

Recommendation

ITU-T Y.3819 (12/2023)

SERIES Y: Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities

Quantum key distribution networks

Quantum key distribution networks – Requirements and architectural model for autonomic management and control enablement

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.3819

Quantum key distribution networks – Requirements and architectural model for autonomic management and control enablement

Summary

As the number and diversity of devices and other resources that make up the individual quantum key distribution networks (QKDNs) continues to grow, automating QKDN control and management tasks becomes ever-more important to avoid untimely actions and improve the quality of service (QoS). To cope with the challenges of QKDN control and management, while minimizing human intervention towards full automation of QKDN services, Recommendation ITU-T Y.3819 specifies requirements and a possible architectural model for autonomic management and control (AMC) enabled QKDN (QKDNamec) including an overview, requirements, considerations for the cognition process, an architectural model, and example procedures.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T Y.3819	2023-12-14	13	11.1002/1000/15749

Keywords

Autonomic management and control (AMC), quantum key distribution (QKD), QKD network (QKDN).

* 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 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.....	3
4	Abbreviations and acronyms	3
5	Conventions	3
6	Overview of QKDNamc	4
7	Considerations for the cognition process of QKDNamc	4
8	Requirements for QKDNamc	6
	8.1 High-level requirements for QKDNamc	6
	8.2 Functional requirements for QKDNamc	6
9	Architectural model for QKDNamc	9
	9.1 General autonomic DEs.....	10
	9.2 Functional elements for QKDNamc.....	10
	9.3 Reference points for QKDNamc	11
10	Example operational procedures of QKDNamc	11
	10.1 Example AMC operational procedure supported by ML-based quantum channel performance prediction	11
	10.2 Example AMC operational procedure supported by ML-based key storage management	13
	10.3 Example AMC operational procedure supported by ML-based key replay routing optimization	15
11	Security considerations.....	17
	Appendix I – Use cases of AMC in QKDN.....	18
	I.1 AMC for optimization of key supply in QKDN.....	18
	I.2 AMC for recovery of key supply in QKDN	18
	Bibliography.....	19

Recommendation ITU-T Y.3819

Quantum key distribution networks – Requirements and architectural model for autonomic management and control enablement

1 Scope

This Recommendation specifies one possible set of functional requirements and a possible architectural model for autonomic management and control (AMC)-enabled QKDN (QKDNamc). In particular, the scope of this Recommendation includes:

- Overview of QKDNamc;
- Requirements for QKDNamc;
- Consideration for the cognition process of QKDNamc;
- Architectural model for QKDNamc;
- Example operational procedures of QKDNamc.

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 X.1710] Recommendation ITU-T X.1710 (2020), *Security framework for quantum key distribution networks*.
- [ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.
- [ITU-T Y.3101] Recommendation ITU-T Y.3101 (2018), *Requirements of the IMT-2020 network*.
- [ITU-T Y.3324] Recommendation ITU-T Y.3324 (2018), *Requirements and architectural framework for autonomic management and control of IMT-2020 networks*.
- [ITU-T Y.3800] Recommendation ITU-T Y.3800 (2019), *Overview on networks supporting quantum key distribution*.
- [ITU-T Y.3801] Recommendation ITU-T Y.3801 (2020), *Functional requirements for quantum key distribution networks*.
- [ITU-T Y.3802] Recommendation ITU-T Y.3802 (2020), *Quantum key distribution networks – Functional architecture*.
- [ITU-T Y.3814] Recommendation ITU-T Y.3814 (2023), *Quantum key distribution networks – Functional requirements and architecture for machine learning enablement*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 autonomic management and control (AMC) [ITU-T Y.3324]: A behaviour or action which is determined in a reactive or proactive manner based on the external stimuli (environment aspects) as well as the goals they are required to fulfil, principles of operation, capabilities, experience and knowledge.

NOTE – In the case of software-defined networks, this definition means that AMC has the ability to dynamically select the network's configuration, control and manage the network, through its self-management functionality that reaches optimal decisions, taking into account the context of operation (environment requirements and characteristics), goals and policies (corresponding to principles of operation), profiles (corresponding to capabilities i.e., functional features supported), and machine learning (for managing and exploiting knowledge and experience).

3.1.2 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.

3.1.3 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.

3.1.4 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.

3.1.5 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 (QKD-Tx) and the receivers (QKD-Rx).

3.1.6 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.

3.1.7 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.

3.1.8 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.

3.1.9 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).

3.1.10 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]).

3.1.11 machine learning-enabled quantum key distribution network (ML-enabled QKDN) [ITU-T Y.3814]: A quantum key distribution network (QKDN) that extends or enhances its functionalities enabled by machine learning (ML) capabilities to achieve different objectives.

NOTE 1 – ML is an optional functionality for QKDN.

NOTE 2 – Examples of different objectives are specified in [b-ITU-T Y-Sup.70].

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 autonomic management and control enabled quantum key distribution network (AMC-enabled QKDN): A quantum key distribution network (QKDN) that extends or enhances its functionalities enabled by autonomic management and control (AMC) capabilities to achieve different objectives.

NOTE – AMC is an optional functionality for QKDN.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AMC	Autonomic Management and Control
CL	Control Layer
CLMO	Cross Layer Management and Orchestration
DE	Decision-making Element
KM	Key Manager
KMA	Key Management Agent
KML	Key Management Layer
KML DE	Key Management Layer autonomic Decision-making Element
KSA	Key Supply Agent
ME	Management Entity
ML	Machine Learning
NE	Network Element
NFV	Network Function Virtualization
NP	Network Performance
OSNR	Optical Signal-to-Noise Ratio
QBER	Quantum Bit-Error Ratio
QKD	Quantum Key Distribution
QKDN	QKD Network
QL	Quantum Layer
QL DE	Quantum Layer autonomic Decision-making Element
SDN	Software-Defined Networking
SPD	Single Photon Detector

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.