ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T Y.3818 (09/2023)

SERIES Y: Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities

Quantum key distribution networks

Quantum key distribution network interworking – Architecture

ITU-T Y-SERIES RECOMMENDATIONS

Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities

GLOBAL INFORMATION INFRASTRUCTURE	Y.100-Y.999
General	Y.100-Y.199
Services, applications and middleware	Y.200-Y.299
Network aspects	Y.300-Y.399
Interfaces and protocols	Y.400-Y.499
Numbering, addressing and naming	Y.500-Y.599
Operation, administration and maintenance	Y.600-Y.699
Security	Y.700-Y.799
Performances	Y.800-Y.899
INTERNET PROTOCOL ASPECTS	Y.1000-Y.1999
General	Y.1000-Y.1099
Services and applications	Y.1100-Y.1199
Architecture, access, network capabilities and resource management	Y.1200-Y.1299
Transport	Y.1300-Y.1399
Interworking	Y.1400-Y.1499
Quality of service and network performance	Y.1500-Y.1599
Signalling	Y.1600-Y.1699
Operation, administration and maintenance	Y.1700-Y.1799
Charging	Y.1800-Y.1899
IPTV over NGN	Y.1900-Y.1999
NEXT GENERATION NETWORKS	Y.2000-Y.2999
Frameworks and functional architecture models	Y.2000-Y.2099
Quality of Service and performance	Y.2100-Y.2199
Service aspects: Service capabilities and service architecture	Y.2200-Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250-Y.2299
Enhancements to NGN	Y.2300-Y.2399
Network management	Y.2400-Y.2499
Computing power networks	Y.2500-Y.2599
Packet-based Networks	Y.2600-Y.2699
Security	Y.2700-Y.2799
Generalized mobility	Y.2800-Y.2899
Carrier grade open environment	Y.2900-Y.2999
FUTURE NETWORKS	Y.3000-Y.3499
CLOUD COMPUTING	Y.3500-Y.3599
BIG DATA	Y.3600-Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	**Y.3800-Y.3999**
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	Y.4000-Y.4999
General	Y.4000-Y.4049
Definitions and terminologies	Y.4050-Y.4099
Requirements and use cases	Y.4100-Y.4249
Infrastructure, connectivity and networks	Y.4250-Y.4399
Frameworks, architectures and protocols	Y.4400-Y.4549
Services, applications, computation and data processing	Y.4550-Y.4699
Management, control and performance	Y.4700-Y.4799
Identification and security	Y.4800-Y.4899
Evaluation and assessment	Y.4900-Y.4999

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

Recommendation ITU-T Y.3818

Quantum key distribution network interworking – Architecture

Summary

Recommendation ITU-T Y.3818 specifies functional architecture models for quantum key distribution network interworking (QKDNi), i.e., functional architectures with gateway and interworking nodes. In order to realize these two models, Recommendation ITU-T Y.3818 specifies detailed functional elements, basic operational procedures and architectural configurations for QKDNi.

History*

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T Y.3818	2023-09-29	13	11.1002/1000/15646

Keywords

Interworking, QKD, QKDN (QKD network).

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

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

Table of Contents

		Page
1	Scope	1
2	References	1
3	Definitions	1
3.1	Terms defined elsewhere	1
3.2	Terms defined in this Recommendation	2
4	Abbreviations and acronyms	2
5	Conventions	3
6	Functional architecture for QKDNi	3
6.1	Functional architecture for QKDNi with GWNs	3
6.2	Functional architecture for QKDNi with IWN	4
7	Functional elements for QKDNi	6
7.1	Functional elements in GWNs	6
7.2	Functional elements in IWN	7
8	Interworking architectural configurations	7
8.1	Configurations of QKDNi with GWNs	7
8.2	Configurations of QKDNi with IWN	9
9	Basic operational procedures for QKDNi	12
9.1	Operational procedures for QKDNi with GWNs	12
9.2	Operational procedures for QKDNi with IWN	15
10	Security considerations	17
Bibliography		18

Recommendation ITU-T Y.3818

Quantum key distribution network interworking – Architecture

1 Scope

This Recommendation specifies functional architectures for quantum key distribution network interworking (QKDNi). In particular, this Recommendation includes the following:

– a functional architecture model for QKDNi;

– functional elements for QKDNi;

– interworking architectural configurations;

– basic operational procedures for QKDNi.

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

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

[ITU-T Y.3810] Recommendation ITU-T Y.3810 (2022), *Quantum key distribution network interworking – Framework*.

[ITU-T Y.3813] Recommendation ITU-T Y.3813 (2022), *Quantum key distribution network interworking – Requirements*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

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

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

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

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

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

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

3.1.5 quantum key distribution network (QKDN) [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.

3.1.6 quantum key distribution network 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.

3.1.7 quantum key distribution network 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.

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

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

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

FCAPS	Fault, Configuration, Accounting, Performance and Security
GWN	Gateway Node
IWF	Interworking Function
IWN	Interworking Node
KM	Key Manager
KMA	Key Management Agent
KML	Key Management Layer
KMLM	Key Manager Layer Management
KSA	Key Supply Agent
QCLM	QKDN Control Layer Management
QKD	Quantum Key Distribution
QKDN	Quantum Key Distribution Network
QKDNi	Quantum Key Distribution Network Interworking
QL	Quantum Layer
QoS	Quality of Service
XLMO	cross-Layer Management Orchestration

5 Conventions

None.

6 Functional architecture for QKDNi

A QKDN is a cryptographic infrastructure to provide secure symmetric keys to cryptographic applications in user networks. A large-scale QKDN that covers a wide area may consist of multiple QKDNs, which interwork.

An overview of QKDNi including interworking QKDNs, reference models, and functional models of gateway functions and interworking functions (IWFs) for QKDNi is given in [ITU-T Y.3810]. Moreover, QKDNi functional requirements are identified in [ITU-T Y.3813].

Based on the conceptual models of QKDNi illustrated in [ITU-T Y.3810] and the QKDNi functional requirements identified in [ITU-T Y.3813], two functional architectures for QKDNi with gateway nodes (GWNs) and interworking node (IWN) are shown in Figures 1 and 2, respectively.

6.1 Functional architecture for QKDNi with GWNs

The functional model for QKDNi with GWNs is specified in [ITU-T Y.3810], and the layer structure for QKDN in [ITU-T Y.3800]. Detailed descriptions of the layers in the structure for QKDNi follow.

– Quantum layer (QL): The functional elements include the QKD link and the QKD module.

– Key management layer (KML): The functional elements include the key management agent (KMA) and key supply agent (KSA). Keys can be relayed between GWNs through KML, and KM can also exchange control and management messages with the key relay between QKDNs.

– QKDN control layer: The functional element is the QKDN controller, which supports interworking of key relay routing and rerouting between GWNs. Key relay routing is performed independently in the QKDN according to the policies of the service provider.

– QKDN management layer: The functional element is the QKDN manager, which manages and supports fault, configuration, accounting, performance and security (FCAPS) functions between GWNs, and support user network management.

Most of the reference points in Figure 1 are specified in [ITU-T Y.3802]; this Recommendation specifies new reference points between QKDNs.

The newly added reference points are as follows.

– **Cxi**: A reference point connecting the control and management functions of two QKDN controllers between the QKDNs. Cxi enables the two QKDN controllers to communicate interworking control information to each other.

– **Kxi-1**: A reference point connecting two KMAs between the QKDNs via an interworking KMA link. Kxi-1 enables the exchange of information and operations required for key relay, key synchronization and authentication between QKDNs.

– **Kxi-2**: A reference point connecting two KSAs between the QKDNs via an interworking KSA link. Kxi-2 enables the exchange of information and operations required for synchronization and authentication of the keys shared between QKDNs.

– **Mxi**: A reference point connecting two QKDN managers between the QKDNs. Mxi enables the two QKDN managers to share QKDN management information with each other.

