International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1710

(10/2020)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Quantum communication – Framework of QKDN security

Security framework for quantum key distribution networks

Recommendation ITU-T X.1710

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	X.1140–X.1149
Security protocols (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.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
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
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
5G SECURITY	X.1800–X.1819

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

Recommendation ITU-T X.1710

Security framework for quantum key distribution networks

Summary

Recommendation ITU-T X.1710 specifies a framework including requirements and measures to combat security threats for quantum key distribution networks (QKDNs).

It specifies a simplified QKDN structure for analysis of the relevant security threats. Security requirements and corresponding security measures are then specified on that basis.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T X.1710	2020-10-29	17	11.1002/1000/14452

Keywords

Key, quantum key distribution, QKD, QKD network, QKDN , trusted node.

[*] 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, 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 TSB patent database 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

Recommendation ITU-T X.1710

Security framework for quantum key distribution networks

1 Scope

This Recommendation is the first in a series on the security of quantum key distribution (QKD) and provides a security framework for other related Recommendations.

In particular, this Recommendation addresses the following items:

- security aspects for quantum key distribution networks (QKDNs);
- security threats to QKDNs;
- security requirements (SReqs) for QKDNs;
- security measures for QKDNs.

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.805]	Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.
[ITU-T Y.3800]	Recommendation ITU-T Y.3800 (2019), *Overview on networks supporting quantum key distribution*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 accountability [b-ITU-T X.800]: The property that ensures that the actions of an entity may be traced uniquely to the entity.

3.1.2 authenticity [b-ITU-T T.411]: The property that the claimed data source can be verified to the satisfaction of the recipient.

3.1.3 availability [b-ITU-T X.800]: The property of being accessible and useable upon demand by an authorized entity.

3.1.4 classical channel [b-ETSI GR QKD 007]: Communication channel that is used by two communicating parties for exchanging data encoded in a form that may be non-destructively read and fully reproduced.

3.1.5 confidentiality [b-ITU-T X.800]: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

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

3.1.7 integrity [b-ITU-T X.1193]: The property that data has not been altered or destroyed in an unauthorized manner.

3.1.8 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.

3.1.9 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.

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

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

3.1.12 quantum channel [b-ETSI GR QKD 007]: Communication channel for transmitting quantum signals.

3.1.13 quantum key distribution [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 [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 [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 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).

3.1.18 threat [b-ISO/IEC 27000]: Potential cause of an unwanted incident, which may result in harm to a system or organization.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 quantum key distribution protocol (QKD protocol): List of steps for establishing symmetric cryptographic keys with information-theoretical security based on quantum information theory.

3.2.2 resilience: Ability to adapt to and recover from adverse conditions and attacks.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AES	Advanced Encryption Standard
APP	Application
DDoS	Distributed Denial of Service
DoS	Denial of Service
SReq	Security Requirement
IT-secure	Information Theoretically secure
KM	Key Manager
NM	Network Manager
OTP	One-Time Pad
QKD	Quantum Key Distribution
QKDN	Quantum Key Distribution Network
QKDNM	Quantum Key Distribution Network Manager
QKD-Rx	Quantum Key Distribution Receiver
QKD-Tx	Quantum Key Distribution Transmitter

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 Recommendation 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

Establishing symmetric keys between two distant parties in a communications network is one of the cryptographic primitives and underlies many cybersecurity systems in use today. This is typically done using public key cryptography. Like public key cryptography, quantum key distribution (QKD) allows for key establishment. Unlike public key cryptography, QKD protocols are based on the laws of quantum mechanics and can be proven in theory to be secure even against an eavesdropper who has unbounded computational ability. This kind of security is referred to as information theoretically secure (IT-secure).

A QKD protocol is executed by a pair of QKD modules connected by a QKD link, which consists of a classical channel and a quantum channel. A key (i.e., a pair of symmetric random bit strings) is then established between these QKD modules, according to the QKD protocol procedure. The ensemble of pairs of QKD modules connected by the QKD link and their corresponding key managers (KMs) concatenated via KM links are the foundation of a QKDN. The QKDN allows cryptographic applications to share a secure key between any two designated nodes by appropriate key relay. Keys themselves once generated in the QKD module must be managed securely in the QKDN in an appropriate way until they are supplied to cryptographic applications in the user network. A basic function and a layered structure of QKDN are specified in [ITU-T Y.3800].

