ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T X.1716 (10/2024)

SERIES X: Data networks, open system communications and security

Quantum communication – Quantum Key Distribution Network (QKDN)

Authentication and authorization in quantum key distribution network

ITU-T X-SERIES RECOMMENDATIONS

Data networks, open system communications and security

PUBLIC DATA NETWORKS	X.1-X.199
OPEN SYSTEMS INTERCONNECTION	X.200-X.299
INTERWORKING BETWEEN NETWORKS	X.300-X.399
MESSAGE HANDLING SYSTEMS	X.400-X.499
DIRECTORY	X.500-X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600-X.699
OSI MANAGEMENT	X.700-X.799
SECURITY	X.800-X.849
OSI APPLICATIONS	X.850-X.899
OPEN DISTRIBUTED PROCESSING	X.900-X.999
INFORMATION AND NETWORK SECURITY	X.1000-X.1099
SECURE APPLICATIONS AND SERVICES (I)	X.1100-X.1199
CYBERSPACE SECURITY	X.1200-X.1299
SECURE APPLICATIONS AND SERVICES (II)	X.1300-X.1499
CYBERSECURITY INFORMATION EXCHANGE	X.1500-X.1599
CLOUD COMPUTING SECURITY	X.1600-X.1699
QUANTUM COMMUNICATION	X.1700-X.1729
Terminologies	X.1700-X.1701
Quantum random number generator	X.1702-X.1704
Quantum Key Distribution Network (QKDN)	**X.1705-X.1749**
DATA SECURITY	X.1750-X.1799
INTERNATIONAL MOBILE TELECOMMUNICATIONS (IMT) SECURITY	X.1800-X.1839
METAVERSE AND DIGITAL TWIN SECURITY	X.2000-X.2199
SOFTWARE SUPPLY CHAIN SECURITY	X.2150-X.2199
ARTIFICIAL INTELLIGENCE (AI) / MACHINE LEARNING (ML) SECURITY	X.2200-X.2249

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

Recommendation ITU-T X.1716

Authentication and authorization in quantum key distribution network

Summary

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

– Identifiers (IDs) and their management in QKDN;

– Public key certification supported by public-key infrastructure (PKI);

– Authentication and authorization in QKDN.

History[*]

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

Keywords

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

[*] To access the Recommendation, type the URL https://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, and information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

		Page
1	Scope	1
2	References	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Recommendation	3
4	Abbreviations and acronyms	3
5	Conventions	3
6	Introduction	3
7	IDs and their management in QKDN	4
	7.1 IDs for QKDN	4
	7.2 IDs for functional elements in QKDN	4
	7.3 IDs for key operations	5
8	Public key certification supported by PKI	5
9	Authentication and authorization in QKDN	5
	9.1 Functional elements and associated reference points in QKDN	5
	9.2 Authentication and authorization of functional elements in QKDN	7
Appendix I – Hierarchical tree of IDs in a QKDN		22
Appendix II – Implicit authentication and authorization scheme		23
Bibliography		24

Recommendation ITU-T X.1716

Authentication and authorization in quantum key distribution network

1 Scope

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

– Identifiers (IDs) and their management in QKDN;

– Public key certification supported by public-key infrastructure (PKI);

– Authentication and authorization in QKDN.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.509] Recommendation ITU-T X.509 (2019), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[ITU-T X.1710] Recommendation ITU-T X.1710 (2020), *Security framework for quantum key distribution networks*.

[ITU-T X.1712] Recommendation ITU-T X.1712 (2021), *Security requirements and measures for quantum key distribution networks – key management*.

[ITU-T X.1717] Recommendation ITU-T X.1717 (2024), *Security requirements and measures for quantum key distribution networks – control and management*.

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

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

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

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

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 access control [b-ITU-T X.800]: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

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

3.1.3 key manager (KM) [ITU-T Y.3800]: A functional module located in a quantum key distribution (QKD) node to perform key management in the key management layer.

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

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

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

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

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

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

3.1.9 key supply agent (KSA) [ITU-T Y.3802]: A functional element to supply keys to a cryptographic application, being located between a key management agent (KMA) and the cryptographic application.

NOTE – Application interfaces for cryptographic applications are installed into the key supply agent (KSA). The KSA synchronizes keys, and verifies their integrity via a KSA link before supplying them to the cryptographic application.

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

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

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

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

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

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

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

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

3.1.16 quantum key distribution network (QKDN) [ITU-T Y.3800]: A network comprised of two or more quantum key distribution (QKD) nodes connected through QKD links.

NOTE – A QKDN allows sharing keys between the QKD nodes by key relay when they are not directly connected by a QKD link.

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

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

3.1.19 quantum key distribution node (QKD node) [ITU-T Y.3800]: A node that contains one or more quantum key distribution (QKD) modules protected against intrusion and attacks by unauthorized parties.

NOTE – A QKD node can contain a key manager (KM).

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

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

5 Conventions

In this Recommendation:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

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

6 Introduction

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

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

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

7 IDs and their management in QKDN

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

7.1 IDs for QKDN

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

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

7.2 IDs for functional elements in QKDN

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

– QKD node ID: ID assigned as a unique ID to identify the QKD node in the QKDN.

– QKDN controller ID: ID assigned as a unique ID to identify the QKDN controller in the QKDN.

– QKDN manager ID: ID assigned as a unique ID to identify the QKDN manager in the QKDN.

– KM ID: ID assigned as a unique ID to identify a key manager (KM) in the QKDN.

– KMA ID: ID assigned as a unique ID to identify a key management agent (KMA) in the QKDN.

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

– KMA link ID: ID assigned as a unique ID to identify a KMA link in the QKDN.

– KSA ID: ID assigned as a unique ID to identify a key supply agent (KSA) in the QKDN.

– KSA link ID: ID assigned as a unique ID to identify a KSA link in the QKDN.

– QKD module ID: ID assigned as a unique ID to identify a QKD module in the QKDN.

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

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

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

7.3 IDs for key operations

The IDs listed below perform key operations such as key generation, key relay and key supply:

– KMA-key ID: ID assigned as a unique ID in the QKDN to identify a KMA-key.

– KSA-key ID: ID assigned as a unique ID in the QKDN to identify a KSA-key.

– QKD-key ID: ID assigned as a unique ID in the QKDN to identify a QKD-key.

