International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3801

(04/2020)

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

Cloud Computing

Functional requirements for quantum key distribution networks

Recommendation ITU-T Y.3801

ITU-T

International Telecommunication Union

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
Network control architectures and protocols	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.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.3801

Functional requirements for quantum key distribution networks

Summary

In the context of quantum key distribution networks (QKDNs), Recommendation ITU-T Y.3801 specifies the functional requirements for quantum layer, the key management layer, the QKDN control layer and the QKDN management layer.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3801	2020-04-29	13	11.1002/1000/14258

Keywords

QKD (quantum key distribution), QKDN (QKD network), QKDN functional requirements.

* 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, 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 TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.3801

Functional requirements for quantum key distribution networks

1 Scope

This Recommendation specifies the functional requirements for quantum key distribution networks (QKDN) as follows:

– functional requirements for quantum layer;

– functional requirements for key management layer;

– functional requirements for QKDN control layer;

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

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 access control [b-ITU-T X.800]: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

3.1.2 classical channel [b-ETSI GR QKD 007]: Communication channel that is used by two communicating parties for exchanging data encoded in a form that may be non-destructively read and fully reproduced.

3.1.3 information theoretically secure (IT-secure) [ITU-T Y.3800]: Secure against any deciphering attack with unbounded computational resources.

3.1.4 key life cycle [ITU-T Y.3800]: A sequence of steps that a key undergoes from its reception by a key manager (KM) through its use in a cryptographic application and until deletion or preservation depending on the key management policy.

3.1.5 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.

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

3.1.7 key manager link (KM link) [ITU-T Y.3800]: A communication link connecting key managers (KMs) to perform key management.

3.1.8 key relay [ITU-T Y.3800]: A method to share keys between arbitrary quantum key distribution (QKD) nodes via intermediate QKD node(s).

3.1.9 key supply [ITU-T Y.3800]: A function providing keys to cryptographic applications.

3.1.10 quantum channel [b-ETSI GR QKD 007]: Communication channel for transmitting quantum signals.

3.1.11 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.

3.1.12 quantum key distribution link (QKD link) [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.

3.1.13 quantum key distribution module (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.

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 and the receivers.

3.1.14 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.

NOTE – A QKDN allows sharing keys between the QKD nodes by key relay when they are not directly connected by a QKD link.

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

3.1.16 quantum key distribution network manager (QKDN manager) [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.

3.1.17 quantum key distribution node (QKD node) [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).

3.1.18 quality of service (QoS) [b-ITU-T Q.1743]: The collective effect of service performances, which determine the degree of satisfaction of a user of a service. It is characterized by the combined aspects of performance factors applicable to all services, such as:

– service operability performance;
– service accessibility performance;
– service retainability performance;
– service integrity performance; and
– other factors specific to each service.

3.1.19 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:

AES Advanced Encryption Standard

IT-secure Information Theoretically secure

KM Key Manager

OTP One-Time Pad

QKD Quantum Key Distribution

QKDN QKD 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.

Some requirements in this Recommendation refer to information (i.e., key management, status, fault, performance, accounting, configuration, security related information) provided by entities within a quantum key distribution network (QKDN) for control and/or management purposes. The information provided under a requirement will depend on the use case and/or implementation. How to specify the information included is outside the scope of this Recommendation and the selection made in an implementation will not prevent a claim of conformance with this Recommendation.

In this Recommendation, "key" means "symmetric random bit strings" produced by QKDN.

6 Introduction

Clauses 7 to 10 specify the functional requirements for QKDN, meeting the QKDN capabilities and the layer structure of QKDN specified in [ITU-T Y.3800]. Since the scope of this Recommendation is to specify the functional requirements from the network aspect, some security requirements are mentioned when the requirement is directly related to the security of keys. General security management of a whole QKDN and detailed security issues in each layer and trusted node are outside the scope of this Recommendation.