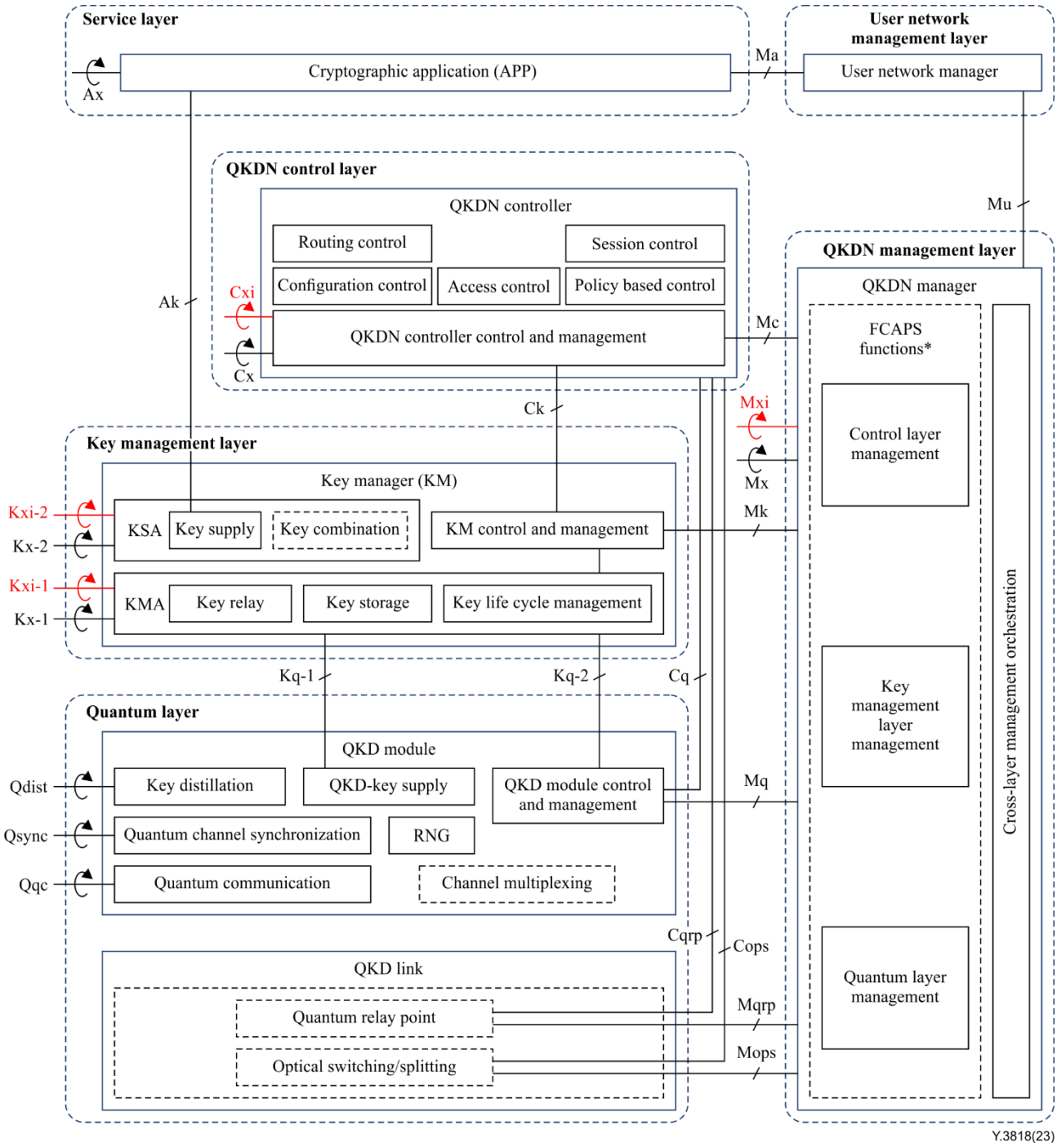

Figure 1 – A functional architecture for QKDNi with GWNs

6.2 Functional architecture for QKDNi with IWN

The functional model for QKDNi with IWN is specified in [ITU-T Y.3810] and the layer structure for QKDN in [ITU-T Y.3800]. Detailed descriptions of the layers in the structure for QKDNi follow.

– QL: The functional elements include the QKD link and the QKD module.

NOTE – In the IWN, there is no Qx between two QKD modules.

– KML: The functional elements include the KMA and KSA. Keys can be transferred in the IWN through the KML, and KMs can also exchange control and management messages with the key transfer between QKDNs.

– QKDN control layer: The functional element is the QKDN controller, which supports the interworking of key transfer in the IWN. Key transfer is performed independently in the QKDN according to the policies of the service provider.

– QKDN management layer: The functional element is the QKDN manager, which manages and supports FCAPS functions in the IWN, and supports user network management.

Most of the reference points in Figure 2 are specified in [ITU-T Y.3802]; this Recommendation specifies new reference points in the IWN.

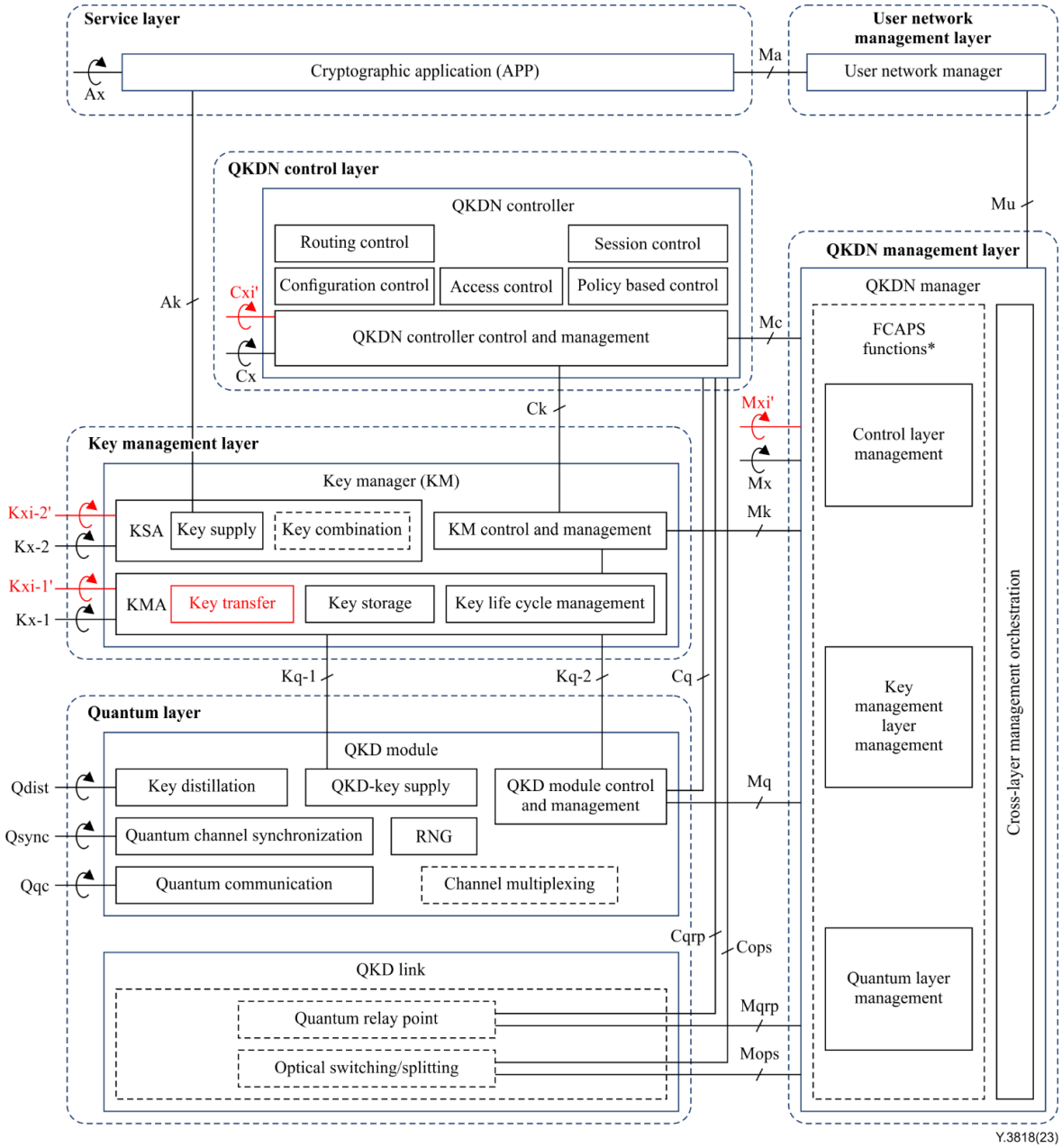

Figure 2 – A functional architecture for QKDNi with IWN

The newly added reference points are as follows.

