INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2022-2024

SG13-TD300/WP3

STUDY GROUP 13

Original: English

Question(s): 16/13

Geneva, 26 July 2023

TD

Source: Editors

Title: Draft Recommendation ITU-T Y.3818 (formerly Y.QKDN-iwac) "Quantum key distribution networks interworking – architecture" - for consent

Contact:	Yazi Wang Beijing University of Posts and Telecommunications. China	Tel: +86-19800372862 E-mail: yazi_wang@bupt.edu.cn
Contact:	Yongli Zhao Beijing University of Posts and Telecommunications. China	Tel: +86-10-61198108 E-mail: yonglizhao@bupt.edu.cn
Contact:	Xiaosong Yu Beijing University of Posts and Telecommunications. China	Tel: +86-10-61198108 E-mail: xiaosongyu@bupt.edu.cn
Contact:	Zhangchao Ma CAS Quantum Network Co., Ltd. China	Tel: +86-10-83057625 E-mail: mazhangchao@casquantumnet.com
Contact:	Junsen Lai China Academy of Information and Communication Technology (CAICT), Ministry of Industry and Information Technology (MIIT), China	Tel: +86-10-62300592 E-mail: laijunsen@caict.ac.cn
Contact:	Dong-Hi SIM SK Telecom Korea, Republic of	E-mail: donghee.shim@sk.com

Keywords: QKD (Quantum Key Distribution); QKD network (QKDN); QKDN interworking (QKDNi)

Abstract: This document includes the updated draft Recommendation Y.QKDN-iwac "Quantum key distribution networks interworking – architecture" for consent (output of Q16/13 meeting, 17 - 21 July 2023)

Summary

This output document is the draft of Y.QKDN-iwac for consent, updated based on the discussion results of C-123 and C-124 in the SG13 meeting (17 - 21 July 2023).

C-123	BUPT	Proposed improvements to ITU-T Y.QKDN-iwac "Quantum key distribution networks interworking – architecture" (for consent)	Q16/13
C-124	NICT, NEC, Toshiba	Proposal for revised texts of ITU-T Y.QKDN_iwac: "Quantum key distribution networks interworking – architecture"	Q16/13

Annex I is the results of the updated draft Recommendation ITU-T Y.QKDN-iwac "Quantum key distribution networks interworking – architectures", as follows;

a Revised the texts in clause 6.1 and 6.2, explaining some have been identified in Y.3810 based on the discussion results of C-123 and C-124.

b Revised the texts of functional elements in clause 7.1 and 7.2 based on the discussion results of C-124, and changing the 'key relay' to 'key transfer' in clause 7.2.

c Deleted the unified configuration examples in clause 8.2.

d Replaced 'Kxi'-1', 'Kxi'-2' with 'Kxi-1'', 'Kxi-2'' to correct this typo.

e Corrected some grammar errors.

f Revised some editorial texts.

The attached Annex A is the final draft Recommendation ITU T X.QKDN-iwac "Quantum key distribution networks interworking – architectures" for consent.

Attachments:

Annex A is updated draft Recommendation ITU T X.QKDN-iwac "Quantum key distribution networks interworking – architecture".

Annex

Draft Recommendation ITU-T Y.3818 (formerly Y.QKDN-iwac)

Quantum key distribution networks interworking – architecture

Summary

For quantum key distribution networks (QKDN), Recommendation ITU-T Y.QKDN_iwac specifies functional architecture models for QKDN interworking (QKDNi), i.e., functional architecture with GateWay Nodes (GWNs) and functional architecture with InterWorking Nodes (IWNs). In order realize these two models, it specifies detailed functional elements, basic operational procedures, and architectural configurations for QKDNi.

Keywords

QKD, QKDN (QKD network), interworking

Table of Contents

Draft Recommendation ITU-T Y.3818 (formerly Y.QKDN-iwac)

Quantum key distribution networks interworking – architectures

1. Scope

This Recommendation specifies functional architectures for QKDN interworking (QKDNi). In particular, the scope of this Recommendation includes the following aspects for QKDNi:

- 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)/Cor.1 (2020), *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 Networks interworking –framework*

[ITU-T Y.3813] Recommendation ITU-T Y.3813 (2022), *Quantum Key Distribution Networks 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 (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.

3.1.4 **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).

3.1.5 **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 (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.

3.1.7 **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.

3.1.8 **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

This Recommendation defines no term.

4. Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

FCAPS Fault, Configuration, Accounting, Performance, Security

GWF GateWay Function

GWN GateWay Node

IT-secure Information-theoretically secure

IWF InterWorking Function

IWN InterWorking Node

KM Key manager

QKD Quantum Key Distribution

QKDN QKD Network

QKDNi QKDN interworking

5. Conventions

None.

6. Functional architecture for QKDNi

Quantum key distribution network (QKDN) is a cryptographic infrastructure to provide secure symmetric keys to cryptographic applications in user networks. Constructing a large scale QKDN which covers wide area, it may consist of multiple QKDNs and they are interworking each other.

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

Based on the conceptual models on 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

