INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2022-2024

SG13-TD232/WP3

STUDY GROUP 13

Original: English

Question(s): 16/13 Geneva, 13 - 24 March 2023

TD

Source: Editors

Title: Draft new Recommendation ITU-T Y.QKDN-iwac "Quantum key distribution networks interworking – architecture"

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 University of Science and Technology Beijing (USTB) China	Tel: +86-10-62332374 E-mail: mazhangchao@ustb.edu.cn
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

Abstract: This document includes the revised draft Recommendation Y.QKDN-iwac "Quantum key distribution networks interworking – architecture"(output of Q16/13 meeting, 13 - 24 March 2023).

Summary

This output document is the updated based on the discussion results of the following contribution in the Q16/13 meeting (Geneva, 13 - 24 March 2023).

Number	Title	Source

C-386	Proposed improvements to ITU-T Y.QKDN-iwac "Quantum key distribution networks interworking - architecture"	BUPT, MIIT, University of Science and Technology Beijing
C-387	Proposal of adding the operational procedures (control layer) for QKDNi with GWF on Draft Recommendation Y.QKDN-iwac	BUPT

- Meeting result

- Regarding the content adjustments made in this proposal, no comments were received during the meeting. Considering the contents need to be improved and supplemented in clause 8, the editors have added some figures and relevant descriptions to specify the basic operational procedures for QKDNi. Simultaneously, these added contents should be improved and discussed in the next meeting, and then try to reach a consensus on this Recommendation before July meeting.

Attachments:

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

Table of Contents

1. Scope 4
2. References 4
3. Definitions 4
3.1. Terms defined elsewhere 4
3.2. Terms defined in this Recommendation 5
4. Abbreviations and acronyms 5
5. Conventions 6
6. Functional architecture for QKDNi 6
6.1. Functional architecture for QKDNi with GWNs 6
6.2. Functional architecture for QKDNi with IWNs 8
7. Functional elements for interworking of QKDNs 9
7.1. Functional elements in GWFs 9
7.2. Functional elements in IWFs 10
8. Basic operational procedures for QKDNi 11
8.1. Operational procedures for QKDNi with GWF 11
8.2. Operational procedures for QKDNi with IWF 14
9. Interworking architectural configurations 15
9.1. Configuration 1: Interworking of distributed QKDNs 15
9.2. Configuration 2: Interworking of a distributed QKDN and a centralized QKDN 18
9.3. Configuration 3: Interworking of centralized QKDNs 20
10. Security consideration 21

Draft new Recommendation ITU-T 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;
- Basic operational procedures for QKDNi;
- Interworking architectural configurations.

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.3810] draft Recommendation ITU-T Y.QKDN_iwfr, *Quantum Key Distribution Networks – interworking framework*~~

~~[ITU-T Y.QKDN_iwrq] draft Recommendation ITU-T Y.QKDN_iwrq, *Quantum Key Distribution Networks – interworking requirements*~~

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

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

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

[ITU-T Y.3809] Recommendation ITU-T Y.3809 (2022), *A role-based model in quantum key distribution networks deployment*

[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*

Formatted: Justified, Indent: Left: 0", First line: 0", Tab stops: Not at 1.18"

Formatted: Font: (Asian) Chinese (Simplified, Mainland China), (Other) English (United States)

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:

AES	Advanced Encryption Standard
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
OTP	One-time pad encryption

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 GWFs and IWFs for QKDNi is addressed in [ITU-T Y.3810]. Moreover, QKDN interworking functional requirements are identified in [ITU-T Y.3813] ~~[ITU-T Y.QKDN-iwrq]~~.

Based on the conceptual models on QKDNi illustrated in [ITU-T Y.3810] and the QKDNi functional requirements identified in [ITU-T Y.3813] ~~[ITU-T Y.QKDN-iwrq]~~, two functional architectures for QKDNi with GWNs and IWNs are shown in Figure 1 and 2, respectively.

6.1. Functional architecture for QKDNi with GWNs

~~*Editor's note – Some descriptions in clauses 6.1 and 6.2 should be revised to keep in line with [ITU-T Y.3810].*~~

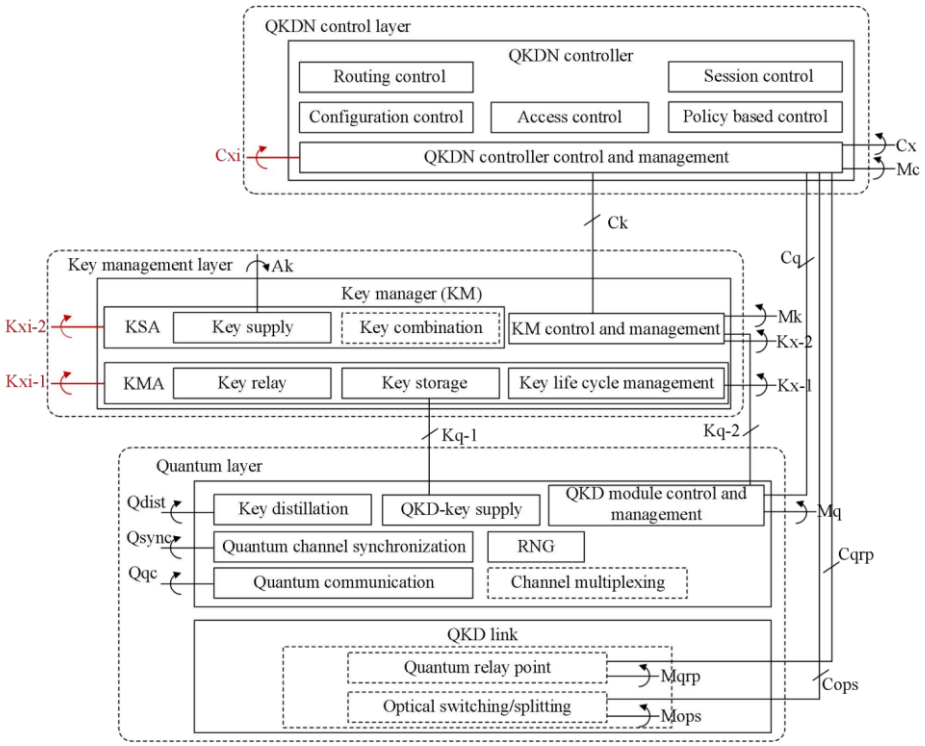


Figure 1 - A functional architecture for QKDNi with GWNs

The functional model for QKDNi with GWNs has been defined in [ITU-T Y.3810], and the layer structure for QKDN 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 QKD module are defined in [ITU-T Y.3802].