The QKDN is subject to various security threats, which would violate its correct operation and compromise the security of the keys. In order to ensure information security of the QKDN, security threats should be identified in consideration of the interests, business relations, legal and regulatory constraints, contractual constraints, etc., among operators and other actors, e.g., users and third parties. Then appropriate security measures should be defined for the QKDN, the user network, and links between the two networks, as appropriate.

Figure 1 illustrates a process for the security assessment on a QKDN. Security threats are inferred from both the basic characteristics of and relations between functional elements, links, and information assets of the QKDN. From the security threats, security requirements for the QKDN can be specified, and the requirements are used to derive efficient security measures for the QKDN.

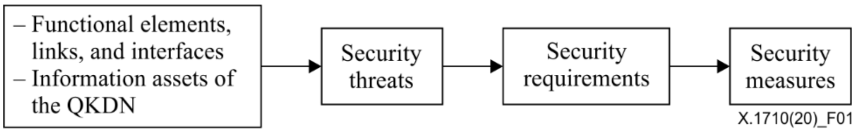
– Functional elements, links, and interfaces
– Information assets of the QKDN
Security threats
Security requirements
Security measures
X.1710(20)_F01

Figure 1 – A process for security assessment on a QKDN

Thus, this Recommendation provides a security framework for QKDNs. Security analyses of QKD protocols are outside the scope of this Recommendation.

7 Security aspects specific to QKDN

QKD protocols allow key establishment with confidentiality proven with information theory and quantum physics under certain assumptions, meaning that no information on keys can be known to any eavesdroppers.

To ensure information security of a QKD node, especially to protect the security of keys, the QKD node must be protected against intrusion and attacks by unauthorized parties. A QKD node with such a protection is called a trusted node. A trusted node acts as a boundary protecting all embedded elements against attackers outside the node.

If the keys are managed in trusted nodes and relayed based on an IT-secure protocol, e.g., a one-time pad (OTP), highly secure keys can be established between any designated nodes in the QKDN. These features bring a unique capability to the QKDN, which is to supply highly secure keys to cryptographic applications that require long-term confidentiality protection of data.

The keys can be altered after their generation depending on the situation, e.g., malicious access during key relay, accidental failure during key storage or breach of key integrity. Therefore, integrity needs to be protected to ensure that the keys remain unaltered until they are consumed in a cryptographic application. Such a functionality can be built on cryptographic protocols (public key cryptography, hash functions, etc.) that are computationally secure or even IT-secure (e.g., [b-Wegman-Carter] message authentication).

To control and manage a QKDN correctly, control and management information also needs to be protected by using appropriate security measures, which can be at most computationally secure.

Thus, in a QKDN, different kinds of cryptographic protocols need to be used in appropriate combination.

8 Security threats to QKDNs

8.1 Elements and information assets of QKDN

As specified in [ITU-T Y.3800] and depicted in Figure 2, a QKDN consists of QKD modules, KMs, QKDN controller(s), QKDN manager(s) and links connecting these functional elements.

