

Recommendation

ITU-T X.1713 (04/2024)

SERIES X: Data networks, open system communications
and security

Quantum communication – Quantum Key Distribution
Network (QKDN)

Security requirements for the protection of quantum key distribution nodes

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	X.1000-X.1099
SECURE APPLICATIONS AND SERVICES (I)	X.1100-X.1199
CYBERSPACE SECURITY	X.1200-X.1299
SECURE APPLICATIONS AND SERVICES (II)	X.1300-X.1499
CYBERSECURITY INFORMATION EXCHANGE	X.1500-X.1599
CLOUD COMPUTING SECURITY	X.1600-X.1699
QUANTUM COMMUNICATION	X.1700-X.1729
Terminologies	X.1700-X.1701
Quantum random number generator	X.1702-X.1704
Quantum Key Distribution Network (QKDN)	X.1705-X.1749
DATA SECURITY	X.1750-X.1799
INTERNATIONAL MOBILE TELECOMMUNICATIONS (IMT) SECURITY	X.1800-X.1839
METAVEVERSE AND DIGITAL TWIN SECURITY	X.2000-X.2199
SOFTWARE SUPPLY CHAIN SECURITY	X.2150-X.2199
ARTIFICIAL INTELLIGENCE (AI) / MACHINE LEARNING (ML) SECURITY	X.2200-X.2249

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

Recommendation ITU-T X.1713

Security requirements for the protection of quantum key distribution nodes

Summary

Quantum key distribution (QKD) enables two remote parties to share a common random binary key that is unknown to a potential eavesdropper. QKD networks based on trusted nodes (QKD nodes) have been widely adopted to enlarge the key distribution distance and enrich QKD-based applications. The trustworthiness of a QKD node is fundamental to ensure the overall security in a QKD network.

Recommendation ITU-T X.1713 provides guidance for the secure implementation and operation of QKD nodes in QKD networks. The Recommendation identifies security threats, provides security requirements for QKD nodes and provides specific techniques to meet the requirements.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T X.1713	2024-04-29	17	11.1002/1000/15885

Keywords

Quantum key distribution, quantum key distribution network, trusted node.

* 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	3
6 Introduction.....	3
7 Assets to be protected in a QKD node in a QKDN	4
8 Security threats to a QKD node in a QKDN.....	5
8.1 Possible attacks.....	5
8.2 Risk and threat analysis	6
9 Security requirements for QKD nodes in a QKD network.....	7
Appendix I A configuration example of security measures for QKD nodes	9
I.1 Configuration example of security measures for unauthorized physical access and unauthorized access through dynamic entities	9
I.2 Configuration example of security measures for QKD links	9
I.3 Configuration example of security measure for unauthorized network access.....	10
I.4 Configuration example of security measures for attacks through installation, maintenance and migration.....	11
I.5 Configuration example of security measures for classical side-channel attacks	12
Appendix II Further considerations on security measures for QKD nodes	13
Bibliography.....	14

Recommendation ITU-T X.1713

Security requirements for the protection of quantum key distribution nodes

1 Scope

This Recommendation is part of a series of ITU-T Recommendations on security requirements for quantum key distribution networks (QKDNs). This Recommendation describes the security requirements for quantum key distribution (QKD) nodes from the following perspectives:

- Security threats to QKD nodes in a QKD network;
- Security requirements for QKD nodes in a QKD network; and
- Typical configuration of security measures for a QKD node.

NOTE – A QKD node is considered to be a trusted node, and the scope of trusted nodes is aligned to [ITU-T X.1710].

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

[ITU-T Y.3802] Recommendation ITU-T Y.3802 (2020), *Quantum key distribution networks – Functional architecture*.

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

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.

3.1.3 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.

