International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3807

(02/2022)

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 – Quality of service parameters

Recommendation ITU-T Y.3807

ITU-T

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.3807

Quantum key distribution networks – Quality of service parameters

Summary

Recommendation ITU-T Y.3800 specifies an overview on networks supporting quantum key distribution (QKD). For the purpose of design, deployment, operation and maintenance to support QKD network (QKDN) implementation, the required quality level of quantum key distribution service should be identified and quantified.

Recommendation ITU-T Y.3806 describes high-level and functional quality of service (QoS) requirements for QKDN.

Recommendation ITU-T Y.3807 describes QoS and network performance (NP) on QKDN and specifies the associated relative parameters for QoS and their definitions.

This Recommendation helps to quantify what kind of QoS requirements should be monitored and measured for this purpose; QoS parameters.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T Y.3807	2022-02-13	13	11.1002/1000/14864

Keywords

Network performance, quality of service, quantum key distribution, 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

Recommendation ITU-T Y.3807

Quantum key distribution networks – Quality of service parameters

1 Scope

This Recommendation specifies quality of service (QoS) parameters on the quantum key distribution network (QKDN) for the purpose of network operation and maintenance as follows:

– Descriptions of QoS and network performance (NP) on QKDN

– Classification of performance concerns for which parameters may be needed

– QoS parameters of QKDN

– Network performance supporting factors

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

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

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 key management [ITU-T Y.3800]: All activities performed on keys during their life cycle starting from their reception from the quantum layer, storage, formatting, relay, synchronization, authentication, to supply to a cryptographic application and deletion or preservation depending on the key management policy.

3.1.2 key supply agent-key (KSA-key) [b-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.

3.1.3 network performance (NP) [b-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.

3.1.4 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]).

3.1.5 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.

3.1.6 quantum key distribution (QKD) module [ITU-T Y.3800]: A set of hardware and software components that implements cryptographic functions and quantum optical processes, including quantum key distribution (QKD) protocols, synchronization, distillation for key generation, and is contained within a defined cryptographic boundary.

3.1.7 quantum key distribution network (QKDN) [ITU-T Y.3800]: A network comprised of two or more quantum key distribution (QKD) nodes connected through QKD links.

3.1.8 user network [ITU-T Y.3800]**:** A network in which cryptographic applications consume keys supplied by a quantum key distribution (QKD) network.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CA	Cryptographic Application
KKDER	KSA-key Delivery Error Ratio
KKDLR	KSA-key Delivery Loss Ratio
KKRD	KSA-key Response Delay
KKRDV	KSA-key Response Delay Variation
KSA	Key Supply Agent
NP	Network Performance
QKD	Quantum Key Distribution
QKDN	Quantum Key Distribution Network
QoS	Quality of Service

5 Conventions

None.

6 Introduction

[ITU-T Y.3800] identifies the layered model-based conceptual structure of the quantum key distribution network (QKDN) and user network. From the user network's perspective, it is expected that the required quality level of quantum key distribution (QKD) service is supported in a way to be observed and measured; where quality of service (QoS) can be observed and measured. On the other hand, it should consider how to support the required quality level of QKD service from QKDN's perspective in the same way; where network performance (NP) can be observed and measured.

Figure 1 shows the demarcation boundary to clarify the QoS and the NP in QKDN. QoS and NP can be observed and measured at the boundary between the user network and QKDN.

