ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

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
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.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/.

Table of Contents

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.

3.1.4 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.

3.1.5 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.

3.1.6 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).

3.1.7 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.

3.1.8 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).

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 trusted node (TN): A node that is protected against intrusion and attacks by unauthorized parties, and acts as a boundary protecting all embedded elements against attackers outside the node.

NOTE 1 – A trusted node can contain one or more quantum key distribution (QKD) modules, key managers (KMs), quantum key distribution network (QKDN) mangers, QKDN controllers, applications and other possible entities.

NOTE 2 – In [ITU-T X.1710], the description of trusted node (TN) is given as: "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."

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

DLP Data Loss Prevention

DoS Denial of Service

EM Electro-Magnetic

HSM Hardware Security Module

IDPS Intrusion Detection and Prevention System

IPS Intrusion Prevention System

ITS Information Theoretic Security

KM Key Manager

KMA Key Management Agent

KSA	Key Supply Agent
L3SW	Layer 3 Switch
QKD	Quantum Key Distribution
QKDN	Quantum Key Distribution Network
SSL	Secure Socket Layer
SSH	Secure Shell
TN	Trusted Node
VESDA	Very Early Smoke Detection Apparatus
ZTNA	Zero Trust Network Access

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.

The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Introduction

Quantum key distribution (QKD) enables two remote parties to share symmetric random bit strings to be used as a secure key that is unknown to potential eavesdroppers. In principle, any eavesdropping attempts will unavoidably introduce quantum disturbances and will be detected by QKD users. The information theoretic security (ITS) of QKD protocol and its security proof is derived from the theory of quantum physics and quantum information. QKD point-to-point link distance is fundamentally limited by the quantum channel loss [b-Pirandola]. In practice, QKD networks (QKDNs) based on trusted nodes (TNs) have been widely adopted to extend the key establishment distance and enrich QKD-key based applications. As described in [ITU-T X.1710], a trusted node in QKDN is a QKD node that is protected against intrusion and attacks by unauthorized parties. Conceptually, a QKD node is also considered as a trusted node.

This Recommendation aligns the concept of the QKD node to [ITU-T X.1710], and addresses security issues of QKD nodes in the QKDN, including assets in a QKD node that need to be protected, security threats and risk analysis in QKD nodes, security requirements in a QKD node that address the threats, and security measures in QKD nodes established to meet the security requirements.