– Key management layer: The functional elements in the key management layer including key management agent (KMA) and key supply agent (KSA) have been defined in [ITU-T Y.3802]. Keys can be relayed between GWNs through key management layer, and KM can also exchange control and management messages with the key relay among different QKDN providers.

– 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 each QKDN according to policies of each service provider.

NOTE – Service layer, QKDN management layer and user network management layer are ~~the same as that~~ described in [ITU-T Y.3802].

Most of the reference points in Figure 1 have been defined in [ITU-T Y.3802], some reference points for QKDNi with GWF have been defined in [ITU-T Y.3810], and this Recommendation defines the new reference points in GWN~~ly added one and presents the existing ones related to QKDNi with GWNs~~.

The newly added reference point is:

– **Kx-1**: a reference point connecting two KMAs in each GWN via an interworking KMA link. It is responsible for exchanging information and operations required for key relay, key synchronization and authentication between different QKDN providers.

– **Kx-2**: a reference point connecting two KSAs in each GWN via an interworking KSA link. It is responsible for exchanging information and operations required for synchronization and authentication of the keys shared between different QKDN providers.

6.2. Functional architecture for QKDNi with IWNs

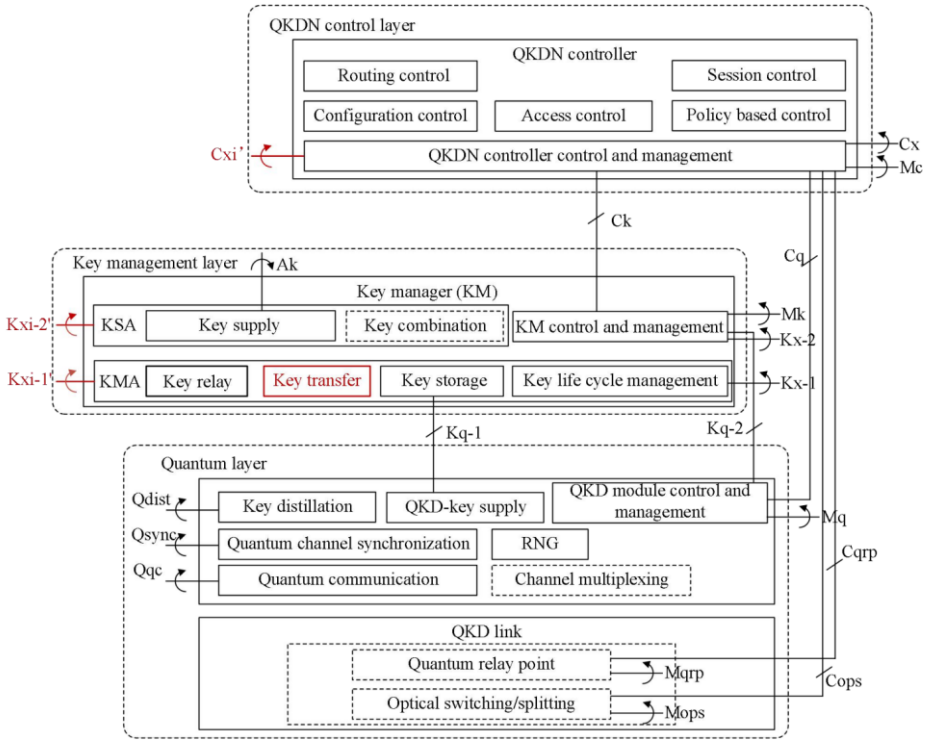


Figure 2 - A functional architecture for QKDNi with IWNs

The functional model for QKDNi with IWNs has been defined in [ITU-T Y.3810], and layer structure for QKDN 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 are the same as GWN.

NOTE – There is no Qx between two IWNs.

– Key management layer: the functional elements in the key management layer are the same as GWN. However, keys can be transferred between QKDN providers through key management layer instead of being relayed.

– QKDN control layer: the functional element in the QKDN control layer is the same as GWN.

Most of the reference points in Figure 1 have been defined in [ITU-T Y.3802], some reference points for QKDNi with GWF have been defined in [ITU-T Y.3810], and this Recommendation defines the newly added one and presents the existing ones related to QKDNi with GWNs.

The newly added reference point is:

– **Kx-1'**: a reference point connecting two KMAs in each IWN via an interworking KMA link. It is responsible for exchanging information and operations required for key transfer, key synchronization and authentication between different QKDN providers.

– **Kx-2'**: a reference point connecting two KSAs in each GWN via an interworking KSA link. It is responsible for exchanging information and operations required for synchronization and authentication of the keys shared between different QKDN providers.