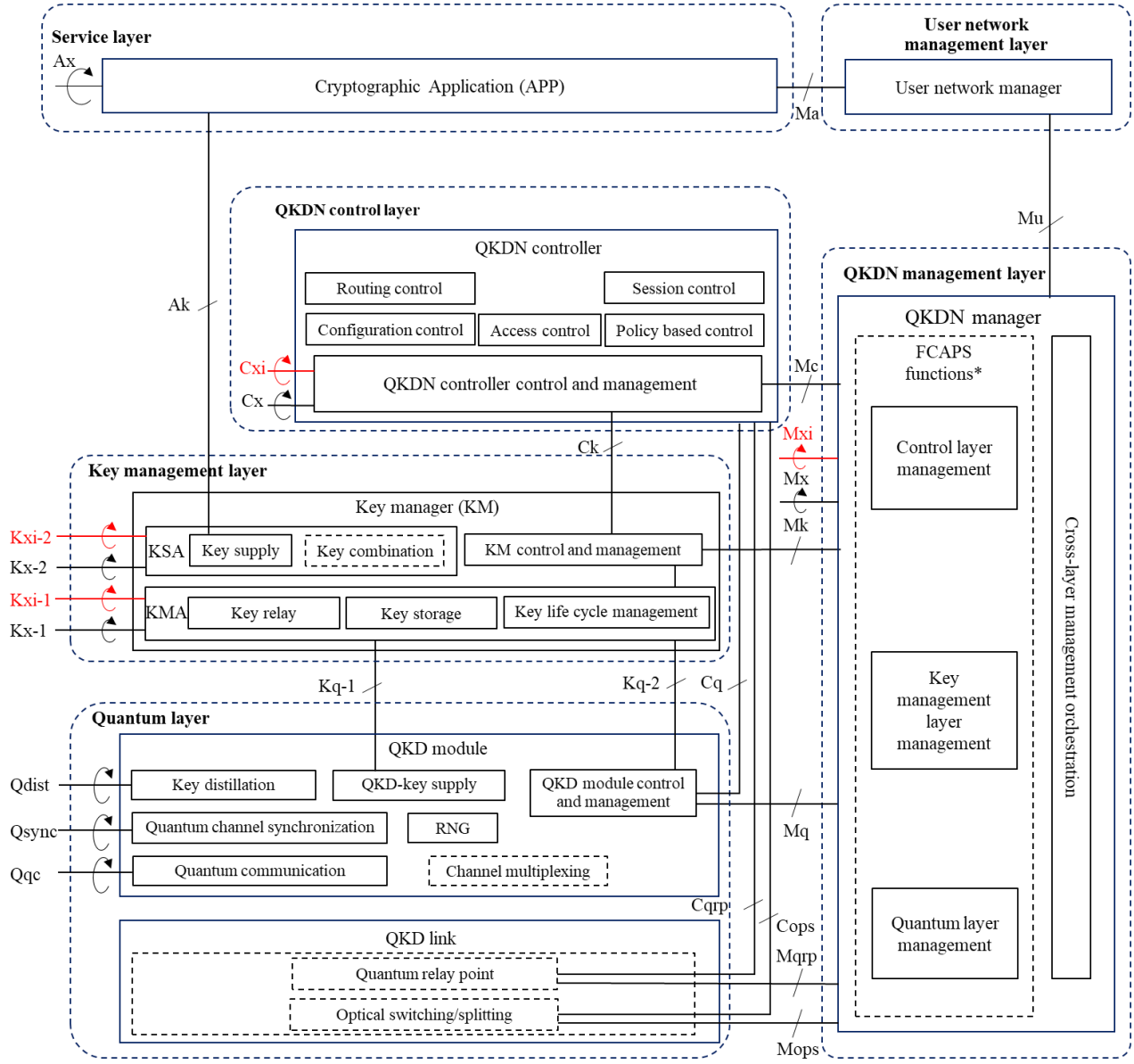

Figure 1 - A functional architecture for QKDNi with GWNs

The functional model for QKDNi with GWNs is defined in [ITU-T Y.3810], and the layer structure for QKDN is defined in [ITU-T Y.3800]. Detailed descriptions of layer structure for QKDNi are given in following.

– Quantum layer: The functional elements in the quantum layer including the QKD link and the QKD module.

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

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

– QKDN management layer: The functional element in the QKDN management layer is the QKDN manager. It 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 defined in [ITU-T Y.3802], and this Recommendation defines the new reference points between the QKDNs.

The newly added reference points are:

– **Cxi**: a reference point connecting two QKDN controllers control and management functions between the QKDNs. It is responsible for the two QKDN controllers to communicate interworking control information with each other.

– **Kxi-1**: a reference point connecting two KMAs between the QKDNs via an interworking KMA link. It is responsible for exchanging 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. It is responsible for exchanging 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. It is responsible for the two QKDN managers to share QKDN management information with each other.

6.2. Functional architecture for QKDNi with IWN

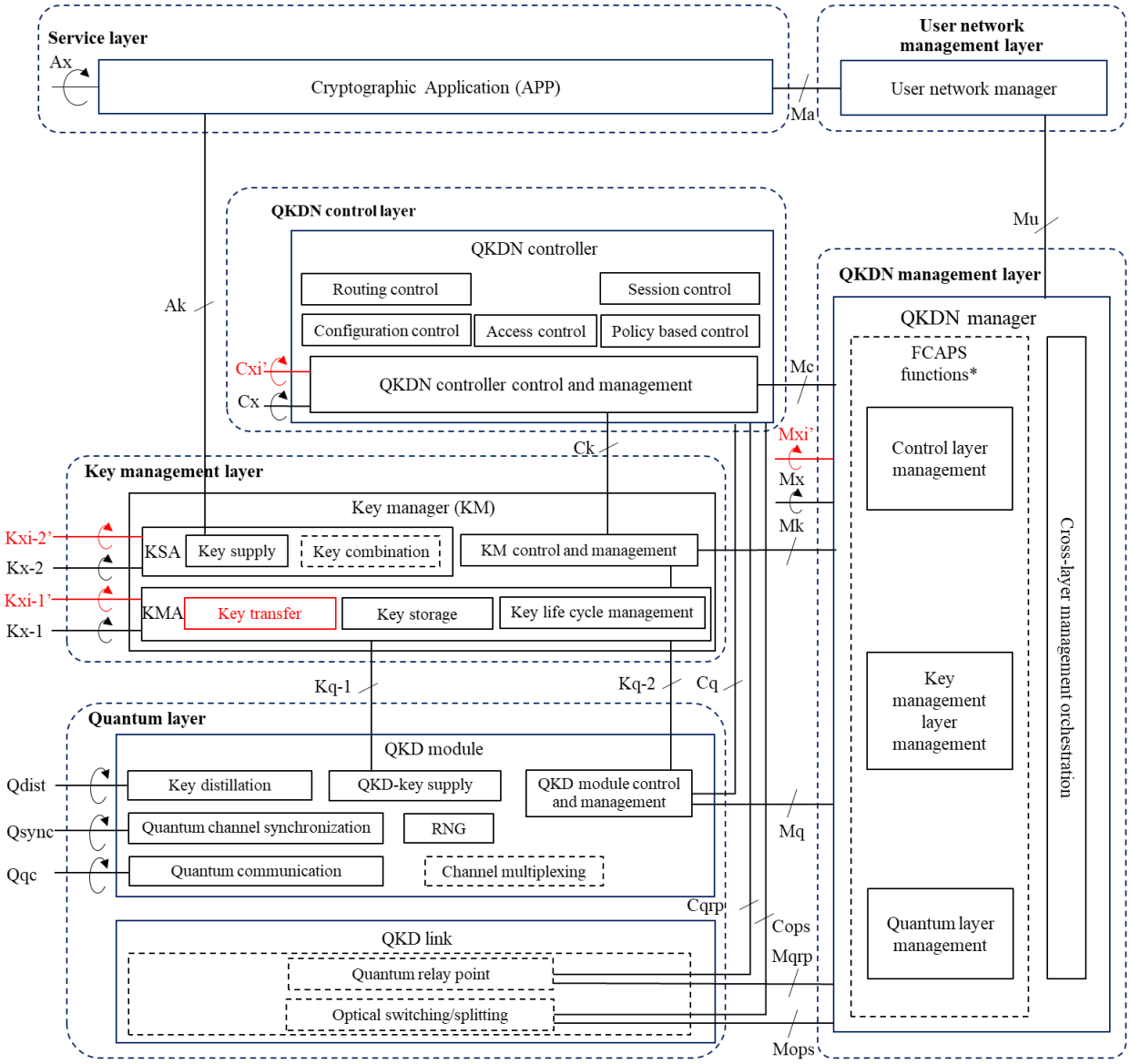

Figure 2 - A functional architecture for QKDNi with IWN

The functional model for QKDNi with IWN is defined in [ITU-T Y.3810], and layer structure for QKDN is defined in [ITU-T Y.3800]. Detailed descriptions of layer structure for QKDNi are given in following.