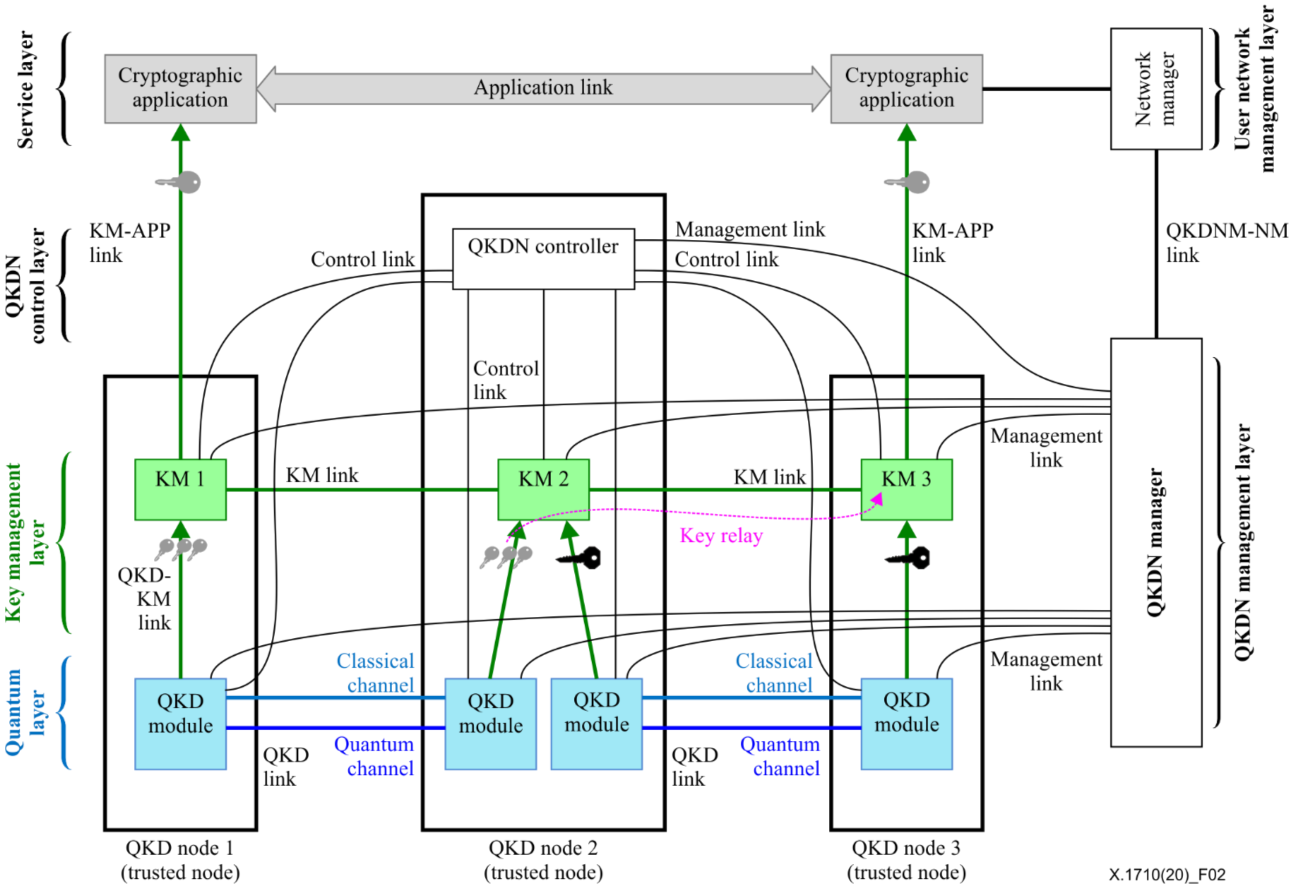

Figure 2 – Typical structure of a QKDN and user network

The functional elements and links inside a QKDN, as well as between the QKDN and a user network, are as follows:

– QKD module: a functional element that generates keys based on QKD protocols;

– KM: a functional element that performs key management;

– QKDN controller: a functional element that controls a QKDN;

– QKDN manager: a functional element that manages a QKDN;

– QKD link: a communication link between QKD modules, which consists of a classical channel and a quantum channel;

NOTE 1 – A QKD link may include optical switches, intermediate measurement stations and quantum repeaters.

– KM link: a communication link between KMs;

– control link: a communication link between the QKDN controller and one of three functional entities; the KM, the QKD module or the QKD link;

– management link: a communication link between the QKDN manager and all other entities in the QKDN, e.g., the QKDN controller, the KM, the QKD module or the QKD link;

– QKD-KM link: a link between the QKD module and the KM;

– KM-APP link: a link between the KM and cryptographic applications in the user network;

– QKDNM-NM link: a link between the QKDN manager (QKDNM) and a network manager (NM) in the user network.

The following types of data and information are transmitted through the links listed in the previous paragraph, and these are identified as information assets of the QKDN:

– key data: data containing the secure keys (symmetric random bit strings);

– metadata: additional data attached to the key data, used for key management;

– control and management information: information related to the control and management of the QKDN, e.g., key management information, key life cycle information, session control information, routing control information, as well as performance and status information of modules and links.

Table 1 summarizes a correspondence between elements or links and information assets in the QKDN.

Table 1 – Relation between elements and information assets in a QKDN

Information assets Element		Key data	Meta-data	Control and management information
	QKD link			x
	KM link	x	x	x
	Control link		x	x
	Management link		x	x
	KM-App link	x	x	
	QKDNM-NM link			x
QKD node (trusted node)	QKD module	x	x	x
	KM	x	x	x
	QKDN controller		x	x
	QKDN manager		x	x
	QKD-KM link	x	x	

This Recommendation describes security threats to QKDN. Detailed threat analyses and specification of requirements and functions of the trusted node are outside the scope of this Recommendation.