7. Functional elements for interworking of QKDNs

~~*Editor's note – This clause is removed from [ITU-T Y.QKDN-iwrq], and it will be discussed further.*~~

7.1. Functional elements in GWFs

A GWF is to support interworking interfaces between ~~two different~~ QKDNs~~, and to support information can be shared with common protocol~~. The GWF is located ~~in~~ at the border of each QKDN provider and it consists of a KM, some QKD modules, and/or a QKDN controller. In addition, a Cxi, Kxi and Qx are connecting between two GWFs. These are further comprised of the following functional elements:

- Unified authentication function: It authenticates the keys shared between ~~end-to-end GFs~~QKDNs through Kxi;

- Interworking key relay function: It relays the keys ~~from end-to-end GFs~~ between two QKDNs ~~providers~~ through Kxi in a highly secure manner with an IT-secure encryption~~, i.e. one-time pad (OTP) [b-Shannon 1949] is recommended~~;

- Interworking session control function: It supports ~~respective~~ KMAs, and controls the session procedures of interworking key relay;

- Interworking routing control function: It provisions an appropriate key relay route between ~~two end-to-end GFs~~QKDNs, and also performs rerouting of key relay via sharing fault, performance, and/or availability status of respective quantum layer and/or respective key management layer;

- Interworking policy based control function: It shares ~~respective~~ QKDN resources based on the quality of service (QoS) between ~~end-to-end GFs~~QKDNs through Cxi with encryption;

- Interworking fault management function: It supports the QKDN controller for the routing and rerouting control of key relay between ~~two end-to-end GFs as needed in case of the faults~~QKDNs;

- Interworking configuration management function: It shares the provisioning of QKDN resources, collects and manages QKDN topology. It also supports the QKDN controller for the provisioning of key relay routes between two end-to-end GFs if QKDN supports key relay;

- Interworking 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 ~~two~~ QKDN ~~providerss~~;

- Interworking performance management function: It monitors and analyses the performance status of the QKDN managed resources, and shares related information with encryption between ~~two~~ QKDN ~~providers~~s;

- Interworking security management function: It collects/receives security related management information from the QKDN, and shares related information with encryption between ~~two QKDN providers~~QKDNs;

~~- Protocol conversion function: It performs to convert the internal protocol in a QKDN to the common protocol for interworking of QKDNs.~~

7.2. Functional elements in IWFs

An IWF is installed in a trusted node other than inside of the QKDN which interworks.~~, and it consists multiple GFs. These are further comprised of the following functional elements:~~

~~NOTE 1 – Interworking of QKDNs have different control scheme. In the case of interworking of distributed QKDNs, QKDN controller is located in IWF. In the case of interworking of a distributed QKDN and a centralized QKDN, QKDN controller can be located in IWF or QKDN A/B. In the case of interworking of centralized QKDNs, QKDN controller is located in QKDN A/B.~~

- Unified authentication function: It authenticates the keys shared between ~~two different QKDN~~QKDNs ~~providers via two internal GFs interfaces~~via Kxi' in IWF;

- Interworking key transfer function: It transfers the keys ~~via~~ between two ~~internal GFs interfaces Kxi' in IWF between two QKDN providers without encryption~~QKDNs;

~~- Interworking session control function: It supports respective KMAs, and controls the session procedures of interworking key relay;~~

- Interworking routing control function: It provisions an appropriate key transfer route between ~~two internal GFs in IWF~~QKDNs, and also performs rerouting of key transfer via sharing fault, performance, and/or availability status of respective quantum layer and/or respective key management layer;

~~- Interworking policy based control function: It shares respective QKDN resources based on the quality of service (QoS) between two internal GFs in IWF through Cxi' without encryption;~~

- Interworking fault management function: It supports the QKDN controller for the routing and rerouting control of key transfer between ~~two internal GFs in IWF as needed in case of the faults~~QKDNs;~~.~~

- Interworking configuration management function: ~~It shares the provisioning of QKDN resources, collects and manages QKDN topology.~~ It ~~also~~ supports the QKDN controller for the provisioning of key transfer routes ~~between two internal GFs in IWF if QKDN supports key transfer~~QKDNs.

~~- Interworking 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 two QKDN providers;~~

~~- Interworking performance management function: It monitors and analyses the performance status of the QKDN managed resources, and shares related information without encryption between two QKDN providers.~~

~~- Interworking security management function: It collects/receives security related management information from the QKDN, and shares related information without encryption between two QKDN providers.~~

~~- Protocol conversion function: It performs to convert the internal protocol in a QKDN to the common protocol for interworking of QKDNs.~~

8. Basic operational procedures for QKDNi

~~8.~~ *Editor's note – The figures and relevant descriptions in clause 8 should be further updated to be consistent with [ITU-T Y.3810] and [ITU-T Y.3813].*

Formatted: Font: Italic

Formatted: Normal, No bullets or numbering

Formatted: Font:

8.1. Operational procedures for QKDNi with GWF

1) Operational procedures for QKDNi with GWF in key management layer

Figure 3 illustrates the procedure of interworking key relay between two QKDN providers with GWNs. In this phase, when GWN-A receives an interworking key relay route requirement, KM-A firstly requests QKDN controller-A the interworking key relay route, controller-A then computes an interworking key relay route and sends interworking route information to KM-A. Finally, KM-A executes the interworking key relay.

