ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T X.1717 (10/2024)

SERIES X: Data networks, open system communications and security

Quantum communication – Quantum Key Distribution Network (QKDN)

Security requirements and measures for quantum key distribution network – Control and management

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.1717

Security requirements and measures for quantum key distribution network – Control and management

Summary

Control and management are concerned with secure, stable, efficient, and robust operations of the quantum key distribution network (QKDN). Recommendation ITU-T X.1717 specifies security requirements and measures for control and management in the quantum key distribution network based on the functional architecture for control and management in the QKDN, which is defined in Recommendation ITU-T Y.3804.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T X.1717	2024-10-29	17	11.1002/1000/16169

Keywords

Quantum key distribution (QKD), QKDN (QKD network), QKDN controller, QKDN manager, 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/.

Table of Contents

Recommendation ITU-T X.1717

Security requirements and measures for quantum key distribution network – Control and management

1 Scope

This Recommendation specifies security requirements and measures for control and management of quantum key distribution network (QKDN). More specifically, this Recommendation covers:

– Definitions of the assets to be protected in control and management of QKDN;

– Analysis of the security threats to control and management of QKDN;

– Security requirements for control and management of QKDN;

– Security measures for control and management of 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.1716] Recommendation ITU-T X.1716 (2024), *Authentication and authorization in quantum key distribution network*.

[ITU-T Y.3804] Recommendation ITU-T Y.3804 (2020), *Quantum key distribution networks – Control and management*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 key manager (KM) [b-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 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.

3.1.3 quantum key distribution link (QKD link) [b-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.

3.1.4 quantum key distribution module (QKD module) [b-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).

3.1.5 quantum key distribution network (QKDN) [b-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.

3.1.6 quantum key distribution network controller (QKDN controller) [b-ITU-T Y.3800]: A functional module, which is located in a quantum key distribution (QKD) network control layer to control a QKD network.

3.1.7 quantum key distribution network manager (QKDN manager) [b-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.

3.1.8 quantum key distribution node (QKD node) [b-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:

BSS Business Support System

DoS Denial of Service

ID Identifier

KM Key Manager

OSS Operation Support System

QBER Quantum Bit Error Rate

QoS Quality of Service

QKD Quantum Key Distribution

QKDN Quantum Key Distribution Network

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

This Recommendation specifies security requirements and measures for control and management for quantum key distribution network (QKDN) based on the functional architecture for control and management in QKDN which is defined in [ITU-T Y.3804].

7 Information assets to be protected in control and management in the QKDN

This clause specifies information assets to be protected in control and management in the QKDN.

7.1 Information assets in control elements

Information assets to be protected in control elements in the QKDN are as follows:

– QKDN controller and associated software elements.

– Routing control information: routing table, key related information (e.g., key consumption rate, residual number of keys), QKD link control information, and QKDN topology information.

– Configuration control information: control related configuration, state of elements (in service, out of service, standby, or reserved), alarm or failure diagnosis, and status of the quantum bit error rate (QBER).

– Policy-based control information: quality of service (QoS) data and charging information.

– Access control information: identifier (ID), authorized rights/roles priorities rule and certificate.

– Session control information: key management policy and charging policy.

7.2 Information assets in management elements

Information assets to be protected in management elements in the QKDN are as follows:

– QKDN manager and associated software elements.

– Fault management information: QKD routing path, QKD link failure data, fault detection data, fault analysis / diagnosis data, failure resolving policy.

– Configuration management information: managed resources, configuration status, network topology, life cycle of resources.

– Account management information: usage data, accounting policy, charging data.

– Performance management information: performance database (performance data and the status of layers), analysis information, key supply service policy.

– Security management information: metadata, event logs, audit trail data, log database (key life cycle, traceability data of key), root certification authority, key management policy.

8 Security threats to control and management of the QKDN

The functional elements for control and management in the QKDN which are referred to in this Recommendation are specified in [ITU-T Y.3804]. This clause focuses on intrinsic security threats to control and management for the QKDN.

