INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2022-2024

SG13-TD44/WP3

STUDY GROUP 13

Original: English

Question(s): 16/13 Geneva, 4 -15 July 2022

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 CAS Quantum Network Co., Ltd. China	Tel: +86-10-83057625 E-mail: mazhangchao@casquantumnet.com
Contact:	Junsen Lai 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 a proposed new work item Y.QKDN-iwac “Quantum key distribution networks interworking – architecture”

Draft A.1 justification for a work item and proposed initial texts are attached as Annex A and B respectively.

Annex A:

A.1 Justification for proposed draft new recommendation

Question:	16/13	**Proposed new ITU-T Recommendation**	Geneva, 4 - 16 July 2022
Reference and title:	ITU-T Y.QKDN- iwac “Quantum key distribution networks interworking – architecture”		
Base text:	SG13-TD44/WP3	**Timing:**	2023-12
Editor(s):	Yazi Wang, BUPT China Yongli Zhao, BUPT China Xiaosong Yu, BUPT China Zhangchao Ma, CAS Quantum Network Co., Ltd. China Junsen Lai, MIIT China Dong-Hi SIM, SK Telecom Korea (Rep. of)	**Approval process:**	AAP

Scope (defines the intent or object of the Recommendation and the aspects covered, thereby indicating the limits of its applicability):

This Recommendation specifies functional architecture for QKDNi. In particular, the scope of this Recommendation includes the following aspects for QKDNi:

- Functional architecture for QKDNi;
- Functional elements for QKDNi;
- Basic operational procedures for QKDNi

Summary (provides a brief overview of the purpose and contents of the Recommendation, thus permitting readers to judge its usefulness for their work):

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 Inter Working Functions (IWFs) for QKDNi is addressed in [ITU-T Y.QKDN-iwfr]. Moreover, QKDN interworking functional requirements are identified in [ITU-T Y.QKDN-iwrq].

Based on the conceptual models on QKDNi illustrated in [ITU-T Y.QKDN-iwfr] and the QKDNi functional requirements identified in [ITU-T Y.QKDN-iwrq], a functional architecture on QKDNi is shown in this document.

Relations to ITU-T Recommendations or to other standards (approved or under development):

This WI will refer to the QKDN Recommendations such as ITU-T Recommendation Y.3800, Y.3801, Y.3802, Y.3803, Y.3804 and X.1710.

The proposed new WI will be studied in a harmonious manner with existing and ongoing works in ITU-T and other SDOs but there are no duplications identified so far. ITU-T SG13 Y.QKDN-iwfr “Quantum key distribution networks interworking - framework” and Y.QKDN-iwrq “Quantum key distribution networks interworking - requirements”.

Liaisons with other study groups or with other standards bodies:

ITU-T SG11 and SG17, ETSI ISG QKD

Supporting members that are committing to contributing actively to the work item:

Beijing University of Posts and Telecommunications, China; CAS Quantum Network Co. Ltd., China; QuantumCTek Co., Ltd., China; Ministry of Industry and Information Technology (MIIT), China, SK Telecom.

Annex B

Draft Recommendation ITU-T 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 for QKDNi.

Keywords

QKD, QKDN (QKD network), interworking

Table of Contents

Draft Recommendation ITU-T Y.QKDN-iwac

Quantum key distribution networks interworking – architectures

1. Scope

This Recommendation specifies functional architectures for 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

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.QKDN_iwfr] 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*

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 Gateway Functions (GWFs) and Inter Working Functions (IWFs) for QKDNi is addressed in [ITU-T Y.QKDN-iwfr]. Moreover, QKDN interworking functional requirements are identified in [ITU-T Y.QKDN-iwrq].

Based on the conceptual models on QKDNi illustrated in [ITU-T Y.QKDN-iwfr] and the QKDNi functional requirements identified in [ITU-T Y.QKDN-iwrq], two functional architectures of QKDNi in two functions are shown in Figure 1 and 2.

