International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1712

Corrigendum 1

(02/2022)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Quantum communication – Security design for QKDN

Security requirements and measures for quantum key distribution networks – key management

Corrigendum 1

Recommendation ITU-T X.1712 (2021) – Corrigendum 1

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 (1)	X.1140–X.1149
Application Security (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.1350–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1399
Distributed ledger technology (DLT) security	X.1400–X.1429
Application Security (2)	X.1450–X.1459
Web security (2)	X.1470–X.1489
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
Cyber Defence	X.1590–X.1599
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
Data protection	X.1770–X.1789
IMT-2020 SECURITY	X.1800–X.1819

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

Recommendation ITU-T X.1712

Security requirements and measures for quantum key distribution networks – key management

Corrigendum 1

Summary

Recommendation ITU-T X.1712 specifies security threats and security requirements for key management in quantum key distribution networks (QKDNs), and security measures of key management to meet the security requirements.

This Recommendation also provides support for the design, implementation, and operation of key management in QKDNs with approved security.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1712	2021-10-29	17	11.1002/1000/14805
1.1	ITU-T X.1712 (2021) Cor. 1	2022-02-13	17	11.1002/1000/14942

Keywords

Key management, key relay, key supply, QKD (quantum key distribution), QKD network.

* 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/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.1712

Security requirements and measures for quantum key distribution networks - key management

Corrigendum 1

Editorial note: This is a complete-text publication. Modifications introduced by this corrigendum are shown in revision marks relative to Recommendation ITU-T X.1712 (2021).

1 Scope

This Recommendation specifies the following items:

– security threats to key management in the quantum key distribution network (QKDN);

– security requirements for key management in the QKDN;

– security measures of key management to meet the security requirements.

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 X.1714] Recommendation ITU-T X.1714 (2020), *Key combination and confidential key supply for quantum key distribution networks.*

[ITU-T Y.3800] Recommendation ITU-T Y.3800 (2019), including Cor.1 (2020), *Overview on networks supporting quantum key distribution.*

[ITU-T Y.3801] Recommendation ITU-T Y.3801 (2020), *Functional requirements for quantum key distribution networks.*

[ITU-T Y.3802] Recommendation ITU-T Y.3802 (2020), including Cor.1 (2021), *Quantum key distribution networks – Functional architecture.*

[ITU-T Y.3803] Recommendation ITU-T Y.3803 (2020), *Quantum key distribution networks – Key management.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

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

3.1.2 key life cycle [ITU-T Y.3800]: A sequence of steps that a key undergoes from its reception by a key manager (KM) through its use in a cryptographic application and until deletion or preservation depending on the key management policy.

3.1.3 key management [ITU-T Y.3800]: All activities performed on keys during their life cycle starting from their reception from the quantum layer, the storage, formatting, relay, synchronization, authentication, to supply to cryptographic application and delete or preserve depending on the key management policy.

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

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

3.1.5 key management agent-key (KMA-key) [ITU-T Y.3803]: Key data stored and processed in a key management agent (KMA), and securely shared between a KMA and a matching KMA.

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

3.1.7 key 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.

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

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

3.1.10 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.

3.1.11 key supply agent-key (KSA-key) [ITU-T Y.3803]: Key data stored and processed in a key supply agent (KSA), and securely shared between a KSA and a matching KSA.

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

3.1.13 message authentication code [b-ETSI GS QKD 008]: Cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of data.

3.1.14 quantum key distribution (QKD) [b-ETSI GR QKD 007]: QKD is a procedure or method for generating and distributing symmetrical cryptographic keys with information theoretical security based on quantum information theory.

3.1.15 quantum key distribution module (QKD module) [ITU-T Y.3800]: A set of hardware and software components that implements cryptographic functions and quantum optical processes, including quantum key distribution (QKD) protocols, synchronization, distillation for key generation, and is contained within a defined cryptographic boundary.

NOTE – A QKD module is connected to a QKD link, acting as an endpoint module in which a key is generated. These are two types of QKD modules, namely, the transmitters (QKD-Tx) and the receivers (QKD-Rx).

3.1.16 quantum key distribution-key (QKD-key) [ITU-T Y.3802]: A pair of symmetric random bit strings generated by a pair of quantum key distribution (QKD) modules, particularly referring to random bit strings before being resized and formatted in a KM.

3.1.17 quantum key distribution link (QKD link) [ITU-T Y.3800]: A communication link between two quantum key distribution (QKD) modules to operate the QKD.