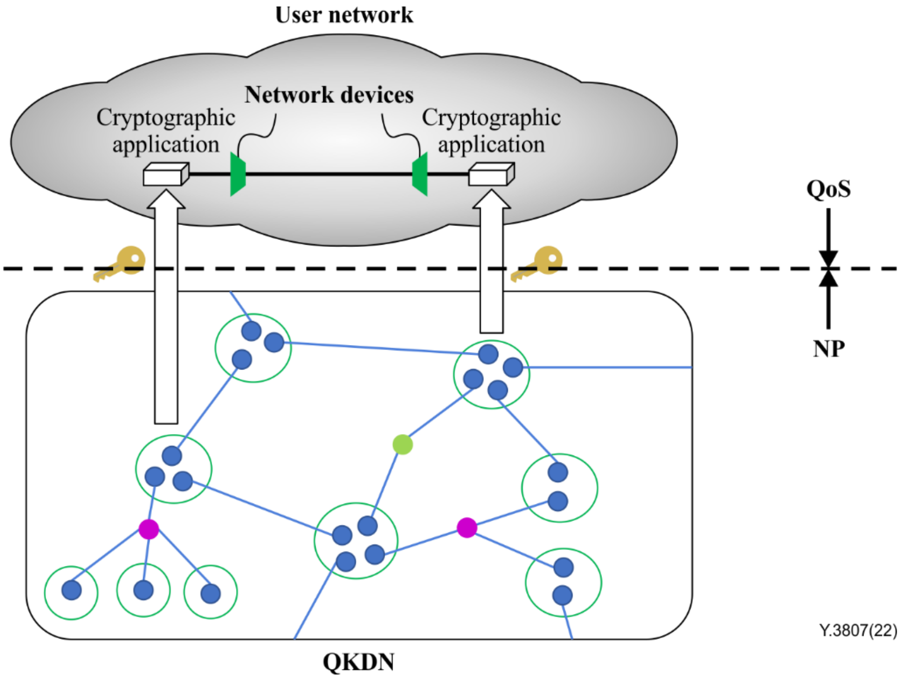


Figure 1 – QoS and NP in a QKD network

In this Recommendation, a study is focusing on QKDN itself and the quality of user network is out of scope.

QoS is defined in [b-ITU-T E.800] as 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."*

The definition of QoS in [b-ITU-T E.800] is a wide one encompassing many areas of work, including subjective customer satisfaction. However, within this Recommendation, the aspects of QoS in QKDN that are covered are restricted to the identification of parameters that can be directly observed and measured at the point at which the QKD service is accessed by the user network (i.e., 99.99% of QKD service availability).

NP is measured in terms of parameters which are meaningful to the QKDN provider and are used for the purpose of design, configuration, control and management of QKDN. NP is defined independently of the user network (i.e., 10 ms delay of key relay between two adjacent QKD nodes).

Table 1 shows some of the characteristics which distinguish QoS and NP in QKDN.

Table 1 – Distinction between QoS and NP in QKDN

QoS	NP
User network-oriented	QKDN operator-oriented
Service attribute	Network elements attribute
Focus on user network-observable effects	Focus on planning, design, control and management
Between (at) QKD service access points	End-to-end or QKDN elements capabilities

7 QoS aspect of QKDN

As shown in Figure 1, from the QoS aspect of QKDN, the demarcation boundary between the user network and QKDN is the only point of interest. Relative procedures in the boundary should be identified as shown in Figure 2.

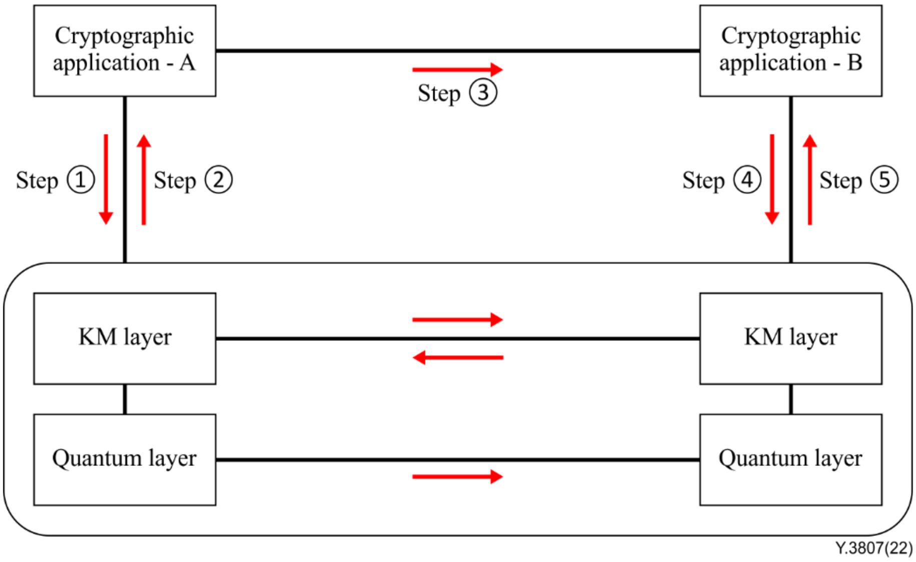


Figure 2 – The possible KSA key supply procedures

- Step①; cryptographic application-A (CA-A) requests to supply KSA-key into QKDN
- Step②; QKDN supplies requested KSA-key to CA-A
- Step③; CA-A sends notification message to CA-B
- Step④; CA-B requests to supply KSA-key into QKDN
- Step⑤; QKDN supplies requested KSA-key to CA-B

The main purpose of QKDN is to supply symmetric KSA-keys to user network. The overall QoS evaluation should be based on the events of completion on the supply. In this document, the evaluated events of QoS are related to step① and step⑤.