8 Public key certification supported by PKI

The public-key infrastructure (PKI) is the infrastructure established to support the issuing, revocation and validation of digital certificates. Details of the PKI are specified in [ITU-T X.509]. In a PKI, the certification authority (CA) is a functional element that issues certificates. CAs form a tree structure to construct trust chains. A CA in the top of the tree is called a root CA and it may be a trust anchor. A QKDN manager receives certificates from the PKI and the QKDN manager can be a root CA in the QKDN. The root CA in the QKDN manager issues certificates for the next Cas, which are located in functional elements in the QKDN such as QKDN controllers, KMs and QKD modules. Functional elements which receive certificates can use them for validation of digital signatures in public-keys. Digital certificates which are provided by CAs can also be used for entity and message authentications in the QKDN.

9 Authentication and authorization in QKDN

9.1 Functional elements and associated reference points in QKDN

Figure 1 illustrates functional elements and associated reference points in a QKDN which are defined in [ITU-T Y.3802] except for the KMi reference point that is introduced in this Recommendation. It is the reference point to the interface connecting KSA and KMA inside the key manager (KM).

– Reference points associated with QKD module: Qdist, Qsync, Qqc.

– Reference points associated with KM: Kx-1, Kx-2, Kq-1, Kq-2, KMi.

– Reference points associated with QKDN controller: Cq, Ck, Cx, Cqrp, Cops.

– Reference points associated with QKDN manager: Mq, Mk, Mc, Mqrp, Mops.

NOTE 1 – QKD links and reference points connecting to them (i.e., Cqrp, Cops, Mqrp, Mops) are not indicated in Figure 1.

NOTE 2 – A Cx reference point connecting two QKDN controllers is not indicated in Figure 1. This reference point is used in a distributed QKDN.

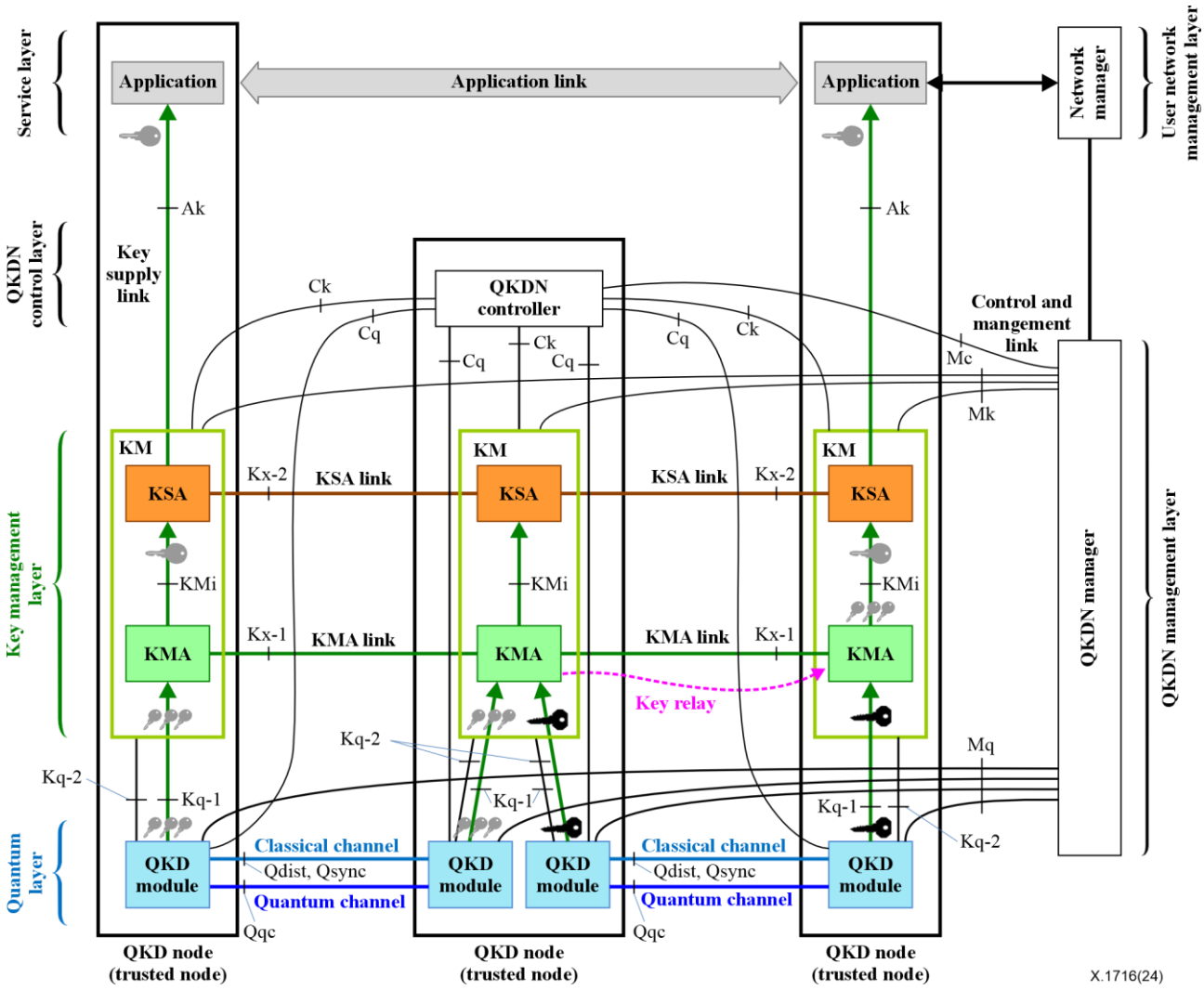

Figure 1 – Functional elements and associated reference points in a QKDN

The functional elements described in Figure 1 communicate information assets in QKDN with another functional element. The information assets of the QKDN include:

- 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.

In the communication between functional elements, there is a need to protect the information assets from being accessed by an unauthorized entity and to ensure that the information assets received by a functional element are coming from the authorized functional element and are unaltered. For this purpose, before starting to communicate the information assets, each functional element verifies the identity of the counterpart (entity authentication), and then confirms that the verified counterpart has a proper access right to the information assets (authorization). During the communication, the functional element also verifies the source and integrity of the received information assets (message authentication).

9.2 Authentication and authorization of functional elements in QKDN

In this clause, the entity authentication, authorization, and message authentication for each pair of functional elements are described.

Table 1 indicates all pairs of two functional elements of QKDN and the reference points of the pairs. The entity authentication, authorization and message authentication for each pair are described in each of the following clauses. Those for the pair of cryptographic applications and the pair of QKD modules are outside the scope of this Recommendation.