6.1. Functional architecture for QKDNi with GWNs

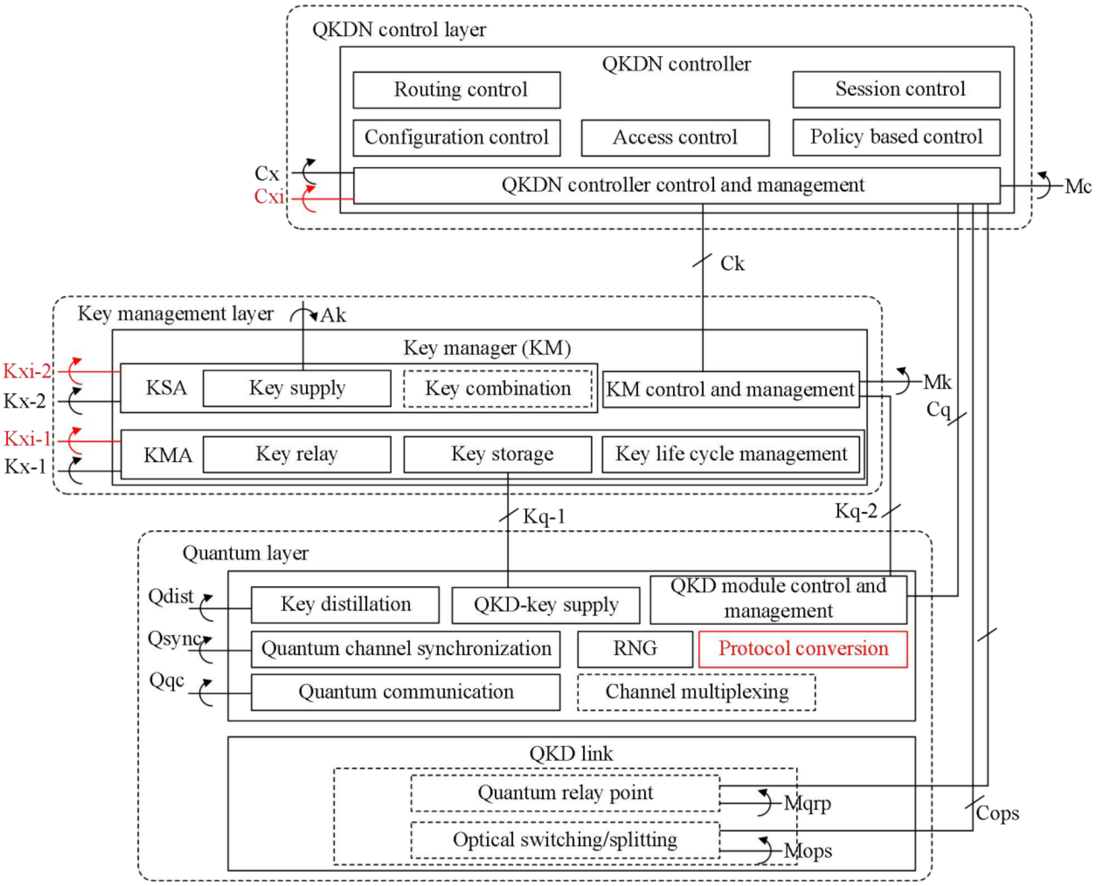

Figure 1 - A functional architecture for QKDNi with GWNs

6.2. Functional architecture for QKDNi with IWNs

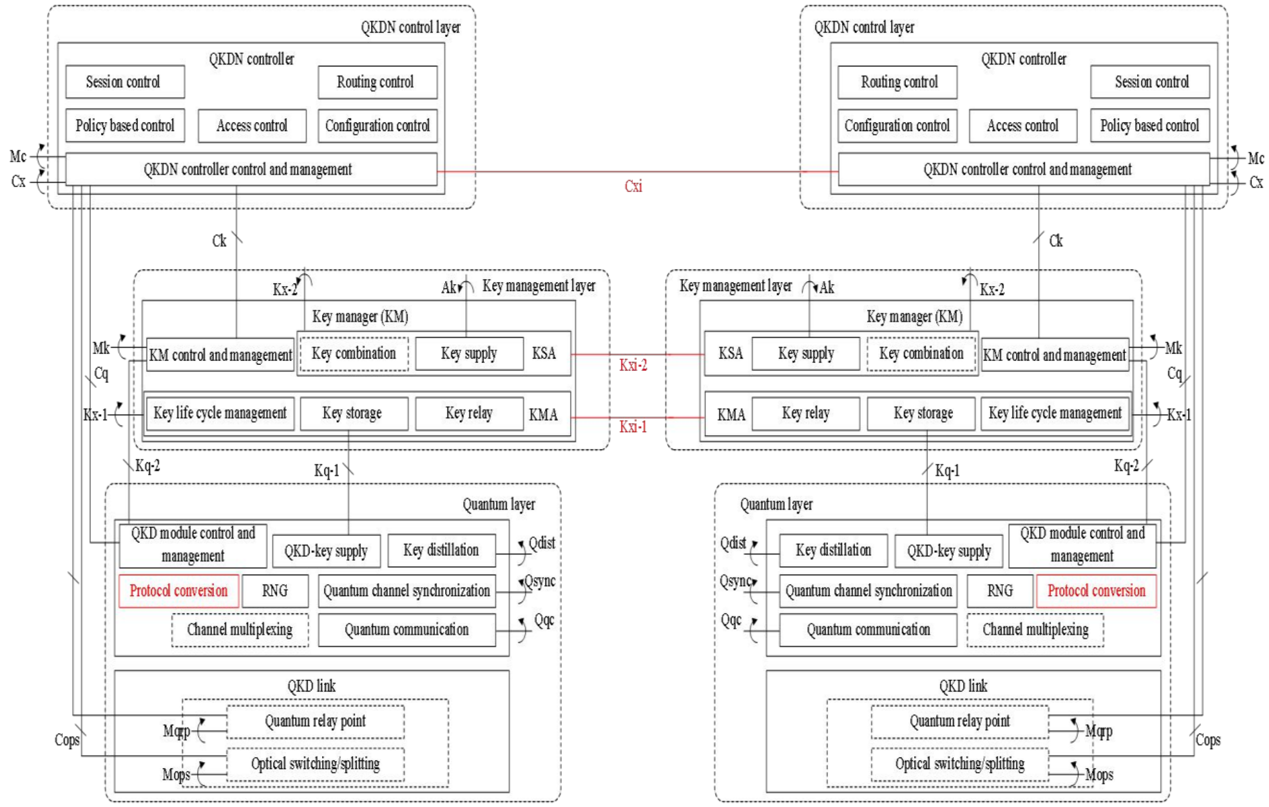

Figure 2 - A functional architecture for QKDNi with IWNs

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 at the next meeting.

7.1. Functional elements in GWFs

A GWF is to support interworking interfaces between two different QKDN providers, and to support information can be shared with common protocol. The GWF is located in 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 through Kxi;
- Interworking key relay function: It relays the keys from end to end GFs between two QKDN 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, 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 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;

- 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 providers;

- 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;

- Interworking security management function: It collects/receives security related management information from the QKDN, and shares related information with 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.

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 providers via two internal GFs interfaces Kxi’ in IWF;

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

- 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, 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.

- 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.

- 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

8.1. Operational procedures for QKDNi with GWF

To be added.

8.2. Operational procedures for QKDNi with IWF

To be added.

9. Security consideration

To be added.

Appendix I

I.1 QKDNi with different control schemes

Editor’s note – This clause is removed from [ITU-T Y.QKDN-iwfr], and it will be discussed at the next meeting.

I.1.1 Interworking of distributed QKDNs

For interworking of distributed QKDNs, scenario I-1 illustrates key relay model with an IWN between distributed QKDNs. Figure I-3 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 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.