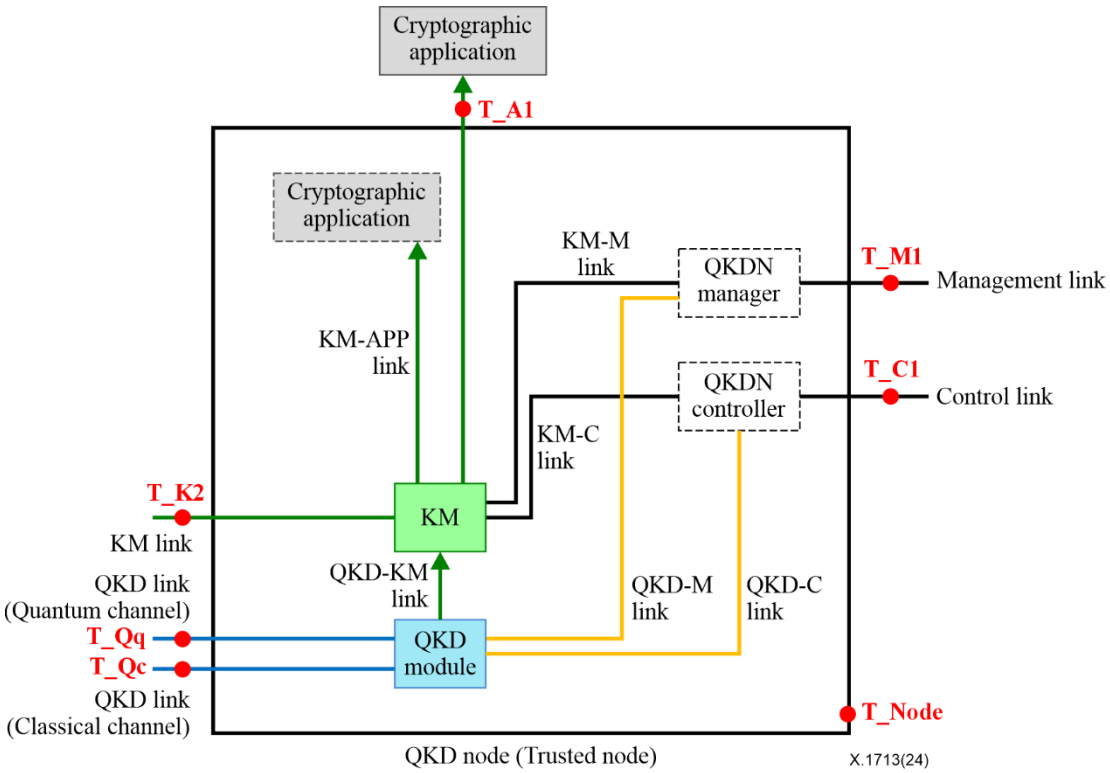

Figure 1 – A typical structure of a QKD node and security threats

In Figure 1 a solid-lined box indicates functional entities contained in the QKD node. A dashed-lined box indicates functional entities optionally contained in the QKD node. Red marks indicate the threats outside the QKD node that arise from the interface points.

As shown in Figure 1, QKD module(s), key manager(s) and internal links are all located in a QKD node. A QKDN controller and a QKDN manager are functional entities that can optionally be included as well. Cryptographic applications can have a point of presence inside a QKD node. It depends on the specific usage of the cryptographic application, arrangement of user devices, security responsibility of different parts of a system or other user cases. Entities in a QKD node, or in other words, the scope of a QKD node, varies depending on the situation and the cryptographic applications. For example, an entity directly supplying key supply agent-keys (KSA-keys) via a key manager (KM) for mobile devices should be regarded as a part of a QKD node.

The security threats (T_Node, T_K2, T_C1, T_M1, T_A1, T_Q1) identified in [ITU-T X.1710] that are addressed by a QKD node include:

– T_Node: Security threat at the QKD node.
– T_K2: Security threat at the KM links.
– T_C1: Security threat at the control link.
– T_M1: Security threat at the management link.
– T_A1: Security threat at the KM-APP link.
– T_Q1: Security threat at the QKD link.

In this Recommendation, security threats at the QKD link T_Q1 are divided into security threats at the quantum channel T_Qq and security threats at the classical channel T_Qc.

7 Assets to be protected in a QKD node in a QKDN

In the QKD node, the assets to be protected include: information assets and QKDN physical entity assets.

The information assets to be protected in a QKD node include:

a) key data – random bit strings that are used as a cryptographic key:
   - QKD-key: key data generated by a pair of QKD modules, and acquired by a key management agent (KMA);
   - KMA-key: key data resized by a KMA by joining or splitting QKD-keys into a predefined size;
   - KSA-key: key data transferred from a KMA to a KSA according to the requested key length, which is supplied to the cryptographic application;

b) metadata – attribute information on key data and key management. Such information is attached to key data as headers and/or footers;

c) information from QKD module and KMs to QKDN controller and QKDN manager (if installed):
   - QKDN controller information that is communicated via the control links between the KM/QKD modules and the QKDN controller;
   - QKDN management information that is communicated via the management links between the KM/QKD modules and the QKDN controller.

QKDN physical entities are assets to be protected in a QKD node. These are devices that implement functionalities belonging to the functional entities described in [ITU-T Y.3802]. Examples of such functional entities include:

- QKD module
- KM
- QKDN controller (if installed)
- QKDN manager (if installed)

Parts of cryptographic applications can also be assets to be protected in a QKD node.