Table 1 – Pairs of functional elements of QKDN and reference points in between

	Application	**KSA**	**KMA (KM)**	**QKD module**	**QKDN Controller**	**QKDN Manager**
Application	Ax					
KSA	Ak	Kx-2				
KMA	–	KMi	Kx-1			
QKD module	–	–	Kq-1 (Kq-2)	Qqc,Qsync, Qdist		
QKDN Controller	–	–	(Ck)	Cq	Cx	
QKDN Manager	–	–	(Mk)	Mq	Mc	–

9.2.1 Explicit schemes and implicit schemes for authentication and authorization

The entity authentication, authorization and message authentication among the functional elements can be achieved using cryptographic protocols explicitly (explicit scheme), but this is not the only way. Depending on implementations, the relationship between the functional elements may vary, and in some cases the authentication and/or the authorization can be regarded as done implicitly (implicit scheme).

Some examples of the implicit authentication and authorization schemes are included in Appendix II.

9.2.2 QKD module and matching QKD module

Authentications and authorizations between the QKD module and the matching QKD module are outside the scope of this Recommendation.

9.2.3 KM and QKD module

9.2.3.1 Entity authentication and authorization

The following security requirements for the KMA, KSA and KM are specified in [ITU-T X.1712] for authentication and access control:

Sreq.9 [ITU-T X.1712] 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.20 [ITU-T X.1712] 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.24 [ITU-T X.1712] 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.

As a measure to meet the above requirements, the KM verifies the identity of the QKD module connected via Kq-1 and Kq-2 using a scheme that can be explicit or implicit. Appropriate schemes can be adopted based on the implementation of the QKDN and the QKDN provider's policy, e.g., considering required time scales of authenticity protection, implementation cost, etc.

If an explicit scheme is adopted, the KM and QKD module perform entity authentication using a cryptographic protocol via Kq-1 and Kq-2. Candidates of the protocol include, but are not limited to, transport layer security TLS, secure shell (SSH), etc. Some of such protocols provide options for the algorithm to use, for example, TLS provides options of PKI-based, pre-shared key (PSK)-based and their hybrid algorithms. An appropriate protocol and algorithm can be adopted according to the QKDN provider's policy. On the other hand, they can be also achieved implicitly described in Appendix II.

Once the identity of the QKD module has been verified, the KM then checks whether the identified QKD module has a right to supply key data, metadata and/or control and management information to the KM. If confirmed as having the right, i.e., if the QKD module is authorized, then the KM can trust the key data, metadata and/or control and management information received from the QKD module via Kq-1 and Kq-2.

The check and confirmation of the right described in the previous paragraph can be explicit or implicit and can be adopted based on the QKDN provider's policy. They include but are not limited to the following schemes:

– The access control function in the QKDN controller has a registry of QKD modules with their rights, and the KM inquires the QKDN controller via Ck whether the identified QKD module has an appropriate right.
– The KM control and management function in the KM has a registry of QKD modules and their rights, and the KMA decides according to the registry.
– The KM implicitly authorizes the QKD module if it has been authenticated successfully, without using any explicit registry of QKD modules' rights.

9.2.3.2 Message authentication

The following security requirements for the KMA and KM are specified in [ITU-T X.1712] to ensure the integrity of the key data and metadata:

Sreq.7 [ITU-T X.1712] The KMA is required to ensure the integrity of the key data that it manages.

Sreq.18 [ITU-T X.1712] The KMA is required to ensure the integrity of the metadata that it manages.

Sreq.23 [ITU-T X.1712] The KMs are required to ensure the integrity of the control and management information that they manage.

As a measure to meet the above requirements, KM verifies that the information assets received via Kq-1 and Kq-2 are coming from the authorized QKD module and are unaltered, using a scheme that can be explicit or implicit. In the case that explicit scheme is adopted, it can be achieved by message authentication code (MAC) on the communication over Kq-1 and Kq-2. Candidates of MAC include, but are not limited to, computationally secure schemes such as hash-based MAC and cipher-based MAC provided as a part of the TLS, and IT-secure schemes such as the Wegman-Carter authentication scheme based on a family of universal hash functions. Appropriate schemes may be adopted based on the implementation of the QKDN and the QKDN provider's policy.

9.2.4 KSA and KMA

9.2.4.1 Entity authentication and authorization

The following security requirements for the KMA and KSA are specified in [ITU-T X.1712] for authentication and access control:

Sreq.9 [ITU-T X.1712] 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 [ITU-T X.1712] 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.

Sreq.20 [ITU-T X.1712] 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 [ITU-T X.1712] 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.

As a measure to meet the above requirements, the KMA and the KSA connected via KMi verify the identity of each other using a scheme that can be explicit or implicit. Appropriate schemes can be adopted based on the implementation of the QKDN and the QKDN provider's policy, e.g., considering required time scales of authenticity protection, implementation cost, etc.

If an explicit scheme is adopted, KMA and KSA perform entity authentication using a cryptographic protocol via KMi. Candidates of the protocol include, but are not limited to, TLS, SSH, etc. Some of such protocols provide options for the algorithm to use, for example, TLS provides options of PKI-based, PSK-based and their hybrid algorithms. Appropriate protocols and algorithms can be adopted according to the QKDN provider's policy. On the other hand, they can be also achieved implicitly described in Appendix II.

Once the identities of the KMA and the KSA have been verified by each other, the KMA and the KSA then check:

– Whether the identified counterpart has a right to supply key data and metadata to it. If confirmed to have the right, i.e., if the counterpart is authorized, then the KMA and the KSA can trust the key data and the metadata received via KMi.

– Whether the identified counterpart has a right to access to the unencrypted key data and metadata that it manages. If confirmed to have the right, i.e., if the counterpart is authorized, then the KMA and the KSA can allow the counterpart to access the key data and the metadata that it manages, e.g., the KMA and the KSA can send them to each counterpart via KMi.

The check and confirmation of the right described in the previous paragraph can be explicit or implicit and adopted based on the policy of the QKDN provider. They include but are not limited to:

– The access control function in the QKDN controller has a registry of KMAs and KSAs with their rights, and the KMA and the KSA inquire of the QKDN controller via Ck whether the identified counterpart has an appropriate right.

– The KM control and management function in the KM has a registry of KMAs and KSAs with their rights, and the KMA and KSA decide according to the registry.

– The KMA and KSA implicitly authorize each other if it has been authenticated successfully, without using any explicit registry of KSAs and KMAs with their rights.

– To always regard the authentication and the authorization as successful in the case that the identity of KMA and KSA are indivisible, e.g., KMA and KSA are implemented in a form of single integrated software module.

9.2.4.2 Message authentication

The following security requirements for the KSA are specified in [ITU-T X.1712] to ensure the integrity of the key data and the metadata that it manages:

SReq.8 [ITU-T X.1712] The KSA is required to ensure the integrity of the key data that it manages.

