

Recommendation

ITU-T X.1716 (10/2024)

SERIES X: Data networks, open system communications
and security

Quantum communication – Quantum Key Distribution
Network (QKDN)

Authentication and authorization in quantum key distribution network

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
METaverse 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.1716

Authentication and authorization in quantum key distribution network

Summary

Recommendation ITU-T X.1716 specifies authentication and authorization of quantum key distribution network (QKDN). In particular, the scope of this Recommendation includes:

- Identifiers (IDs) and their management in QKDN;
- Public key certification supported by public-key infrastructure (PKI);
- Authentication and authorization in QKDN.

History*

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T X.1716	2024-10-29	17	11.1002/1000/16168

Keywords

Authentication, authorization, public-key infrastructure (PKI), quantum key distribution (QKD), QKD network (QKDN), security measures, security requirements.

* 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, and 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 2025

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	3
7 IDs and their management in QKDN	4
7.1 IDs for QKDN	4
7.2 IDs for functional elements in QKDN.....	4
7.3 IDs for key operations	5
8 Public key certification supported by PKI.....	5
9 Authentication and authorization in QKDN	5
9.1 Functional elements and associated reference points in QKDN	5
9.2 Authentication and authorization of functional elements in QKDN	7
Appendix I – Hierarchical tree of IDs in a QKDN	22
Appendix II – Implicit authentication and authorization scheme	23
Bibliography.....	24

Recommendation ITU-T X.1716

Authentication and authorization in quantum key distribution network

1 Scope

This Recommendation specifies authentication and authorization of quantum key distribution network (QKDN). In particular, the scope of this Recommendation includes:

- Identifiers (IDs) and their management in QKDN;
- Public key certification supported by public-key infrastructure (PKI);
- Authentication and authorization in QKDN.

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.509] Recommendation ITU-T X.509 (2019), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.
- [ITU-T X.1710] Recommendation ITU-T X.1710 (2020), *Security framework for quantum key distribution networks*.
- [ITU-T X.1712] Recommendation ITU-T X.1712 (2021), *Security requirements and measures for quantum key distribution networks – key management*.
- [ITU-T X.1717] Recommendation ITU-T X.1717 (2024), *Security requirements and measures for quantum key distribution networks – control and management*.
- [ITU-T Y.3800] Recommendation ITU-T Y.3800 (2019), *Overview on networks supporting quantum key distribution*.
- [ITU-T Y.3801] Recommendation ITU-T 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 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 information theoretically secure (IT-secure) [ITU-T Y.3800]: Secure against any deciphering attack with unbounded computational resources.

3.1.3 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.

3.1.4 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.

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

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

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

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

3.1.9 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.

3.1.10 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.

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

3.1.12 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.

3.1.13 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.

3.1.14 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.

3.1.15 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 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.

3.1.17 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.

3.1.18 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.

3.1.19 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).

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CA	Certification Authority
ID	Identifier
IT-secure	Information-Theoretically secure
KM	Key Manager
KMA	Key Management Agent
KSA	Key Supply Agent
MAC	Message Authentication Code
PKI	Public-Key Infrastructure
PSK	Pre-Shared Key
QKD	Quantum Key Distribution
QKDN	QKD Network
SSH	Secure Shell
TLS	Transport Layer Security

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

6 Introduction

Information assets in quantum key distribution network (QKDN) (i.e., key data, metadata and control and management information) can be breached and altered during key generation, key relay, key

storage, etc. Confidentiality and integrity of information assets need to be protected by appropriate security measures. Such measures can be built on cryptographic protocols (public key cryptography, hash functions, etc.) that are computationally secure or even information-theoretically secure (IT-secure), for example Wegman-Carter message authentication. Appropriate security measures also include physical protection of elements constituting QKDN.

Basic functions and layered structures of the QKDN are defined in [ITU-T Y.3800]. Functional requirements and architectures are specified in [ITU-T Y.3801] and [ITU-T Y.3802], respectively. A security framework for the QKDN is specified in [ITU-T X.1710], by addressing the security threats against the QKDN, and deriving the general security requirements and the security measures for the QKDN. Based on [ITU-T X.1710], security requirements and measures for key management in the QKDN are described in [ITU-T X.1712]. This Recommendation describes functions and procedures for authentication and authorization to ensure security of information assets in QKDN including related technologies such as ID management and public-key infrastructure (PKI) based on Recommendations above.

7 IDs and their management in QKDN

The following is a basic list of identifiers (IDs) which are used in a QKDN. Other IDs might be defined for various implementations.

7.1 IDs for QKDN

The IDs listed below are assigned by a QKDN provider or administrator of QKDNs:

- QKDN ID: ID assigned as a unique ID to identify the QKDN.

7.2 IDs for functional elements in QKDN

The IDs listed below identify a functional element for management and security purposes such as configuration, authentication and authorization:

- QKD node ID: ID assigned as a unique ID to identify the QKD node in the QKDN.
- QKDN controller ID: ID assigned as a unique ID to identify the QKDN controller in the QKDN.
- QKDN manager ID: ID assigned as a unique ID to identify the QKDN manager in the QKDN.
- KM ID: ID assigned as a unique ID to identify a key manager (KM) in the QKDN.
- KMA ID: ID assigned as a unique ID to identify a key management agent (KMA) in the QKDN.

NOTE 1 – Matching KMA ID, source KMA ID and destination KMA ID are described in [ITU-T Y.3803]. Details of these IDs and operations are specified in [ITU-T Y.3803].

- KMA link ID: ID assigned as a unique ID to identify a KMA link in the QKDN.
- KSA ID: ID assigned as a unique ID to identify a key supply agent (KSA) in the QKDN.
- KSA link ID: ID assigned as a unique ID to identify a KSA link in the QKDN.
- QKD module ID: ID assigned as a unique ID to identify a QKD module in the QKDN.

NOTE 2 – Matching QKD module ID is described in [ITU-T Y.3803]. Details of it and operations are specified in [ITU-T Y.3803].

- Application ID: This ID is assigned as a unique ID in the QKDN to identify an application which requests and acquires the keys from QKDN.

NOTE 3 – Application source ID and application destination ID are described in [ITU-T Y.3803]. Details of these IDs and operations are specified in [ITU-T Y.3803].