Links between QKDN physical entities where included are also to be protected in a QKD node. This can form part of the protection of the information assets and QKDN physical entity assets.

Entities in the QKD node can change over time, depending on the implementation. For example, some mobile applications such as smartphones, drones and other mobile terminals can connect to a KSA to receive keys within the QKD node, but can consume the keys mostly outside the QKD node. Meanwhile, a QKD node can optionally contain a QKDN controller and/or a QKDN manager.

8 Security threats to a QKD node in a QKDN

A conceptual structure of a QKDN is specified in [ITU-T Y.3800], and its security framework is described in [ITU-T X.1710]. As specified in these Recommendations, a QKD node can contain QKD modules, KMs, QKDN controllers, QKDN managers, cryptographic applications, interfaces (QKD-KM, KM-APP, KM-C, KM-M, QKD-C, QKD-M) and other possible entities as needed. Several links are connected to the QKD node, including the QKD links, the KM links, the control links, the management links (and the KM-App interfaces if the cryptographic applications are outside the QKD nodes). In [ITU-T X.1710], the security framework of QKDN describes how a QKD node is protected against intrusion and attacks, and that such a protected QKD node is called a trusted node. Clause 8.1 analyses threats to a QKD node, some of which are also considered in [ITU-T X.1710].

8.1 Possible attacks

Figure 1 illustrates a typical structure of a QKD node and its possible attack interface points. Major threats to the QKD node via these points are categorized into the following six types of attack:

a) Unauthorized physical access (T_Node)

Attackers can physically intrude into the QKD node using different approaches, such as the vulnerabilities of access control mechanisms or misconfigurations (e.g., weak passwords) or by posing as authorized agents. Attackers can then directly access QKD modules, KMs, interfaces (QKD-KM, KM-APP, KM-C, KM-M, QKD-C, QKD-M), QKDN controller, QKDN manager and other entities inside the QKD node to steal information assets or for other purposes such as causing loss or corruption of information, forgery, spoofing, repudiation or denial of service (DoS). Attackers can also interrupt, influence and even take control of the operations of QKDN physical entities and their interfaces.

b) Attacks against the QKD link (T_Qq, T_Qc)

Through the QKD link, in particular the quantum channel (T_Qq), attackers can attempt to send light into QKD modules to affect the behaviour of internal components or to detect light leakage. This can potentially enable the attackers to achieve knowledge of key information without being detected if a QKD module is not properly implemented [b-ITU-T FG-QIT4N D2.3]. As the quantum channel is an open channel for the QKD transmitter and receiver to exchange quantum signals, even if the internal components of a QKD module can be protected by its own security enclosure, attackers can still attempt to send light or receive optical signals through the quantum channel (T_Qq). Attackers can also attempt to modify the post processing information through the classical channel (T_Qc) in the QKD link, which can also lead to leakage of key information if a vulnerability exists in a QKD module.

c) Unauthorized network access (T_Qc, T_K2, T_C1, T_M1, T_A1)

Attackers can try to access the functional elements inside the QKD node through the external links and/or interfaces (T_Qc, T_K2, T_C1, T_M1, T_A1). The threats caused by this type of attack include unauthorized access to the information assets, cryptographic vulnerability exploitation, functions abuse, failure explosion, audit circumvention and malicious update.

d) Unauthorized access through dynamical entities (T_Node)

Some of the entities can enter and exit a QKD node. For example, cryptographic applications can include mobile terminals such as smart phones and drones that can receive keys inside the QKD node and consume them mostly outside the QKD node. In such a system, attackers can send unauthorized mobile terminals into the QKD node to access entities in the QKD node with the objective of performing attacks.

e) Attacks through installation, maintenance and migration (T_Node)

Attackers can attack the entities in the QKD node when these are installed, or under maintenance or migration, e.g., installing backdoors and/or unauthorized entities (QKD modules, KMs, and QKDN controllers or managers). In addition, some QKD modules can have a maintenance port to check the proper operation of the devices. Such ports can potentially open loopholes for attacks, e.g., if not properly disabled.