Attack surfaces of control and management in the QKDN are summarized in Figure 1 in red circles.

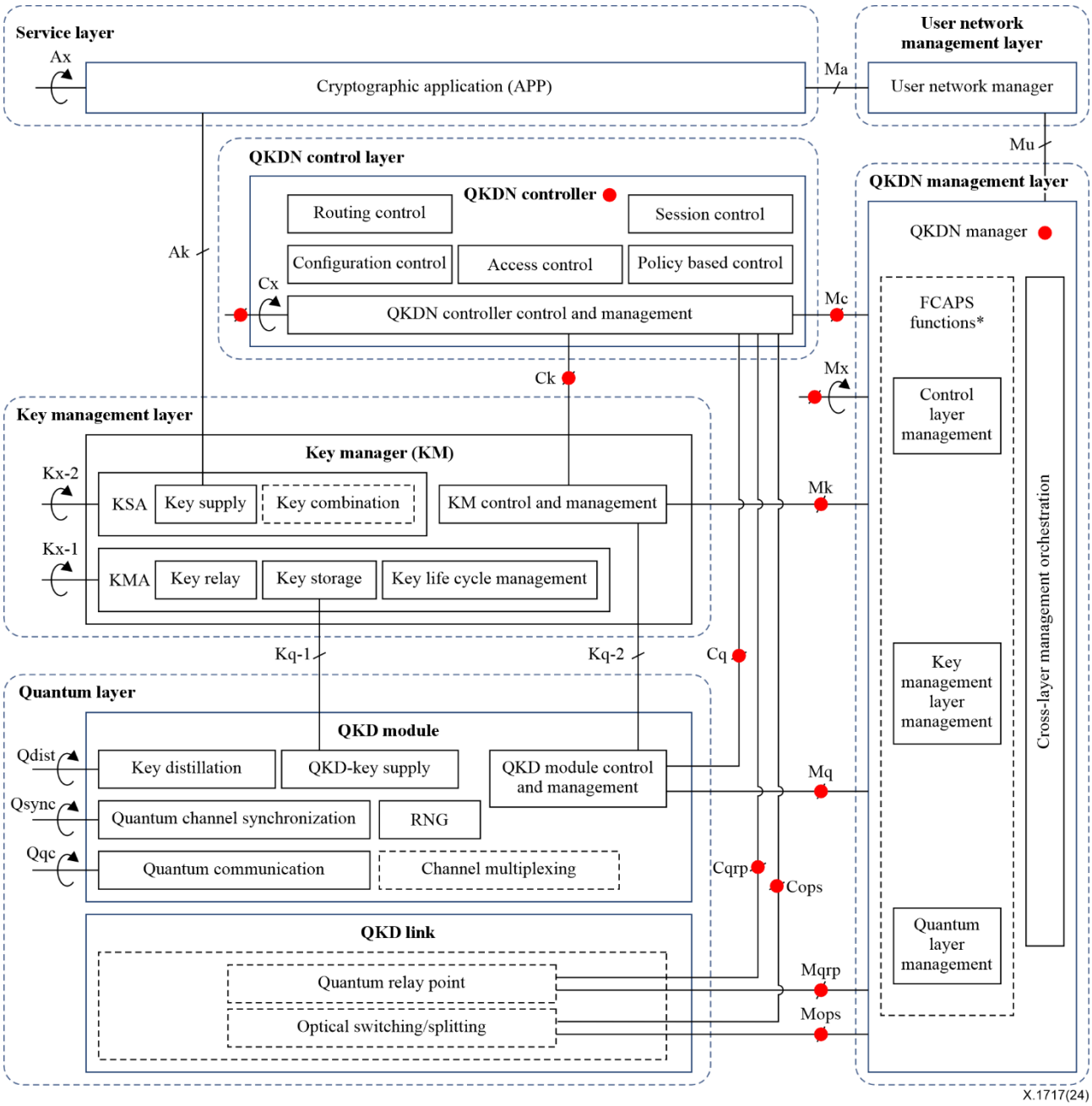

Figure 1 – Attack surfaces of control and management in the QKDN

On each attack surface, the following threats could arise:

– Spoofing (masquerade): An attacker masquerades as a QKDN controller or QKDN manager to maliciously fabricate an information asset.