– Quantum layer: The functional elements in the quantum layer including the QKD link and the QKD module.

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

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

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

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

Most of the reference points in Figure 2 are defined in [ITU-T Y.3802], and this Recommendation defines the new reference points in the IWN.

The newly added reference points are:

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

– **Kxi-1'**: a reference point connecting two KMAs in the IWN via an interworking KMA link. It is responsible for exchanging 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. It is responsible for exchanging 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. It is responsible for the two QKDN managers to share QKDNi management information with each other. It exists the two OkDN managers to share in the IWN when OKDN managers of both OKDNs are accommodated in the IWN, Otherwise, Mxi in clause 6.1 can be used.

7. Functional elements for QKDNi

7.1. Functional elements in GWNs

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

- Key relay function: It relays the keys between two QKDNs through Kxi-1 in a highly secure manner with an IT-secure encryption;
- Key supply function: It synchronizes and authenticates the keys shared between different KSAs through Kxi-2, and supplies the keys to cryptographic applications;
- Session control function: It supports KMAs, and controls the session procedures of interworking key relay;
- Routing control function: It provisions an appropriate key relay route between QKDNs, also performs rerouting of key relay via sharing fault, performance, and/or availability status of respective quantum layer and/or respective key management layer, for ensuring the continuation of interworking key relay and interworking key supply;
- Policy based control function: It shares QKDN resources based on the quality of service (QoS) between QKDNs with encryption;
- Configuration control function: It supports the QKDN controller for the provisioning of key relay routes between QKDNs if QKDN supports key relay;
- Fault management function: It supports the QKDN manager for the routing and rerouting control of key relay between QKDNs as needed in case of the faults;
- Configuration management function: It supports the QKDN manager for the provisioning of key relay routes between QKDNs if QKDN supports key relay;
- Accounting management function: It shares the usage of key supply services and support for charging/billing system to determine the costs of key usage by cryptographic applications between QKDNs;
- Performance management function: It monitors and analyses the performance status of the QKDN managed resources, and shares related information with encryption between QKDNs;

- Security management function: It collects/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 of both interworking QKDNs and in between them, and it consists of KMs, QKD modules, and/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 comprised of the following functional elements:

- Key transfer function: It transfers the keys between QKDNs through Kxi-1'. It also supports key relay in a QKDN;
- Key supply function: It synchronizes and authenticates the keys shared between different KSAs through Kxi-2', and supplies the keys to cryptographic applications;
- Session control function: It supports KMAs, and controls the session procedures of interworking key transfer;
- Routing control function: It provisions an appropriate key transfer route between QKDNs, also performs rerouting of key transfer via sharing fault, performance, and/or availability status of respective quantum layer and/or respective key management layer;
- Policy based control function: It shares QKDN resources based on the quality of service (QoS) between QKDNs with encryption;
- Configuration control function: It supports the QKDN controller for the provisioning of key transfer routes between QKDNs;
- Fault management function: It 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: It supports the QKDN manager for the provisioning of key transfer routes between QKDNs;
- Accounting management function: It shares the usage of key supply services and support for charging/billing system to determine the costs of key usage by cryptographic applications between QKDNs;
- Performance management function: It monitors and analyses the performance status of the QKDN managed resources, and shares related information with encryption between QKDNs;
- Security management function: It collects/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 GWNs or QKDNi with IWN), architectures of interworking QKDNs (distributed control or centralized control), and/or implementation schemes of functional elements for QKDNi. In this clause several examples of configurations for QKDNi are described.