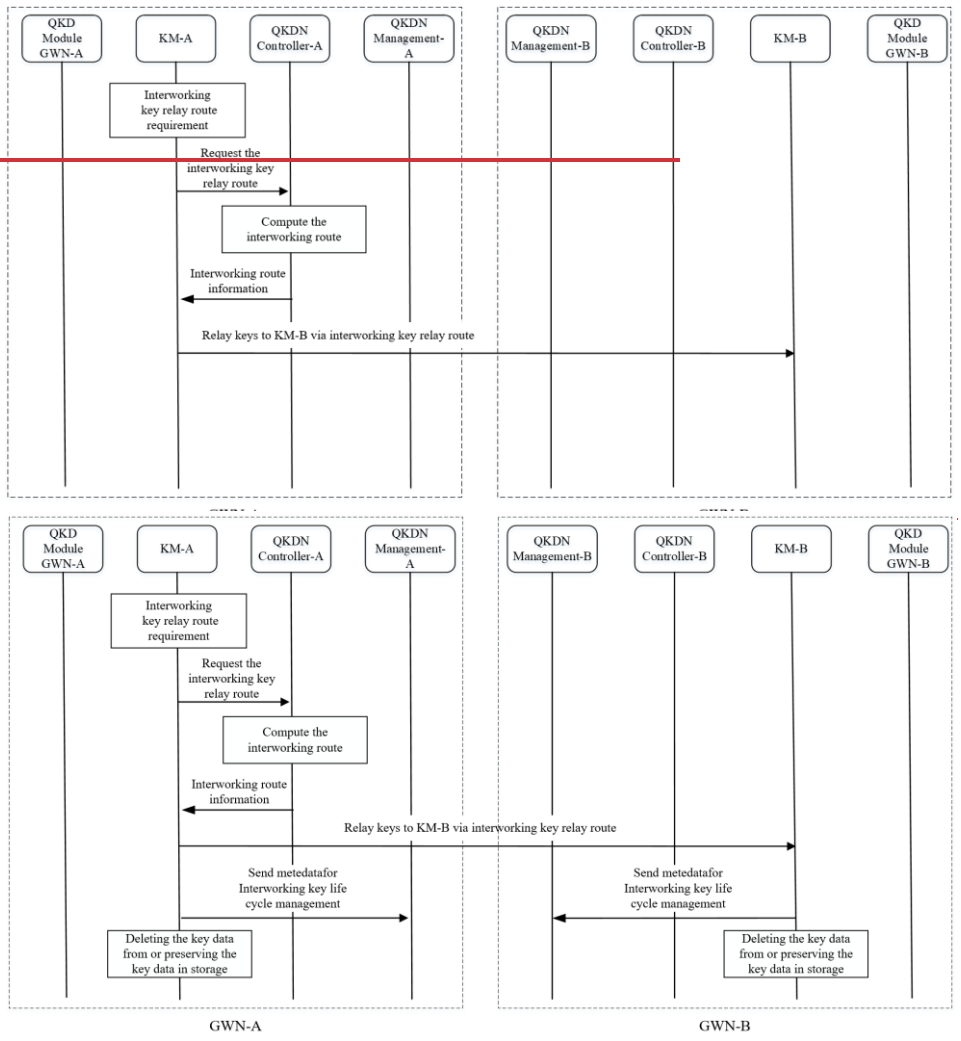


Figure 3. Interworking key relay between two QKDN providers with GWNs

2) Operational procedures for QKDNi with GWF in QKDN control layer

Figure 4 illustrates the operational procedures for QKDNi with GWF in QKDN control layer. This procedure describes interworking key generation and rerouting control.

Before interworking key generation, controller-A and controller -B firstly establish pre-connection to ensure share or exchange follow-up information successfully. Then controllers requests QKD modules respectively to initiate key generation and the modules push up the generated interworking keys to KM-A and KM-B. The KMs report the status of interworking key generation to their controllers respectively. Finally, controller-A and controller-B check and share the status of key generation.

To the interworking key rerouting, QKD modules send status information and optionally of a QKD link to their controllers. Controller-A and controller-B analyse the provided information and decides whether the rerouting of interworking key relay 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.

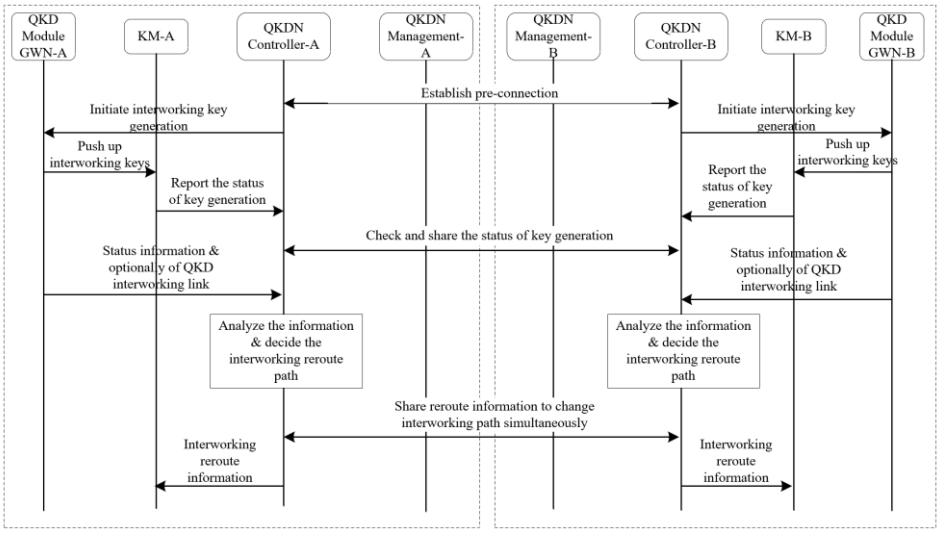


Figure 4. Control procedures between two QKDNs with GWNs~~TBD~~

Formatted: Centered

3) Operational procedures for QKDNi with GWF in QKDN management layer

An example of fault management procedures for key relay failure is shown. KM layer management in QKDN manager-A reports KM relay failure to cross layer management, and the cross layer management then sends KM relay failure diagnosis information to control layer management to let it decide control actions. Controller layer management in QKDN-A sends relay failure information to controller layer management in QKDN-B. If there are relevant KMs involved, controller layer management (QKDN-B) will notify controller-B to solve the failure.