The observations of step① and step⑤ can be classified in three events as successful, errored and lost events, as shown in Figure 3.

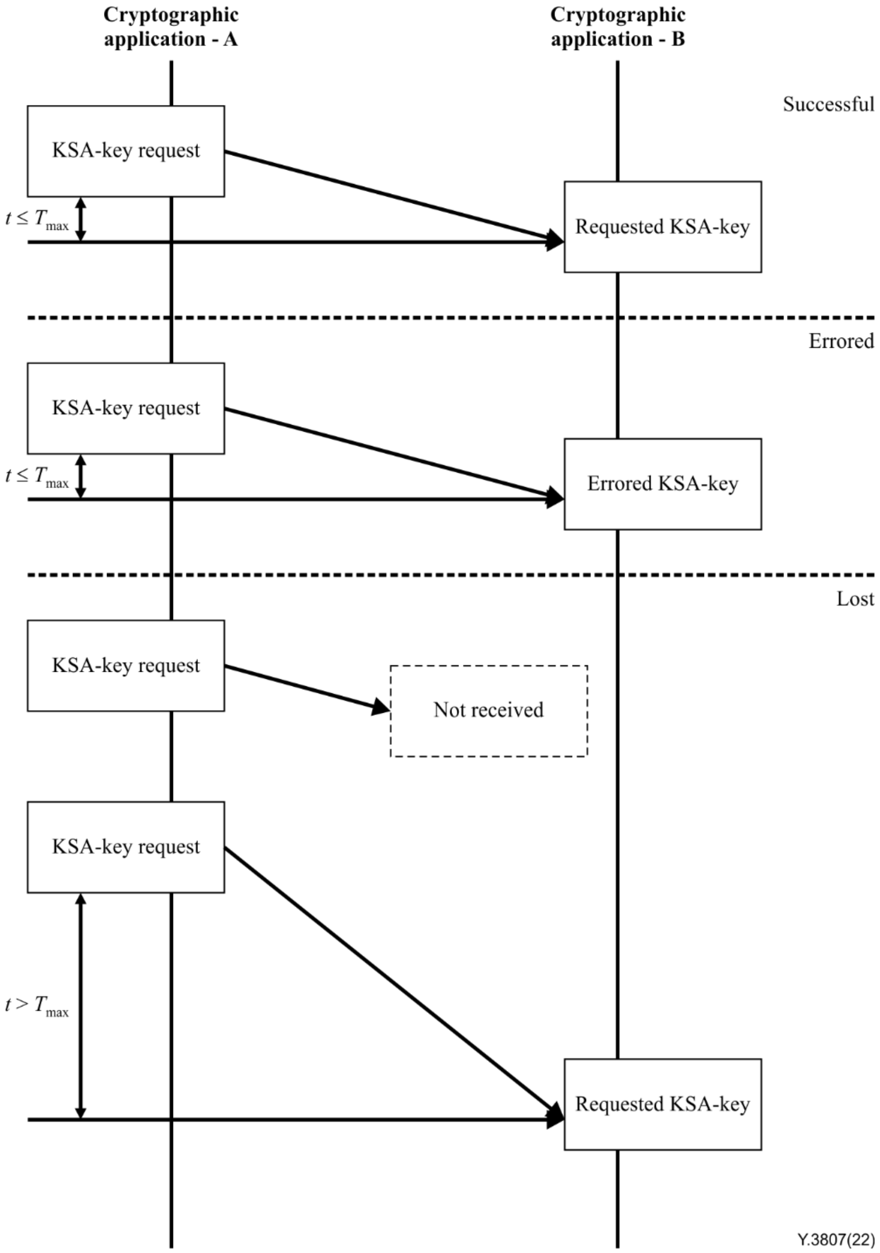


Figure 3 – The observed events on demarcation boundary

The time taken by step③ is determined by the cryptographic application and is not associated with QoS of the QKDN itself. Such delays and any instances where a cryptographic application does not make a request to both nodes or does not accept a response from the QKDN may be excluded from QKDN QoS measurement results which influence QoS parameters. The calculation of QoS parameters may be modified accordingly.

8 QoS parameters of QKDN

8.1 Throughput

It is useful to characterize performance in terms of throughput that is used to evaluate the ability of QKDN to generate and supply quantities of KSA-keys. It should be noted that a parameter intended to characterize the throughput of a boundary would not be equal to the number of generated KSA-keys from the QKDN. This is because the KSA-keys can experience errors or loss during delivery from the QKDN to the boundary.