8.1. Configurations of QKDNi with GWNs

8.1.1. Configurations of QKDNi with GWNs for two distributed QKDNs

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

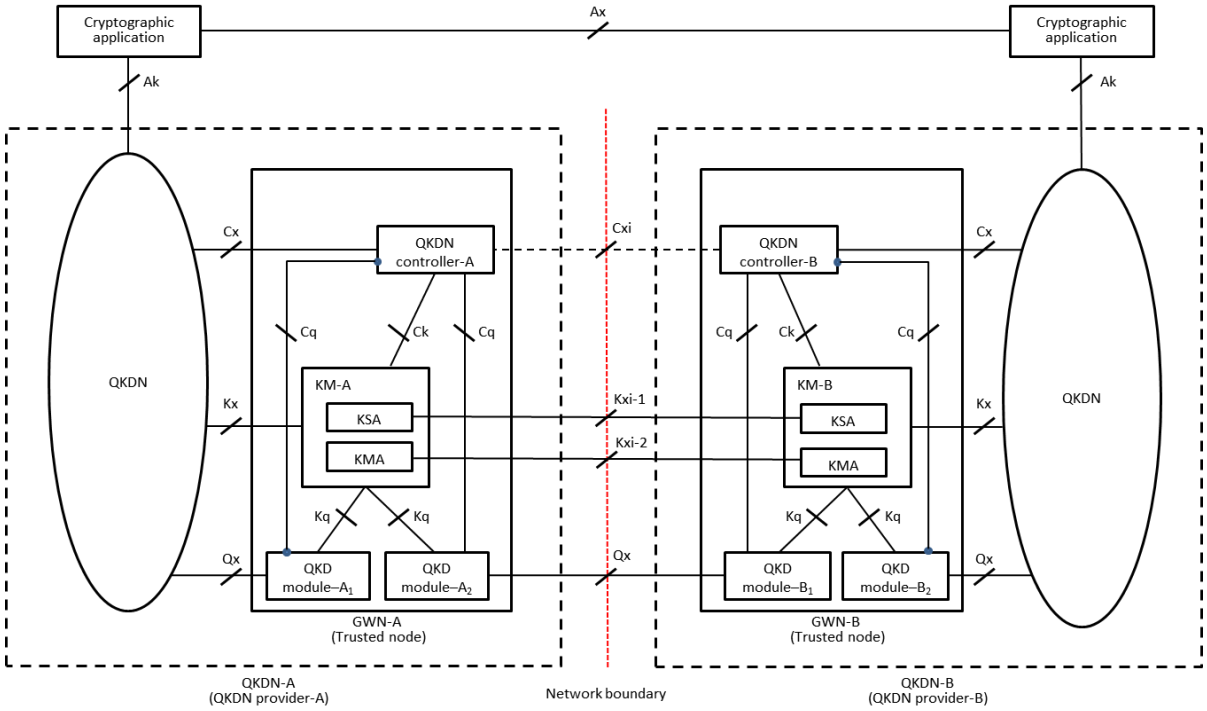

Figure 3 - Interworking of distributed QKDNs with GWNs

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

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

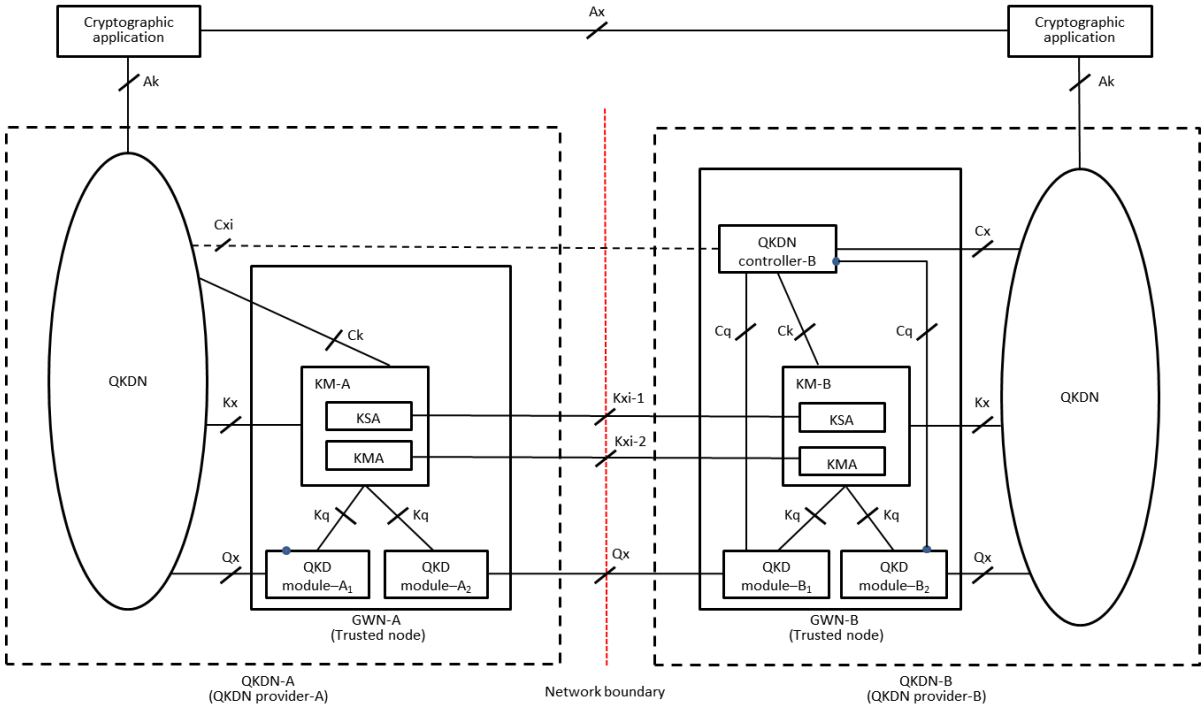

Figure 4 - Interworking of a centralized QKDN and a distributed QKDN with GWNs

8.1.3. Configurations of QKDNi with GWNs for two centralized QKDNs

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

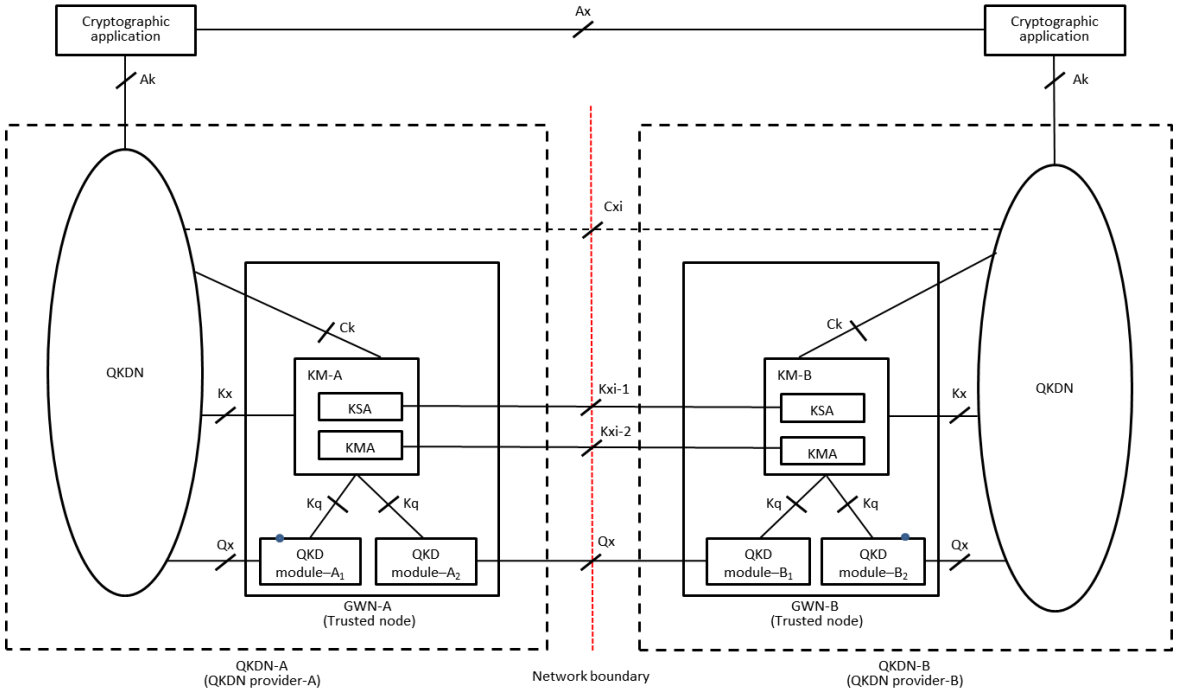

Figure 5 - Interworking of centralized QKDNs with GWNs

8.2. Configurations of QKDNi with IWN

8.2.1. Configurations of QKDNi with IWN for two distributed QKDNs

Figure 6 shows the 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 interworking function interact with respective QKDN controller interworking function.