NOTE – A QKD link consists of a quantum channel for the transmission of quantum signals, and a classical channel used to exchange information for synchronization and key distillation.

3.1.18 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 a key relay when they are not directly connected by a QKD link.

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

3.1.20 quantum key distribution network manager (QKDN manager) [ITU-T Y.3800]: A functional module, which is located in a quantum key distribution (QKD) network management layer to monitor and manage a QKD network.

3.1.21 quantum key distribution node (QKDN 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).

3.1.22 quantum key distribution protocol (QKD protocol) [ITU-T X.1710]: List of steps for establishing symmetric cryptographic keys with information-theoretical security based on quantum information theory.

3.1.23 security demarcation boundary [ITU-T Y.3800]: A boundary to demarcate one layer~~QKDN~~'s responsibility on the keys to be supplied from another layer~~the user network~~'s responsibility ~~for~~ on the use of ~~the~~ keys.

3.1.24 user network [ITU-T Y.3800]: A network in which cryptographic applications consume keys supplied by a quantum key distribution (QKD) network.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AES	Advanced Encryption Standard
DoS	Denial of Service
ID	Identifier
IT-secure	Information-Theoretically secure
KM	Key Manager
KMA	Key Management Agent
KSA	Key Supply Agent
MAC	Message Authentication Code

OTP One-Time Pad

QKD Quantum Key Distribution

QKDN Quantum Key Distribution Network

5 Conventions

In this Recommendation:

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

6 Introduction

A QKD network (QKDN) enables the supply of secure keys to cryptographic applications for protecting the long-term confidentiality of data. Basic functions and layered structures of the QKDN are defined in [ITU-T Y.3800]. Functional requirements and architectures are specified in [ITU-T Y.3801] and [ITU-T Y.3802], respectively. A security framework for the QKDN is specified in [ITU-T X.1710], by addressing the security threats against the QKDN, and deriving the general security requirements and the security measures for the QKDN.

This Recommendation addresses security issues of key management of the QKDN and specifies security requirements for key management as defined in clause 3.1.3, based on the key management framework described in [ITU-T Y.3803]. In terms of the layered model specified in [ITU-T Y.3800], the key management layer is the unique layer that will be considered in this Recommendation. In addition, the interfaces between the key management layer and other layers listed below are within the scope of this Recommendation:

– a quantum layer;
– a QKDN control layer;
– a QKDN management layer;
– a service layer.

7 Information assets to be protected in key management in the QKDN

Information assets to be protected in key management in the QKDN are as follows.

7.1 Key data

Key data comprise random bit strings. The individual key data can be used as a symmetric cryptographic key.

There are several kinds of key data in the process of key management which are as follows:

– QKD-key: key data generated by a QKD module, and acquired by a KMA;
– KMA-key: key data resized by the KMA by combining or splitting QKD-keys into a prescribed size;
– KSA-key: key data transferred from the KMA to a KSA according to a requested key length, which is supplied to the cryptographic application.

7.2 Metadata

Metadata are attribute information on key data and key management. Such information may include but is not limited to:

– key identifier (ID) (QKD-key ID, KMA-key ID, source KMA-key ID, KSA-key ID);
– generation time stamp;
– QKD module ID;
– matching QKD module ID;

NOTE 1 – For a QKD module *X*, the other QKD module *Y* to which QKD module *X* is directly connected via a QKD link is called the matching QKD module.

– key length;
– hash value;
– key type (encryption key/decryption key);
– KMA ID;
– source KMA ID;
– matching KMA ID;

NOTE 2 – For a KMA *X*, the other KMA *Y* to which KMA *X* is directly connected via a KMA link is called the matching KMA.

– destination KMA ID;
– key relay time stamp;
– key relay encryption method including relevant parameters;
– KMA-key metadata;
– supply time stamp;
– application name;
– application source ID;
– application destination ID; and so on.

The items above are not always mandatory but optional.

7.3 Control and management information

Control and management information relevant to key management is as follows:

– key management information, which is communicated via the KMA and KSA links in the key management layer;
– QKDN control information, which is communicated via control links between the key management layer and the QKDN control layer;
– QKDN management information, which is exchanged among the key management layer, the QKDN control layer, and the QKDN management layer;
– QKD module status information, which is communicated via links between the key management layer and the quantum layer.