Throughput is defined for the total number of KSA-keys successfully received during a specified time interval divided by the time interval duration (equivalently, the number of successfully received KSA-keys per service-second).

8.2 KSA-key response delay (KKRD)

Once the user network asks QKDN to send the KSA-key, the reaction timing should be measured in terms of response delay. The KSA-key response delay (KKRD) could be calculated as follows.

KKRD is defined for all successful and errored KSA-keys across the boundary. KKRD is the time, (T_B – T_A) between the occurrence of two corresponding events, the sending of KSA-key request message at time-A (T_A) in CA-A and the receiving of the requested KSA-key at time-B (T_B) in CA-B, where ($T_B > T_A$).

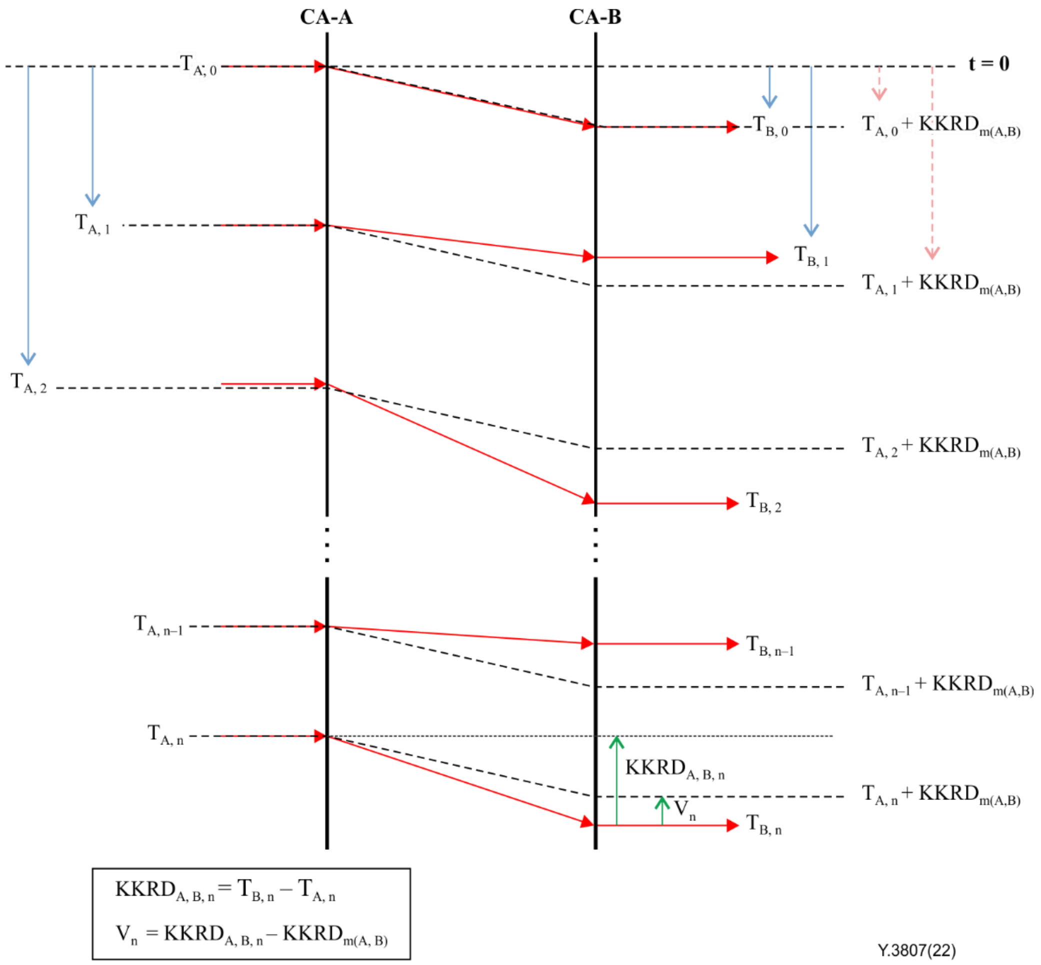
KKRD can be measured for every occurrence of a KSA-key request by CA-A that is followed by a corresponding key being successfully received by CA-B, $\text{KKRD}_{A,B,n}$.

8.3 KSA-key response delay variation (KKRDV)

The variations in KKRD are also important. Some types of cryptographic applications aim to replace keys with fresh keys from a key supply agent (KSA) on a periodic schedule. Extreme variations in KKRD could lead to a key refresh not completing with any required time period.