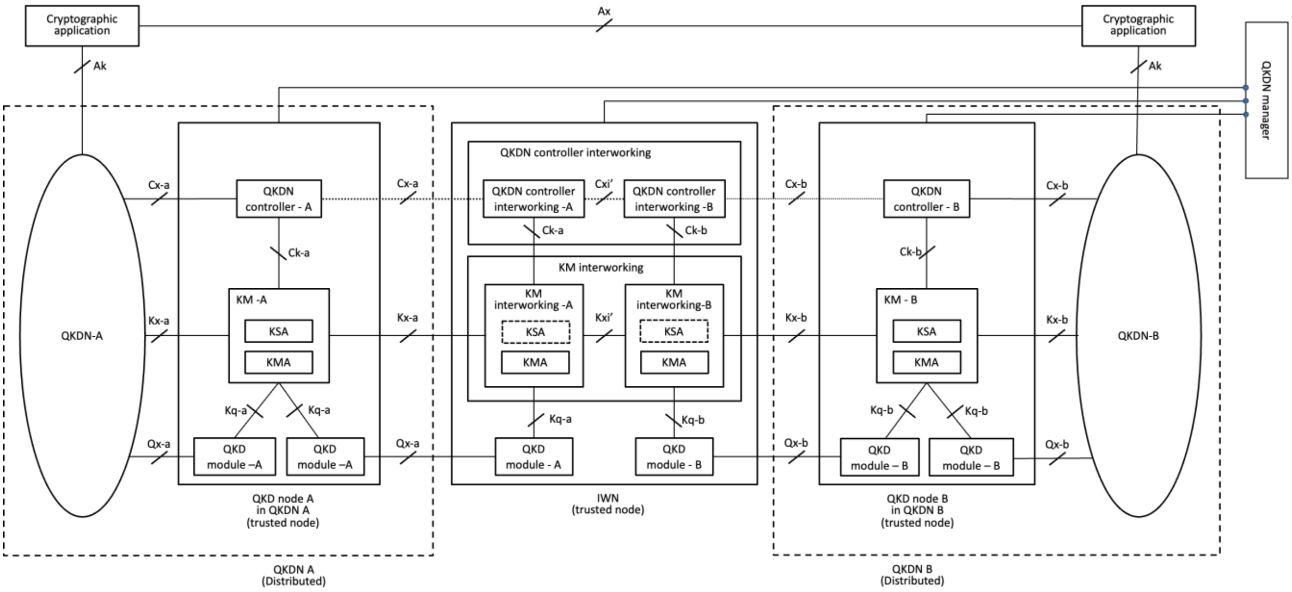

Figure I-3 – Interworking of distributed QKDNs (Scenario I-1)

Scenario I-2 illustrates the model that QKDN controller interworking functions are unified to be one controller function, which are separate in scenario I-1. A single QKDN controller interworking function controls both KM interworking-A and KM interworking-B by interacting respectively as shown in figure I-4.