8 Security threats of key management in QKDN

The key management framework and functional elements used in this Recommendation have been described in [ITU-T Y.3803]. This clause focuses on intrinsic security threats to key management for the QKDN.

In addition to a QKD link, a KMA link and a KSA link which are defined in [ITU-T Y.3800] and [ITU-T Y.3802], this Recommendation refers to the following links in this clause.

– Key supply link: A communication link connecting a QKD module and a KMA, a KMA and a KSA, or a KSA and a cryptographic application to supply QKD-keys, KMA-keys and KSA-keys, respectively. It also transmits metadata and the relevant parameters.

– Control and management link: A communication link to convey control and management information. These links connect a QKDN controller and its entities, a QKDN manager and its entities, or a QKD module and a KM.

Attack surfaces against key management in the QKDN are summarized in Figure 1 by red circles. The links that convey the key data include:

1) KMA links and key supply links, which include links between a QKD module and a KMA, links between a KMA and a KSA, and links between a KSA and a cryptographic application.

While the links that do not convey the key data include:

2) KSA links,

3) Control and management links connected to KMs.

NOTE 1 – Once key data has been supplied from KSAs to the cryptographic applications, the applications are responsible for the key data and its use.

NOTE 2 – The following items are outside the scope of this Recommendation:

(i) Attacks on functional entities outside the key management layer (e.g., the QKD modules, the QKDN controller, and the QKDN manager).

(ii) Attacks on links that are not directly connected to the KMs (e.g., the QKD link comprising the quantum and classical channels).

(iii) Insider attacks against the KM.

NOTE 3 – Insider attacks are attacks originating from an action within an organization that is legitimately involved in the QKDN, e.g., malicious attacks by a trusted operator of a QKDN, their business associates, or an outsider that has access to a controlled location within a QKDN by deception, etc.

(iv) Side-channel attacks, trapdoors, human errors, and natural disasters against the KM.

NOTE 4 – Assuming that the functions of the KM are digital, the side-channel attacks in (iv) are against the digital (not quantum) functions. Potential attacks include, for example, power analysis, timing analysis, fault induction and TEMPEST.

On each attack surface, the following security threats could arise:

– spoofing (masquerade);

– eavesdropping;

– deletion or corruption

– destruction of system resources, and

– denial of service (DoS).

NOTE 5 – The meanings of the terms of the security threats are specified in [ITU-T X.1710].

Even under the restrictions in (iii) and (iv), the KMAs and the KSAs may also suffer from the security threats listed in Figure 1 because malicious attacks such as a man-in-the-middle-attack could be launched against the links, causing effects on those functional elements in the KMs.

As shown in Figure 1, the KMAs and the KSAs, both of which deal with keys, should be located inside the trusted nodes for proper key management. Key supply links are also located inside the trusted nodes in most cases.

NOTE 6 – In most cases, cryptographic applications, the QKDN controller and the QKDN manager are located inside the trusted nodes. On the other hand, in some cases, while a cryptographic application receives keys in the trusted node, it consumes the keys outside the trusted node. Typical examples include cryptographic applications in mobile terminals such as smartphones and drones. This being the case, the key supply link between the KSA and the cryptographic applications may or may not be located inside the trusted node.