SReq.19 [ITU-T X.1712] The KSA is required to ensure the integrity of the metadata that it manages.

As a measure to meet the above requirements, KSA verifies that the key data and the metadata received via KMi are coming from the authorized KMA and remain unaltered, using a scheme that can be explicit or implicit. If an explicit scheme is adopted, it can be achieved by MAC on the communication over KMi. Candidates of MAC include, but are not limited to, computationally secure schemes such as hash-based MAC and cipher-based MAC provided as a part of the TLS, and IT-secure schemes such as Wegman-Carter authentication scheme based on a family of universal hash functions. Appropriate schemes may be adopted based on the implementation of the QKDN and the QKDN provider's policy.

9.2.5 KSA and cryptographic application

9.2.5.1 Entity authentication and authorization

The following security requirements for the KMA and KSA are specified in [ITU-T X.1712] for authentication and access control:

SReq.10 [ITU-T X.1712] 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.

SReq.21 [ITU-T X.1712] 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.

As a measure to meet the above requirements, the KSA verifies the identity of the cryptographic application connected via Ak using a cryptographic authentication scheme. Candidates for the protocol include, but are not limited to, TLS that is a part of the REST-based key delivery application programming interface (API) described in [b-ETSI GS QKD 014].

NOTE – Authentication of the identity of KSA by the cryptographic application is outside the scope of this Recommendation, while [b-ETSI GS QKD 014] requires the authentication between the secure application entity and the key management entity (corresponding to the cryptographic application and the KSA respectively) to be mutual.

Once the identity of the cryptographic application has been verified, the KSA then checks whether the identified cryptographic application has a right to access to the unencrypted key data and metadata. If confirmed to have the right, i.e., if the cryptographic application is authorized, then the KSA can allow the cryptographic application to access the unencrypted key data and the metadata, e.g., the KSA can send them to the cryptographic application via Ak.

The check and confirmation of the right described in the previous paragraph can be explicit or implicit and adopted based on the QKDN provider's policy. They include but are not limited to:

– The access control function in the QKDN controller has a registry of possible cryptographic applications with their rights, and the KSA inquires of the QKDN controller via Ck whether the identified cryptographic application has an appropriate right.

– The KM control and management function in the KM has a registry of cryptographic applications with their rights, and the KSA decides according to the registry.

– The KSA implicitly authorizes the cryptographic application if it has been authenticated successfully, without using any explicit registry of cryptographic applications with their rights.

9.2.5.2 Message authentication

Requirements for the cryptographic applications are outside the scope of this Recommendation.

NOTE 1 – The cryptographic application verifies that the key data and the metadata received via Ak are coming from the KSA and are unaltered, using a scheme that can be explicit or implicit.

NOTE 2 – [b-ETSI GS QKD 014] requires using TLS1.2 or higher for communication between the secure application entity and the key management entity (corresponding to the cryptographic application and the KSA respectively).

9.2.6 Cryptographic applications

Authentication and authorization between cryptographic applications connected via Ax is outside the scope of this Recommendation.

9.2.7 KMA and matching KMA

9.2.7.1 Entity authentication and authorization

The following security requirements for the KMA and KSA are specified in [ITU-T X.1712] for authentication and access control:

SReq.9 [ITU-T X.1712] 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 [ITU-T X.1712] 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.

SReq.20 [ITU-T X.1712] 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 [ITU-T X.1712] 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.

As a measure to meet the above requirements, a KMA and a matching KMA connected via Kx-1 verify the identity of each other using a cryptographic authentication scheme. Candidates for the protocol include, but are not limited to, TLS, SSH, etc. Some of such protocols provide options for the algorithm to use, for example, TLS provides options of PKI-based, PSK-based and their hybrid algorithms. Appropriate protocols and algorithms can be adopted according to the QKDN provider's policy, however, considering the following requirement in [ITU-T X.1712] for confidentiality of the key data in KMA links, it is also recommended for the verification of the identity of the KMAs to be performed in a highly secure manner, for example, by using a PSK-based algorithm (including a hybrid algorithm) or even IT-secure algorithm.

SReq.2 [ITU-T X.1712] The KMAs are recommended to use IT-secure confidentiality measures for a key relay in KMA links.

Once the identity of the matching KMA has been verified by the KMA, then the KMA checks:

– Whether the identified matching KMA has a right to supply key data and metadata to the KMA. If confirmed to have the right, i.e., if the matching KMA is authorized, then the KSA can trust the key data and the metadata received from the matching KMA via Kx-1.

– Whether the identified matching KMA has a right to access to the unencrypted key data and the metadata that the KMA manages. If confirmed to have the right, i.e., if the matching

KMA is authorized, then the KMA can allow the matching KMA to access the key data and the metadata that the KMA manages, e.g., the KMA can send them to the matching KMA via Kx-1.

The check and confirmation of the right described in the previous paragraph can be explicit or implicit and adopted based on the policy of the QKDN provider. They include but are not limited to:

– The access control function in the QKDN controller has a registry of KMAs with their rights, and the KMA inquires of the QKDN controller via Ck whether the identified matching KMA has an appropriate right.
– The KM control and management function in the KM has a registry of matching KMAs with their rights, and the KMA decides according to the registry.
– The KMA implicitly authorizes the matching KMA if it has been authenticated successfully, without using any explicit registry of KMAs with their rights.

9.2.7.2 Message authentication

The following security requirements for the KMA are specified in [ITU-T X.1712] to ensure the integrity of the key data and metadata that they manage:

– SReq.7 [ITU-T X.1712] The KMA is required to ensure the integrity of the key data that it manages.
– SReq.18 [ITU-T X.1712] The KMA is required to ensure the integrity of the metadata that it manages.

As a measure to meet the above requirements, the KMA verifies that the key data and the metadata received via Kx-1 are coming from the authorized matching KMA and are unaltered. This can be achieved by MAC on the communication over Kx-1. Candidates of MAC include, but are not limited to, computationally secure schemes such as hash-based MAC and cipher-based MAC provided as a part of TLS, and IT-secure schemes such as the Wegman-Carter authentication scheme based on a family of universal hash functions. Appropriate protocols may be adopted based on the implementation of the QKDN and the QKDN provider's policy.

9.2.8 KSA and matching KSA

9.2.8.1 Entity authentication and authorization

The following security requirements for the KMA and KSA are specified in [ITU-T X.1712] for authentication and access control:

SReq.20 [ITU-T X.1712] 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 [ITU-T X.1712] 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.