– **Cxi'**: A reference point connecting the control and management functions of two QKDN controllers in the IWN. Cxi' enables the two QKDN controllers to communicate interworking control information to each other. It exists in the IWN when OKDN controllers of both OKDNs are accommodated in the IWN. Otherwise, Cxi (see clause 6.1) can be used.

– **Kxi-1'**: A reference point connecting two KMAs in the IWN via an interworking KMA link. Kxi-1' enables the exchange of information and operations required for key transfer, key synchronization and authentication between QKDNs.

– **Kxi-2'**: A reference point connecting two KSAs in the IWN via an interworking KSA link. Kxi-2' enables the exchange of information and operations required for synchronization and authentication of the keys shared between QKDNs.

– **Mxi'**: A reference point connecting two QKDN managers in the IWN. Mxi' enables the two QKDN managers to share QKDNi management information with each other. It exists for the two OkDN managers to share in the IWN when they are both accommodated within it. Otherwise, Mxi (see clause 6.1) can be used.

7 Functional elements for QKDNi

7.1 Functional elements in GWNs

GWNs are trusted to support interworking interfaces between QKDNs in the functional architecture for QKDNi with GWNs. GWNs are located at the border of each QKDN, and each consists of a KM, QKD modules or a QKDN controller. Two GWNs are connected to each other by links identified as Cxi, Kxi, Mxi and Qx. The GWNs are further composed of the following functional elements.

– Key relay function: This function relays the keys between two QKDNs through Kxi-1 in a highly secure manner with an information theoretically secure encryption.

– Key supply function: This function synchronizes and authenticates the keys shared between different KSAs through Kxi-2 and supplies keys to cryptographic applications.

– Session control function: This function supports KMAs and controls the session procedures of interworking key relay.

– Routing control function: This function provisions an appropriate key relay route between QKDNs, also performs rerouting of key relay via sharing fault, performance or availability status of the corresponding QL or KML, to ensure the continuation of interworking key relay and interworking key supply.

– Policy-based control function: This function shares QKDN resources based on the quality of service (QoS) between QKDNs with encryption.

– Configuration control function: This function supports the QKDN controller for the provisioning of key relay routes between QKDNs if they support key relay.

– Fault management function: This function supports the QKDN manager for routing and rerouting control of key relay between QKDNs as needed in case of the faults.

– Configuration management function: This function supports the QKDN manager for the provisioning of key relay routes between QKDNs if they support key relay.

– Accounting management function: This function shares the usage of key supply services and support for a charging or billing system to determine the costs of key usage by cryptographic applications between QKDNs.

– Performance management function: This function monitors and analyses the performance status of QKDN managed resources, and shares related information with encryption between QKDNs.

– Security management function: This function collects or receives security-related management information from the QKDN, and shares related information with encryption between QKDNs.

7.2 Functional elements in IWN

The IWN is a trusted node to support interworking interfaces between QKDNs in the functional architecture for QKDNi with IWN. The IWN is located outside both interworking QKDNs and in between them, and it consists of KMs, QKD modules or QKDN controllers. In the IWN, the KMs and the QKDN controllers are connected with each counterpart by links identified as Kxi' and Cxi' respectively. The QKD modules in the IWN are not connected with each other. The IWN is further composed of the following functional elements.

– Key transfer function: This function transfers the keys between QKDNs through Kxi-1'. It also supports key relay in a QKDN.
– Key supply function: This function synchronizes and authenticates the keys shared between different KSAs through Kxi-2', and supplies the keys to cryptographic applications.
– Session control function: This function supports KMAs and controls session procedures of interworking key transfer.
– Routing control function: This function provisions an appropriate key transfer route between QKDNs, also performs rerouting of key transfer via sharing fault, performance or availability status of the corresponding QL or KML.
– Policy-based control function: This function shares QKDN resources based on the QoS between QKDNs with encryption.
– Configuration control function: This function supports the QKDN controller for the provisioning of key transfer routes between QKDNs.
– Fault management function: This function supports the QKDN manager for the routing and rerouting control of key transfer between QKDNs as needed in case of the faults.
– Configuration management function: This function supports the QKDN manager for the provisioning of key transfer routes between QKDNs.
– Accounting management function: This function shares the usage of key supply services and support for a charging or billing system to determine the costs of key usage by cryptographic applications between QKDNs.
– Performance management function: This function monitors and analyses the performance status of QKDN managed resources, and shares related information with encryption between QKDNs.
– Security management function: This function collects or receives security-related management information from the QKDN and shares related information with encryption between QKDNs.

8 Interworking architectural configurations

There are multiple possible configurations for QKDNi depending on its functional model (QKDNi with either GWNs or an IWN), architectures of interworking QKDNs (distributed or centralized control), or implementation schemes of functional elements for QKDNi. Clauses 8.1 and 8.2 describe several examples of configurations for QKDNi.

8.1 Configurations of QKDNi with GWNs

8.1.1 Configurations of QKDNi with GWNs for two distributed QKDNs

Figure 3 shows a functional model of a configuration of QKDNi with GWNs for two distributed QKDNs.

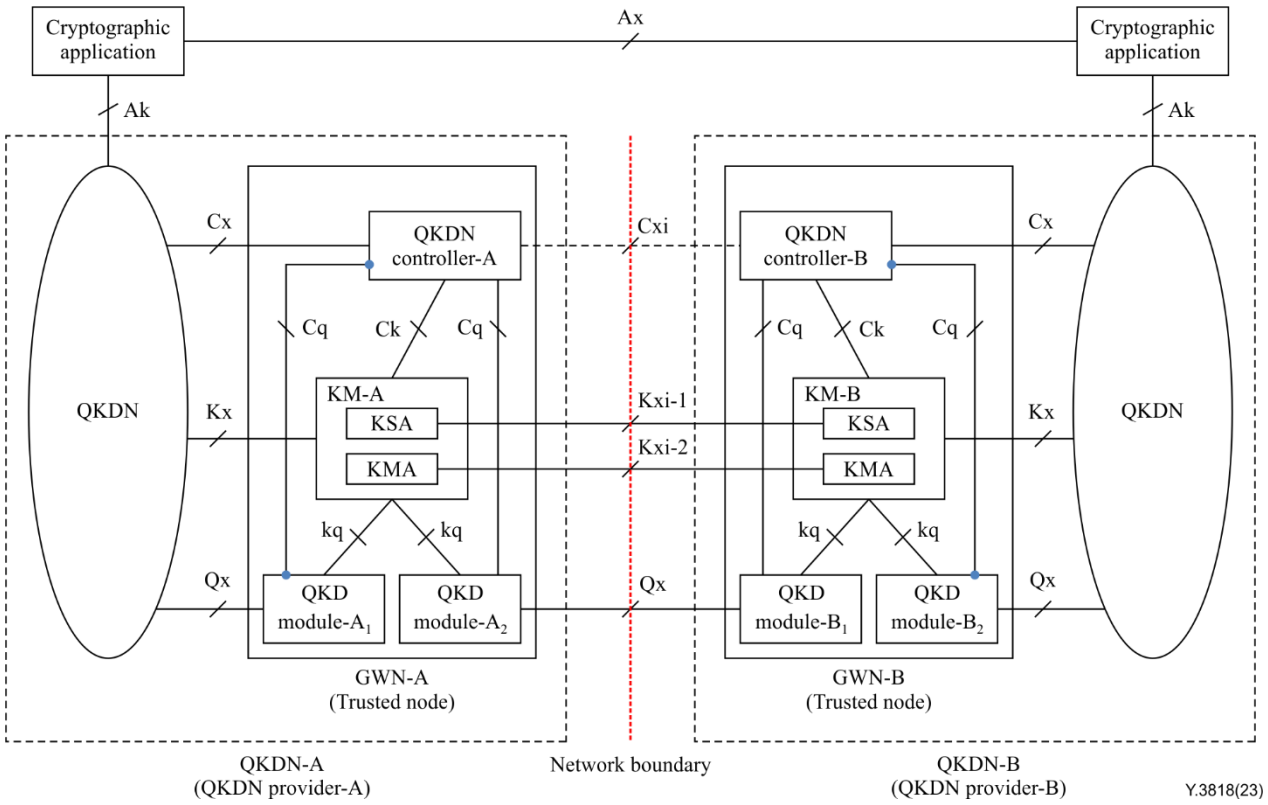

Figure 3 – Interworking of distributed QKDNs with GWNs

8.1.2 Configurations of QKDNi with GWNs for a distributed QKDN and a centralized QKDN

Figure 4 shows a functional model of a distributed QKDN and a centralized QKDN, with separate KMs in the GWNs.

