

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1712

(10/2021)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Quantum communication – Security design for QKDN

Security requirements and measures for quantum key distribution networks – key management

Recommendation ITU-T X.1712

ITU-T X-SERIES RECOMMENDATIONS
DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security (1)	X.1140–X.1149
Application Security (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1350–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1399
Distributed ledger technology (DLT) security	X.1400–X.1429
Application Security (2)	X.1450–X.1459
Web security (2)	X.1470–X.1489
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
Cyber Defence	X.1590–X.1599
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
Data protection	X.1770–X.1789
IMT-2020 SECURITY	X.1800–X.1819

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1712

Security requirements and measures for quantum key distribution networks – key management

Summary

Recommendation ITU-T X.1712 specifies security threats and security requirements for key management in quantum key distribution networks (QKDNs), and security measures of key management to meet the security requirements.

This Recommendation also provides support for the design, implementation, and operation of key management in QKDNs with approved security.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1712	2021-10-29	17	11.1002/1000/14805

Keywords

Key management, key relay, key supply, QKD (quantum key distribution), QKD 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/>.

© ITU 2021

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	Introduction	4
7	Information assets to be protected in key management in the QKDN	4
	7.1 Key data.....	4
	7.2 Metadata	4
	7.3 Control and management information.....	5
8	Security threats of key management in QKDN	5
	8.1 Threats to KMA links (T_K2-1) and key supply links (T-K1, T_K3, T_A1)	7
	8.2 Threats to KSA links (T_K2-2).....	7
	8.3 Threats to control and management links (T_C, T_M, T_C&M)	8
	8.4 Threats to KMA and KSA (T_KMA, T_KSA)	8
9	Security requirements and measures for information assets of key management in QKDN.....	8
	9.1 Security requirements and measures on the key data.....	8
	9.2 Security requirements and measures on the metadata	11
	9.3 Security requirements and measures on the control and management information	13
	9.4 Loss and corruption, and DoS	14
	Bibliography.....	15

Recommendation ITU-T X.1712

Security requirements and measures for quantum key distribution networks - key management

1 Scope

This Recommendation specifies the following items:

- security threats to key management in the quantum key distribution network (QKDN);
- security requirements for key management in the QKDN;
- security measures of key management to meet the security requirements.

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 X.1714] Recommendation ITU-T X.1714 (2020), *Key combination and confidential key supply for quantum key distribution 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.3803] Recommendation ITU-T Y.3803 (2020), *Quantum key distribution networks – Key management*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

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

3.1.2 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.

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

3.1.4 key management agent (KMA) [ITU-T Y.3802]: A functional element to manage keys generated by a quantum key distribution (QKD) module/QKD modules in a QKD node (trusted node).

NOTE – KMA acquires keys from one or multiple QKD module/QKD modules, synchronizes, resizes, formats, and stores them. It also relays keys through key management agent (KMA) links.

3.1.5 key management agent-key (KMA-key) [ITU-T Y.3803]: Key data stored and processed in a key management agent (KMA), and securely shared between a KMA and a matching KMA.

3.1.6 key management agent link (KMA link) [ITU-T Y.3802]: A communication link connecting KMAs to perform IT-secure key relay and communications for key management.

3.1.7 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.

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

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

3.1.10 key supply agent (KSA) [ITU-T Y.3802]: A functional element to supply keys to a cryptographic application, being located between a key management agent (KMA) and the cryptographic application.

NOTE – Application interfaces for cryptographic applications are installed into the key supply agent (KSA). The KSA synchronizes keys and verifies their integrity via a KSA link before supplying them to the cryptographic application.

3.1.11 key supply agent-key (KSA-key) [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.

3.1.12 key supply agent link (KSA link) [ITU-T Y.3802]: A communication link connecting KSAs to perform key synchronization and integrity verification.

3.1.13 message authentication code [b-ETSI GS QKD 008]: Cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of data.

3.1.14 quantum key distribution (QKD) [b-ETSI GR QKD 007]: QKD is a procedure or method for generating and distributing symmetrical cryptographic keys with information theoretical security based on quantum information theory.

3.1.15 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).

3.1.16 quantum key distribution-key (QKD-key) [ITU-T Y.3802]: A pair of symmetric random bit strings generated by a pair of quantum key distribution (QKD) modules, particularly referring to random bit strings before being resized and formatted in a KM.

3.1.17 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.

3.1.18 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 a key relay when they are not directly connected by a QKD link.