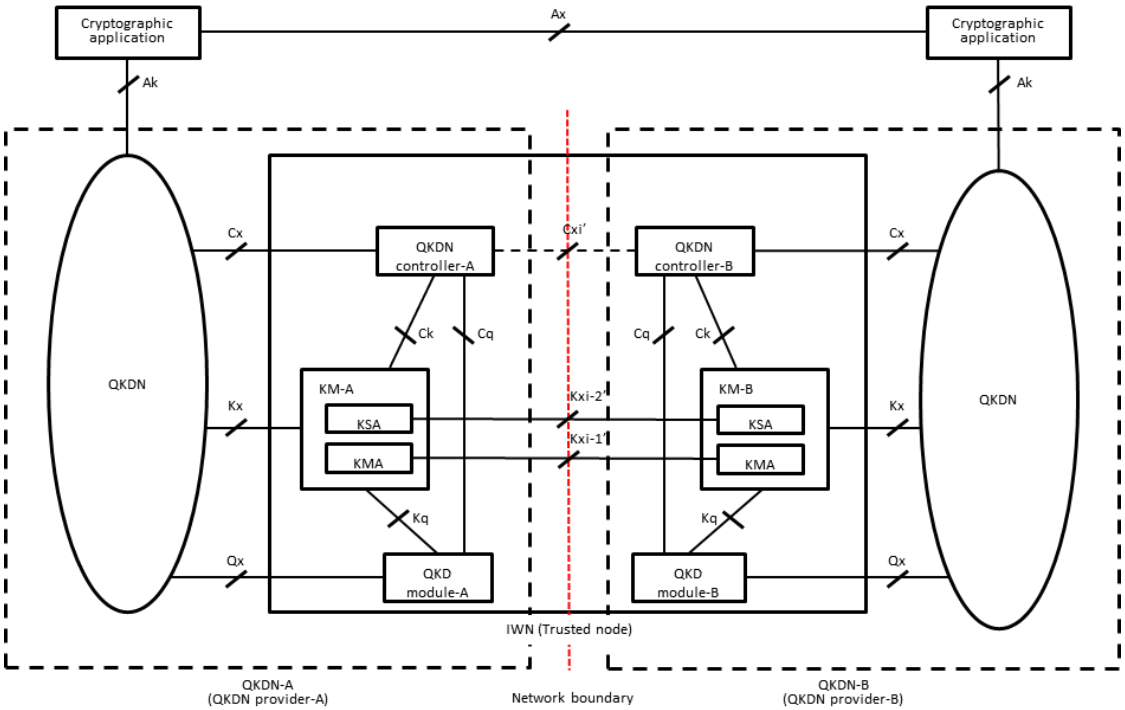

Figure 6 - Interworking of distributed QKDNs

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

Figure 7 shows the 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, KM interworking function interacts with QKDN controller-A. In addition, as QKDN-B is distributed, KM interworking function interacts with QKDN controller-B.

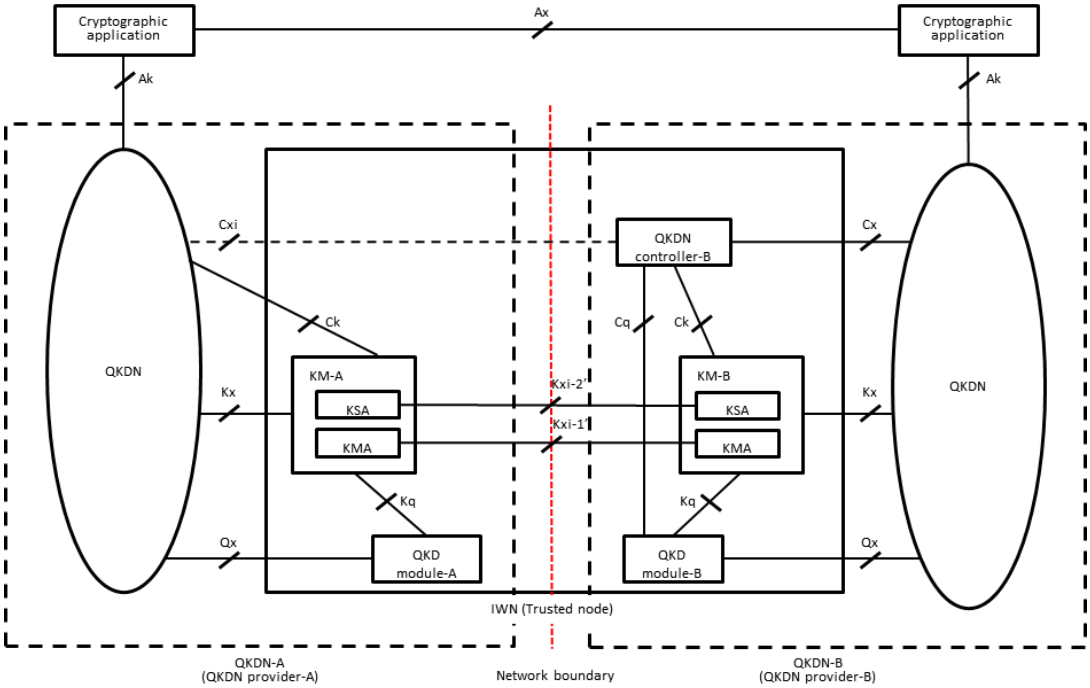

Figure 7 - Interworking of a centralized QKDN and a distributed QKDN

8.2.3. Configurations of QKDNi with IWN for two centralized QKDNs

Figure 8 illustrates the 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 the complexity.

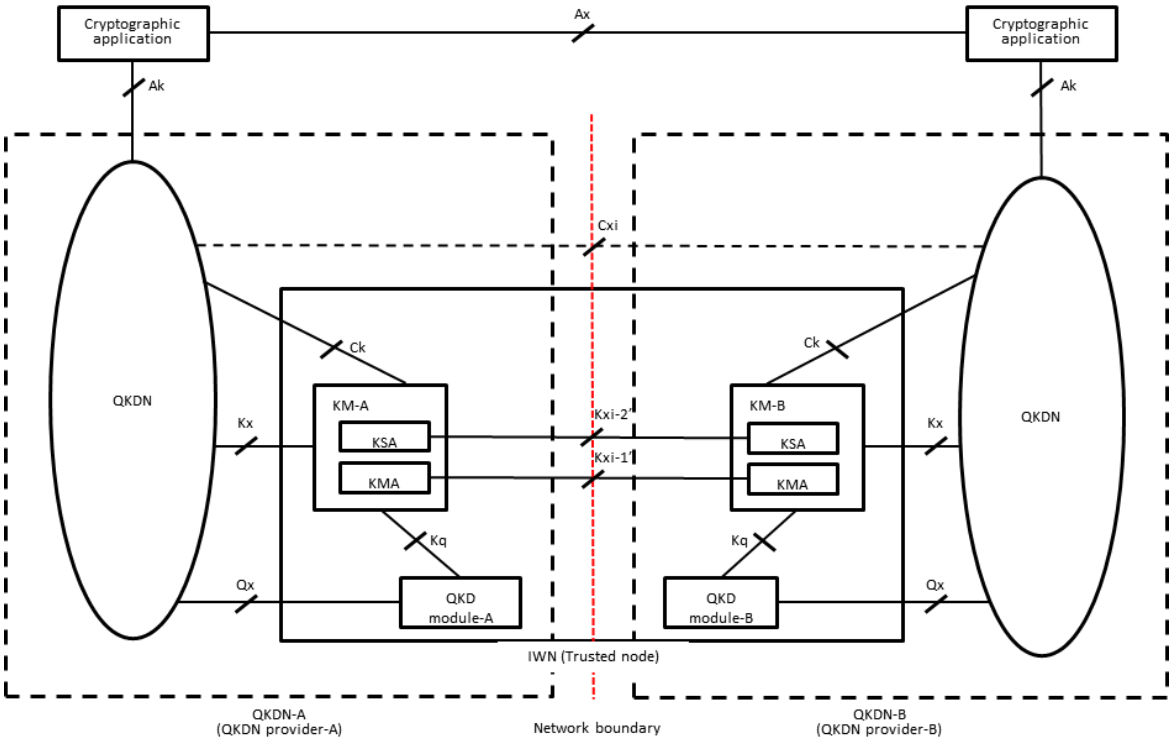

Figure 8 - Interworking of centralized QKDNs

9. Basic operational procedures for QKDNi

9.1. Operational procedures for QKDNi with GWNs

1) Key relay for interworking

Figure 9 illustrates an example key relay procedure between interworking QKDNs with GWNs. In this procedure, when GWN-A receives an interworking key relay route requirement, KM-A firstly 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.