7 Functional requirements for quantum layer

To generate keys in a QKDN, quantum key distribution (QKD) protocols should meet the following requirements:

Req_Q.1 The QKD protocols are required to be provably secure and allow IT-secure key establishment.

To generate keys in a QKDN, a QKD module should meet the following requirements:

Req_Q.2 The QKD module is required to implement functions that are necessary to execute one or more QKD protocols with a corresponding QKD module connected by a QKD link.

NOTE 1 – Functions of the QKD modules may include random number generation, quantum communication, distillation for key generation, and quantum channel synchronization.

NOTE 2 – The QKD module acts as an endpoint module in which a key is generated.

NOTE 3 – A QKD link may include one or more quantum relay point(s) to extend a distance of QKD as described in [ITU-T Y.3800].

Req_Q.3 The QKD module is required to be contained within a defined cryptographic boundary.

Req_Q.4 A pair of QKD modules connected by a QKD link is required to transfer a key to corresponding key managers (KMs) via an appropriate interface.

Req_Q.5 The QKD module is recommended to provide status information of the QKD module and optionally of the QKD link to the KM.

Req_Q.6 The QKD module is required to provide status information of the QKD module and optionally of the QKD link to the QKDN controller.

Req_Q.7 The QKD module is required to provide fault and performance information of the QKD module to the QKDN manager.

8 Functional requirements for key management layer

To manage keys in a QKDN securely, reliably, and efficiently, a KM should meet the following requirements:

Req_KM 1 The KM is recommended to be compatible with various kinds of QKD modules which implement different protocols.

Req_KM 2 The KM is required to receive keys from a QKD module(s) via an appropriate interface, and to store them securely when storage is necessary.

Req_KM 3 The KM is recommended to format keys where necessary for internal purposes or for key supply or key relay, including combining or splitting where lengths are not appropriate.

Req_KM 4 The KM is recommended to receive status information of QKD module(s) and QKD link(s) from the QKD module(s) in the quantum layer.

NOTE 1 – The KM can forward the status information to the QKDN controller.

Req_KM 5 The KM is required to provide:

– information on key management for QKDN control functions to the QKDN controller;

– information on key management for QKDN management functions to the QKDN manager;

– fault and performance information of the KM and KM links to the QKDN manager.

NOTE 2 – Information on key management may include information such as which QKD module the key comes from, which node the key is relayed to, timestamp, the cryptographic application to which the key is supplied, shared key amount of a KM link, key consumption rate, KM link status, accounting and alarm on fault.

Req_KM 6 The KM is recommended to support key relay employing highly secure encryption (e.g., one-time pad (OTP) [b-Shannon 1949]) via trusted node(s) to establish keys between any two remote KMs connected to a QKDN with three or more nodes.

Req_KM 7 The KM is recommended to support another appropriate method (e.g., advanced encryption standard (AES) [b-ISO/IEC 18033-3], [b-FIPS PUB 197]) for key relay according to key management policy.

Req_KM 8 To make key relay reliable and secure, the KMs and KM links are recommended to have capabilities of key synchronization, entity authentication and message authentication.

Req_KM 9 To make key relay efficient, the KMs are recommended to cooperate with each other under the control of the QKDN controller.

Req_KM 10 Where a QKD node supplies keys by design or configuration to the user network, the following requirements are applied:

– the KM is required to receive key requests from authorized cryptographic applications via the key supply interface;

NOTE 3 – In some cases key requests are received by the KM through a KM link.

– the KM is required to supply the requested number of keys to a cryptographic application in the service layer of the user network via a key supply interface, subject to any key management policies, when sufficient keys are available;

– the KM is required to supply keys to cryptographic applications in the service layer of the user network via a key supply interface with security capabilities;

– the KM is recommended to present a key supply interface that various cryptographic applications in the service layer of the user network can utilize;

NOTE 4 – Cryptographic applications may have diverse requirements and run on various environments. Design goals for key supply interfaces include broad usability and flexible extensibility for current and future applications.

– the KM is recommended to support access control of cryptographic applications.