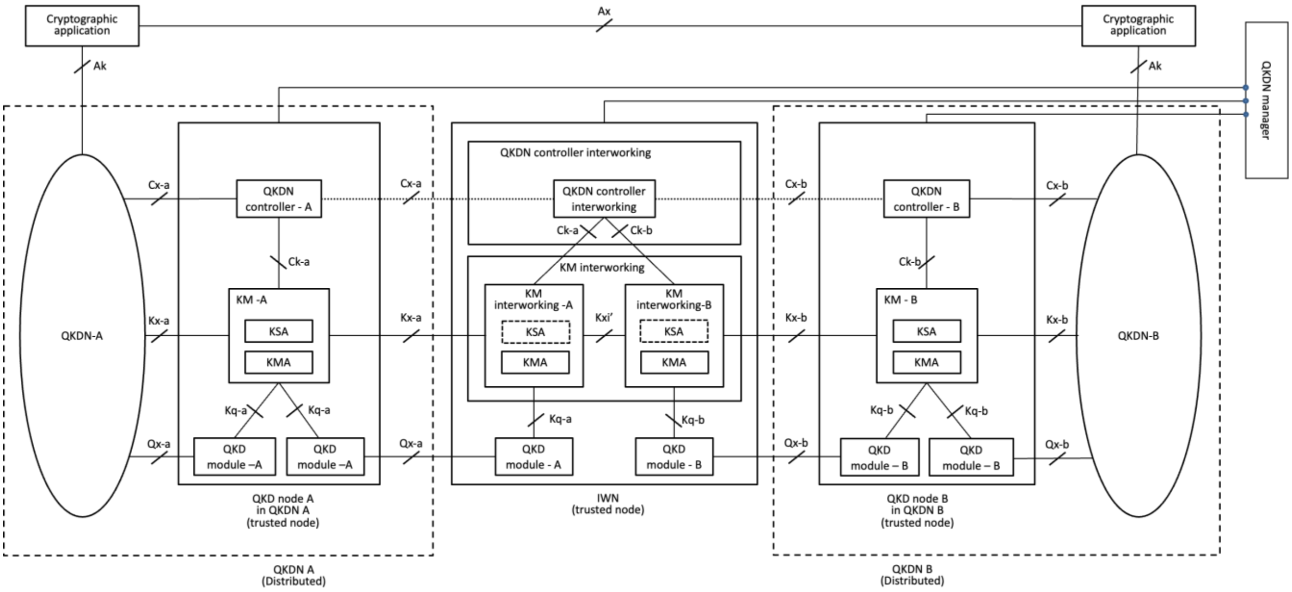

Figure I-4 – Interworking of distributed QKDNs (Scenario I-2)

In Scenario I-3, a single KM interworking function interacts with both QKD module-A and QKD module-B for key relay, while in scenario I-2, 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 I-5.

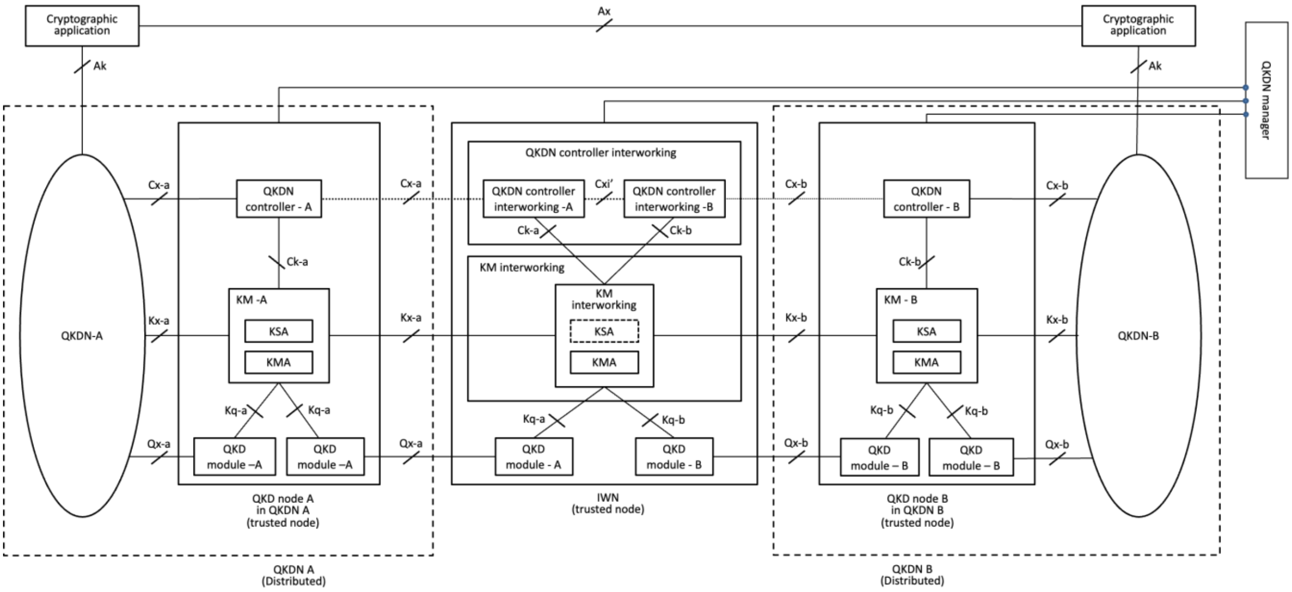

Figure I-5 – Interworking of distributed QKDNs (Scenario I-3)

In scenario I-4, both QKDN controller interworking function and KM interworking function are unified. A QKDN controller interworking function controls a KM interworking function and the information from QKDN A and QKDN B, and a single KM interworking 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.