As a measure to meet the above requirements, a KSA and a matching KSA connected via Kx-2 verify the identity of each other using a cryptographic authentication scheme. Candidates for the protocol include, but are not limited to, TLS, SSH, etc. Some of such protocols provide options for the algorithm to use, for example, TLS provides options of PKI-based, PSK-based and their hybrid algorithms. Appropriate protocols and algorithms can be adopted according to the QKDN provider's policy.

Once the identity of the matching KSA has been verified by the KSA, then the KSA checks:

– Whether the identified matching KSA has a right to supply metadata to the KSA. If confirmed to have the right, i.e., if the matching KSA is authorized, then the KSA can trust the metadata received from the matching KSA via Kx-2.

– Whether the identified matching KSA has a right to access to the unencrypted metadata that the KSA manages. If confirmed to have the right, i.e., if the matching KSA is authorized, then the KSA can allow the matching KSA to access the metadata that the KSA manages, e.g., the KSA can send them to the matching KSA via Kx-2.

The check and confirmation of the right described in the previous paragraph can be explicit or implicit and adopted based on the policy of the QKDN provider. They include but are not limited to:

– The access control function in the QKDN controller has a registry of KSAs with their rights, and the KSA inquires of the QKDN controller via Ck whether the identified matching KSA has an appropriate right.
– The KM control and management function in the KM has a registry of matching KSAs with their rights, and the KSA decides according to the registry.
– The KSA implicitly authorizes the matching KSA if it has been authenticated successfully, without using any explicit registry of KSAs with their rights.

9.2.8.2 Message authentication

The following security requirements for the KSA are specified in [ITU-T X.1712] to ensure the integrity of the key data and the metadata that it manages:

SReq.8 [ITU-T X.1712] The KSA is required to ensure the integrity of the key data that it manages.

SReq.19 [ITU-T X.1712] The KSA is required to ensure the integrity of the metadata that it manages.

As a measure to meet the above requirements, KSA verifies that the metadata received via Kx-2 are coming from the authorized matching KSA and unaltered. It can be achieved by MAC on the communication over Kx-2. Candidates of MAC include, but are not limited to, computationally secure schemes such as hash-based MAC and cipher-based MAC provided as a part of TLS. Appropriate protocols may be adopted based on the implementation of the QKDN and the QKDN provider's policy.

9.2.9 QKDN controller and KM

9.2.9.1 Entity authentication and authorization

For the KM, the following security requirements are specified in [ITU-T X.1712] for authentication and access control.

SReq.24 [ITU-T X.1712] 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 [ITU-T X.1712] 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.

For the QKDN controller, the following security requirement is specified in [ITU-T X.1717] for authentication and access control.

SReq.7 [ITU-T X.1717] The QKDN controller is required to ensure that the control and management information received from other entities is not trusted unless the identity of the sending entity has been authenticated and the sending entity is authorized to supply the control and management information.

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

SReq.8 [ITU-T X.1717] The QKDN controller is required to ensure that they do not allow another entity access to the unencrypted control and management information without ensuring that the entity is authorized to receive it.

As a measure to meet the above requirements, the KM and the QKDN controller connected via Ck verify the identity of each other using a scheme that can be explicit or implicit. Appropriate schemes may be adopted based on the implementation of the QKDN and the QKDN provider's policy, e.g., considering required time scales of authenticity protection, implementation cost, etc.

If an explicit authentication is adopted, the KM and QKDN controller perform entity authentication using a cryptographic protocol via Ck. Candidates of the protocol include, but are not limited to, TLS, SSH, etc. Some of such protocols provide options for the algorithm to use, for example, TLS provides options of PKI-based, PSK-based and their hybrid algorithms. Appropriate protocols and algorithms can be adopted according to the QKDN provider's policy.

Once the identities of the KM and the QKDN controller have been verified by each other, the KM and the QKDN controller then check:

– Whether each one's identified counterpart has a right to supply control information to it. If confirmed to have the right, i.e., if the counterpart is authorized, then the KM and the QKDN controller can trust the control information received via Ck.

– Whether the identified counterpart has a right to access to the unencrypted control information that it manages. If confirmed to have the right, i.e., if the counterpart is authorized, then the KM and the QKDN controller can allow the counterpart to access the unencrypted control information that they manage, e.g., the KM and the QKDN controller can send it to each counterpart via Ck.

The check and confirmation of the right described in the previous paragraph can be explicit or implicit and adopted based on the policy of the QKDN provider. They include but are not limited to:

– The KM control and management function in the KM has a registry of QKDN controllers with their rights, and the KM decides according to the registry.

– The QKDN controller and KM implicitly authorize each other if it has been authenticated successfully, without using any explicit registry of QKDN controllers and KMs with their rights.

9.2.9.2 Message authentication

For the KM, the following security requirement is specified in [ITU-T X.1712] to ensure the integrity of control information that it manages.

SReq.23 [ITU-T X.1712] The KMs are required to ensure the integrity of the control and management information that they manage.

For the QKDN controller, the following security requirement is specified in [ITU-T X.1717] to ensure the integrity of the control information.

SReq.6 [ITU-T X.1717] The QKDN controller is required to ensure the integrity of the control and management information that it manages.

As a measure to meet the above requirements, KM and QKDN controller verify that the control information received via Ck is coming from the authorized counterpart and is unaltered, using a scheme that can be explicit or implicit. If an explicit scheme is adopted, this can be achieved by MAC on the communication over Ck. Candidates of MAC include, but are not limited to, hash-based MAC and cipher-based MAC provided as a part of the TLS, and IT-secure schemes such as Wegman-Carter authentication scheme based on a family of universal hash functions. Appropriate schemes may be adopted based on the implementation of the QKDN and the QKDN provider's policy.

9.2.10 QKDN manager and KM

9.2.10.1 Entity authentication and authorization

For the KM, the following security requirements are specified in [ITU-T X.1712] for authentication and access control.

SReq.24 [ITU-T X.1712] 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 [ITU-T X.1712] 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.

For the QKDN manager, the following security requirement is specified in [ITU-T X.1717] for authentication and access control.

SReq.19 [ITU-T X.1717] The QKDN manager is required to ensure that the control and management information received from other entities is not trusted unless the identity of the sending entity has been authenticated and the sending entity is authorized to supply the control and management information.

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

SReq.20 [ITU-T X.1717] The QKDN manager is required to ensure that they do not allow another entity access to the unencrypted management information without ensuring that the entity is authorized to receive it.