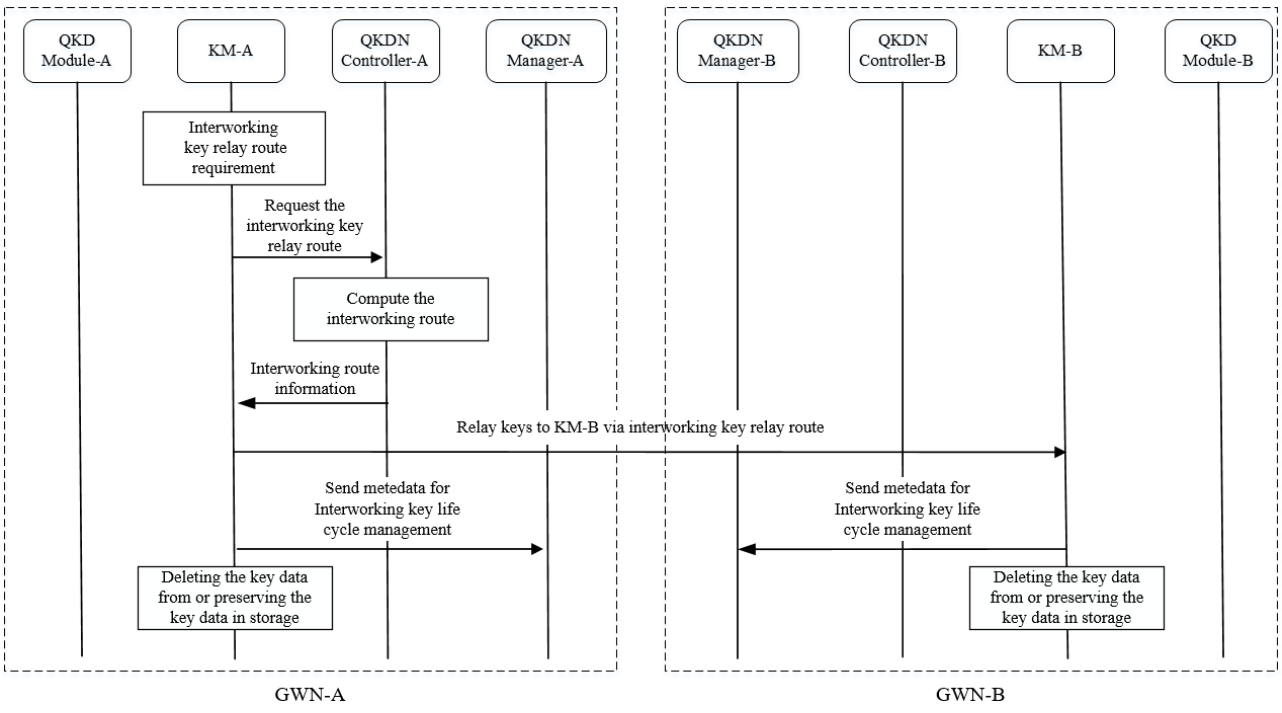

Figure 9 – An example of key relay for interworking between two QKDN providers with GWNs

2) Key generation and rerouting control for interworking

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

Each QKDN controller asks QKD modules, QKD links and KMs for status information of 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 of a QKD link to their controllers. QKDN controller-A and QKDN controller -B analyse the provided information and decide whether the interworking key relay rerouting is necessary or not. Then they share information to change rerouting path simultaneously. After confirming commands of controllers are consistently, they send interworking rerouting information to KM -A and KM-B.

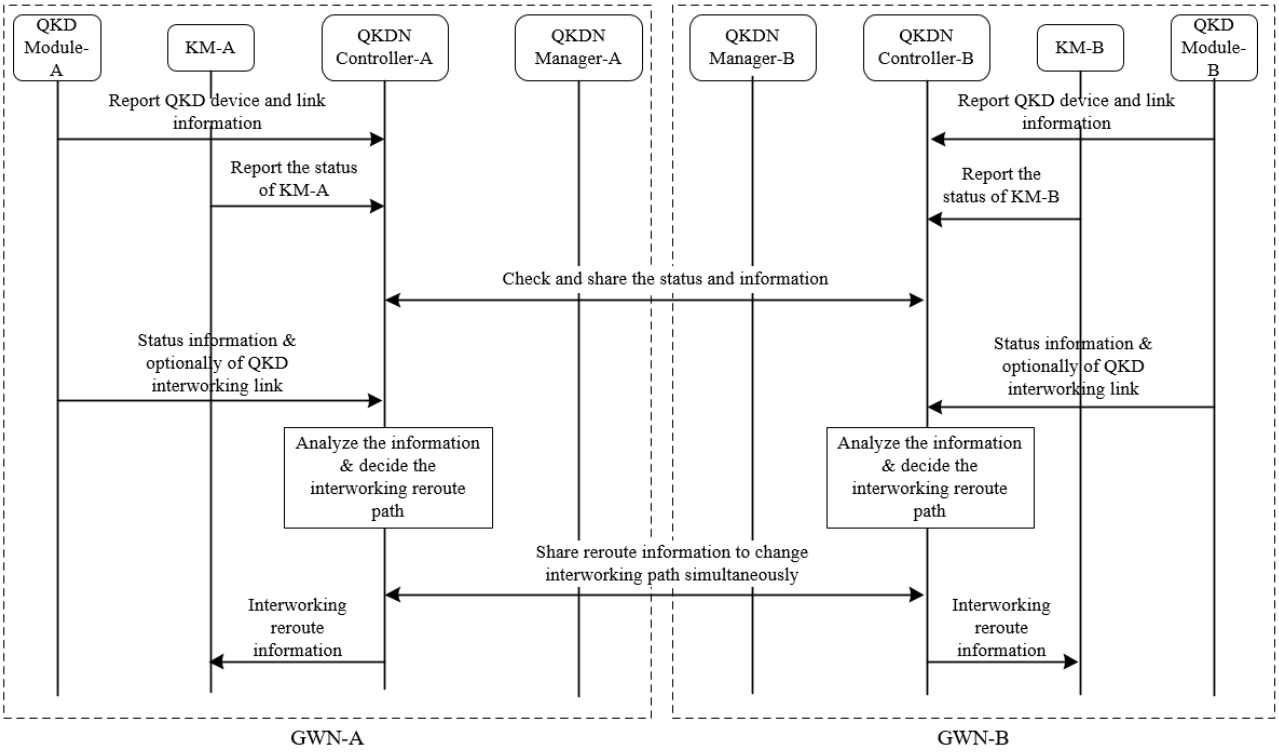

Figure 10 – An example of key generation and rerouting control for interworking between two QKDNs with GWNs

3) Fault management of key relay failure for interworking

Figure 11 shows an example of QKDNi fault management procedure between two QKDNs with GWNs. If interworking relay has something wrong, KMLM-A reports relay failure to XLMO-A, XLMO-A then send it to XLMO-B. XLMO-A and B report interworking relay failure diagnosis information to QCLMs respectively and QCLMs make the next decision.