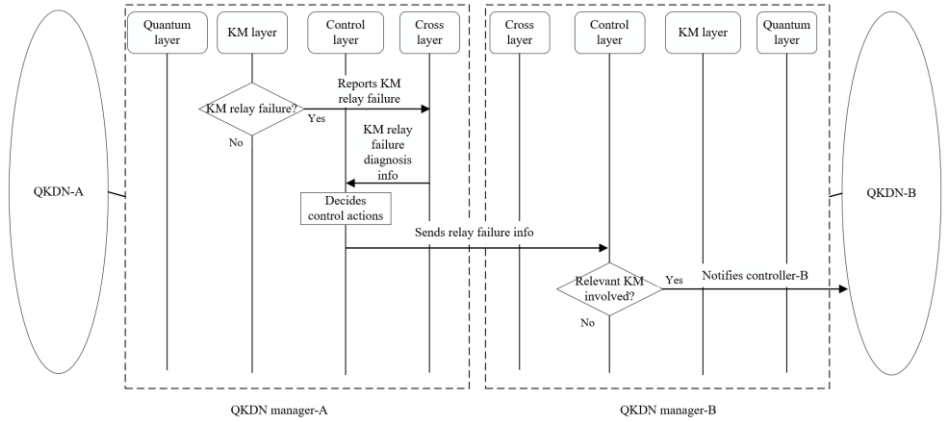


Figure 5. QKDNi management procedures between two QKDNs with GWNs~~TBD~~

Formatted: Centered

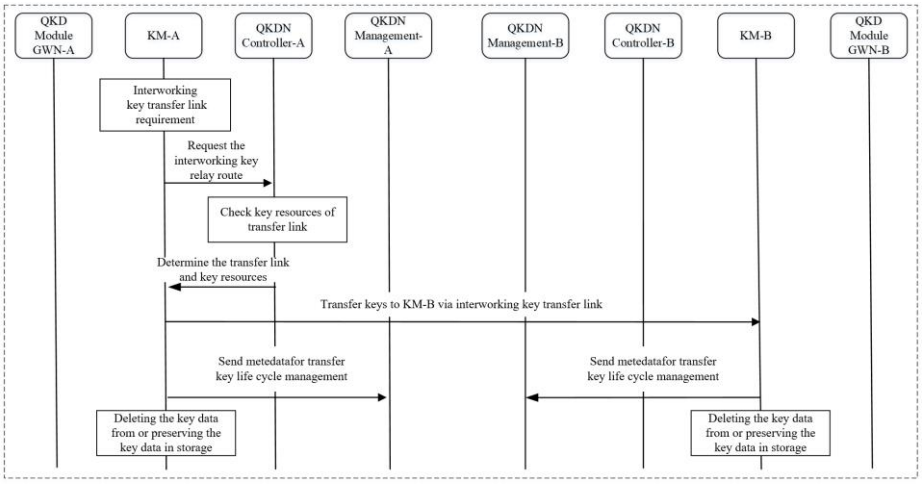
8.2. Operational procedures for QKDNi with IWF

1) Operational procedures for QKDNi with IWF in key management layer

KM-A firstly receives an interworking key transfer link requirement and sends it to QKDN controller-A. Controller-A checks status of key resources on transfer link between KM-A and KM-B, if key resources are enough to be provided, controller-A then determine the transfer link and keys. After receiving massage 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.

Formatted: Font:

Formatted: Normal, No bullets or numbering



~~2)~~ Figure 6. Interworking key relay between two QKDN providers with IWNs~~Figure 3~~

Formatted: Normal, Centered, No bullets or numbering

~~3)~~2) Operational procedures for QKDNi with IWF in QKDN control layer

~~TBD~~This procedure is mainly about key generation. QKDN controller-A and controller-B establish pre-connection before communication, then they respectively initiate transfer key generation. QKD modules push up transfer keys to KMs, and KM-A and KM-B report the status of transfer key generation. Finally, two controllers check and share the status of transfer key generation.

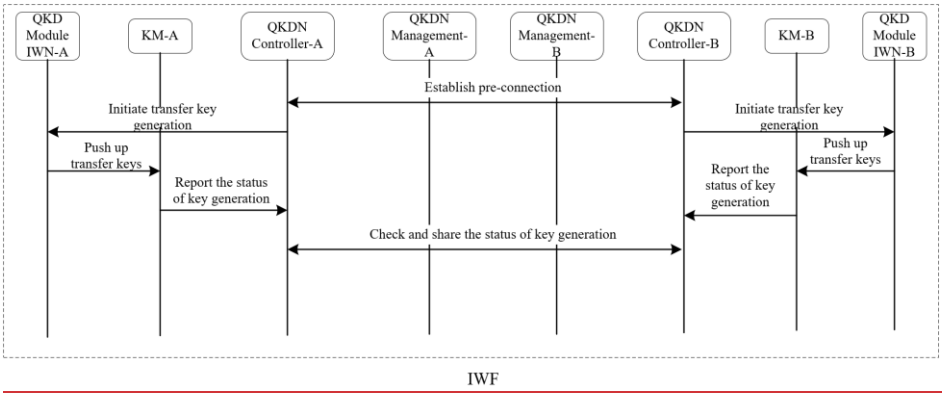
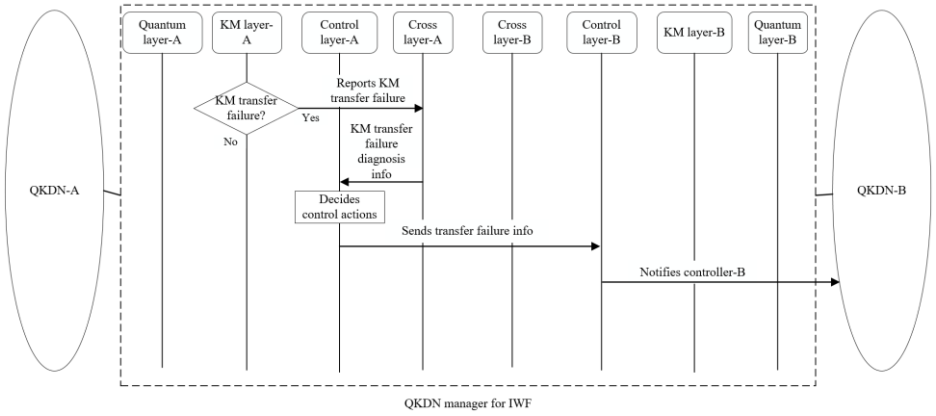


Figure 7. QKDNi management procedures between two QKDNs with IWNs

4)3) Operational procedures for QKDNi with IWF in QKDN management layer

An example of fault management procedures for key transfer failure is shown. KM layer management-A reports KM transfer failure to cross layer management-A, and the cross layer management-A then sends KM transfer failure diagnosis information to control layer management-A to let it decide control actions. Controller layer management-A sends relay failure information to controller layer management-B and then controller layer management-B will notify controller-B to solve the transfer failure.