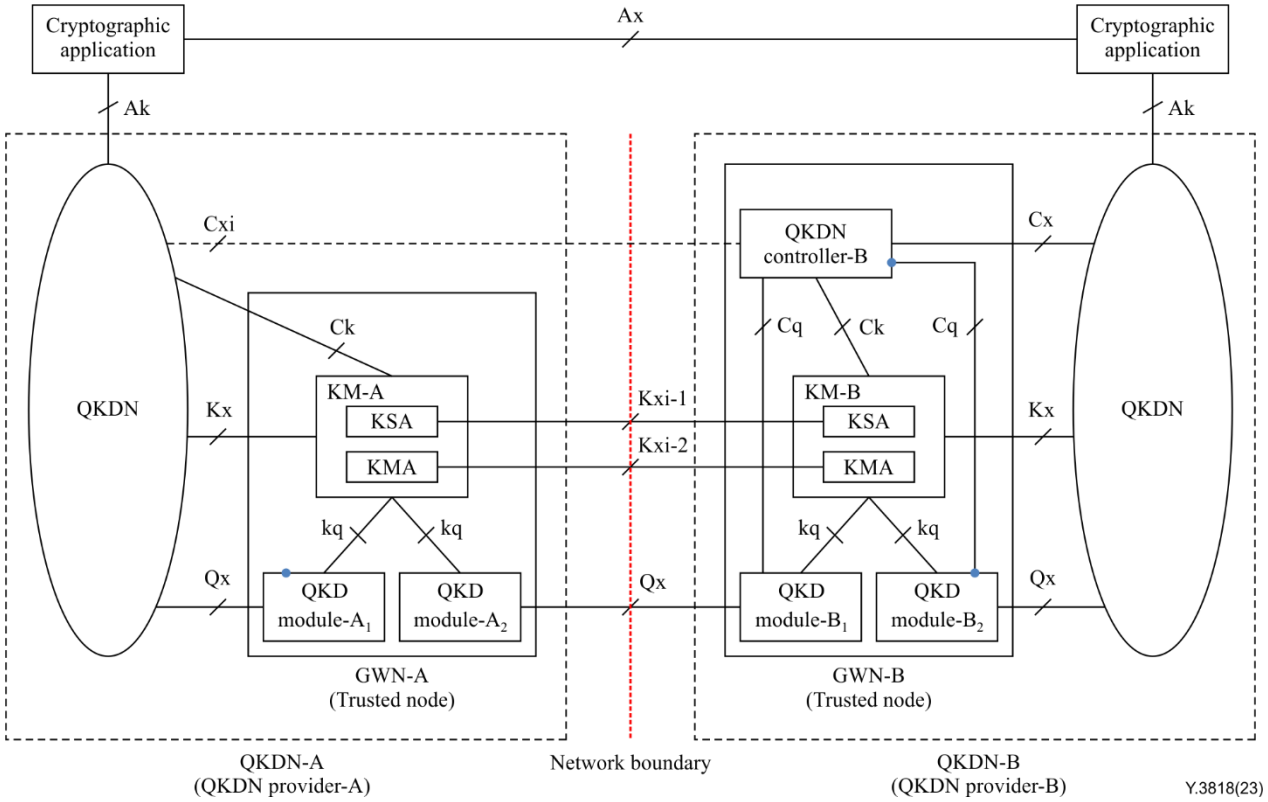

Figure 4 – Interworking of a centralized QKDN and a distributed QKDN with GWNs

8.1.3 Configurations of QKDNi with GWNs for two centralized QKDNs

Figure 5 illustrates a functional model for interworking of two centralized QKDNs.

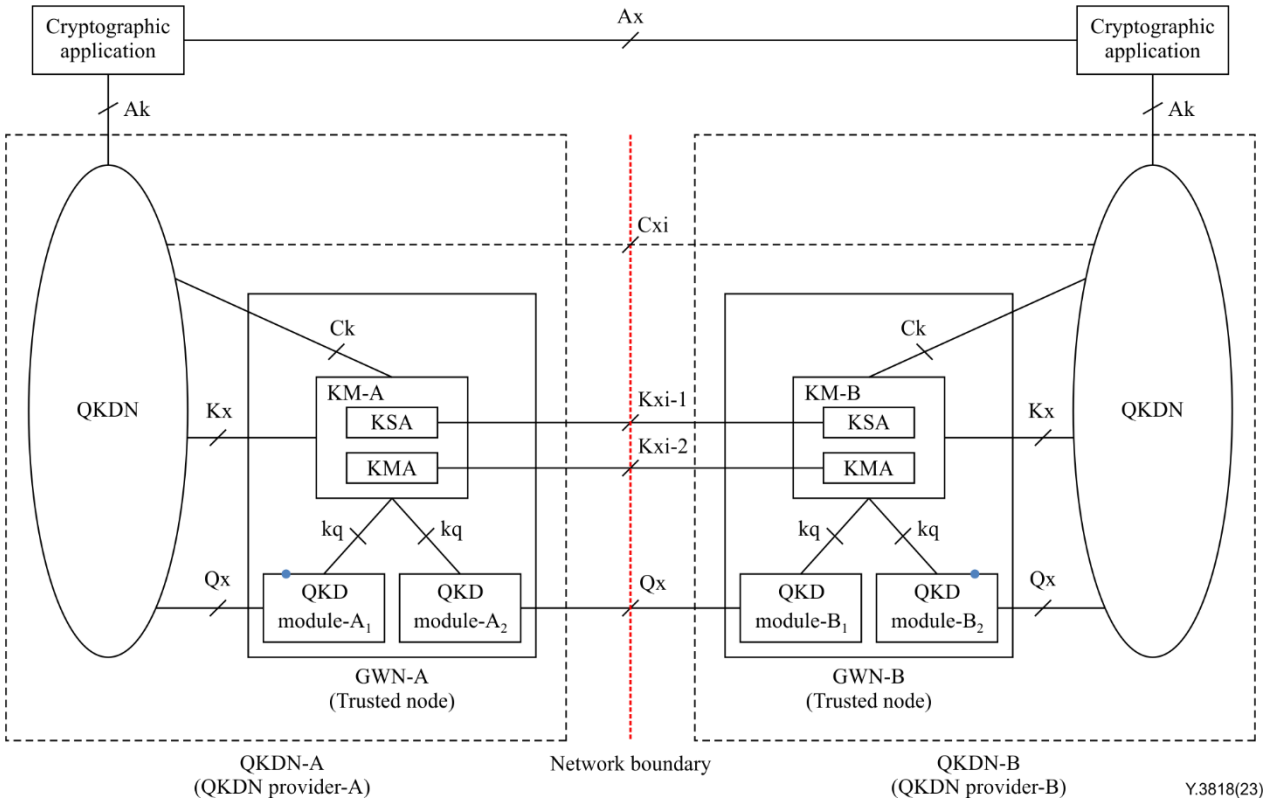

Figure 5 – Interworking of centralized QKDNs with GWNs

8.2 Configurations of QKDNi with IWN

8.2.1 Configurations of QKDNi with IWN for two distributed QKDNs

Figure 6 shows a functional model of a configuration of QKDNi with IWN for two distributed QKDNs, with separate KMs and separate QKDN controllers in IWN. Key transfer is performed in the IWN. In this configuration, QKD module-A and QKD module-B interact with KM-A and KM-B respectively and each KM IWF interacts with the corresponding QKDN controller IWF.