As a measure to meet the above requirements, the KM and the QKDN manager connected via Mk verify the identity of each other using a scheme that can be explicit or implicit. Appropriate schemes can be adopted based on the implementation of the QKDN and the QKDN provider's policy, e.g., considering required time scales of authenticity protection, implementation cost, etc.

If an explicit authentication is adopted, KM and QKDN manager perform entity authentication using a cryptographic protocol via Mk. Candidates for the protocol include, but are not limited to, TLS, SSH, etc. Some of such protocols provide options for the algorithm to use, for example, TLS provides options of PKI-based, PSK-based and their hybrid algorithms. Appropriate protocols and algorithms can be adopted according to the QKDN provider's policy. On the other hand, they can be also achieved implicitly described in Appendix II.

Once the identities of the KM and the QKDN manager have been verified by each other, then the KM and the QKDN manager check:

– Whether the identified counterpart has a right to supply management information to it. If confirmed to have the right, i.e., if the counterpart is authorized, then the KM and the QKDN controller can trust the management information received via Mk.

– Whether the identified counterpart has a right to access to the unencrypted management information that it manages. If confirmed to have the right, i.e., if the counterpart is authorized, then the KM and the QKDN manager can allow the counterpart to access the unencrypted management information that it manages, e.g., the KM and the QKDN manager can send it to each counterpart via Mk.

The check and confirmation of the right described in the previous paragraph can be explicit or implicit and adopted based on the policy of the QKDN provider. They include but are not limited to:

– The access control function in the QKDN controller has a registry of QKDN managers and KMs with their rights, and the QKDN manager and the KM inquires of the QKDN controller via Mc and Ck, respectively, whether the identified counterpart has an appropriate right.

– The KM control and management function in the KM has a registry of QKDN managers with their rights, and the KM decides according to the registry.
– The QKDN manager and KM implicitly authorize each other if it has been authenticated successfully, without using any explicit registry of QKDN managers and KMs with their rights.

9.2.10.2 Message authentication

For the KM, the following security requirement is specified in [ITU-T X.1712] to ensure the integrity of management information that it manages.

SReq.23 [ITU-T X.1712] The KMs are required to ensure the integrity of the control and management information that they manage.

For the QKDN manager, the following security requirement is specified in [ITU-T X.1717] to ensure the integrity of the management information.

SReq.18 [ITU-T X.1717] The QKDN manager is required to ensure the integrity of the management information that it manages.

As a measure to meet the above requirements, KM and QKDN manager verify that the management information received via Mk is coming from the authorized counterpart and is unaltered, using a scheme that can be explicit or implicit. If an explicit scheme is adopted, it can be achieved by MAC on the communication over Mk. Candidates of MAC include, but are not limited to, computationally secure schemes such as hash-based MAC and cipher-based MAC provided as a part of the TLS, and IT-secure schemes such as Wegman-Carter authentication scheme based on a family of universal hash functions. Appropriate schemes may be adopted based on the implementation of the QKDN and the QKDN provider's policy.

9.2.11 QKDN controller and QKD module

9.2.11.1 Entity authentication and authorization

The following security requirement for the QKDN controller is specified in [ITU-T X.1717] for authentication and access control:

SReq.7 [ITU-T X.1717] The QKDN controller is required to ensure that the control and management information received from other entities is not trusted unless the identity of the sending entity has been authenticated and the sending entity is authorized to supply the control and management information.

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

SReq.8 [ITU-T X.1717] The QKDN controller is required to ensure that they do not allow another entity access to the unencrypted control and management information without ensuring that the entity is authorized to receive it.

As a measure to meet the above requirements, QKDN controller verifies the identity of the QKD module connected via Cq using a scheme that can be explicit or implicit. Appropriate schemes may be adopted based on the implementation of the QKDN and the QKDN provider's policy, e.g., considering required time scales of authenticity protection, implementation cost, etc.

If an explicit scheme is adopted, the QKDN controller and QKD module perform entity authentication using a cryptographic protocol via Cq. Candidates of the protocol include, but are not limited to, TLS, SSH, etc. Some of such protocols provide options for the algorithm to use, for example, TLS provides options of PKI-based, PSK-based and their hybrid algorithms. Appropriate protocols and algorithms can be adopted according to the QKDN provider's policy. On the other hand, they can be also achieved implicitly described in Appendix II.

Once the identity of the QKD module has been verified, then the QKDN controller checks whether the identified QKD module has a right to supply control information to the QKDN controller. If confirmed to have the right, i.e., if the QKD module is authorized, then the QKDN controller can trust the control information received from the QKD module via Cq.

The check and confirmation of the right described in the previous paragraph can be explicit or implicit and adopted based on the QKDN provider's policy. They include but are not limited to:

– The access control function in the QKDN controller has a registry of QKD modules with their rights, and the QKDN controller decides according to the registry.
– The QKDN controller implicitly authorizes the QKD module if it has been authenticated successfully, without using any explicit registry of QKD modules' rights.

9.2.11.2 Message authentication

The following security requirement for the QKDN controller is specified in [ITU-T X.1717] to ensure the integrity of the control information.

> SReq.6 [ITU-T X.1717] The QKDN controller is required to ensure the integrity of the control and management information that it manages.

As a measure to meet the above requirements, the QKDN controller verifies that the control information received via Cq is coming from the authorized QKD module and is unaltered, using a scheme that can be explicit or implicit. If an explicit scheme is adopted, this can be achieved by MAC on the communication over Cq. Candidates of MAC include, but are not limited to, computationally secure schemes such as hash-based MAC and cipher-based MAC provided as a part of the TLS, and IT-secure schemes such as the Wegman-Carter authentication scheme based on a family of universal hash functions. Appropriate schemes may be adopted based on the implementation of the QKDN and the QKDN provider's policy.

9.2.12 QKDN manager and QKD module

9.2.12.1 Entity authentication and authorization

The following security requirement for the QKDN manager is specified in [ITU-T X.1717] for authentication and access control:

> SReq.19 [ITU-T X.1717] The QKDN manager is required to ensure that the control and management information received from other entities is not trusted unless the identity of the sending entity has been authenticated and the sending entity is authorized to supply the control and management information.

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

> SReq.20 [ITU-T X.1717] The QKDN manager is required to ensure that they do not allow another entity access to the unencrypted management information without ensuring that the entity is authorized to receive it.

As a measure to meet the above requirements, the QKDN manager verifies the identity of the QKD module connected via Mq using a scheme that can be explicit or implicit. Appropriate schemes can be adopted based on the implementation of the QKDN and the QKDN provider's policy, e.g., considering required time scales of authenticity protection, implementation cost, etc.