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

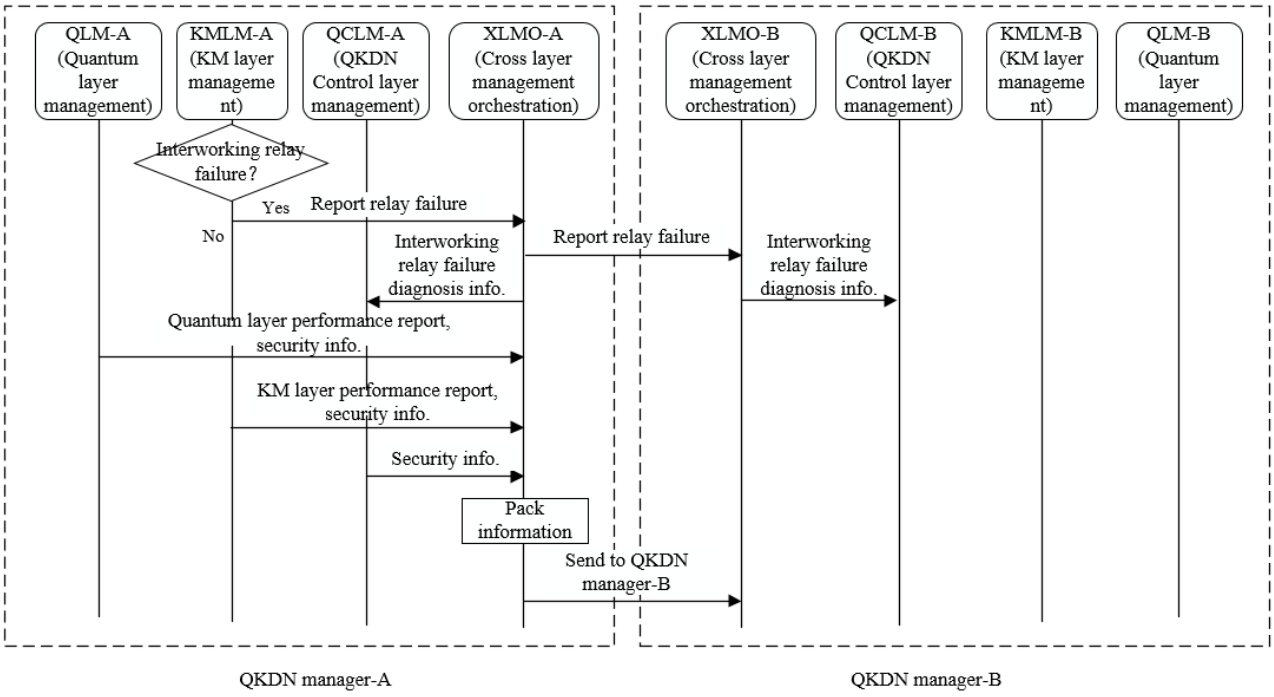

Figure 11 - An example of fault management of key relay failure for interworking between two QKDNs with GWNs

9.2. Operational procedures for QKDNi with IWN

1) Key transfer for interworking

Figure 12 illustrates an example 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 status of key resources between KM-A and KM -B, if keys are enough to be provided, controller-A then determines the transfer link and keys. After receiving message from controller-A, KM-A transfers keys to KM-B via interworking key transfer link. To ensure information synchronization, KM -A and KM -B send metadata for transfer key life cycle management to their controllers, and delete the key data from or preserving the key data in storage.

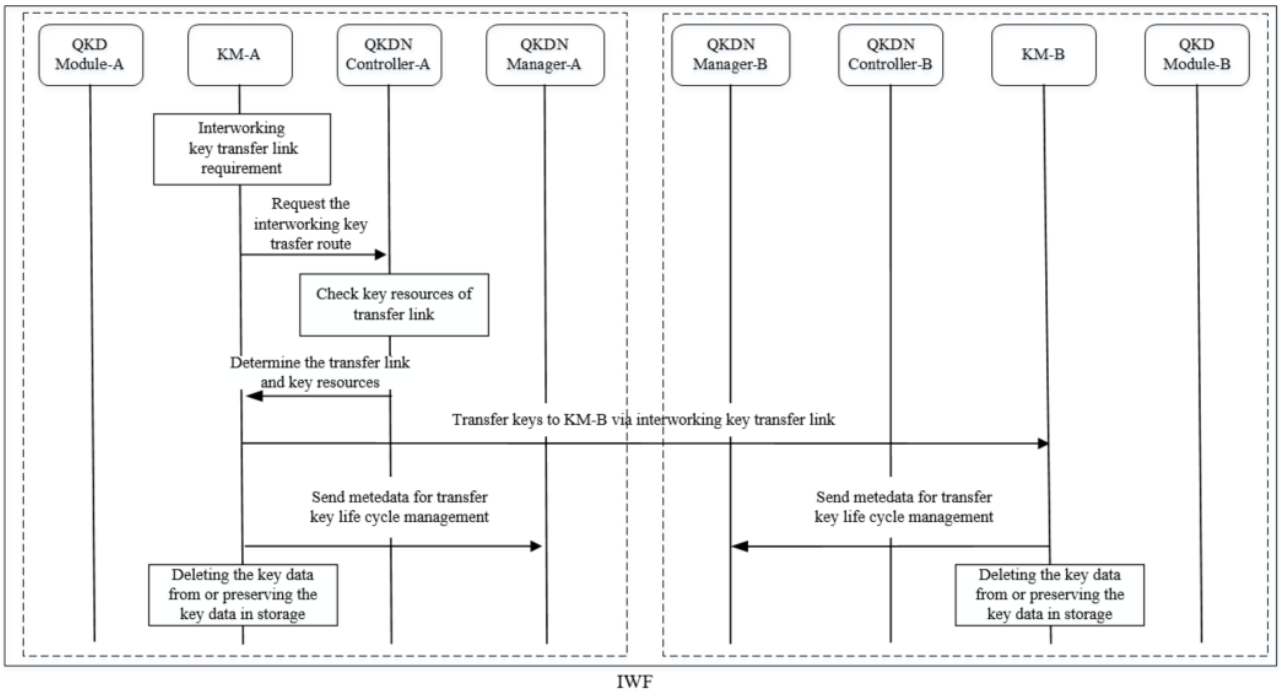

Figure 12 - An example of key transfer for interworking between two QKDNs with IWN

2) Key generation control for interworking

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

This procedure is similar to the procedure shown in Figure 15. Each QKDN controller is responsible for collecting information from QKD module and KM, and shares information to another controller. Differently, when a fault happening, QKDN controller-A and QKDN controller - B receive related information and decide rerouting paths of key transfer.