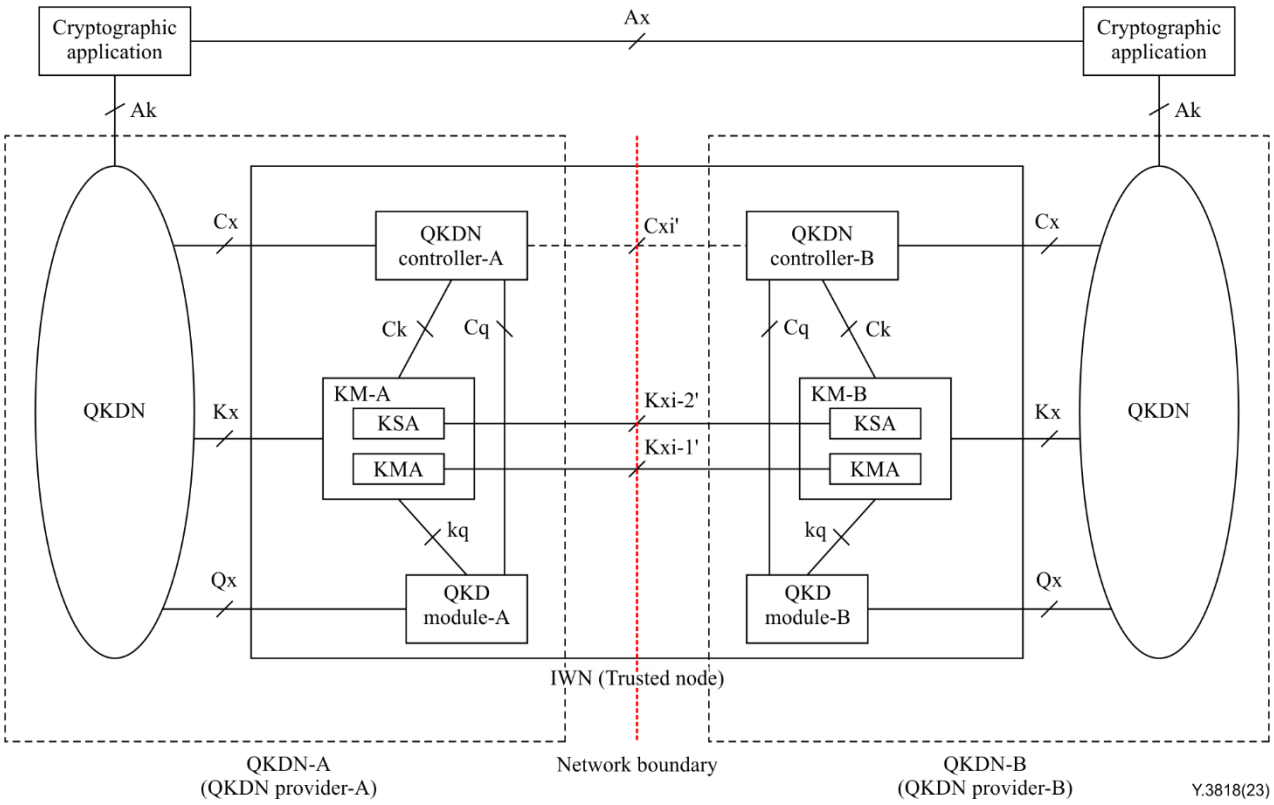

Figure 6 – Interworking of distributed QKDNs

8.2.2 Configurations of QKDNi with IWN for a distributed QKDN and a centralized QKDN

Figure 7 shows a functional model of a configuration of a distributed QKDN and a centralized QKDN, with separate KMs in the IWN. In this configuration, QKD module-A and QKD module-B interact with KM-A and KM-B respectively. As QKDN-A is centralized, the KM IWF interacts with QKDN controller-A. In addition, as QKDN-B is distributed, the KM IWF interacts with QKDN controller-B.

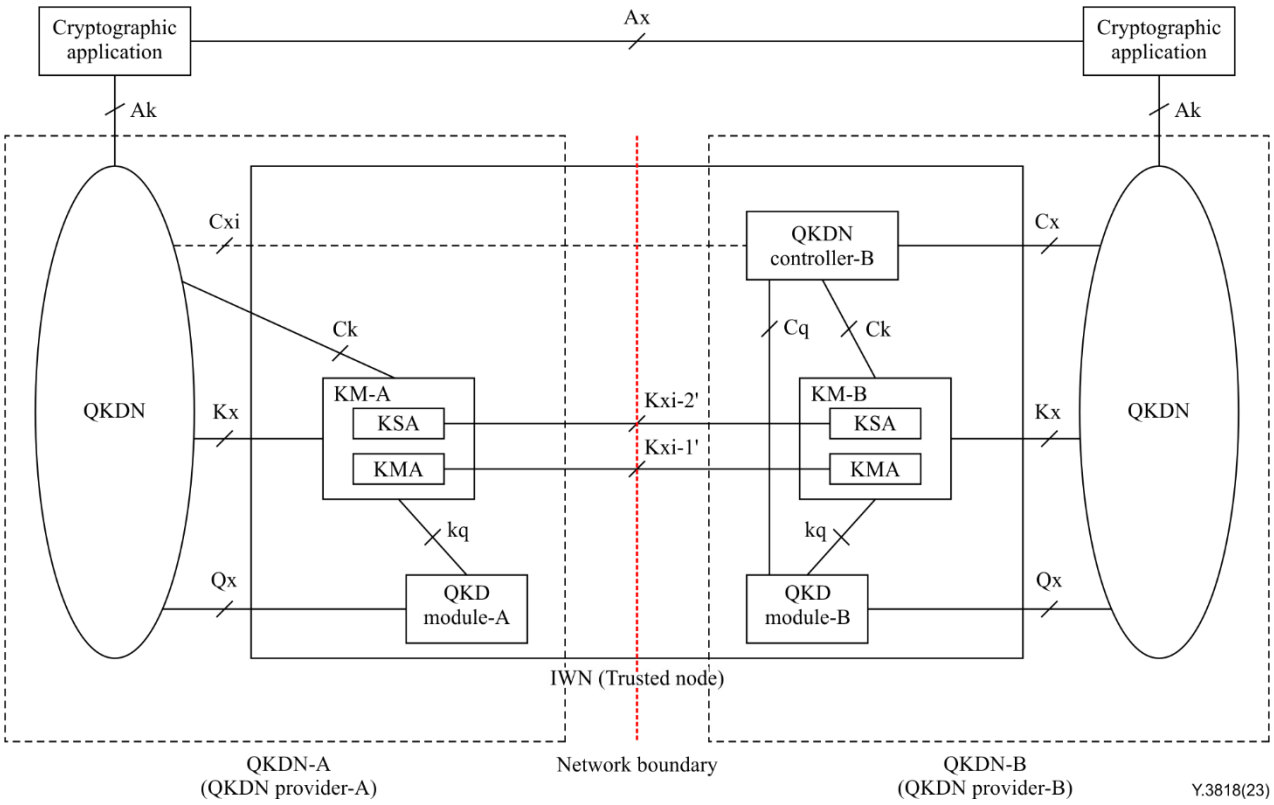

Figure 7 – Interworking of a centralized QKDN and a distributed QKDN

8.2.3 Configurations of QKDNi with IWN for two centralized QKDNs

Figure 8 illustrates a functional model of a configuration of two centralized QKDNs, with separate KMs in the IWN. In this configuration, QKD module-A and QKD module-B interact with KM-A and KM-B, respectively. Since both QKDN-A and QKDN-B are centralized, KM-A interacts with QKDN controller-A, and KM-B interacts with QKDN controller-B.

NOTE – In Figure 8, QKDN controllers and Cq interfaces are not described in order to avoid complexity.