f) Classical side-channel attacks (T_Node)

There are several physical security attacks to cryptographic modules, known as (classical) side-channel attacks, such as power analysis, timing analysis, fault induction. These attacks typically involve detecting some outputs from the modules (e.g., power consumption, radiative electromagnetic (EM) signals, etc.) or applying external forces (EM waves, control of temperature, voltage, etc.). Both invasive and non-invasive attacks can be threats for a QKD node. These attacks are discussed for example in [b-NIST FIPS 140-2], [b-ISO/IEC TS 30104] and [b-ISO/IEC 17825].

8.2 Risk and threat analysis

This clause describes security risks and threats caused by the attacks described in clause 8.1 and their relevance.

a) Cryptographic vulnerability exploitation threats

QKDN physical entities employ different cryptographic mechanisms such as key agreement, secure system authentication, etc. Through attacks a), b), c), d), e), f) as presented in clause 8.1, attackers can attempt to compromise the cryptographic mechanisms by exploiting the algorithmic vulnerabilities and the design and implementation vulnerabilities in cryptographic functions, including the functions for message encryption, and authentication and identification of users, etc. This can result in the compromise of QKDN physical entities in a QKD node, direct loss of information in the links, etc.

b) Functions abuse threats

Through attacks a), b), c), d), e) presented in clause 8.1, attackers can abuse functions that are not intended for use once physical entities have been delivered, or otherwise in an unintended life-cycle phase (e.g., the test or debugging functions reserved for development and maintenance phases), in order to compromise the QKDN physical entities in a QKD node.

c) Failure exploitation threats

Through attacks a), b), c), d), e), f) presented in clause 8.1, attackers can take advantage of the failures induced during system initialization, and operation, and compromise the QKDN physical entities in a QKD node.

d) Audit circumvention threats

Through attacks a), c), d), e), f) presented in clause 8.1, attackers can attempt to access, change, or modify the security functionality of the physical entities without being detected. This can result in the attackers finding an avenue (e.g., misconfiguration, flaw in the product) to compromise a QKDN physical entity in a QKD node, without QKDN administrators knowing about it.

e) Malicious update threats

Through attacks a), c), d), e) presented in clause 8.1, attackers can attempt to provide a compromised update to the software or firmware, which undermines the security functionality of the QKDN physical entities in a QKD node. Unvalidated updates or updates validated using insecure or weak cryptography can leave software or firmware vulnerable to malicious alteration.

9 Security requirements for QKD nodes in a QKD network

The trustworthiness aspect and the security aspect of the QKD node is a fundamental element to ensure the overall security in QKDN. It has been shown that a partially corrupted QKD node can lead to failures of the security of keys relayed using a corrupted QKD node where no honest path exists, and potentially in other insecure circumstances dependent upon the QKDN implementation [b-Salvail]. At a basic level, the security of a QKDN can be analysed under the assumption that QKD nodes have been configured to be secure and that they keep QKDN physical entities out of reach of attackers aside from links between QKD nodes. In practice such assumptions give rise to several security requirements.

The following security requirements have been devised to help protect the information assets and the QKDN physical entity assets inside a QKD node against the security threats addressed in clause 8. The security requirements addressed in this clause are given on a high-level basis. Some considerations of security measures for QKD nodes are discussed in Appendix I and Appendix II.

SReq.1: The QKD node is required to provide boundary protection against physical intrusion by adversary entities into areas containing its QKDN physical entities and links between them.

NOTE 1 – For example, by using door access control, intrusion detection and/or alarms for the QKD node.

SReq.2: The QKD node is recommended to provide protection of its QKDN physical entities and the links between them by appropriate means.

NOTE 2 – For example, additional physical protection (e.g., secure cages) and tamper protection measures can be considered.

SReq.3: The QKD node is required to protect against alteration, interruption and corruption of its QKDN physical entities and the links between them by adversary entities.