– Eavesdropping: An attacker intercepts information assets from each interface of control and management.

– Deletion or corruption: An attacker deletes or modifies the information assets from each interface of control and management.

– Denial of service (DoS): An attacker attacks functional elements using communication interruption or flooding data traffic.

The following text describes the security threats for each link and functional element for control and management in the QKDN:

1) Security threat at the Ck, Cq, Cx, Cqrp and Cops link:

– eavesdropping: intercepting and deciphering the control information;
– deletion or corruption: deleting or modifying the control information;
– DoS: communication interruption or flooding data traffic.

2) Security threat at the Mc, Mk, Mq, Mx, Mqrp and Mops link:
– eavesdropping: intercepting and deciphering the control information;
– deletion or corruption: deleting or modifying the control information;
– DoS: communication interruption or flooding data traffic.

3) Security threat at the QKDN controller through the Ck, Cq, Cx, Cqrp and Cops link:
– spoofing: an attacker masquerades as a QKDN controller to breach information security or an attacker maliciously fabricates a control information and claims that such a control information was received from another functional element or sent to another functional element;
– eavesdropping: stealing and deciphering the control information;
– deletion or corruption: deleting or modifying the control information;
– DoS: communication interruption or flooding data traffic.

4) Security threat at the QKDN manager through the Mc, Mk, Mq, Mx, Mqrp and Mops link:
– spoofing: an attacker masquerades as a QKDN manager to breach information security or an attacker maliciously fabricates a management information and claims that such a management information was received from another functional element or sent to another functional element;
– eavesdropping: stealing and deciphering the management information;
– deletion or corruption: deleting or modifying the management information;
– DoS: communication interruption or flooding data traffic.

9 Security requirements and measures for control and management of the QKDN

This clause specifies security requirements and measures for each functional element derived from the security threats addressed in clause 8.

9.1 Security requirements and measures for the QKDN controller

The requirements and measures for control elements are summarized as follows:

SReq 1. The QKDN controller is recommended to ensure the confidentiality of the key manager control information in a Ck link in collaboration with the key manager (KM).

SReq 2. The QKDN controller is recommended to ensure the confidentiality of the QKD module control information in a Cq link in collaboration with the QKD module.

SReq 3. The QKDN controller is recommended to ensure the confidentiality of the QKD link control information in a Cqrp link and Cops link in collaboration with the QKD link.

SReq 4. The QKDN controller is recommended to the ensure confidentiality of the QKD control information in a Mc link in collaboration with the QKDN manager.

SReq 5. The QKDN controller is recommended to ensure the confidentiality of the control information with the matching QKDN controller in a Cx link.

Toward SReq.1, SReq.2, SReq.3, SReq.4 and SReq.5 the following security measures are considered:

The confidentiality of control information is protected by appropriate means, which include physical protection of the control links and/or cryptographic methods by the QKDN controller and the corresponding elements.

The QKDN controller and the corresponding elements are protected by appropriate means, which include tamper protection measures and/or the use of cryptographic measures.

SReq 6. The QKDN controller is required to ensure the integrity of the control and management information that it manages.

Toward SReq.6, the QKDN controller verifies the integrity of the control information received from the corresponding elements.

SReq 7. The QKDN controller is required to ensure that the control and management information received from other entities is not trusted unless the identity of the sending entity has been authenticated and the sending entity is authorized to supply the control and management information.

NOTE 1 – Rejecting the unauthenticated control and management information is required, but accepting authenticated control and management information is not always required.

SReq 8. The QKDN controller is required to ensure that they do not allow another entity access to the unencrypted control and management information without ensuring that the entity is authorized to receive it.