NOTE 2 – In some cases, a cryptographic application uses the keys outside the trusted node after receiving keys in the trusted node. Typical examples include cryptographic applications in mobile terminals, such as smart phones and drones.

8.2 Security threats

This clause identifies security threats against the QKDN. Figure 3 schematically overlays these threats on the structure depicted in Figure 2.

Attack surfaces can be identified in the QKD links, KM links, control links and management links, which are located between the trusted nodes and exposed to external environments. Another type of attack surfaces can be identified in the KM-APP and QKDN-MN links, due to access paths from outside the trusted nodes.

The other attack surface can be identified inside the trusted node, i.e., the QKD-KM links, even though the links are protected in the trusted nodes.

The functional elements (the QKD module, KM, QKDN controller and QKDN manager), even if they are located inside the trusted nodes, may also suffer from security threats addressed in this clause.

This Recommendation distinguishes three kinds of threat:

– intentional: a threat that involves a malicious entity that may attack either communication itself or network resources;

– administrative: a threat that arises from a failure of security administration;

– accidental: a threat whose origin does not involve any malicious intent and results from technical failures.

In order to give a more accurate analysis, this Recommendation focuses only on intentional threats.

NOTE 1 – Administrative and accidental threats are outside the scope of this Recommendation.

Analyses on intentional threats have been undertaken for various kinds of systems and networks, e.g., in [b-ITU-T X.800] for open systems interconnection and [b-ITU-T X.1038] for software-defined networking.

In a similar way, a threat analysis of QKDN should address the following items.

– Spoofing (masquerade): pretending to be a different entity in order to gain an illegitimate advantage. For example, an attacker masquerades as a KM to access keys and modify them.

– Eavesdropping: breaching confidentiality by deciphering information assets. It is possible for attackers to get sensitive system information (e.g., configuration data, user credentials) for a future attack.

– Deletion or corruption: compromising the integrity of information assets transferred or stored by unauthorized deletion, insertion, modification, re-ordering, replay or delay.

– Repudiation: denying the fact of executing some tasks. For example, an administrator, enforcing a malicious network policy (e.g., copying and forwarding specific traffic flows to a malicious nodes), may claim that he/she did not make such network policy enforcement.

– Denial of service (DoS): performing activities to disrupt proper operations of QKDN. This may include denial of access to the QKDN and denial of key generation and other communication by flooding the QKDN. Recent threats are distributed denial of service (DDoS) attacks that are attempts to make an online service unavailable by overwhelming it with a massive amount of traffic from multiple sources.

In the following text, the security threats are described for each link and functional element of the QKDN. The security threats with respect to QKD protocols, including quantum and classical attacks on the QKD links and including the QKD-specific side-channel attacks on the QKD modules, are outside the scope of this Recommendation.

NOTE 2 – A proper implementation of the QKD protocol as well as QKD-specific side-channel attack countermeasures allows the QKDN to protect the QKD modules and the QKD links from these threats.