5) Figure 8. QKDNi management procedures between two QKDNs with IWNsTBD

9. Interworking architectural configurations

Editor's note – The figures in clause 9 should be revised to be consistent with [ITU-T Y.3810].

9.1. Configuration 1: Interworking of distributed QKDNs

Figure 93 shows the functional models of distributed QKDNs. Key relay is performed in the IWN. In this case, QKD module-A and QKD module-B interact with KM interworking-A and KM interworking-B respectively, because of their protocol difference and each KM interworking function interact with respective QKDN controller interworking function. The reference point

Formatted: Centered

Formatted: Font:

Formatted: Normal, No bullets or numbering

Formatted: Normal, Centered, No bullets or numbering

Cxi' and Kxi' in the IWN are internal interfaces for Cxi and Kxi.

In this figure, Cq interface between QKD module and QKDN controller in the IWN is not described in order to avoid complexity.

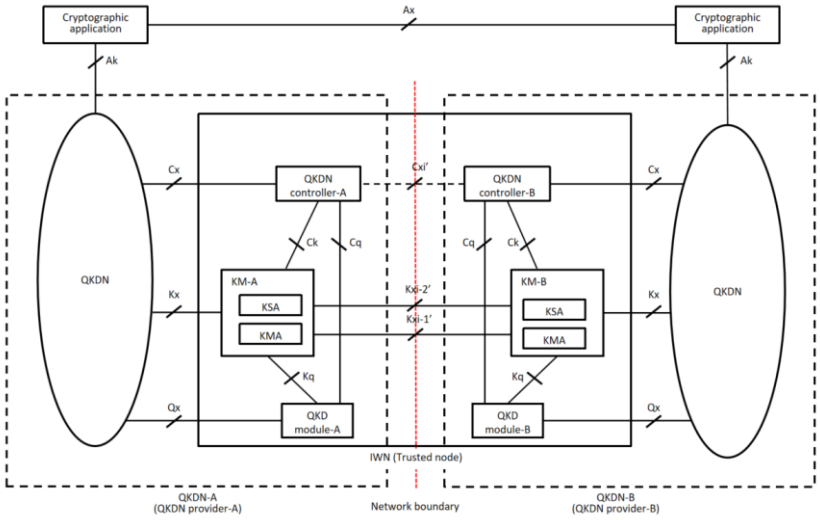


Figure 94 - Interworking of distributed QKDNs

A single QKDN controller interworking function controls both KM interworking-A and KM interworking-B by interacting respectively as shown in figure 104.

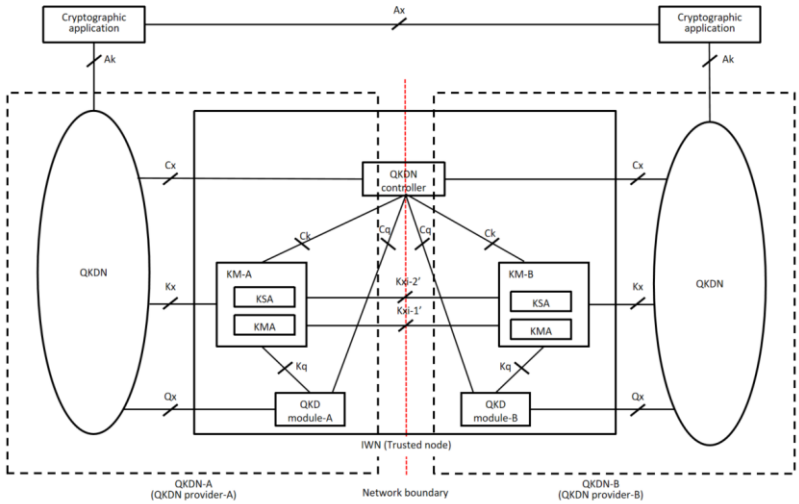


Figure 10~~5~~ - Interworking of distributed QKDNs with unified QKDNi controller

In figure ~~5~~11, a single KM interworking function interacts with both QKD module-A and QKD module-B for key relay, while in ~~scenario~~ Figure ~~4~~10, two KM interworking functions involve. ~~QKDN controller interworking-A and -B have individual control on KM interworking function and a single KM interworking function is involved in key relay between QKDN A and QKDN B as shown in Figure 5.~~QKDN controller interworking-A and -B have individual control on KM interworking function, and a single KM interworking function is involved in key relay between QKDN A and QKDN B as shown in Figure 11.