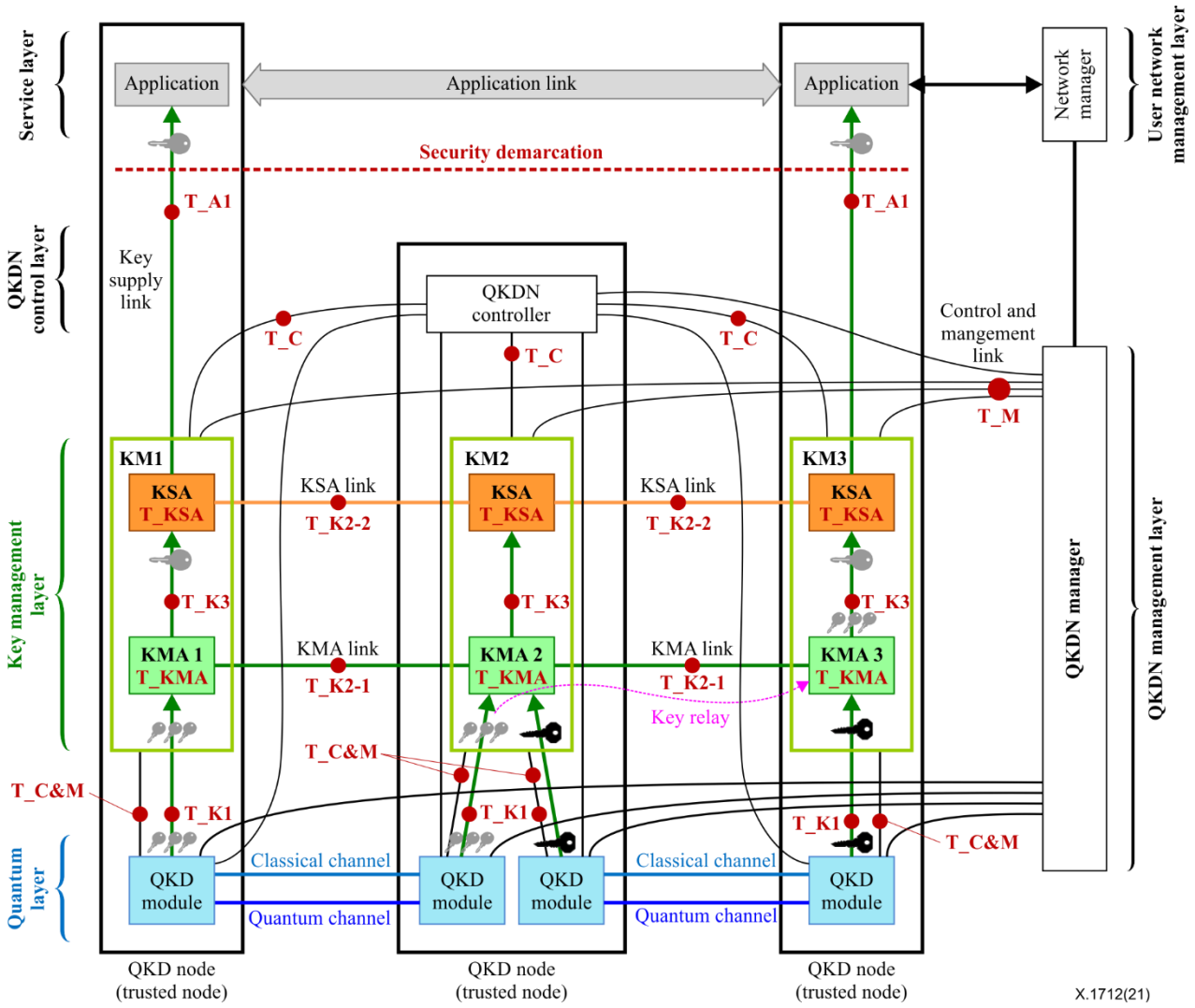

Figure 1 – Attack surfaces of key management in the QKDN (red circle)

NOTE 7 – Key supply links and KMA links are shown in green, KSA links are shown in orange, control and management links are shown in black in Figure 1.

8.1 Threats to KMA links (T_K2-1) and key supply links (T-K1, T_K3, T_A1)

The links that are shown in green in Figure 1 convey key data, metadata and control and management information. The potential threats involving the links include:

– Eavesdropping: intercepting and deciphering key data, metadata, and control and management information;

– Deletion or corruption: deletion or modifying key data, metadata, and control and management information;

– DoS: communication interruption or flooding data traffic.

8.2 Threats to KSA links (T_K2-2)

The links that are shown in orange in Figure 1 are the KSA links through which the metadata, control and management information are exchanged.

– Eavesdropping: intercepting and deciphering metadata, control and management information on the KSA link;

– Deletion or corruption: deletion or modifying metadata, control and management information on the KSA link;

– DoS: communication interruption or flooding data traffic.

8.3 Threats to control and management links (T_C, T_M, T_C&M)

The control and management links are shown in black in Figure 1. The links convey the metadata, control and management information.

– Eavesdropping: intercepting and deciphering the metadata, control and management information;

– Deletion or corruption: deletion or modifying the metadata, control and management information;

– DoS: communication interruption or flooding data traffic.

8.4 Threats to KMA and KSA (T_KMA, T_KSA)

Security threats at the KMA and KSA through the KMA links, KSA links and key supply links include:

– Spoofing: an attacker masquerades as a KMA and a KSA 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;

– Eavesdropping: intercepting and deciphering the key data and the metadata;

– Deletion or corruption: deletion or modifying key data and metadata;

– Destruction of system resources: physical attacks against equipment.