SReq.4: The QKD node is recommended to be equipped with real-time sensors to monitor environmental parameters such as voltage, temperature and humidity, and to report significant anomalies detected.

SReq.5: The QKD node is recommended to have the capability to trace physical access, for example, through a video monitoring system.

SReq.6: The QKD node is recommended to adopt physical protection measures to protect against accidental physical damage to its QKDN physical entities and the links between them.

NOTE 3 – For example, fire extinguishing system, and/or design measures to limit the risk of water damage.

SReq.7: The QKD node can optionally assist QKD modules to reduce possible light injections from an attacker to the QKD modules via the quantum channel, and unwanted light leakage of QKD modules to the quantum channel.

NOTE 4 – Active or passive components can be added on the quantum channel in the QKD link against T_Qq, such as a light monitor, isolator, circulator, filter or power limiter. Such measures can interfere with the correct operation of QKD modules, unless carefully customised for the QKD modules in use. QKD modules can include appropriate protection against T_Qq.

SReq.8: The QKD node can optionally implement protection against threats T_Qc, T_A1, T_K2, T_M1 and T_C1 to the integrity of information in the relevant links.

NOTE 5 – Measures introduced against T_Qc can interfere with the correct operation of QKD modules, unless carefully customised for the QKD modules in use. QKD modules can include appropriate integrity protection against T_Qc.

Appendix I

A configuration example of security measures for QKD nodes

(This appendix does not form an integral part of this Recommendation.)

I.1 Configuration example of security measures for unauthorized physical access and unauthorized access through dynamic entities

Security measures in QKD nodes include preventing unauthorized physical access and unauthorized access through dynamic entities, and protection of the functional entities contained in QKD nodes.

QKD nodes are protected by the following measures:

– **Access control (physical access control):** Physical access is managed by multi-factor authentication using an integrated circuit card, biometric authentication or pass-code / password authentication using a numeric keypad. When entering or leaving a room, identification for physical access by personnel such as security guards, anti-pass packs, interlock control, or the like are used to prevent unauthorized physical access.

– **Surveillance camera:** If it is difficult for personnel such as security guards to be permanently at the entrance to the QKD node facilities, unauthorized physical access can be prevented by remote monitoring using surveillance cameras. In addition, surveillance images are stored for a certain period of time and can used for forensic investigations, etc.

To increase the availability of the QKD node, the defects of environmental factors due to disasters such as fires can be detected and suppressed by the following measures:

– **Fire detection system:** By detecting a fire at an early stage and implementing an initial response, the expansion of the impact on the entire QKD node can be suppressed. Small amounts of smoke in the initial state of a fire before it spreads can be detected by incorporating the ultra-sensitive very early smoke detection apparatus (VESDA) smoke detection system in the air circulation system of the server room. Furthermore, by sensing the circulating air flow, a certain amount of smoke in the server room or the like can be detected.

– **Fire extinguishing system:** Gas fire extinguishing systems cause less damage to equipment and are suitable for installation in the QKD node.

A typical implementation of security measures in QKD nodes is shown in Appendix II.

I.2 Configuration example of security measures for QKD links

Security measures can be considered for the QKD link interface. For the quantum channel against T_Qq, active or passive components can be added to reduce light injection to or light leakage from the quantum channel. These include but are not limited to light monitors, isolators, circulators, filters and power limiters. For the classical channel against T_Qc, additional checks to verify the data integrity using different techniques, e.g., Wegman-Carter message authentication code, can be considered. Counter measures against DoS attacks for post processing communication on the classical channel can also be considered.

NOTE – Adding additional components on the quantum channel interface can increase the quantum signal loss, which further degrades the performance, i.e., QKD key rate of QKD modules. Such measures can also interfere with other aspects of the correct operation of QKD modules, unless carefully customised for the QKD modules in use. QKD modules can include appropriate protection.