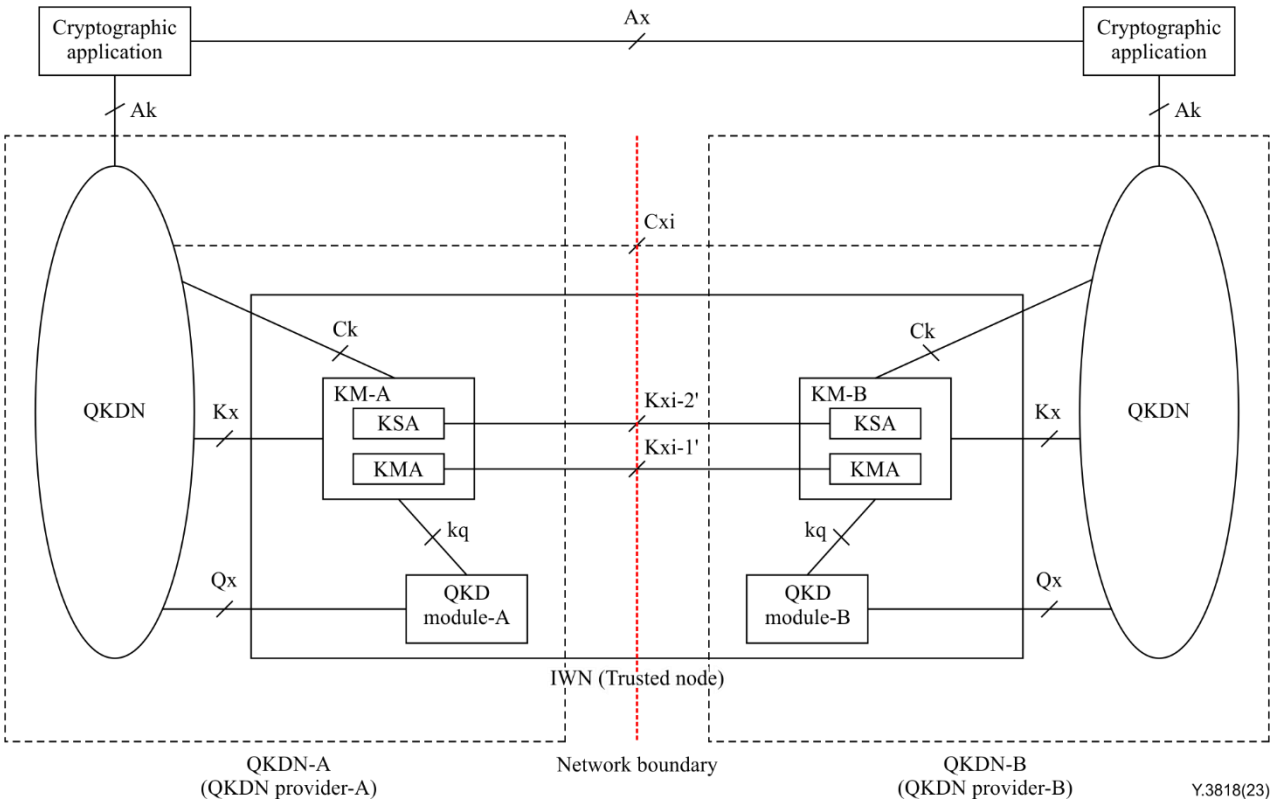

Figure 8 – Interworking of centralized QKDNs

9 Basic operational procedures for QKDNi

9.1 Operational procedures for QKDNi with GWNs

1) Key relay for interworking

Figure 9 illustrates an example of a key relay procedure between interworking QKDNs with GWNs. In this procedure, when GWN-A receives an interworking key relay route requirement, KM-A first requests QKDN controller-A, then controller-A computes an interworking key relay route and sends interworking route information to KM-A. Finally, KM-A executes the interworking key relay.

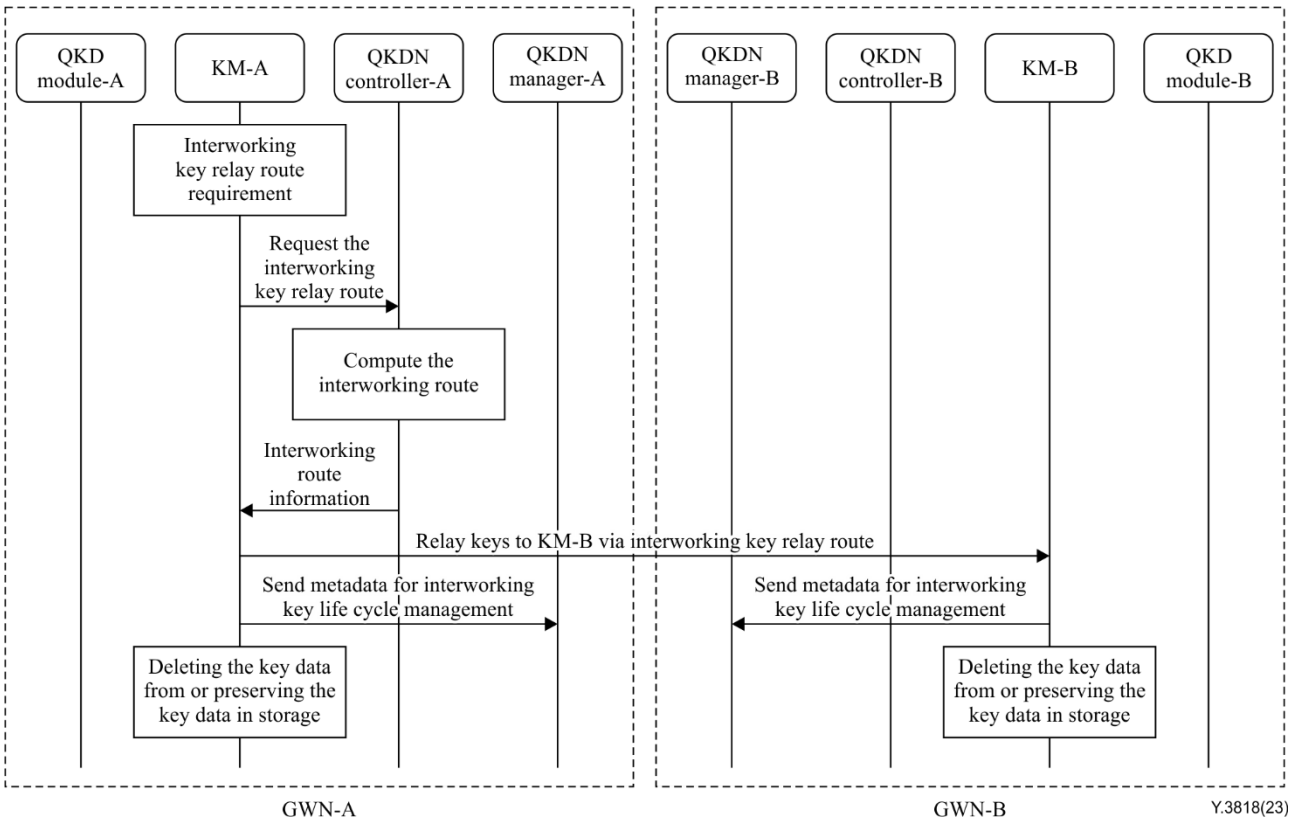

Figure 9 – An example of key relay for interworking between two QKDN providers with GWNs

2) Key generation and rerouting control for interworking

Figure 10 illustrates an example of a procedure for key generation and rerouting control for interworking between QKDNs with GWNs.

Each QKDN controller asks QKD modules, QKD links and KMs for status information about them and these modules push up the related information to their controller. Then, QKDN controller-A and QKDN controller-B check and share these messages for subsequent operations.

In terms of interworking rerouting, QKD modules send status information and optionally a QKD link to their controllers. QKDN controller-A and QKDN controller-B analyse the information provided and decide whether interworking key relay rerouting is necessary. They then share information to change rerouting path simultaneously. After confirming commands of controllers are consistent, they send interworking rerouting information to KM-A and KM-B.