9 Security requirements and measures for information assets of key management in QKDN

To protect the information assets against the security threats addressed in the previous clause, security requirements and measures are derived for each asset.

Security measures for key management to meet the security requirements are studied in line with the procedures of the key management specified in [ITU-T Y.3803]. The procedures include key acquisition from QKD modules, key synchronization, storage, key relay in KMAs, and key supply from KSAs to cryptographic applications.

NOTE 1 – Security requirements and measures described in Tables 1, 2 and 3 address the KMA and KSA, but some of them are not performed solely by the KMA and the KSA. They should be performed in collaboration with the corresponding entities.

NOTE 2 – Security measures listed in Tables 1, 2, and 3 are necessary but not sufficient to fulfil the corresponding security requirements. Some security measures contribute to multiple security requirements.

NOTE 3 – Details of authentications and authorizations of entities and messages in a QKDN are outside the scope of this Recommendation.

9.1 Security requirements and measures on the key data

The requirements and measures for security protection of the key data are summarized in Table 1.

Table 1 – Security requirements and measures on the key data

	Description	Security requirements	Security measures
(i) confidentiality	Any information on the key data is protected from being leaked to unauthorized elements and parties.	SReq.1 The KMAs are required to ensure confidentiality of key data in a KMA link. SReq.2 The KMAs are recommended to use IT-secure confidentiality measures for a key relay in KMA links. SReq.3 The KMAs are required to ensure confidentiality of the key data in the key supply links between the KMA and a QKD module(s) in collaboration with the QKD module(s). SReq.4 The KMAs and KSAs are required to ensure confidentiality of the key data in the key supply links between the KMA and the KSA. SReq.5 The KSAs are required to ensure confidentiality of the key data in the key supply links between the KSA and a cryptographic application in collaboration with the cryptographic application. SReq.6 The KMA and the KSA are required to ensure confidentiality of key data when processed by or stored in the KMA and the KSA.	– Towards SReq.1, the KMAs have capabilities to perform key relay with encryption/decryption to protect the required confidentiality. – Towards SReq.2, KMAs encrypt the key data by IT-secure encryption/decryption such as a one-time pad (OTP) when it is relayed to other KMAs. – Towards SReq.3, SReq.4 and SReq.5, the confidentiality of key data is protected by appropriate means, which include physical protection of the key supply links and/or cryptographic methods by the KMA and the KSA. – Towards SReq.6, the KMA and the KSA are protected by appropriate means, which include tamper protection measures and/or the use of cryptographic measures. NOTE 1 – Tamper protection measures may be implemented together with security measures provided by a trusted node.

Table 1 – Security requirements and measures on the key data

	Description	Security requirements	Security measures
(ii)integrity	The key data remains unaltered.	SReq.7 The KMA is required to ensure the integrity of the key data that it manages. SReq.8 The KSA is required to ensure the integrity of the key data that it manages.	– Towards SReq.7, the following items (i), (ii) and (iii) are performed. (i) The KMA verifies the integrity of QKD-keys received from QKD modules. (ii) When the KMA creates a KMA-key from the received QKD-key, the KMA checks the integrity of the processing of the KMA-key. (iii) The KMA verifies the integrity of the KMA-keys received from other KMAs. – Towards SReq.8, the following item (i) and (ii) are performed. (i) The KSA verifies the integrity of KMA-keys received from KMA. (ii) When the KSA creates a KSA-key from the received KMA-key, the KSA checks the integrity of the processing of the KSA-key. – Towards SReq.7 and SReq.8, the KMA and the KSA are protected by appropriate means, which could include tamper protection measures and/or the use of cryptographic measures. NOTE 2 – Tamper protection measures may be implemented together with security measures provided by a trusted node.
(iii) authentication and access control	The key data comes from authorized entities and access to the key data is restricted to authorized entities.	SReq.9 The KMA and KSA are required to ensure that the key data received from other entities is not trusted unless the identity of the sending entity has been authenticated and is authorized to supply the key data. SReq.10 The KMA and KSA are required to ensure that they do not allow another entity access to the unencrypted key data without ensuring that the other entity is authorized to receive it.	– Towards SReq.9 and SReq.10, the KMA and the KSA could, for example, perform mutual authentication with other entities with which they communicate or utilize other approaches. – Towards SReq.9 and SReq.10, the KMA and KSA have the capability to handle attributes and to implement access control security policies.
(iv) availability	The key data is available whenever required.	SReq.11 The KMA is required to have the capability to store key data. SReq.12 The KMA is recommended to supply the key data when it is requested from the KSA even if the two QKD nodes do not have direct QKD links between them.	– Towards SReq.11, the KMA has a certain amount of storage space for key storage. – Towards SReq.12, if the QKD nodes do not have direct QKD links between them, the KMA at the QKD node performs a key relay between the two endpoint KMAs to share the necessary amount of KMA-keys under the control of the QKDN controller for routing, rerouting and other possible actions.