I.3 Configuration example of security measure for unauthorized network access

Security measures in QKD nodes ensure that information flows only between the authorized end points, which means that it is protected against unauthorized access and disclosure by outsiders [b-ITU-T X.1039].

QKD nodes are protected by the following measures:

– **Firewall:** The firewall is a typical implementation of the security gateway that controls the incoming and outgoing network traffic based on an applied rule set. A firewall establishes a barrier between a trusted, secure internal network and another external network (e.g., the Internet) that is assumed not to be secure and trusted.

– **Intrusion detection system:** An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.

– **Intrusion prevention system:** Intrusion prevention systems (IPSs), also known as intrusion detection and prevention systems (IDPSs), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it. Intrusion prevention systems are considered extensions of intrusion detection systems.

A security gateway, which can include the measures mentioned above, is implemented when different network segments are connected:

– **Security gateway:** A security gateway is placed at the boundary between two network segments, for example, between the organization's internal network and a public network, to filter the traffic flowing across the boundary in accordance with the documented security gateway service access policy for that boundary.

NOTE 1 – Appendix I in [b-ITU-T X.1039] also specifically describes physical and environment security, which is applicable to QKDN nodes.

Figure I.1 depicts the typical implementation of security measures in QKD nodes.

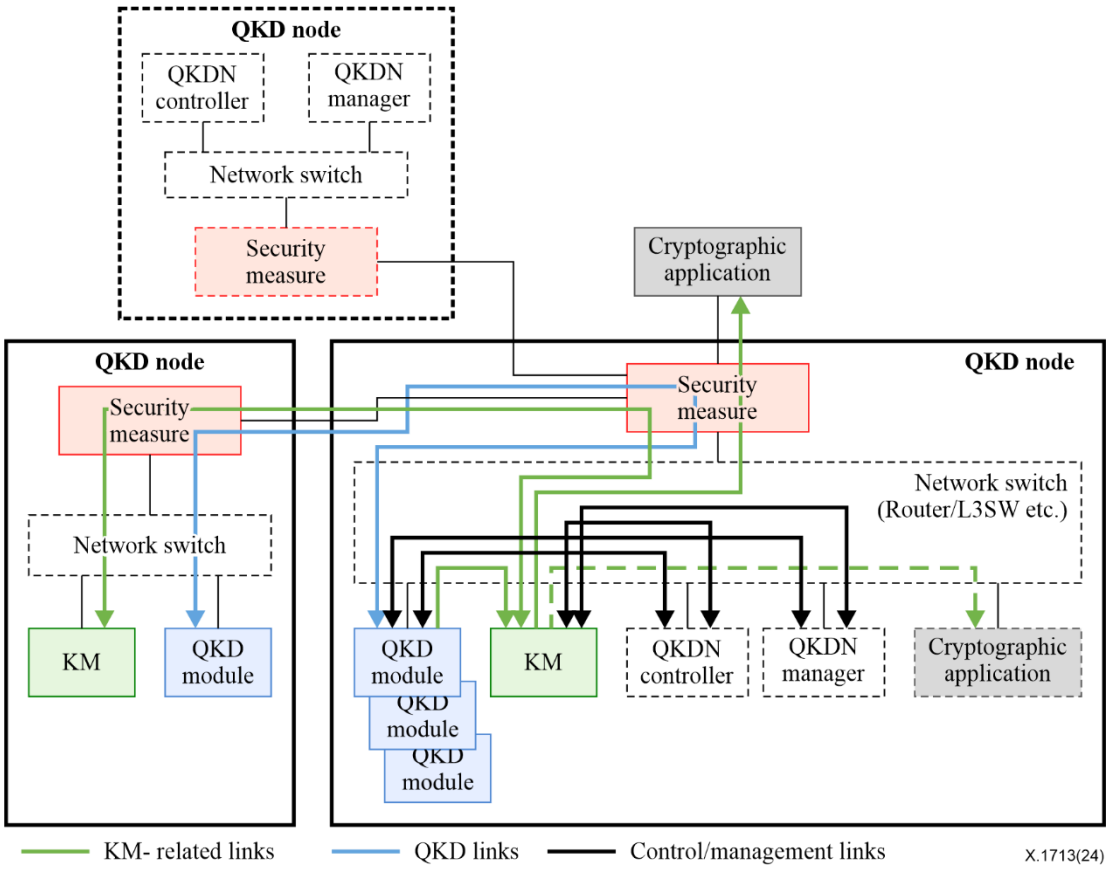

Figure I.1 – A security configuration example of QKD nodes

NOTE 2 – Solid-lined boxes are components contained in the QKD node. Dashed-lined boxes are components optionally contained in the QKD node.

NOTE 3 – Network switches (router or layer 3 switch (L3SW), etc.) relay communications between components in the QKD node and components of other QKD nodes.

Communications via QKD nodes are characterized by the type of their transmission layer: QKDN control layer, key management layer, quantum layer and QKDN management layer, and security measures are selected according to their characteristics.

Except for the quantum layer, a firewall is one of major practical methods for the internal protection of QKD nodes. Firewalls relay all communications between QKD nodes, and the QKD node and cryptographic applications, and perform boundary monitoring and protection in QKD nodes. The router or L3SW separates links, which are QKD module-KM links, KM-application links, QKD module-QKDN manager links, KM-QKDN manager links, QKD module-QKDN controller links and KM-QKDN controller links, either in a physical or logical manner, and manages them.

