ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T Y.3813 (01/2023)

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 – Functional requirements

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.3813

Quantum key distribution network interworking – Functional requirements

Summary

For quantum key distribution networks (QKDNs), Recommendation ITU-T Y.3813 specifies functional requirements for QKDN interworking (QKDNi). This Recommendation describes the functional requirements for the key management layer, QKDN control layer and QKDN management layer, for interworking using gateway nodes (GWNs) and/or interworking nodes (IWNs).

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3813	2023-01-13	13	11.1002/1000/15243

Keywords

Quantum key distribution (QKD), QKD network (QKDN), QKDN interworking (QKDNi).

* 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.3813

Quantum key distribution networks interworking – Functional requirements

1 Scope

This Recommendation specifies the functional requirements for quantum key distribution network (QKDN) interworking (QKDNi) as follows.

– Functional requirements for the key management layer;

– Functional requirements for the QKDN control layer;

– Functional requirements for the QKDN management layer.

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.3810] Recommendation ITU-T Y.3810 (2022), *Quantum key distribution networks - interworking framework.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 key manager (KM) [b-ITU-T Y.3800]: A functional module located in a quantum key distribution (QKD) node to perform key management in the key management layer.

3.1.2 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.

3.1.3 quantum key distribution link (QKD link) [b-ITU-T Y.3800]: A communication link between two quantum key distribution (QKD) modules to operate the QKD.

NOTE – A QKD link consists of a quantum channel for the transmission of quantum signals, and a classical channel used to exchange information for synchronization and key distillation.

3.1.4 quantum key distribution module (QKD module) [b-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.

NOTE – A QKD module is connected to a QKD link, acting as an endpoint module in which a key is generated. These are two types of QKD modules, namely, the transmitters (QKD-Tx) and the receivers (QKD-Rx).

3.1.5 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.

3.1.6 quantum key distribution network controller (QKDN controller) [b-ITU-T Y.3800]: A functional module, which is located in a quantum key distribution (QKD) network control layer to control a QKD network.

3.1.7 quantum key distribution network manager (QKDN manager) [b-ITU-T Y.3800]: A functional module, which is located in a quantum key distribution (QKD) network management layer to monitor and manage a QKD network.

3.1.8 quantum key distribution node (QKD node) [b-ITU-T Y.3800]: A node that contains one or more quantum key distribution (QKD) modules protected against intrusion and attacks by unauthorized parties.

NOTE – A QKD node can contain a key manager (KM).

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

GWF	Gateway Function
GWN	Gateway Node
IWF	Interworking Function
IWN	Interworking Node
KM	Key manager
OTP	One-time pad encryption
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
QKDN	QKD Network
QKDNi	QKDN interworking

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 with 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

The functional requirements for QKDNi are specified in order to meet QKDNi capabilities and the layer structure described in [ITU-T Y.3810].

This Recommendation specifies the functional requirements for QKDNi using gateway nodes (GWNs) and interworking nodes (IWNs) as specified in [ITU-T Y.3810]. The functional requirements are defined for the key management layer, QKDN control layer and QKDN management layer.

Based on the functions (i.e., gateway function (GWF) and interworking function (IWF)) and the reference models for QKDNi specified in [ITU-T Y.3810], keys can be relayed between GWNs, and keys can be transferred in the IWN.

7 Functional requirements for the key management layer

7.1 Key management layer requirements for QKDNi

Req_KM 1. The key management layers of interworking QKDNs are required to receive keys from their own QKD module(s).

Req_KM 2. The key management layers of interworking QKDNs are recommended to receive status information of the interworking QKD module(s).

Req_KM 3. The key management layers of interworking QKDNs are recommended to exchange key metadata between QKDNs, such as key ID, QKD module ID and key generation date.

Req_KM 4. The key management layers of interworking QKDNs are recommended to share key management information between QKDNs.

NOTE – Information on key management may include information such as to which KM the key is transferred, timestamp, the cryptographic application to which the key is supplied, shared key number of a KM link, key consumption rate, KM link status, accounting and alarm on fault.

7.2 Key management layer requirements for QKDNi with GWNs

Req_KM 5. The key management layers of interworking QKDNs are required to support key relays between GWNs.