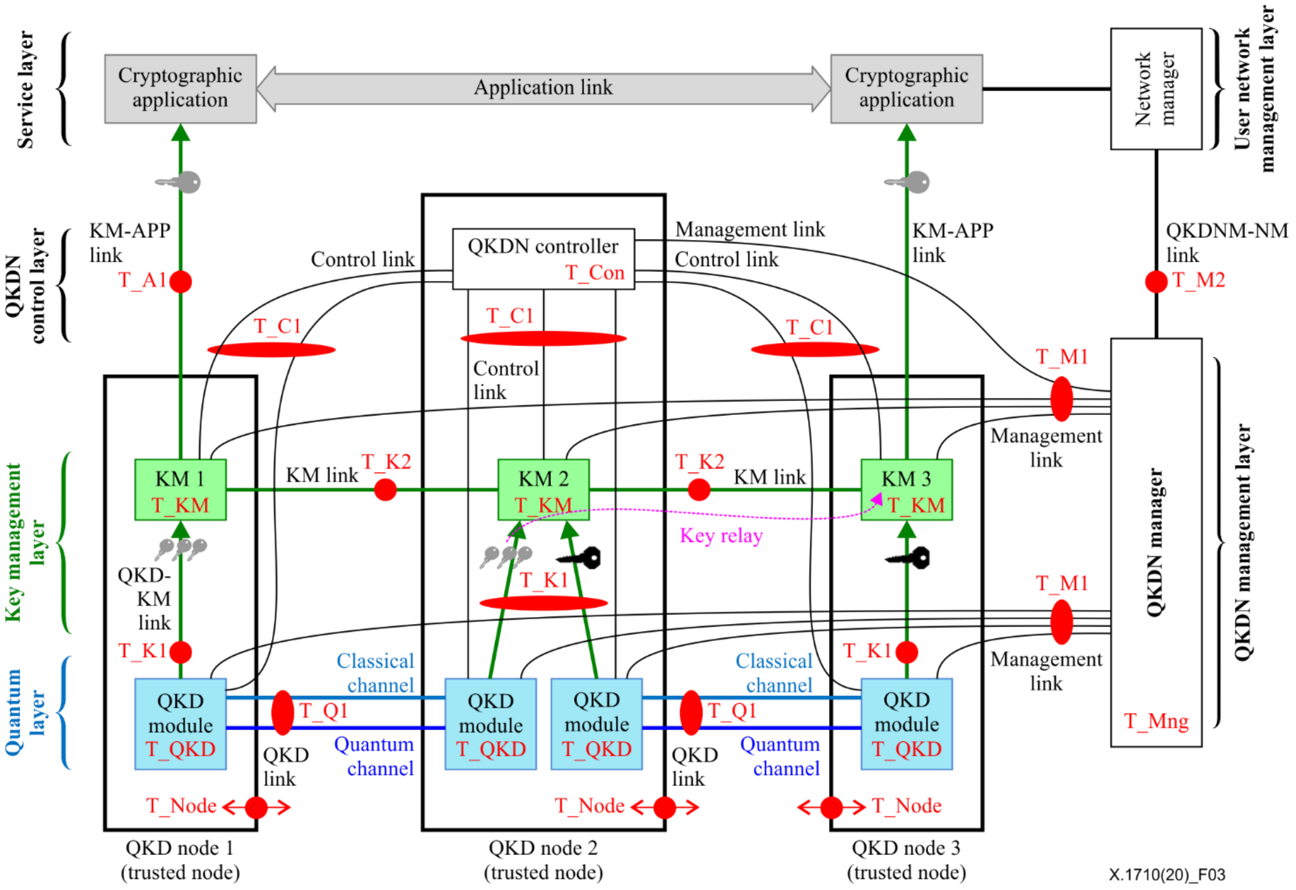

Figure 3 – Security threats to QKDN

1) T_Q1: Security threats at the QKD link:

- deletion or corruption: deleting or modifying the information in the classical channel;
- DoS: communication interruption or flooding data traffic.

2) T_QKD: Security threats at the QKD module through the QKD link, control link or management link:

- eavesdropping: quantum side-channel attacks;
- deletion or corruption: deleting or modifying the information in the QKD module;
- DoS: denial of access or flooding data traffic.

3) T_K1: Security threat at the QKD-KM links:

- eavesdropping: intercepting and deciphering the key data and the metadata;
- deletion or corruption: deleting or modifying the key data and the metadata;
- DoS: communication interruption or flooding data traffic.

4) T_K2: Security threat at the KM links:

- eavesdropping: intercepting and deciphering the key data and the metadata;
- deletion or corruption: deleting or modifying the key data and the metadata;
- DoS: communication interruption or flooding data traffic.

5) T_KM: Security threat at the KM through the KM links, QKD-KM links, KM-APP links, as well as the control or management links:

- eavesdropping: stealing and deciphering the key data and the metadata;

- spoofing: an attacker masquerades as a KM to breach information security – an attacker maliciously fabricates an information asset and claims that such an asset was received from another functional element or cryptographic application, or sent to another functional element or cryptographic application;
- repudiation: an attacker maliciously performs key management functions and subsequently denies that fact;
- DoS: denial of access or flooding data traffic.

6) T_A1: Security threats at the KM-APP link:

- eavesdropping: intercepting and deciphering the key data, the metadata, and information from the cryptographic applications;
- deletion or corruption: deleting or modifying the key data, the metadata, and information from the cryptographic applications such as key request;
- DoS: communication interruption or flooding data traffic.

7) T_C1: Security threat at the control link:

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

8) T_Con: Security threat at the QKDN controller through the control and management links:

- eavesdropping: stealing and deciphering the control information;
- spoofing: an attacker masquerades as a QKDN controller to breach information security – an attacker maliciously fabricates QKDN control and management information and claims that such information was received from another functional element or sent to another functional element;
- repudiation: an attacker maliciously performs QKDN control functions and subsequently denies that fact;
- DoS: denial of access or flooding data traffic.