I.4 Configuration example of security measures for attacks through installation, maintenance and migration

The QKD node prevents attacks during deployment, maintenance and migration by:

– **Storage encryption:** Stored information in the QKD node such as the key are encrypted by using, for example, a hardware security module (HSM). The encryption method to be used can be determined taking into account the identification of the required level of protection based on the risk assessment and taking into account the type, strength and quality of the required encryption algorithm.

– **Checking the validity of the update file:** A signature such as a hash value is added to the update file, and the validity is verified when the operator performs maintenance.

– **Operator authentication:** When an operator performs maintenance or accesses the system, password authentication or authentication using such as a secure shell (SSH) secret key set for each operator is examined, and only operations authorized for each operator can be performed. Authorized operations for each operator are reviewed periodically to identify and remove or disable user IDs that are not needed.

– **Save operation log:** The QKD node records information such as the user ID of the operator, the authentication / security-related operation to be performed, and the time of execution as a log, and stores it. To synchronize the time of the log, the clocks of all information processing systems in the organization or security area are synchronized with a single reference time source. Protection should be provided against unauthorized editing or deletion of log files to protect log functions and log information from tampering and unauthorized access. Back up files are stored in a secure storage regularly.

I.5 Configuration example of security measures for classical side-channel attacks

It is useful to shield the entire installation site, to prevent electromagnetic waves from leaking from the equipment, also to prevent electromagnetic wave radiation attacks from outside the site.

It is necessary to determine the required amount of attenuation of electromagnetic waves based on the configuration of the station house and the system configuration, and to design it according to the environment in which electromagnetic wave shielding is introduced.

NOTE – [b-IEC 61000-4-20] discusses EM interference /EM compatibility testing.

Some other side channel attacks such as power analysis attacks, timing analysis attacks, energy attacks, and their defence are discussed in [b-ISO/IEC TS 30104] and [b-ISO/IEC 17825].

Appendix II

Further considerations on security measures for QKD nodes

(This appendix does not form an integral part of this Recommendation.)