Toward SReq.7 and SReq.8, the QKDN controller and the corresponding elements perform mutual authentication with other entities which they communicate with or utilize other approaches.

NOTE 2 – Details of authentication and authorization of the QKDN controller are specified in clause 9 of [ITU-T X.1716].

SReq 9. The QKDN controller is required to supply the control information following a request from the QKDN manager.

SReq 10. The QKDN controller is recommended to supply the control information following a request from the matching QKDN controller.

Toward SReq.9 and SReq.10, the QKDN controller has the capability to support the protection and recovery of its functions to enhance resiliency and robustness.

SReq 11. The QKDN controller is recommended to have the capabilities to trace the control information following a request from the QKDN manager.

SReq 12. The QKDN controller is recommended to have the capabilities to trace the control information following a request from the matching QKDN controller.

Toward SReq.11 and SReq.12, the QKDN controller creates and stores log data of the control information provided to the QKDN manager and the matching QKDN controller.

9.2 Security requirements and measures for QKDN manager

The requirements and measures for management elements are summarized as follows:

SReq 13. The QKDN manager is recommended to ensure confidentiality of the key manager management information in a Mk link in collaboration with the KM.

SReq 14. The QKDN manager is recommended to ensure confidentiality of the QKD module management information in a Mq link in collaboration with the QKD module.

SReq 15. The QKDN manager is recommended to ensure confidentiality of the QKD link management information in a Mqrp link and Mops link in collaboration with the QKD link.

SReq 16. The QKDN manager is recommended to ensure the confidentiality of the QKD management information in a Mc link in collaboration with the QKDN controller.

SReq 17. The QKDN manager is recommended to ensure the confidentiality of the QKD management information in a Mu link in collaboration with the user network manager.

Toward SReq.13, SReq.14, SReq.15, Sreq.16 and Sreq.17, the following security measures are considered:

The confidentiality of management information is protected by appropriate means, which include physical protection of the management links and/or cryptographic methods by the QKDN manager and the corresponding elements.

The QKDN manager and the corresponding elements are protected by appropriate means, which include tamper protection measures and/or the use of cryptographic measures.

SReq 18. The QKDN manager is required to ensure the integrity of the management information that it manages.

Toward SReq.18, the QKDN manager verifies the integrity of the management information received from the corresponding elements.

SReq 19. The QKDN manager is required to ensure that the control and management information received from other entities is not trusted unless the identity of the sending entity has been authenticated and the sending entity is authorized to supply the control and management information.

NOTE 1 – Rejecting the unauthenticated control and management information is required, but accepting authenticated one is not always required.

SReq 20. The QKDN manager is required to ensure that they do not allow another entity access to the unencrypted management information without ensuring that the entity is authorized to receive it.

Toward SReq.19 and SReq.20, the QKDN manager and the corresponding elements perform mutual authentication with other entities which they communicate with or utilize other approaches.

NOTE 2 – Details of authentication and authorization of the QKDN manager are specified in clause 9 of [ITU-T X.1716].

SReq 21. The QKDN manager is recommended to supply the management information following a request from the external management entities, e.g., operator's operation support system (OSS), business support system (BSS), etc.

Toward SReq.21, the QKDN manager has the capability to support the protection and recovery of its functions to enhance resiliency and robustness.

SReq 22. The QKDN manager is recommended to have the capabilities to trace the management information following a request from the external management entities (e.g., operator's OSS, BSS, etc.).

Toward SReq.22, the QKDN manager creates and stores log data of the management information and sends it to the external management entities.

Bibliography

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

[b-ETSI GR QKD 007] ETSI GR QKD 007 V1.1.1 (2018), *Quantum Key Distribution (QKD); Vocabulary*.
https://www.etsi.org/deliver/etsi_gr/QKD/001_099/007/01.01.01_60/gr_qkd007v010101p.pdf

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

Published in Switzerland
Geneva, 2025