If an explicit scheme is adopted, the QKDN manager and QKD module perform entity authentication using a cryptographic protocol via Mq. Candidates of the protocol include, but are not limited to, TLS, SSH, etc. Some of such protocols provide options for the algorithm to use, for example, TLS provides options of PKI-based, PSK-based and their hybrid algorithms. Appropriate protocols and algorithms can be adopted according to the QKDN provider's policy. On the other hand, they can be also achieved implicitly described in Appendix II.

Once the identity of the QKD module has been verified, then the QKDN manager checks whether the identified QKD module has a right to supply management information to the QKDN manager. If confirmed to have the right, i.e., if the QKD module is authorized, then the QKDN manager can trust the management information received from the QKD module via Mq.

The check and confirmation of the right described in the previous paragraph can be explicit or implicit and adopted based on the QKDN provider's policy. They include but are not limited to:

– The access control function in the QKDN controller has a registry of QKD modules with their rights, and the QKDN manager inquires of the QKDN controller via Mc whether the identified QKD module has an appropriate right to supply management information to the QKDN manager.
– The QKDN manager has a registry of QKD modules with their rights, and the QKDN manager decides according to the registry.
– The QKDN manager implicitly authorizes the QKD module if it has been authenticated successfully, without using any explicit registry of QKD modules' rights.

9.2.12.2 Message authentication

The following security requirement for the QKDN manager is specified in [ITU-T X.1717] to ensure the integrity of the management information:

SReq.18 [ITU-T X.1717] The QKDN manager is required to ensure the integrity of the management information that it manages.

As a measure to meet the above requirements, QKDN manager verifies that the management information received via Mq is coming from the authorized QKD module and is unaltered, using a scheme that can be explicit or implicit. In the case that an explicit scheme is adopted, this can be achieved by MAC on the communication over Mq. Candidates of MAC include, but are not limited to, computationally secure schemes such as hash-based MAC and cipher-based MAC provided as a part of the TLS, and IT-secure schemes such as the Wegman-Carter authentication scheme based on a family of universal hash functions. Appropriate schemes may be adopted based on the implementation of the QKDN and the QKDN provider's policy.

9.2.13 QKDN manager and QKDN controller

9.2.13.1 Entity authentication and authorization

The following security requirements for the QKDN controller and the QKDN manager are specified in [ITU-T X.1717] for authentication and access control:

SReq.7 [ITU-T X.1717] The QKDN controller is required to ensure that the control and management information received from other entities is not trusted unless the identity of the sending entity has been authenticated and the sending entity is authorized to supply the control and management information.

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

SReq.8 [ITU-T X.1717] The QKDN controller is required to ensure that they do not allow another entity access to the unencrypted control and management information without ensuring that the entity is authorized to receive it.

SReq.19 [ITU-T X.1717] The QKDN manager is required to ensure that the control and management information received from other entities is not trusted unless the identity of the sending entity has been authenticated and the sending entity is authorized to supply the control and management information.

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

SReq.20 [ITU-T X.1717] The QKDN manager is required to ensure that they do not allow another entity access to the unencrypted management information without ensuring that the entity is authorized to receive it.

As a measure to meet the above requirements, the QKDN manager and the QKDN controller connected via Mc verify the identity of each other using a scheme that can be explicit or implicit. Appropriate schemes can be adopted based on the implementation of the QKDN and the QKDN provider's policy, e.g., considering required time scales of authenticity protection, implementation cost, etc.

If an explicit authentication is adopted, the QKDN manager and QKDN controller perform entity authentication using a cryptographic protocol via Mc. Candidates for the protocol include, but are not limited to, TLS, SSH, etc. Some of such protocols provide options for the algorithm to use, for example, TLS provides options of PKI-based, PSK-based and their hybrid algorithms. Appropriate protocols and algorithms can be adopted according to the QKDN provider's policy. On the other hand, they can be also achieved implicitly described in Appendix II.

Once the identities of the QKDN manager and the QKDN controller have been verified by each other, then the QKDN manager and the QKDN controller check:

– Whether the identified counterpart has a right to supply management information to it. If confirmed to have the right, i.e., if the counterpart is authorized, then the QKDN manager and the QKDN controller can trust the management information received via Mc.

– Whether the identified counterpart has a right to access to the unencrypted management information that it manages. If confirmed to have the right, i.e., if the counterpart is authorized, then the QKDN manager and the QKDN controller can allow the counterpart to access the unencrypted management information that it manages, e.g., the QKDN manager and the QKDN controller can send it to each counterpart via Mc.

The check and confirmation of the right described in the previous paragraph can be explicit or implicit and adopted based on the policy of the QKDN provider. They include but are not limited to:

– The access control function in the QKDN controller has a registry of QKDN managers with their rights, and the QKDN controller decides according to the registry.

– The QKDN manager has a registry of QKDN controllers with their rights, and the QKDN manager decides according to the registry.

– The QKDN manager and the QKDN controller implicitly authorizes the counterpart if it has been authenticated successfully, without using any explicit registry of QKDN controllers and QKDN managers with their rights.

9.2.13.2 Message authentication

The following security requirements for the QKDN controller and the QKDN manager are specified in [ITU-T X.1717] to ensure the integrity of the control and management information:

SReq.6 [ITU-T X.1717] The QKDN controller is required to ensure the integrity of the control and management information that it manages.

SReq.18 [ITU-T X.1717] The QKDN manager is required to ensure the integrity of the management information that it manages.

As a measure to meet the above requirements, QKDN manager and QKDN controller verify that the management information received via Mc is coming from the authorized counterpart and is unaltered, using a scheme that can be explicit or implicit. If an explicit scheme is adopted, it can be achieved by MAC on the communication over Mc. Candidates of MAC include, but are not limited to, computationally secure schemes such as hash-based MAC and cipher-based MAC provided as a part of the TLS, and IT-secure schemes such as Wegman-Carter authentication scheme based on a family

of universal hash functions. Appropriate schemes may be adopted based on the implementation of the QKDN and the QKDN provider's policy.

9.2.14 QKDN controller and matching QKDN controller

9.2.14.1 Entity authentication and authorization

The following security requirement for the QKDN controller is specified in [ITU-T X.1717] for authentication and access control:

> SReq.7 [ITU-T X.1717] The QKDN controller is required to ensure that the control and management information received from other entities is not trusted unless the identity of the sending entity has been authenticated and the sending entity is authorized to supply the control and management information.
>
> SReq.8 [ITU-T X.1717] The QKDN controller is required to ensure that they do not allow another entity access to the unencrypted control and management information without ensuring that the entity is authorized to receive it.