KSA-key response delay variation (KKRDV) is defined based on the observations of corresponding KSA-key request's sending events at CA-A and the requested KSA-key's receiving events at CA-B. These observations characterize the variability in the pattern of actual KSA-key receiving events in comparison to the median KKRD.

The KKRDV for KSA-keys is the difference between the actual KKRD ($\text{KKRD}_{A,B,n}$) and a median KKRD ($\text{KKRD}_{m(A,B)}$) between CA-A and CA-B (see Figure 4); $V_n = \text{KKRD}_{A,B,n} - \text{KKRD}_{m(A,B)}$



CA-A
CA-B
t = 0
$T_{A,0}$
$T_{B,0}$
$T_{A,0} + KKRD_{m(A,B)}$
$T_{A,1}$
$T_{B,1}$
$T_{A,1} + KKRD_{m(A,B)}$
$T_{A,2}$
$T_{A,2} + KKRD_{m(A,B)}$
$T_{B,2}$
$T_{A,n-1}$
$T_{B,n-1}$
$T_{A,n-1} + KKRD_{m(A,B)}$
$T_{A,n}$
$KKRD_{A,B,n}$
$T_{A,n} + KKRD_{m(A,B)}$
V_n
$T_{B,n}$
$KKRD_{A,B,n} = T_{B,n} - T_{A,n}$
$V_n = KKRD_{A,B,n} - KKRD_{m(A,B)}$
Y.3807(22)

Variables:
$T_{A,n}$: KSA-key request sending time at CA-A
$T_{B,n}$: Requested KSA-key's actual receiving time at CA-B
$KKRD_{A,B}$: Actual response delay of KSA-keys between CA-A and CA-B
$KKRD_{m(A,B)}$: Median response delay of KSA-keys between CA-A and CA-B
V_n: KKRDV value between CA-A and CA-B

Figure 4 – QoS parameter; KSA-key response delay variation

8.4 KSA-key delivery error ratio (KKDER)

KKDER is the ratio of total errored KSA-keys to the total of successfully received KSA-keys plus errored KSA-keys.

8.5 KSA-key delivery loss ratio (KKDLR)

KKDLR is the ratio of total lost KSA-keys to the total of successfully received KSA-keys plus lost KSA-keys.

8.6 Availability

The QoS parameters which are defined above are intended to characterize QKDN in the available state. An availability serves to classify the total scheduled service time for a QKD service into available and unavailable periods. On the basis of this classification, both the percent QKDN availability and the percent QKDN unavailability should be specified.

NOTE – The scheduled service time for QKDN is assumed to be 24 hours a day, seven days a week.

8.6.1 Service restoration time

Service restoration time is defined as the time from KSA-key not-supplied to the time KSA-key re-supplied.

NOTE – The performance parameters defined in this Recommendation can be measured by in-service and out-of-service measurement methods. In order to implement these methods, new functions could be added; time stamp and numbering of KSA-keys (in-service) or the user network could inform those functions into the QKDN manager through the Mu reference point introduced in [ITU-T Y.3802] (out-of-service). The details of the functions are out of scope of this Recommendation.

9 Network performance supporting factors

9.1 Network performance related physical elements

9.1.1 Link distance

Link distance can negatively influence delay-related parameters as longer links are introduced.

9.1.2 Link complexity

Link complexity can negatively influence delay/error-related parameters as more QKD nodes are introduced.

9.1.3 Key storage and pool

Storing of keys may influence delay-related parameters as longer remaining is introduced.

10 Security considerations

In order to mitigate security threats and potential attacks, issues of confidentiality, integrity, authenticity, non-repudiation, availability and traceability need to be addressed, and appropriate security and privacy protection schemes should be considered in the QoS aspects of QKDN. Details are outside the scope of this Recommendation.

Bibliography

[b-ITU-T E.417]	Recommendation ITU-T E.417 (2005), *Framework for the network management of IP-based networks*.
[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 P10/G.100 (2017), *Vocabulary for performance, quality of service and quality of experience*.
[b-ITU-T Y.3801]	Recommendation ITU-T Y.3801 (2020), *Functional requirements for quantum key distribution networks*.
[b-ITU-T Y.3803]	Recommendation ITU-T Y.3803 (2020), *Quantum key distribution networks – Key management*.
[b-ITU-T Y.3804]	Recommendation ITU-T Y.3804 (2020), *Quantum key distribution networks – Control and management*.
[b-ITU-T Y.3806]	Recommendation ITU-T Y.3806 (2021), *Quantum key distribution networks – Requirements for quality of service assurance*.
[b-ETSI GR QKD 007]	ETSI GR QKD 007 (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

Printed in Switzerland
Geneva, 2022