

Recommendation

ITU-T Y.3821 (04/2024)

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 resilience



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.3821

Quantum key distribution networks – requirements for resilience

Summary

For quantum key distribution networks (QKDN), Recommendation ITU-T Y.3821 specifies the general requirements for resilience, and separately specifies the requirements for supporting protection and recovery.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T Y.3821	2024-04-29	13	11.1002/1000/15876

Keywords

Quantum key distribution (QKD), QKD network (QKDN), requirement, resilience.

* 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/>.

© ITU 2024

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

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.....	2
4 Abbreviations and acronyms	2
5 Conventions	2
6 Introduction.....	2
7 General requirements for QKDN resilience	3
7.1 Requirements for quantum layer to support resilience.....	3
7.2 Requirements for key management layer to support resilience.....	3
7.3 Requirements for control layer to support resilience.....	3
7.4 Requirements for management layer to support resilience	3
8 Requirements of protection to support resilience	3
9 Requirements of recovery to support resilience	4
Bibliography.....	5

Recommendation ITU-T Y.3821

Quantum key distribution networks - requirements for resilience

1 Scope

This Recommendation specifies the general requirements for quantum key distribution network (QKDN) resilience, as well as the requirements for supporting protection and recovery.

In particular, the Recommendation covers:

- Introduction to QKDN resilience
- General requirements for QKDN resilience
- Requirements of protection to support resilience
- Requirements of recovery to support resilience.

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.3815] Recommendation ITU-T Y.3815 (2023), *Quantum key distribution networks – overview of resilience*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 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.

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

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

3.1.4 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.

3.1.5 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.

3.1.6 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.

3.1.7 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 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.

3.1.9 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.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

FCAPS	Fault, Configuration, Accounting, Performance, Security
KM	Key Manager
KSA	Key Supply Agent
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 document is to be claimed.

The keywords "is recommended to" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Introduction

Resilience for quantum key distribution network (QKDN) [ITU-T Y.3800] is the ability to provide and maintain an acceptable service level even in the case of network failures. This Recommendation specifies the general requirements for QKDN resilience. Based on the models of protection and recovery identified in [ITU-T Y.3815], clauses 8 and 9 specify the requirements for protection and recovery to support resilience.

7 General requirements for QKDN resilience

7.1 Requirements for quantum layer to support resilience

Req_Qr 1 Additional QKD modules and links are recommended to be pre-set in advance to prevent the interruption of key supply caused by failures in working QKD modules and links.

7.2 Requirements for key management layer to support resilience

Req_KMr 1 A key manager (KM) is recommended to switch to the available key relay route allocated by control and management functions in case of failures of the working key relay route.

7.3 Requirements for control layer to support resilience

Req_Cr 1 A QKDN controller is recommended to provide resilience-oriented routing control of key relay.

NOTE – In some cases, multiple key relay routes may be allocated for resilience.

Req_Cr 2 A QKDN controller is recommended to provide resilience-oriented charging policy control.

Req_Cr 3 A QKDN controller is recommended to provide resilience-oriented session control.

Req_Cr 4 A QKDN controller is recommended to provide resilience information to a QKDN manager.

7.4 Requirements for management layer to support resilience

Req_Mr 1 A QKDN manager is recommended to provide resilience management to support:

- collecting/receiving status information of resilience-oriented functional components;
- management of resilience policies, and interactions with relevant functional components for resilience actions.

8 Requirements of protection to support resilience

Req_P 1 Protection QKD links are recommended to be pre-set for protection of key supply;

Req_P 2 Protection QKD modules are recommended to be pre-set for protection of key supply;

Req_P 3 A protection QKD module is recommended to support the same QKD protocol as the working QKD module;

Req_P 4 A protection QKD link is recommended to provide equivalent QKD capability as the protected QKD link(s);

Req_P 5 A protection QKD link is recommended to be deployed in separate optical fibre from the working QKD link;

Req_P 6 A protection QKD module /link is recommended to be pre-configured to automatically switch over to the protection QKD module /link in case of failures of the working QKD module /link;

Req_P 7 A KM is recommended to switch to the protection key relay route(s) for seamless key supply in case of failures of the working key relay route(s);

Req_P 8 A protection key relay route is recommended to provide equivalent capability to that of the protected key relay route(s) for KSA-key delivery;

Req_P 9 A QKDN controller is recommended to allocate protection key relay route to enable seamless key supply under failures;

Req_P 10 A QKDN controller is recommended to provide a QKDN manager with updated information on fault, configuration, accounting, performance, security (FCAPS) following a protection switch;

Req_P 11 A QKDN manager is recommended to record the correspondence between working QKD modules/links/key relay routes, and their respective protection QKD modules/links/key relay routes;

Req_P 12 A QKDN manager is recommended to establish and maintain protection-oriented network topology and resource information to support routing calculation for protection switching;

Req_P 13 A QKDN manager is recommended to record logs for protection switching related events to support post-event analysis;

Req_P 14 A QKDN is recommended to support coordinated protection switching that spans the quantum layer and the key management layer, and encompasses QKD modules, QKD links, and key relay routes.

9 Requirements of recovery to support resilience

Req_R 1 A KM is recommended to balance key supply rates between working and recovery key relay routes according to quality of service (QoS) considerations and security requirements of cryptographic applications;

Req_R 2 A KM is recommended to ensure seamless key supply to cryptographic applications when switching key supply to a key relay route for recovery;

Req_R 3 A QKDN controller is recommended to dynamically recalculate and establish key relay routes to recover interrupted key supply based on network conditions;

Req_R 4 A QKDN controller can optionally enable multiple key relay routes for recovery of key supply;

Req_R 5 A QKDN controller is recommended to recalculate the key relay route for recovery within the toleration time of the cryptographic application;

Req_R 6 A QKDN manager is required to record recovery operations to update the status of key relay routes;

Req_R 7 A QKDN manager is recommended to retain diagnostic information and records related to alarms for the purpose of analysing the root cause of key supply disruptions that trigger recovery mechanisms.

Bibliography

- [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