9) T_M1: Security threat at the management link:

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

10) T_Mng: Security threat at the QKDN manager through the control, management links and QKDNM-NM link:

- spoofing: an attacker masquerades as a QKDN manager to breach information security – an attacker maliciously fabricates QKDN management information and claims that such information was received from another functional element or sent to another functional element;
- repudiation: an attacker maliciously performs QKDN management functions and subsequently denies that fact;
- DoS: denial of access or flooding data traffic.

11) T_M2: Security threat at the QKDNM-NM link:

- eavesdropping: stealing and deciphering the QKDN and the user network management information;

- deletion or corruption: deleting or modifying the QKDN and the user network management information;
- DoS: communication interruption or flooding data traffic.

12) T_Node: Security threat at the QKD node:

- unauthorized physical access: adversaries may physically intrude into the QKD node and directly access the QKD modules, KMs, QKD-KM interfaces and other entities inside the QKD node to steal information assets or other purposes, e.g., loss or corruption of information, spoofing, repudiation, and DoS.

NOTE 3 – Unauthorized access to T_Node may include cyber-attacks through links and physical attack.

Furthermore, these security threats may occur during and after the deployment, maintenance, update, and migration of QKDN due to physical access, e.g., building trespass, malicious access through network connections by unauthorized parties or backdoors installation in the system. For example, QKD modules may have maintenance ports that can be loopholes for threats.

The main threats during the deployment and maintenance of a QKDN are spoofing and unauthorized access to entities under deployment or maintenance. As an example, spoofing of an entity might lead to a man in-the-middle attack, unauthorized access might lead to backdoor infection.

The relation between security threats and each element of a QKDN are summarized in Table 2, with three different priority levels.

Table 2 – Relation between security threats and QKDN functional elements, and their links, with three different priority levels.

Threat Element		Spoofing	Eavesdropping	Deletion or corruption	Repudiation	DoS
	QKD link			3		1
	KM link		3	2		1
	Control link		1	2		1
	Management link		1	2		1
	KM-App link		3	2		1
	QKDNM-NM link		1	2		1
QKD node (trusted node)	QKD module		3	3		1
	KM	3			2	1
	QKDN controller	2			2	1
	QKDN manager	2			2	1
	QKD-KM link		3	2		1

The numbers in Table 2 indicate the following levels of threat.

– 3: High level

This level is fatal if a threat occurs. Such a threat could result in a break in confidentiality of key data.

– 2: Medium level

It is essential for this level of threat to be averted. These are threats against, for example, control and operational information in the key management, QKDN control and QKDN management layers. If such threats occur, secure and reliable operations of a QKDN cannot be achieved.

– 1: Low level

This level includes two kinds of threat. The first is the DoS attack that is recognizable and needs to be considered. If such a threat occurs, a QKDN cannot operate normally. The second is eavesdropping of the control and management information of the QKDN, which can be done unrecognizably. This causes neither leakage of the key data nor disruption of QKDN operations but may be beneficial to the adversary.

9 Security requirements and security measures

This clause describes security requirements (SReqs) and security measures to fulfil them in the QKDN. The SReqs are specified to address the threats listed in clause 8.

The requirements are organized from the viewpoint of security dimensions, which are sets of security measures designed to address a particular aspect of network security specified in clause 6 of [ITU-T X.805]. Accountability is moreover added to the dimensions for security management of the QKDN. Relations between security dimensions and security threats are mapped in Table 3, which is limited to dimensions that have a substantial impact on the functional elements, links and QKDN operations.

A detailed specification of the security requirements is outside the scope of this Recommendation, as are non-repudiation and reliability of a QKDN.

NOTE – Security measures to protect quantum and classical attacks on QKD links and QKD-specific side-channel attacks on QKD modules are outside the scope of this Recommendation.

Table 3 – Mapping of security dimensions and security threats

Threat **Dimensions**		**Spoofing**	**Eavesdropping**	**Deletion or corruption**	**Repudiation**	**DoS**
Authentication		x			x	
Access control		x		x	x	
Confidentiality		x	x			
Integrity		x		x		
Availability	Key accumulation and key relay			x		
	Damage control and recovery			x		
	Robustness against DoS					x
Accountability	Activity logging	x		x		x
	Alarm reporting	x		x		x
	Audit	x			x	x

9.1 Security measures for the QKDN operation

9.1.1 Authentication

SReq.1: A QKDN is required to establish identifiers and verify the claimed identities of functional elements in the QKDN, as well as those in the user network, and any other entities if these are connected to the QKDN from outside.

