furthermore, based on QoS related requirements defined in [ITU-T Y.3801], the high-level and functional requirements for QoS assurance for QKDN are defined in clauses 7 and 8.

– It is required that QoS be considered at the level of the overall QKD network architecture, as well as at the system level.
– QKDN is required to support SLA based QoS assurance. QKDN is required to support a QoS model and its associated QoS profile.
– QKDN is required to support QoS negotiation between an application and the QKDN.

NOTE 1 – The QoS negotiation can be performed via either pre-provisioning or on-demand (e.g., signalling). It depends on the provider's policy.

– QKDN is recommended to provide QoS class alone without a QoS profile.
– QKDN is recommended for the QoS class to be determined for indicating a range of values for the attributes in the QoS profile.
– QKDN is required to assure latency, integrity, throughput, and availability for key distribution.
– QKDN is required to assure the quality of real-time control and management traffic flows.

NOTE 2 – The assurance mechanism which will define QKDN QoS assurance functional architecture and mechanisms is for further study.

– QKDN is required for the KM layer to provide an appropriate key to cryptographic applications according to the QoS information.
– QKDN is recommended to assure the secure key rate.
– QKDN is recommended to assure the maximum secure distance.
– QKDN is recommended to assure the quantum bit error rate (QBER).
– QKDN is recommended to assure the operating frequency.
– QKDN is recommended for the KM layer to request a new key to the quantum layer if the QoS information of the stored keys (e.g., size, volume, etc.) are not enough to meet the requested QoS from cryptographic applications.
– QKDN is recommended to support QoS mapping between a user node and QAN, and between QAN and QBB.
– QKDN is recommended to support QoS capability exposure.

NOTE 3 – The QoS mapping can be performed in an access node and a relay node.

8 Functional requirements of QoS assurance for QKDN

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 also specified below for each category.

8.1 Quality of service planning requirements for QKDN

– QKDN is required to support service-driven QoS planning for QKDN.

NOTE – Service-driven QoS planning means an intent-based QoS planning. The capability of mapping the intent (business objectives) into SLA is associated with this requirement (e.g., a gold service as an intent can be translated into SLA specific parameters such as target latency, jitter, and throughput).

– QKDN is required to support SLA-based QoS planning for QKDN.

– QKDN is required to convert service models to traffic models accurately.

– QKDN is required to support an accurate estimate of network coverage, capacity and resources demands.

– QKDN is recommended to estimate and allocate network resources in a way that maximizes its utilization.

8.2 Quality of service monitoring requirements for QKDN

– QKDN is required to provide a mechanism for supporting real-time E2E (End to end) QoS monitoring.

– QKDN is required to measure and analyse the throughput of quantum key generation.

– QKDN is required to measure and analyse KSA key response delays.

– QKDN is recommended to measure and analyse KSA key delivery error ratio (KKDER).

– QKDN is recommended to measure and analyse KSA key delivery loss ratio (KKDLR).

– QKDN is recommended to measure and analyse the QoS class of real-time control and management traffic.

– QKDN is required to measure and analyse the amount of QKD key generated by QKD system per unit time by the QKD module.

– QKDN is recommended to measure and analyse the quantum bit error rate (QBER).

– QKDN is recommended to measure and analyse the operating frequency which is the frequency of sending quantum signals when a pair of QKD devices work together.

– QKDN is required to provide performance analysis information to provisioning and optimization functional entities to support QoS-based provisioning and optimization.

– QKDN is recommended to expose QoS capability to the user network.

8.3 Quality of service optimization requirements for QKDN

– QKDN is optional to support QoS-based resource utilization optimization.

– QKDN is recommended to assure optimal throughput of quantum key generation.

– QKDN is recommended to optimize response delay.

– QKDN is recommended to optimize KSA key error ratio (QKER).

– QKDN is recommended to optimize KSA key loss ratio (QKLR).

– QKDN is recommended to optimize QoS class for real-time control and management traffic.

– QKDN is recommended to optimize the amount of final key generated by QKD system per unit time by the QKD module.

– QKDN is recommended to optimize quantum bit error rate (QBER).

– QKDN is recommended to optimize operating frequency which is the frequency of sending quantum signals when a pair of QKD devices work together.

8.4 Quality of service provisioning requirements for QKDN

– QKDN is recommended to provision network and key-related resources in a way that maximizes its utilization.

– QKDN is required to support QoS provisioning policy control of the QKDN controller.

– QKDN is required to support QoS-based routing and rerouting provisioning control of the QKDN controller.

– QKDN is required to support QoS-based fault associated provisioning of the QKDN fault manager.

– QKDN is required to support QoS-based performance associated provisioning of the QKDN performance manager.

– QKDN is recommended to support the availability and reliability of quantum key distribution by providing QoS-based provisioning of redundancy of QKD links provided by the quantum layer.

– QKDN is required to support service-driven QoS provisioning.

– QKDN is required to support SLA-based QoS provisioning.

– QKDN is recommended to support cross-layer QoS provisioning.

8.5 Quality of service protection/recovery requirements for QKDN

– QKDN is recommended to assure key request session recovery ratio.

– QKDN is recommended to assure recovery wavelength reservation ratio.

– QKDN is recommended to assure recovery time.

9 Security considerations

This Recommendation describes the high-level and functional requirements of QoS assurance for quantum key distribution networks (QKDN), 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

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

Printed in Switzerland
Geneva, 2021