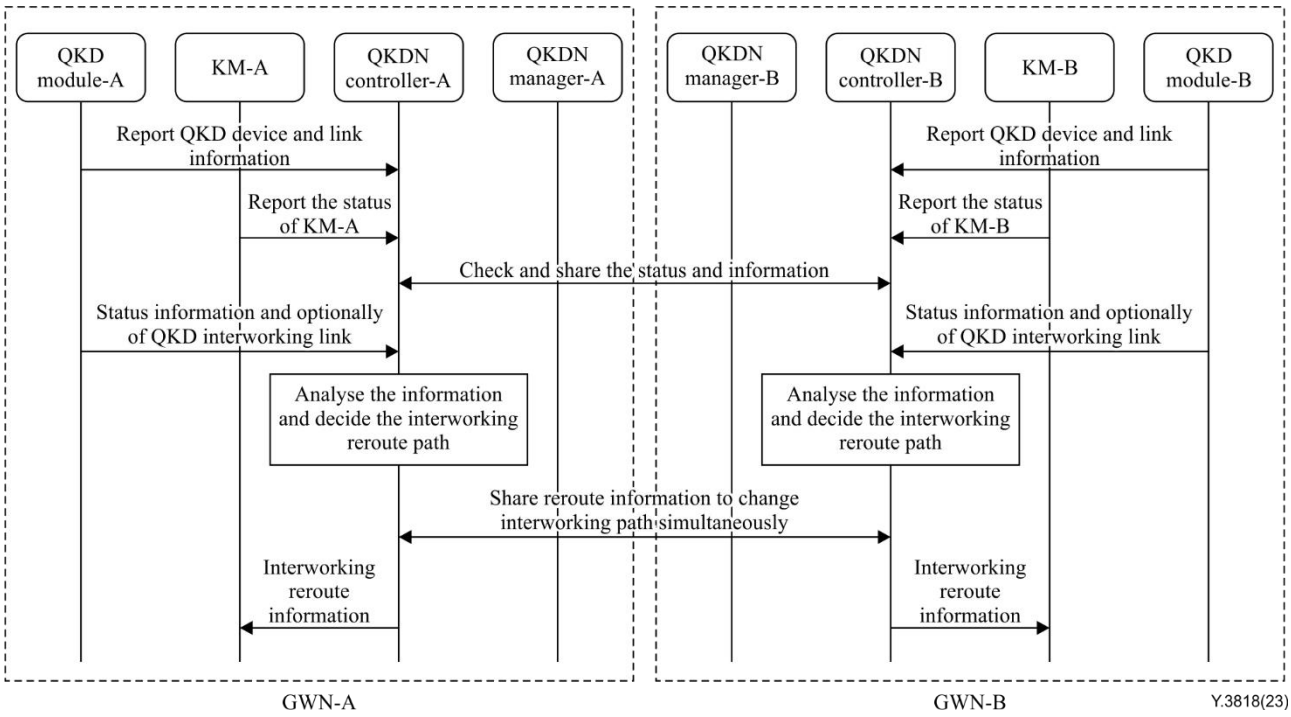

Figure 10 – An example of key generation and rerouting control for interworking between two QKDNs with GWNs

3) Fault management of key relay failure for interworking

Figure 11 shows an example of a QKDNi fault management procedure between two QKDNs with GWNs. If interworking relay has something wrong, key manager layer management-A (KMLM-A) reports relay failure to cross-layer management orchestration-A (XLMO-A), XLMO-A then sends it to XLMO-B. XLMO-A and B report interworking relay failure diagnosis information to the corresponding QKDN control layer management (QCLM), which makes the next decision.

In addition, management in each layer sends a performance report and security information to XLMO-A, which are packed by XLMO-A and then sent to XLMO-B.

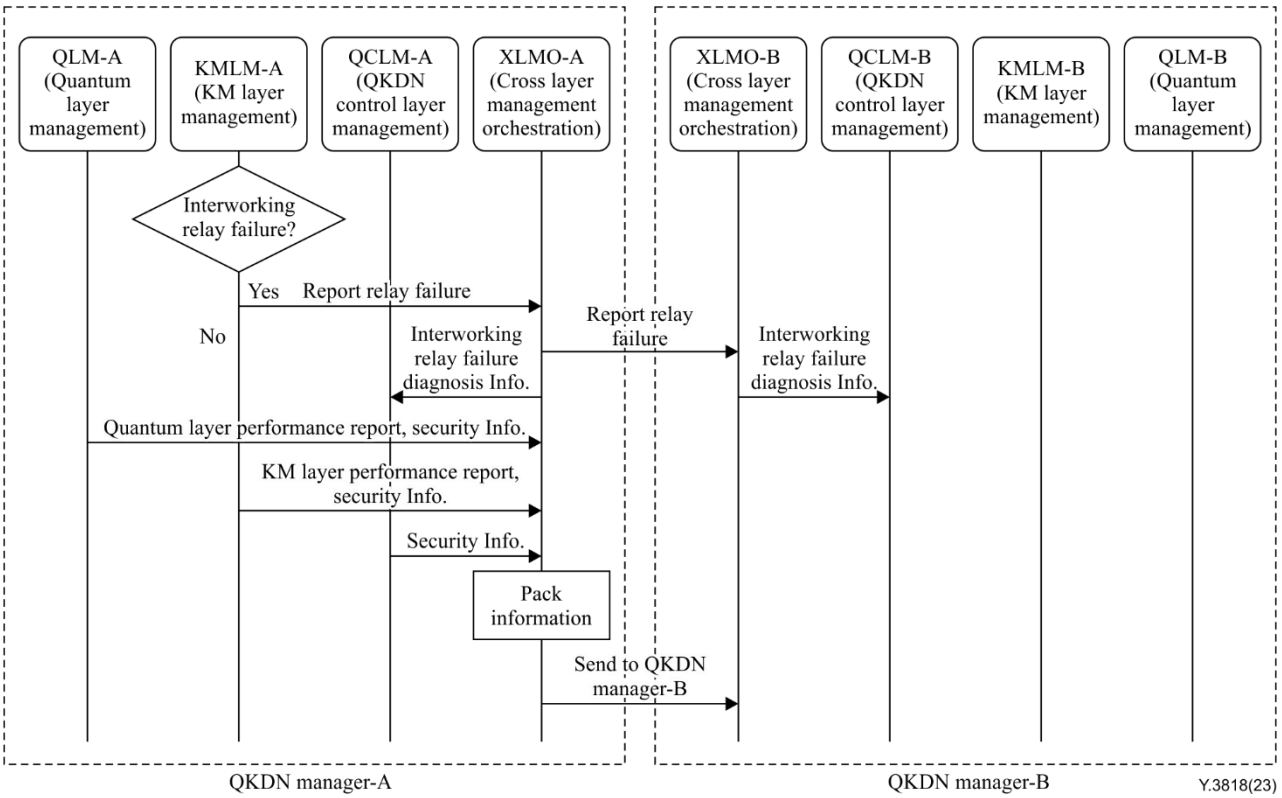

Figure 11 – An example of fault management of key relay failure for interworking between two QKDNs with GWNs

9.2 Operational procedures for QKDNi with IWN

1) Key transfer for interworking

Figure 12 illustrates an example of a key transfer procedure of interworking between QKDNs with IWN.

In this procedure, KM-A receives an interworking key transfer requirement and sends it to QKDN controller-A. Controller-A checks the status of key resources between KM-A and KM–B; if there are sufficient keys to be provided, controller-A then determines the transfer link and keys. After receiving a message from controller-A, KM-A transfers the keys to KM-B via an interworking key transfer link. To ensure information synchronization, KM-A and KM-B send metadata for transfer key lifecycle management to their controllers, and delete or store the key data.

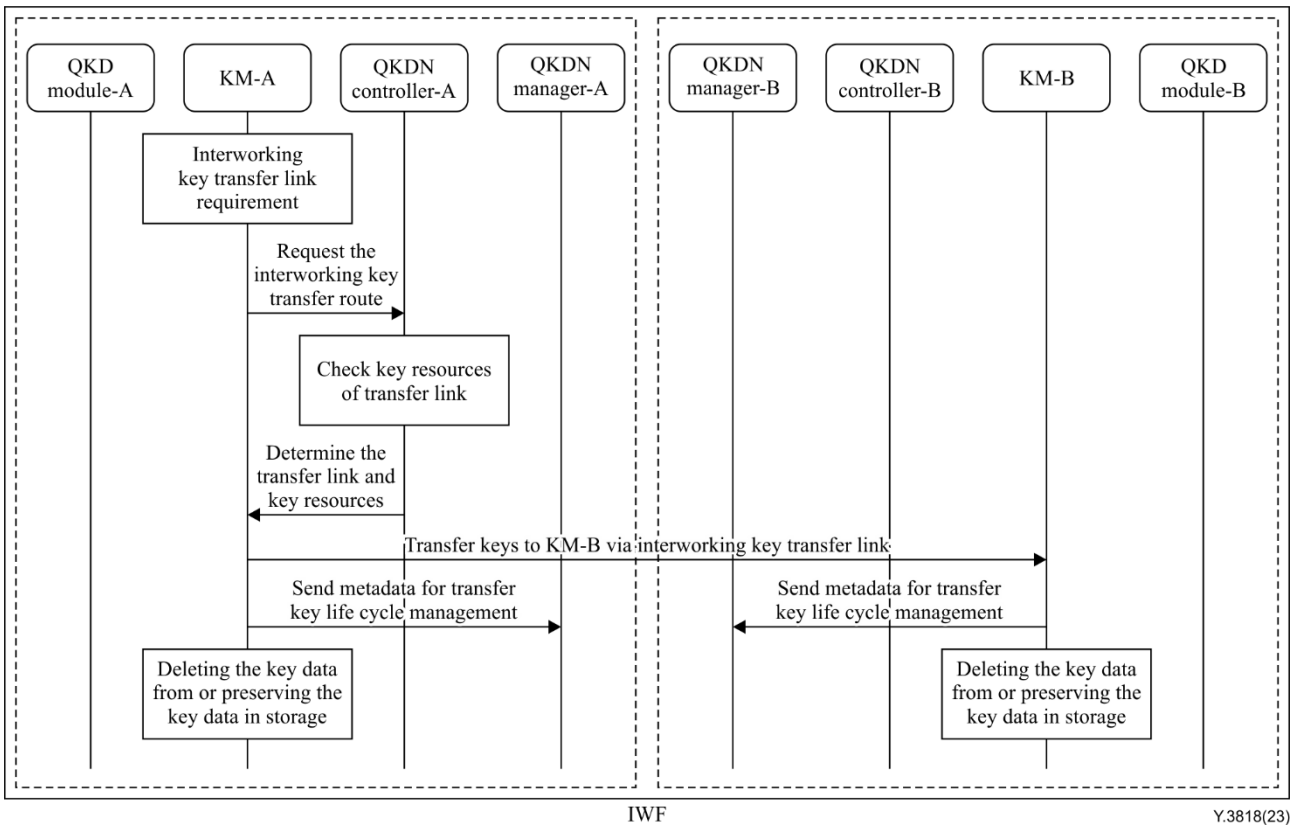

Figure 12 – An example of key transfer for interworking between two QKDNs with IWN

2) Key generation control for interworking

Figure 13 illustrates an example of a procedure for key generation and rerouting control for interworking between QKDNs with IWN.