As a measure to meet the above requirements, a QKDN controller and its matching QKDN controller connected via Cx verify the identity of each other using a cryptographic authentication scheme. Candidates for the protocol include, but are not limited to, TLS, SSH, etc. Some of such protocols provide options for the algorithm to use, for example, TLS provides options of PKI-based, PSK-based and their hybrid algorithms. Appropriate protocols and algorithms can be adopted according to the QKDN provider's policy.

Once the identity of the matching QKDN controller has been verified by the QKDN controller, then the QKDN controller checks:

– Whether the identified matching QKDN controller has a right to supply control information to the QKDN controller. If confirmed to have the right, i.e., if the matching QKDN controller is authorized, then the QKDN controller can trust the control information received from the matching KSA via Cx.

– Whether the identified matching QKDN controller has a right to access to the unencrypted control information that the QKDN controller manages. If confirmed to have the right, i.e., if the matching QKDN controller is authorized, then the QKDN controller can allow the matching QKDN controller to access the control information that the QKDN controller managers, e.g., the QKDN controller can send it to the matching QKDN controller via Cx.

The check and confirmation of the right described in the previous paragraph can be explicit or implicit and adopted based on the policy of the QKDN provider. They include but are not limited to:

– The access control function in the QKDN controller has a registry of matching QKDN controllers and their rights, and the QKDN controller decides according to the registry.

– The QKDN controller implicitly authorizes a matching QKDN controller if it has been authenticated successfully, without using any explicit registry of matching QKDN controllers with their rights.

9.2.14.2 Message authentication

The following security requirement for the QKDN controller is specified in [ITU-T X.1717] to ensure the integrity of the control and management information:

> SReq.6 [ITU-T X.1717] The QKDN controller is required to ensure the integrity of the control and management information that it manages.

As a measure to meet the above requirements, QKDN controller verifies that the control information received via Cx is coming from the authorized matching QKDN controller and unaltered. It can be achieved by MAC on the communication over Cx. Candidates of MAC include, but are not limited to, computationally secure schemes such as hash-based MAC and cipher-based MAC provided as a

part of TLS, and IT-secure schemes such as Wegman-Carter authentication scheme based on a family of universal hash functions. Appropriate protocols may be adopted based on the implementation of the QKDN and the QKDN provider's policy.

Appendix I

Hierarchical tree of IDs in a QKDN

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

The hierarchical tree of IDs in Figure I.1 shows an example of the relationships between the IDs in a QKDN.

– Root ID of the hierarchical tree is the QKDN ID.

– 2-level IDs of the hierarchical tree include the QKD node ID, QKDN manager ID, QKDN controller ID and application ID. According to the network topology and the different architectural configurations in the real implementation of the QKDN, the 2-level IDs may have different hierarchical sub-trees.

– Hierarchical sub-tree in a QKD node: in the subtree, QKD node ID is the root ID; KM ID and QKD module ID are the 2-level ID; a KM ID has its down-level KMA ID and KSA ID; a QKD module ID has its down-level QKD-key ID; a KMA ID has its down-level KMA-link ID and KMA-key ID; a KSA ID has its down-level KSA link ID.

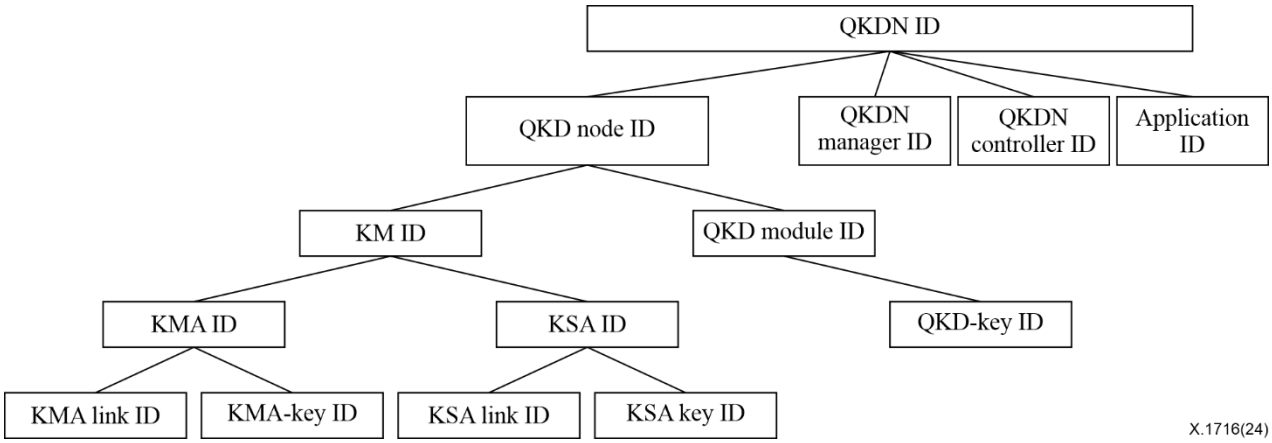

Figure I.1 – Hierarchical tree of IDs in a QKDN

Appendix II

Implicit authentication and authorization scheme

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

This appendix includes some examples of implicit authentication and authorization schemes as follows:

– Two or more functional elements can be implemented within a single physical entity, avoiding physical interfaces among them. In such cases, each functional element within the single physical entity can regard the other functional elements authenticated and authorized without performing any cryptographic authentication and authorization protocol or message authentication code. An example of such cases is KMA and KSA implemented as a single software module.

– Similar to the cases above, implicit authentication and authorization can be applicable to cases where a pair of functional elements is located within a same QKD node (trusted node), provided the functional elements are installed and operated properly according to QKDN provider's policy. In other words, ensuring the validity of installation and operation of the functional elements in a QKD node can be a measure for authentication and authorization. An example of such cases is a pair of QKD module and KM in a QKD node.

– Entity authentication and authorization can be covered by another entity authentication and authorization done by another functional element implemented within the same single physical entity. For example, if KSA and KMA are implemented as a single software module and their identities are indivisible, the entity authentication between the KSA and its matching KSA can be regarded as covered by the entity authentication between the KMA and its matching KMA.

Note that an explicit scheme can still be adopted, or both the implicit and explicit schemes can be used in combination even if an implementation falls under the above examples, based on the QKDN provider's policy.

Bibliography

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

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

[b-ETSI GS QKD 008] ETSI GS QKD 008 (2010), *Quantum Key Distribution (QKD); QKD Module Security Specification*.

[b-ETSI GS QKD 014] ETSI GS QKD 014 (2019), *Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Published in Switzerland
Geneva, 2025