Table 1 – Security requirements and measures on the key data

	Description	Security requirements	Security measures
(v) accountability	The key life cycle is traceable.	SReq.13 The KMA and the KSA are required to have the capabilities to trace the key as requested. SReq.14 The KMA is recommended to inform a QKDN controller and/or a QKDN manager of the encryption method of the key relay and the relevant parameters.	– Towards SReq.13, the KMA and the KSA create and store metadata such as key ID, etc. for key life cycle management. – Towards SReq.14, the KMA has capabilities to create the metadata and the relevant parameters and send them to a QKDN controller and/or a QKDN manager. NOTE 3 – Alternatively, in the case of KMA with a fixed encryption method for a key relay, the QKDN controller and QKDN manager can be initialized with the KMA encryption method, and the relevant parameters added to their configurations. NOTE 4 – Actual actions for information to a QKDN controller and/or a QKDN manager depend on the implementation. ~~NOTE 5 – For confidentiality, the key relay function is capable of employing IT-secure encryption. For example, when the required amount of key for an IT-secure key relay is not available, some backup key relay schemes with a symmetric key cipher such as an advanced encryption standard (AES), using at least 256-bit symmetric keys, need to be launched as described in [ITU-T X.1714].~~ ~~NOTE 6 – The authentication can be performed by IT-secure authentication or authentication with public key certificates, etc.~~ ~~NOTE 7 – Wegman-Carter authentication [b-Wegman-Carter] is an example of an IT-secure message authentication code based on an almost strongly universal$_2$ family of hash functions.~~

NOTE 1 – For confidentiality, the key relay function is capable of employing IT-secure encryption. For example, when the required amount of key for an IT-secure key relay is not available, some backup key relay schemes with a symmetric key cipher such as an advanced encryption standard (AES), using at least 256-bit symmetric keys, need to be launched as described in [ITU-T X.1714].

NOTE 2 – The authentication can be performed by IT-secure authentication or authentication with public key certificates, etc.

NOTE 3 – Wegman-Carter authentication [b-Wegman-Carter] is an example of an IT-secure message authentication code based on an almost strongly universal$_2$ family of hash functions.

9.2 Security requirements and measures on the metadata

The requirements and measures on security protection of the metadata are summarized in Table 2.

Table 2 – Security requirements and measures on the metadata

	Description	Security requirements	Security measures
(i) confidentiality	Any information on the metadata is protected from being leaked to unauthorized elements and parties.	SReq.15 The KMA is recommended to ensure confidentiality of the metadata in KMA links and key supply links in collaboration with the QKD module(s) when they are transmitted through them. SReq.16 The KSA is recommended to ensure confidentiality of the metadata in KSA links and key supply links in collaboration with the cryptographic application when they are transmitted through them. SReq.17 The KMA and the KSA are recommended to ensure confidentiality of metadata when processed by or stored in the KMA and KSA.	– Towards SReq.15 and 16, the confidentiality of metadata is protected by appropriate means, which include physical protection of the key supply links and/or cryptographic methods by the KMA and the KSA. – Towards SReq.17, the KMA and the KSA are protected by appropriate means, which include tamper protection measures and/or the use of cryptographic measures. NOTE 1 – Tamper protection measures may be implemented together with security measures provided by a trusted node.
(ii) integrity	The metadata remains unaltered.	SReq.18 The KMA is required to ensure the integrity of the metadata that it manages. SReq.19 The KSA is required to ensure the integrity of the metadata that it manages.	– Towards SReq.18, the following items (i), (ii) and (iii) are performed. (i) The KMA verifies the integrity of metadata received from QKD modules. (ii) When the KMA creates a KMA-key from the received QKD-key, the KMA checks the integrity of the processing of the metadata of the KMA-key. NOTE 2 – Checking of the integrity of the processing of the metadata of the KMA-key may involve the KMA and the matching KMA. (iii) The KMA verifies the integrity of metadata received from other KMAs. – Towards SReq.19, the following items (i) and (ii) are performed. (i) The KSA verifies the integrity of metadata received from KMA. (ii) When the KSA creates a KSA-key from the received KMA-key, the KSA checks the integrity of the processing of the metadata of the KSA-key. NOTE 3 – Checking of the integrity of the processing of the metadata of the KSA-key may involve the KSA and the matching KSA. – Towards SReq.18 and SReq.19, the KMA and the KSA are protected by appropriate means, which could include tamper protection measures and/or the use of cryptographic measures. NOTE 4 – Tamper protection measures may be implemented together with security measures provided by a trusted node.