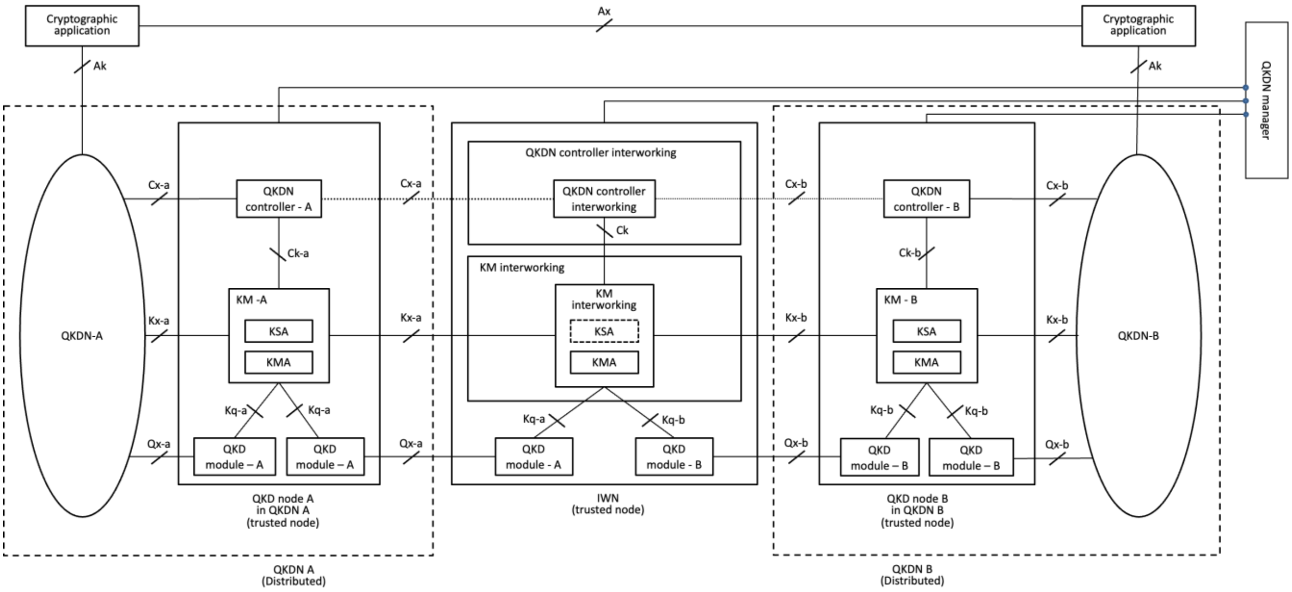

Figure I-6 – Interworking of distributed QKDNs (Scenario I-4)

I.1.2 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. As described in Figure 5 in clause 9.1, there is no connection between QKD modules and the keys are transferred to the KM in unencrypted form.

Scenario I-5 illustrates key relay model within the IWN between a distributed QKDN and a centralized QKDN similarly described in I.2.1.

Figure I-7 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.