NOTE – Secure key relay with OTP encryption between GWNs is defined in [ITU-T Y.3810].

7.3 Key management layer requirements for QKDNi with IWNs

Req_KM 6. The key management layers of interworking QKDNs are required to support key transfers in the IWN.

NOTE – Secure key transfer in the IWN is defined in [ITU-T Y.3810].

8 Functional requirements for the QKDN control layer

8.1 QKDN control layer for QKDNi

Req_C 1. The QKDN control layers of interworking QKDNs are recommended to share QKDN control information between QKDNs.

NOTE – QKDN control information on QKDN control layer may include routeing control information, session control information, authentication control information and quality of service (QoS) policy control information.

Req_C 2. The QKDN control layers of interworking QKDNs are recommended to provide charging policy control between QKDNs.

Req_C 3. The QKDN control layers of interworking QKDNs are recommended to support access control to perform authentication.

NOTE – The authentication between QKDNs can be based on their certificates.

Req_C 4. The QKDN control layers of interworking QKDNs are recommended to exchange QKDN routeing control information to support the interworking route.

NOTE – QKDN routeing control information may include QKD node addresses, KM IDs, key consumption rate and residual number of keys from the KMs.

Req_C 5. The QKDN control layers of interworking QKDNs are recommended to work together to provide routeing control for interworking.

8.2 QKDN control layer for QKDNi with GWNs

Req_C 6. The QKDN control layers of interworking QKDNs are recommended to provide session control to relay the key between GWNs.

NOTE – The session in GWN is the communication to relay the key between QKDNs.

8.3 QKDN control layer for QKDNi with IWNs

Req_C 7. The QKDN control layers of interworking QKDNs are recommended to provide session control to transfer the key in the IWN.

NOTE – Keys can then be transferred between two KMs through Kxi' within the secure operational environment of the IWN, and an IWN might contain multiple KMs.

9 Functional requirements for QKDN management layer

NOTE – [ITU-T Y.3810] has defined that network topologies and technology are not usually disclosed to other QKDN providers even in interworking cases, and that interworking interfaces are strictly prohibited to transfer unauthorized information.

9.1 QKDN management layer for QKDNi

Req_M 1. The QKDN management layers of interworking QKDNs are recommended to provide configuration management to support:

– managing of resource provisioning between QKDNs.

Req_M 2. The QKDN management layers of interworking QKDNs are recommended to provide fault management to support:

– capabilities of monitoring, detecting and diagnosing between QKDNs;

– management of failure resolving policies, and interactions with relevant functional components for healing actions between QKDNs.

Req_M 3. The QKDN management layers of interworking QKDNs are recommended to provide accounting management to support:

– key supply services and their policies between QKDNs;

– costs determination of key usage between QKDNs.

Req_M 4. The QKDN management layers of interworking QKDNs are recommended to provide performance management to support:

– monitoring and analysing the performance status of QKDNi;

– analysing the QKDN performance information collected/received from QKDNi;

– quality of service (QoS) of key supply between QKDNs.

Req_M 5. The QKDN management layers of interworking QKDNs are recommended to provide security management to support:

– collecting/receiving security related management information between QKDNs;

– management of authentication and authorization between QKDNs;

– the key life cycle management between QKDNs.

Req_M 6. The QKDN management layers of interworking QKDNs can optionally share status information.

NOTE – Status information shared between QKDNs may include information such as quantum bit error rate (QBER), key rate and QKD link status.

Req_M 7. The QKDN management layers of interworking QKDNs are recommended to provide configuration management to support:

– routeing and rerouteing for interworking.

Req_M 8. The QKDN management layers of interworking QKDNs are recommended to provide fault management to support:

– routeing and rerouteing for interworking as needed in case of the faults.

10 Security considerations

In order to mitigate security threats and potential attacks issues of, for example, confidentiality, integrity, authenticity, non-repudiation, availability and traceability need to be addressed, and appropriate security and privacy protection schemes should be considered in the QKDN, the user network and the interfaces between the two networks. Details are outside the scope of this Recommendation.

Bibliography

[b-ITU-T Y.3800] Recommendation ITU-T Y.3800 (2019)/Corr.1 (2020), *Overview on networks supporting quantum key distribution.*

[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

Published in Switzerland
Geneva, 2023