Table 2 – Security requirements and measures on the metadata

	Description	Security requirements	Security measures
(iii) authentication and access control	The metadata comes from authorized entities and access to the metadata is restricted to authorized entities.	SReq.20 The KMA and KSA are required to ensure that the metadata received from other entities is not trusted unless the identity of the sending entity has been authenticated and, it is then authorized to supply the metadata. SReq.21 The KMA and KSA are required to ensure that they do not allow another entity to have access to the unencrypted metadata without ensuring that the other entity is authorized to receive it.	– Towards SReq.20 and SReq.21, the KMA and the KSA could, for example, perform mutual authentication with other entities with which they communicate, or utilize other approaches. – Towards SReq.20 and SReq.21, the KMA and KSA have the capability to handle attributes and to implement access control security policies.
(iv) availability	N/A	N/A	N/A
(v) accountability	N/A	N/A	N/A

9.3 Security requirements and measures on the control and management information

The requirements and measures on security protection of the control and management information are summarized in Table 3.

NOTE – When the KMs are the subject of a security requirement, one or more of its embedded functions are in charge of this requirement. The possible embedded functions in the KMs include KMA, KSA or KM control and management as specified in [ITU-T Y.3802].

Table 3 – Security requirements and measures on the control and management information

	Description	Security requirements	Security measures
(i) confidentiality	Any information on the control and management information is protected from being leaked to unauthorized elements and parties.	SReq.22 The KMs are recommended to ensure confidentiality of the control and management information in the control and management links when they are transmitted through them.	– Towards SReq.22, the KMs protect the control and management information in the control and management links by appropriate cryptographic methods.

Table 3 – Security requirements and measures on the control and management information

	Description	Security requirements	Security measures
(ii) integrity	The control and management information remains unaltered.	SReq.23 The KMs are required to ensure the integrity of the control and management information that they manage.	– Towards SReq.23, the KMs secure the integrity of the control and management information when communicated.
(iii) authentication and access control	The control and management information comes from authorized entities and access to the control and management information is restricted to authorized entities.	SReq.24 The KMs are 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 it is then authorized to supply the control and management information. SReq.25 The KMs are required to ensure that they do not allow another entity access to the unencrypted control and management information without ensuring that the other entity is authorized to receive it.	– Towards SReq.24 and SReq.25, the KMs could, for example, perform mutual authentication with other entities with which they communicate, or utilize other approaches. – Towards SReq.24 and SReq.25, the KMs have the capability to handle attributes and to implement access control security policies.
(iv) availability	N/A	N/A	N/A
(v) accountability	N/A	N/A	N/A

9.4 Loss and corruption, and DoS

Loss of information can be made up for by detection of data loss and resending them. In addition, DoS can be protected by controlled access in conjunction with appropriate packet filtering by firewalls and intrusion prevention systems (IPS), etc.

Bibliography

[b-ETSI GS QKD 005] ETSI Group Specification QKD 005 V1.1.1 (2010), *Quantum Key Distribution (QKD); Security Proofs*.
https://www.etsi.org/deliver/etsi_gs/QKD/001_099/005/01.01.01_60/gs_QKD005v010101p.pdf

[b-ETSI GR QKD 007] ETSI Group Report 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

[b-ETSI GS QKD 008] ETSI Group Specification QKD 008 V1.1.1 (2010), *Quantum Key Distribution; QKD module security specification*.
https://www.etsi.org/deliver/etsi_gs/qkd/001_099/008/01.01.01_60/gs_qkd008v010101p.pdf

[b-Wegman-Carter] Wegman, M., N and Carter, J., L. (1981). *New hash functions and their use in authentication and set equality*. Journal of Computer and System Sciences, Volume 22, Issue 3, 1981, Pages 265-279, ISSN 0022-0000.
https://www.sciencedirect.com/science/article/pii/0022000081900337

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, 2022