This procedure is similar to that shown in Figure 12. Each QKDN controller is responsible for collecting information from the QKD module and KM, and shares information to another controller. In contrast, when a fault occurs, QKDN controller-A and QKDN controller-B receive related information and decide rerouting paths of key transfer.

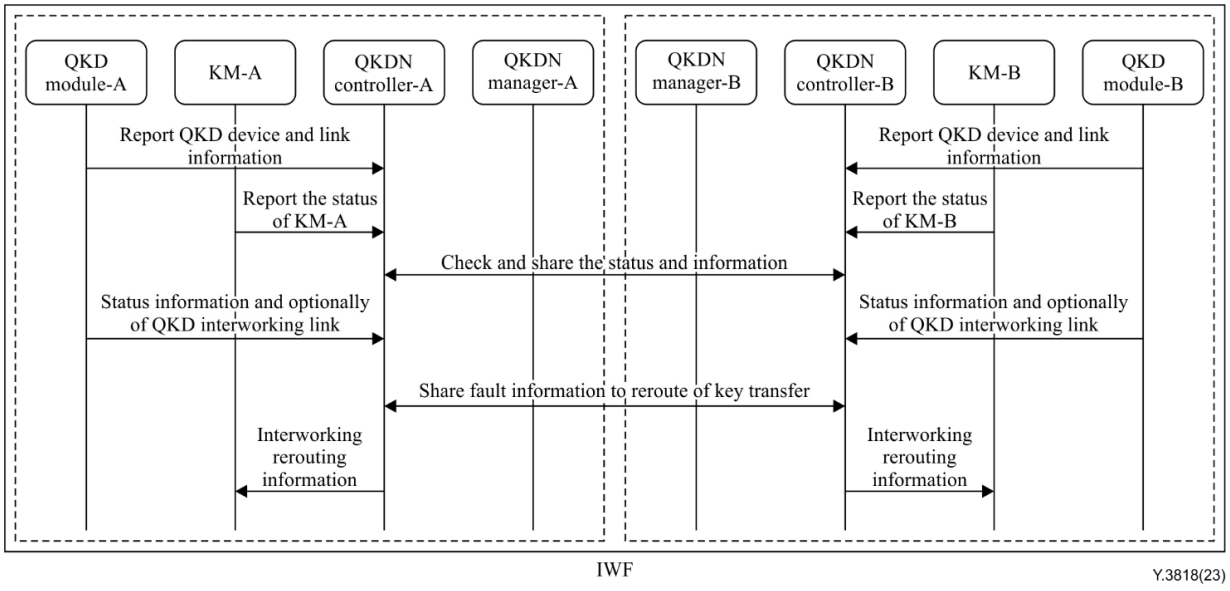

Figure 13 – An example of key generation and rerouting control for interworking between two QKDNs with IWN

3) Fault management of key transfer failure for interworking

Figure 14 shows an example of a fault management procedure of key transfer failure for interworking between QKDNs with IWN.

If interworking key transfer has some problem, KMLM-A reports relay failure to XLMO-A, which then sends it to XLMO-B. XLMO-A and B report interworking key transfer failure diagnosis information to the corresponding QCLM, which makes the next decision.

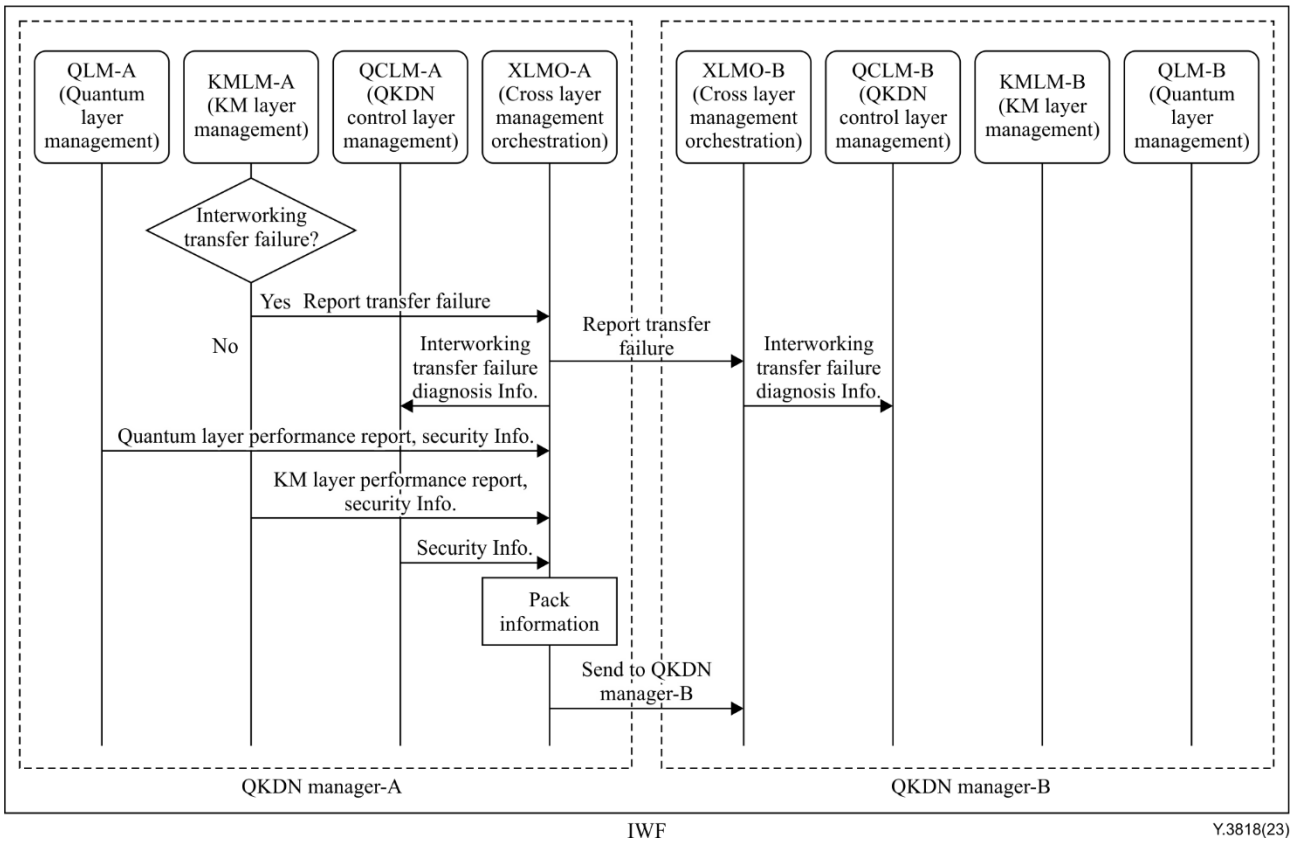

Figure 14 – An example of fault management of key transfer failure for interworking between two QKDNs with IWN

10 Security considerations

To mitigate security threats and potential attacks, for example, issues of confidentiality, integrity, authenticity, non-repudiation, availability and traceability need to be addressed, and appropriate security and privacy protection schemes should be considered in the QKDN, the user network and interfaces between the two networks. Details lie outside the scope of this Recommendation.

Bibliography

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

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, 2023