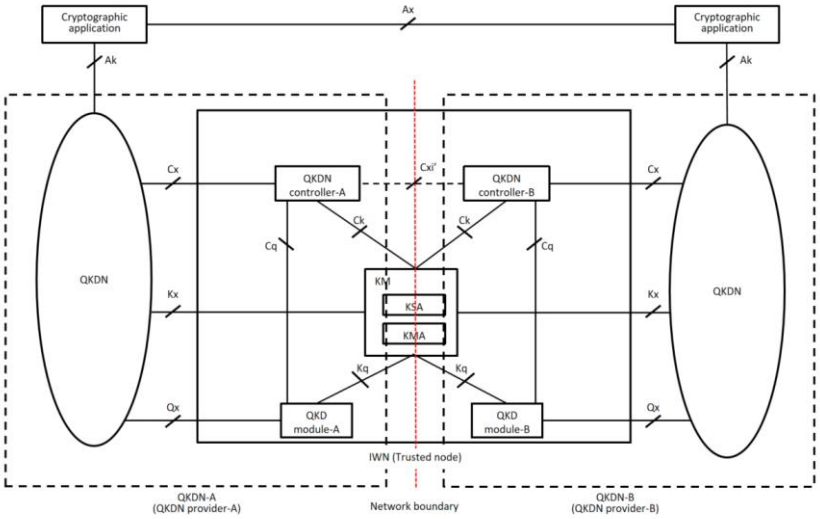


Figure 11~~6~~ - Interworking of distributed QKDNs with unified QKDNi KM

In Figure 12~~4~~, both QKDN controller interworking function and KM interworking function are unified. A QKDNi controller function controls a QKDNi KM function and the information from QKDN A and QKDN B, and a single QKDNi KM function is involved in the key relay between QKD module-A and QKD module-B. In this case, an IWN is the same structure with a QKD node.

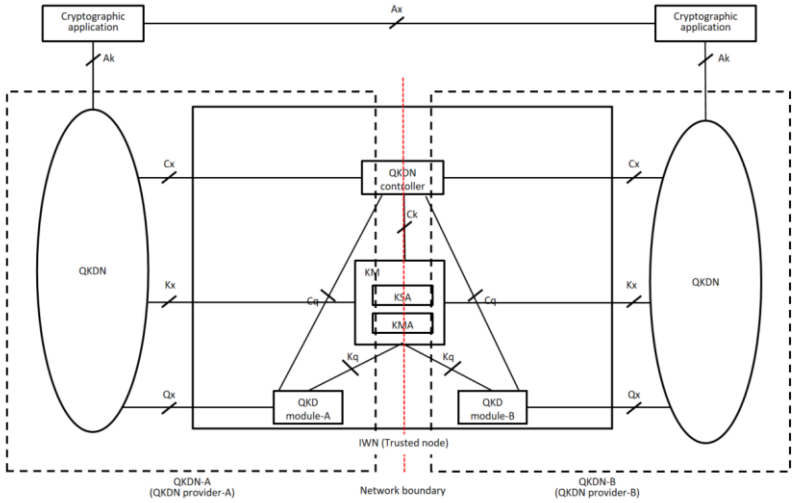


Figure 12~~7~~ - Interworking of distributed QKDNs with unified QKDNi controller and QKDNi KM

9.2. Configuration 2: Interworking of a distributed QKDN and a centralized QKDN

In the case of interworking of a distributed QKDN and a centralized QKDN, the networks are connected inside of the trusted node to perform key relays. And there is no connection between QKD modules and the keys are transferred to the KM in unencrypted form.

Figure ~~5~~ 13 illustrates key relay model within the IWN between a distributed QKDN and a centralized QKDN.

Figure ~~7~~ 13 shows the functional model for interworking with distributed QKDN and a centralized QKDN, and key relay is performed in the IWN. ~~-~~In this case, QKD module-A and QKD module-B interact with KM interworking-A and KM interworking-B respectively because of their protocol difference. 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 interworking.

In this figure, Cq interface between QKD module and QKDN controller in the IWN is not described in order to avoid the complexity.

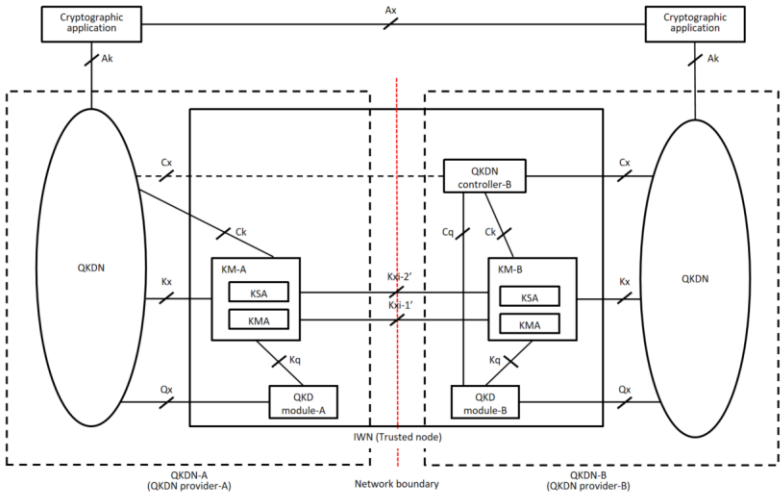


Figure 13~~8~~ - Interworking of a distributed QKDN and a centralized QKDN

Figure 14 illustrates the model with unified KM interworking function and with centralized QKDN B, which has sole control of QKDN controller. As shown in the figure, KM interworking function in the IWN is controlled only by QKDN B.