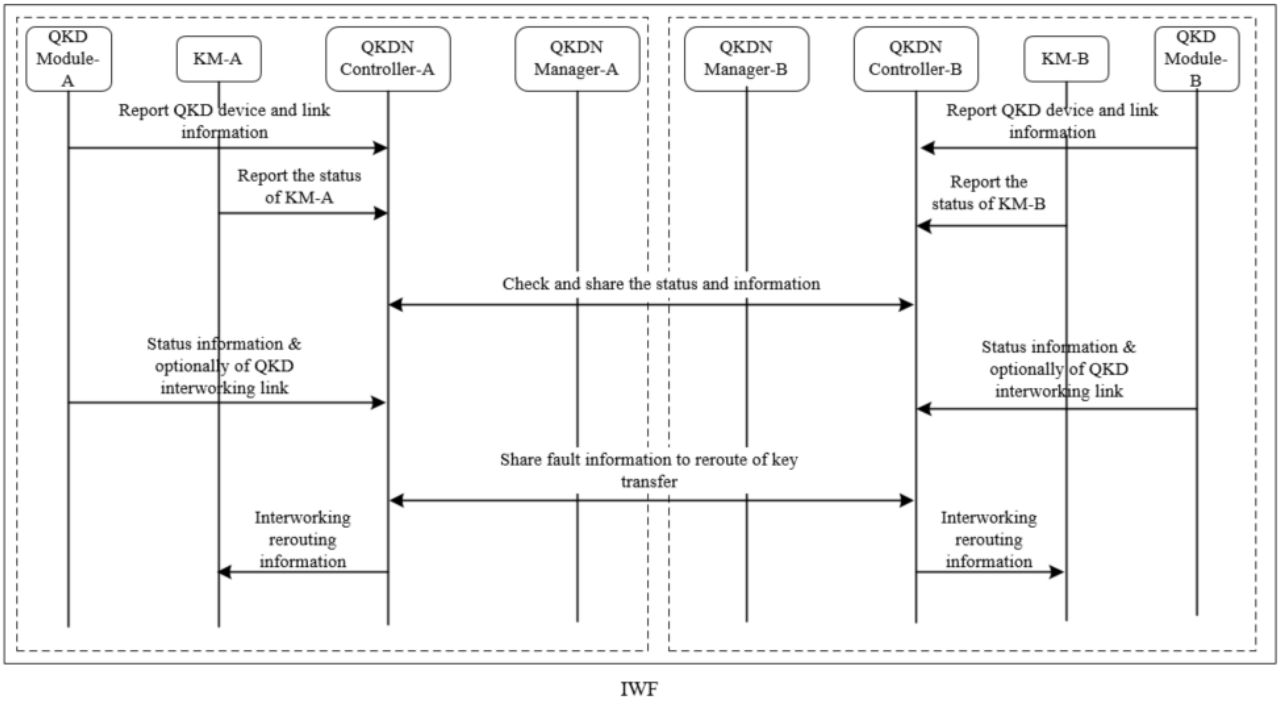

Figure 13 - An example of key generation and rerouting control for interworking between two QKDNs with IWN

3) Fault management of key transfer failure for interworking

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

If interworking key transfer has something problem, KMLM-A reports relay failure to XLMO-A, XLMO-A then sends it to XLMO-B. XLMO-A and B report interworking key transfer failure diagnosis information to QCLMs respectively and QCLMs make the next decision.

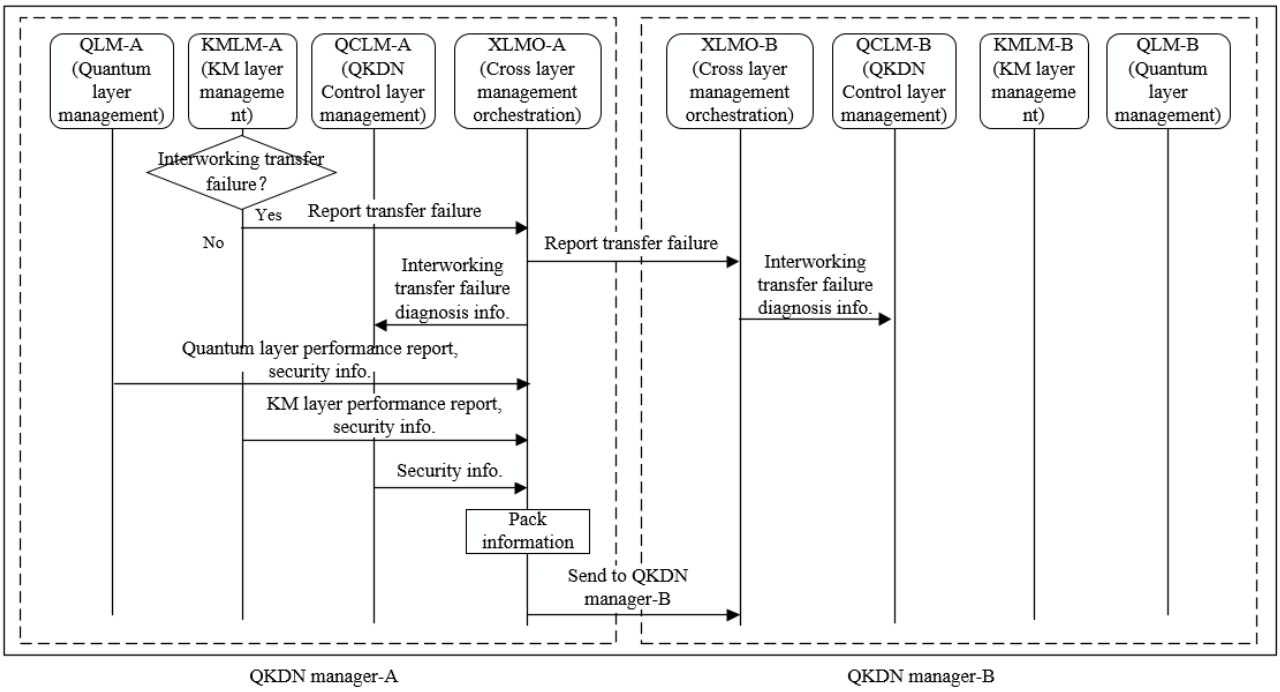

Figure 14 - An example of fault management of key transfer failure for interworking between two QKDNs with IWN

10. Security consideration

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 are outside the scope of this Recommendation.

Bibliography

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

_____