The security measures supporting SReq.1 include:

– user authentication: establishes the proof of the identity of the functional elements in the user network that are connected to the QKDN, e.g., cryptographic applications or network managers;

– entity authentication: establishes the proof of the identity of the functional elements in the QKDN during their communications;

– data origin authentication: establishes the proof of identity responsible for the origin of a specific data unit.

Authentication functions play an essential role in protecting the confidentiality of the key data (see clause 9.1.3) by ensuring that only authorized parties can access the key data, and also in ensuring the integrity and authenticity of key data (see clause 9.1.4). Their details are outside the scope of this Recommendation.

SReq.1.1: The QKDN is recommended to employ entity authentication between relevant functional elements before delivering the key.

The usage of authentication functions establishes proof for a particular instant in time. To ensure continued proof, authentication has to be repeated or linked to an integrity service.

NOTE – For example, authentication tags are generated from key data or metadata (key ID, functional element ID, timestamp, etc.), attached as a new element to the metadata, and processed in relevant functional entities in the QKDN.

9.1.2 Access control

SReq.2: A QKDN is recommended to ensure that functional elements in the QKDN are prevented from gaining access to information or resources that the elements are not authorized to access.

Access control functions provide means to ensure that resources are accessed by subjects only in an authorized manner. Resources concerned may be physical systems, system software, applications, or data. The limitations of access are laid out in access control information, which specifies:

– a means to determine which entities are authorized to have access;

– what kind of access is allowed (reading, writing, modifying, creating, deleting).

Access control can be supported by authentication functions.

NOTE – Physical access control can be handled in a trusted node. In this case, the access control of all functional entities within a single trusted node can be performed by a single security measure.

9.1.3 Confidentiality

SReq.3: A QKDN is required to ensure the confidentiality of stored and transferred key data.

To fulfil SReq.3, the following requirements are needed.

SReq.3.1: Information on keys is recommended not to be available to unauthorized parties for a sufficiently long period of time specified by cryptographic applications.

NOTE 1 – For key data supplied from a KM, this long-term confidentiality is often requested even when resisting attacks with advanced and future computational technologies.

In order to preserve the long-term confidentiality of the transferred key data, when the key is relayed through the KM links in the QKDN, highly secure encryption method(s) should be employed.

SReq.3.2: The QKDN is recommended to use IT-secure protocols, e.g., OTP encryption, for key relay.

In addition, another appropriate method, such as the advanced encryption standard (AES) ([b-ISO/IEC 18033-3]and [b-FIPS PUB 197]), should be an option according to key management policy, e.g., if the necessary number of keys for OTP-key relay is not available.

SReq.3.3: The QKDN is recommended to create metadata to record an encryption method used for individual key relay; this metadata is also used for key life cycle management of relayed keys.

NOTE 2 – When the cryptographic application requests keys that have the same security level as that of keys generated by QKD modules, the QKDN should select keys that were relayed by OTP encryption, using the metadata on key relay encryption methods.

SReq.3.4: When a key is transferred via a QKD-KM link/a KM-APP link inside a trusted node, the QKDN is recommended to encrypt the key data.

SReq.3.5: In order to preserve the long-term confidentiality of stored key data, secure key storage and key leakage prevention technologies are recommended to be employed.

SReq.4: A QKDN is recommended to ensure the confidentiality of stored and transferred metadata, control and management information, and other data in the QKDN.

The confidentiality of the control and management information is not necessarily at the IT-confidentiality level in most cases since it should be protected only during the time of QKDN operation. Computational cryptographic algorithms, e.g., post-quantum cryptographic techniques, may be applied.

9.1.4 Data integrity

SReq.5: A QKDN is required to protect the integrity of stored and transferred data.

The data integrity functions provide means to ensure the correctness of stored and transferred data, protecting against modification, deletion, creation (insertion) and replay of exchanged data. For key data, integrity should be protected in transfer and storage until its consumption in a cryptographic application. For control and management information, integrity should be protected during the operation of the QKDN.

In most cases, cryptographic algorithms with appropriate computational security can be used. Post-quantum cryptographic techniques should be employed in accordance with their standardizations and practical deployments. In addition, IT-secure methods (e.g., [b-Wegman-Carter] message authentication) can be employed to protect integrity for data transfer.

9.1.5 Availability

9.1.5.1 Key accumulation and key relay

SReq.6: A QKDN is recommended to ensure the availability of key data.