The following further security measures for QKD nodes can be considered:

1) **Attack surface reduction**: The attack surface of a software environment is where an unauthorized user can try to inject data to or extract data from an environment. The following methods help reduce the attack surface:
   - detecting and preventing attacks that occur on a host on which it is installed (e.g., Host intrusion prevention systems (IPS));
   - uninstalling non-essential software or applications from hosts;
   - checking and assessing vulnerabilities in the network (e.g., running vulnerability or compliance scans);
   - avoiding human error (e.g., cyber awareness training for employees).
2) **Anti-malware software**: Running anti-malware software to scan hosts and remove viruses and malware.
3) **Service assignment** [b-ITU-T X.1060]: The organization operating a QKDN should clarify specifically which team should implement the QKDN service. The kind of service assignment can be insourcing, outsourcing or a combination of both.
4) **Layer 7 inspection/secure socket layer (SSL) decryption**: Layer 7 inspection/SSL decryption is the process of checking for cyber threats of encrypted traffic as part of a full SSL inspection procedure. It can be considered for protection against threats, e.g., T_M1, T_C1, T_K2 and T_Qc on links accessing the QKD nodes.

   NOTE – Such techniques can compromise security measures incorporated within QKDN physical entities. It is important to consider the full security implications of such methods, including the security of any additional equipment involved. For example, decrypting management communications on hardware shared with other applications at the same site as the QKD node can be inconsistent with a network adopting a policy to implement QKDN functionality on dedicated hardware.
5) **Data loss prevention**: Data loss prevention (DLP) is a security tool or system to ensure that sensitive data is not lost, misused or accessed by unauthorized users. Advanced security measures employ machine learning and temporal reasoning algorithms to detect abnormal access to data. DLP can be applied to the specific QKD (e.g., data protection in the key management layer).
6) **Zero trust network access** [b-NIST SP800-207]: The zero-trust security model is an approach to the design and implementation of systems based on the concept "never trust, always verify". Zero trust network access (ZTNA) is a security architecture where only traffic from authenticated users, devices and applications is granted access to other users, devices and applications within an organization, and this framework can be deployed to the QKDN.
7) **Cyber defence services** [b-ITU-T X.1060]: Cyber defence services consist of strategic management; real-time analysis; deep analysis; incident response; checking and evaluation; collection, analysis and evaluation of threat intelligence; development and maintenance of cyber defence platforms; support of internal fraud response; and active relationship with external parties. Incident response takes specific actions based on the results of real-time analysis and threat information to deter and eliminate threats. It aims to minimize the impact on the system and the business, including coordination and reporting with stakeholders.

Bibliography

[b-ITU-T X.1039] Recommendation ITU-T X.1039 (2016), *Technical security measures for implementation of ITU-T X.805 security dimensions*.

[b-ITU-T X.1060] Recommendation ITU-T X.1060 (2021), *Framework for the creation and operation of a cyber defence centre*.

[b-ITU-T FG-QIT4N D2.3] Technical Report ITU-T FG-QIT4N D2.3-part 1 (2021), *Quantum key distribution network protocols Quantum layer*.

[b-ETSI GR QKD 007] ETSI GR QKD 007 (2018), *Quantum Key Distribution (QKD); Vocabulary*.

[b-IEC 61000-4-20] IEC 61000-4-20:2022, *Electromagnetic compatibility (EMC) – Part 4-20: Testing and measurement techniques – Emission and immunity testing in transverse electromagnetic (TEM) waveguides*.

[b-ISO/IEC 17825] ISO/IEC 17825:2024, *Information technology – Security techniques – Testing methods for the mitigation of non-invasive attack classes against cryptographic modules*.

[b-ISO/IEC TS 30104] ISO/IEC TS 30104:2015, *Information Technology – Security Techniques – Physical Security Attacks, Mitigation Techniques and Security Requirements*.

[b-NIST FIPS 140-2] NIST FIPS 140-2 (2001), *Security Requirements for Cryptographic Modules*.

[b-NIST SP800-207] NIST Special Publication 800-207 (2020), *Zero Trust Architecture*.

[b-Pirandola] Pirandola, S., Laurenza, R., Ottaviani, C. et al. (2017), Fundamental limits of repeaterless quantum communications, Nat. Commun. 8, 15043.

[b-Salvail] Salvail, Louis et al. (2010), *Security of Trusted Repeater Quantum Key Distribution Networks*. Journal of Computer Security 18, 61-87.

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, 2024