Formatted: English (United States)

Formatted: English (United States)

Formatted: Left, Indent: Left: 0.1", Right: 0.08", Space After: 6 pt, Line spacing: Multiple 1.1 li, No widow/orphan control

Formatted: English (United States)

Formatted: English (United States)

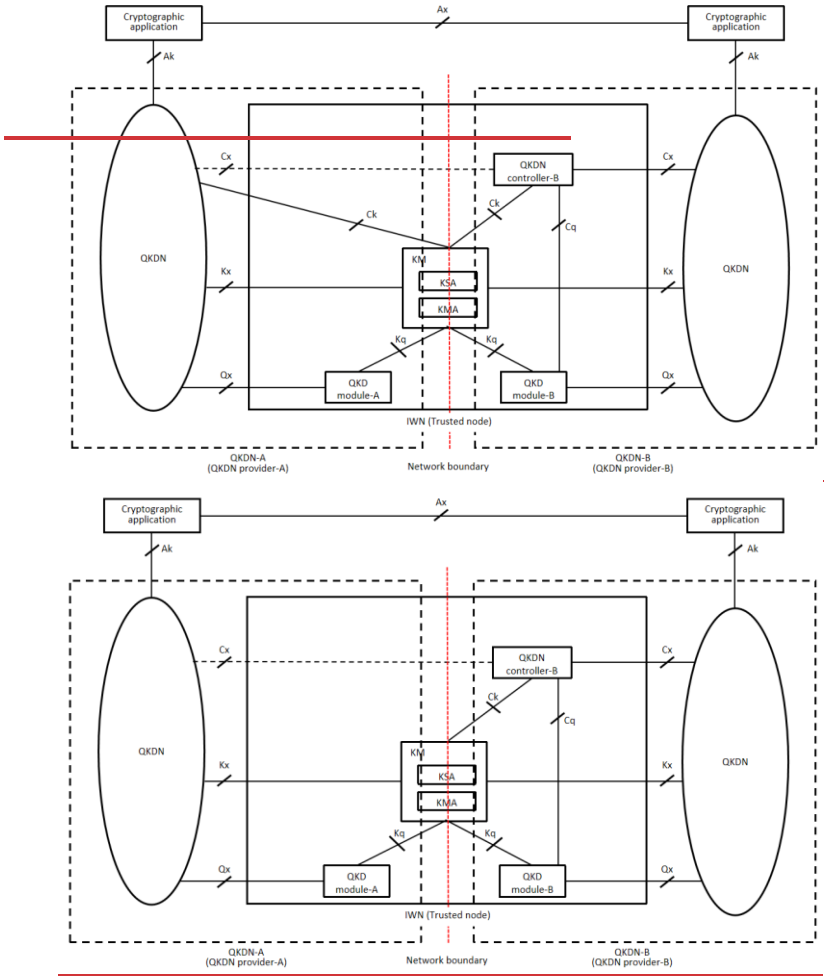


Figure 14~~9~~ - Interworking of a distributed QKDN and a centralized QKDN

9.3. Configuration 3: Interworking of centralized QKDNs

Figure ~~9~~ 15~~0~~ illustrates the functional model of centralized QKDNs and key relay is performed in the IWN. In this case, QKD module-A and QKD module-B interact with KM interworking-A and KM interworking-B respectively, because of their protocol difference. Since both QKDN A and QKDN B are centralized, KM interworking function-A interacts with QKDN controller-A, and KM interworking function-B interacts with QKDN controller-B interworking.

In this figure, Cq interface between QKD module and QKDN controller in interworking QKD node is not described in order to avoid the complexity.

Formatted: Not Highlight

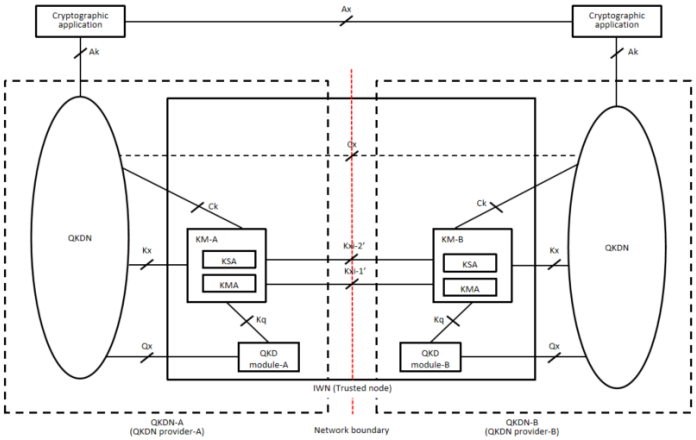


Figure 15~~0~~ - Interworking of centralized QKDNs

Figure ~~10~~ 16 illustrates the model with unified KM interworking function and with centralized QKDN A which has sole control of QKDN controller. As shown in the figure, KM interworking function in the IWN is controlled only by QKDN A.

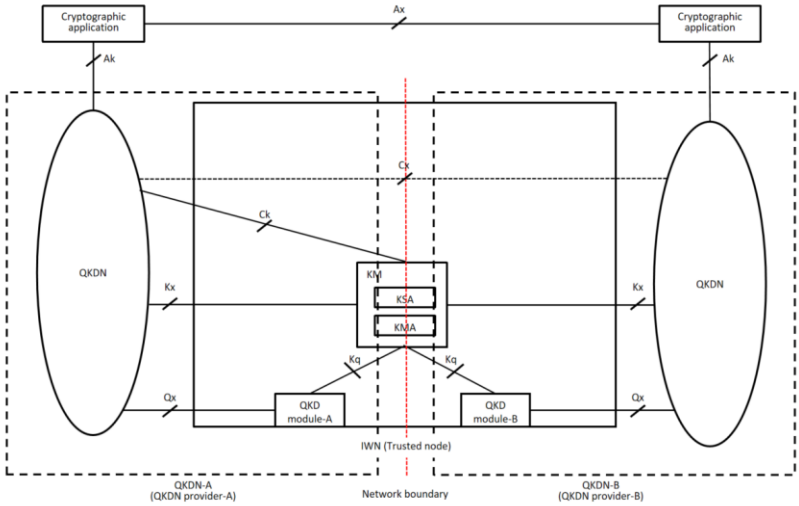


Figure 16~~1~~ - Interworking of centralized QKDNs

10. Security consideration

In order 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.

Formatted: Normal, Indent: Left: 0.3", No bullets or numbering

~~To be added.~~

Bibliography

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

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

[b-ITU-T Y.3804] Recommendation ITU-T Y.3804 (2020), *Quantum key distribution networks – Control and management*