– the KM is required to apply the key management policy.

NOTE 5 – Key management policy may include deleting the keys or preserving the keys in key storage after the key supply has been executed.

Req_KM 11 The KM is required to provide elements of key life cycle management.

9 Functional requirements for QKDN control layer

To control a QKDN for secure, stable, efficient, and robust operations and services, a QKDN controller should meet the following requirements:

Req_C 1 The QKDN controller is required to provide routing control of key relay if the key relay function is supported by a QKDN.

Req_C 2 The QKDN controller is recommended to provide configuration control of QKD modules, QKD links, KMs and KM links.

Req_C 3 The QKDN controller is recommended to provide charging policy control.

Req_C 4 The QKDN controller is recommended to provide quality of service (QoS) policy control.

Req_C 5 The QKDN controller is recommended to support and ensure access control of functional elements in the quantum layer and the key management layer.

Req_C 6 The QKDN controller is recommended to provide session control.

NOTE – The session is the communication between KMs to establish the end-to-end key or to supply keys to cryptographic applications in the service layer of the user network. The session control initiates, maintains, and terminates the session.

Req_C 7 The QKDN controller is recommended to provide fault, performance, accounting, and configuration information to a QKDN manager.

10 Functional requirements of QKDN management layer

To support monitoring, and management of a QKDN as a whole, and to support user network management, a QKD manager should meet the following requirements.

Req_M 1 The QKDN manager is required to provide fault management to support:

– collecting/receiving status information provided by the quantum, key management, and QKDN control layers;

– analysing the status information collected/received for fault indicators.

Req_M 2 The QKDN manager is recommended to provide fault management to support:

– root-cause analysis capability;
– diagnosis capability;
– management of failure resolving policies, and interactions with relevant functional components for healing actions.

Req_M 3 The QKDN manager is required to provide configuration management to support:
– management of resource provisioning.

Req_M 4 The QKDN manager is recommended to provide configuration management to support:
– routing and rerouting of key relay if the QKDN supports key relay.
– collecting and managing a network topology;
– resource configuration for inventory management;
– changing of managed resources based on the demand and availability;
– discovering QKD managed resources in the managed QKDN.

Req_M 5 The QKDN manager is recommended to provide accounting management to support:
– key supply services and their policies.

Req_M 6 The QKDN manager is required to provide performance management to support:
– collecting/receiving performance information from the quantum layer, the key management layer and the QKDN control layer;
– analysing the QKDN performance information collected/received.

Req_M 7 The QKDN manager is recommended to provide performance management to support:
– QoS of key supply;
– management of key supply service policies.

Req_M 8 The QKDN manager is required to provide security management to support:
– collecting/receiving security related management information from the QKDN.

Req_M 9 The QKDN manager is required to support key life cycle management for KMs.

Req_M 10 The QKDN manager is recommended to provide security management to support:
– management of authentication and authorization.

Req_M 11 The QKDN manager is recommended to perform cross-layer management orchestration and also to support management requests from a user network management.

11 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 QKDN, the user network and interfaces between the two networks. Details are outside the scope of this Recommendation.

Bibliography

[b-ITU-T Q.1743] Recommendation ITU-T Q.1743 (2016), *IMT-Advanced references to Release 11 of LTE-Advanced evolved packet core network*.

[b-ITU-T X.800] Recommendation ITU-T X.800, *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ETSI GR QKD 007] ETSI GR QKD 007 (2018), *Quantum Key Distribution (QKD); Vocabulary*.

[b-ISO/IEC 18033-3] ISO/IEC 10833-3:2010 (2010), *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers.*

[b-FIPS PUB 197] Federal Information Processing Standards Publication 197 (2001), *Announcing the ADVANCED ENCRYPTION STANDARD (AES)*.

[b-Shannon 1949] Shannon, Claude, 1949, *Communication Theory of Secrecy Systems*, Bell System Technical Journal, vol. 28, pp. 666–682.

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, 2020