Security measures to support capability are:

– accumulation of key data in the KM;

– key relay by the KM(s) and the KM links, and rerouting of key relay routes.

The functions might be restricted by key generation performances of the QKD modules and key management policies.

9.1.5.2 Damage control and recovery

SReq.7: A QKDN is required to have capabilities for network resilience.

Network resilience is required to have the ability to adapt to and recover from situation changes, including disruption, in order to continue acceptable levels of service in the face of security threats.

NOTE – [b-NIST SP 800-160-2] introduces security measures on resilience applicable to the QKDN (e.g., system redundancy, network segmentation).

If security violations are detected, this capability ensures their handling in a controlled way, minimizing the damage caused. In addition, it ensures recovery of the system, restoring it at a required security level.

9.1.5.3 Robustness against denial of service attacks on QKD links

SReq.8: A QKDN is required to implement counter-measures against DoS attacks.

DoS attacks can be treated as a part of the system damage category in clause 9.1.5.2; however, consideration of this threat is a prominent security point for QKDNs, as well as for other networks (e.g., optical transport network). Key generation rates may be reduced (even to zero) due to DoS attacks on QKD links. This issue could be mitigated by appropriate methods, including switching to backup QKD links and rerouting key relay.

Another backup option may be to apply another appropriate key relay method, e.g., employment of a post-quantum cryptographic scheme (such as AES). In such case, the KM should report the method and relevant parameters for the key relay.

The details of anti-DoS measures on QKD links are outside the scope of this Recommendation.

9.1.6 Accountability

SReq.9: A QKDN is recommended to ensure that records of security critical actions are traceable uniquely to functional elements that performed the actions.

SReq.10: A QKDN is recommended to support traceability of key data.

SReq.9 and SReq.10 are supported by the functions of activity logging (see clause 9.1.6.1), and security audit (see clause 9.1.6.3).

Another possible but potentially weaker realization of accountability is achieved by the appropriate combinations of the authentication, access control and audit trail functions.

9.1.6.1 Activity logging

SReq.11: A QKDN is recommended to have the capability of storing information about security relevant activities in the QKDN.

Functional elements of the QKDN may communicate with logging functions.

9.1.6.2 Security alarm notification

SReq.12: A QKDN is recommended to generate alarm notifications on security events.

The security alarm notifications are information regarding operations pertaining to security.

9.1.6.3 Security audit on logged data

SReq.13: A QKDN is recommended to have the capability to analyse logged data on security events.

NOTE – An audit is seen as an independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with the established security policy and operational procedures, and to detect breaches in security. The result of the audit would identify changes in control, policy, and procedures.

9.2 Deployment, support, maintenance, and migration

SReq.14: A QKDN is required to have security measures for deployment, support, maintenance, and migration in order to continuously provide the security control of the QKDN during and after these operations.

Deployment, support, and maintenance are necessary to start and to keep a QKDN running.

Bibliography

[b-ITU-T T.411] Recommendation ITU-T T.411 (1993), *Information technology – Open Document Architecture (ODA) and interchange format: Introduction and general principles.*

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.1038] Recommendation ITU-T X.1038 (2016), *Security requirements and reference architecture for software-defined networking*.

[b-ITU-T X.1193] Recommendation ITU-T X.1193 (2011), *Key management framework for secure Internet protocol television (IPTV) services*.

[b-ISO/IEC 18033-3] ISO/IEC 18033-3:2010, *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers.*

[b-ISO/IEC 27000] ISO/IEC 27000:2010, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ETSI GR QKD 007] ETSI GR QKD 007, V1.1.1 (2018), *Quantum key distribution (QKD); Vocabulary*.

[b-FIPS PUB 197] Federal Information Processing Standards Publication 197 (2001), *Advanced encryption standard (AES).*

[b-NIST SP 800-160-2] Ross, R., Pillitteri, V., Graubart, R. Bodeau, D., McQuaid, R. (2019). Developing cyber resilient systems: A systems security engineering approach, NIST Special Publication 800-160, Volume 2. Gaithersburg, MD: National Institute of Standards and Technology. 205 pp. Available [viewed 2020-07-04] at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf

[b-Wegman-Carter] Wegman, M.N., Carter, J.L. (1981). New hash functions and their use in authentication and set equality. *J. Comput. Syst. Sci.* 22, pp. 265-279

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

Printed in Switzerland
Geneva, 2021