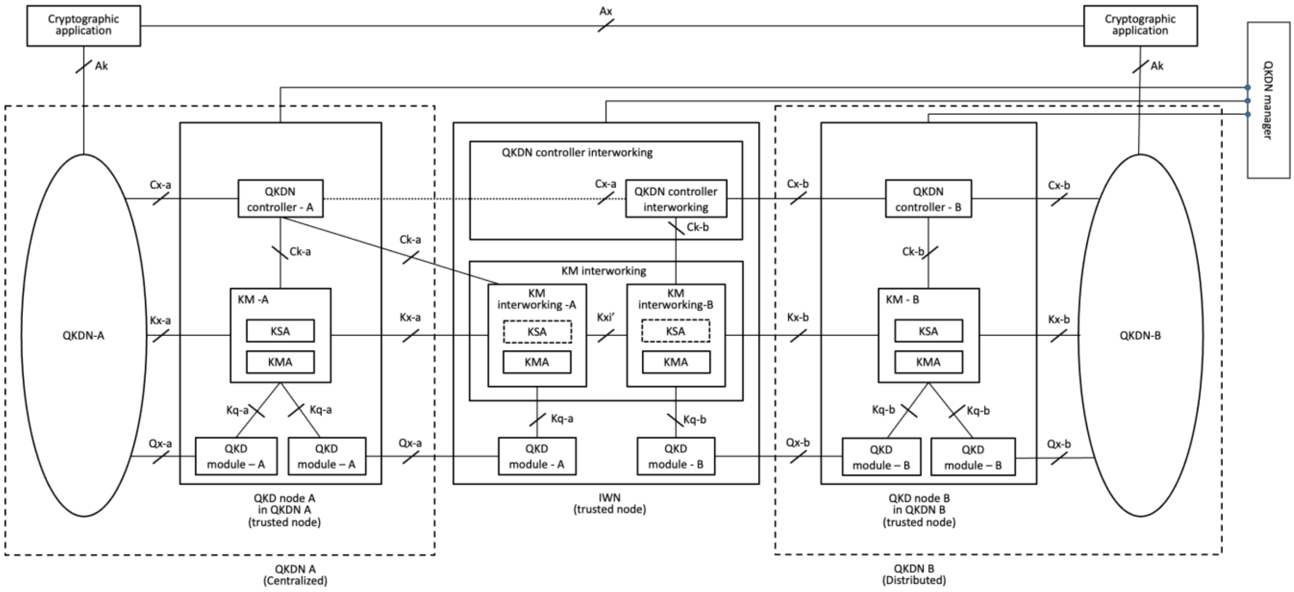

Figure I-7 – Interworking of a distributed QKDN and a centralized QKDN (Scenario I-5)

Scenario I-6 in figure I-8 illustrate 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.

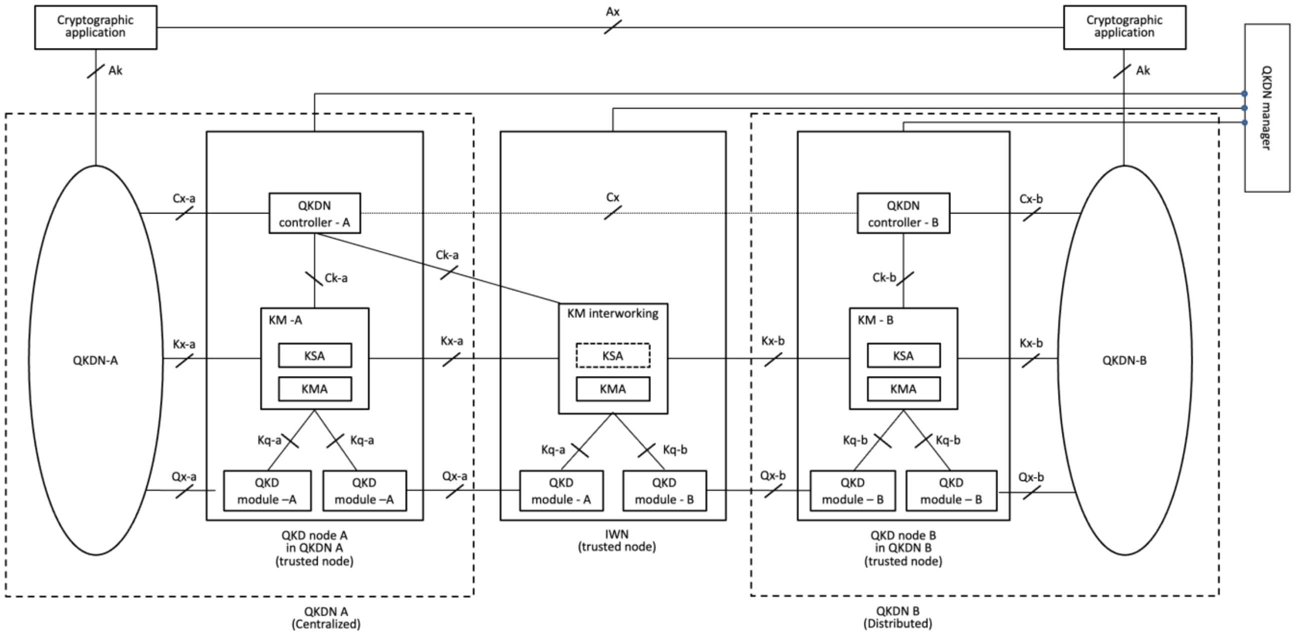

Figure I-8 – Interworking of a distributed QKDN and a centralized QKDN (Scenario I-6)

I.1.3 Interworking of centralized QKDNs

For interworking of centralized QKDNs, scenario I-7 is the model of Key relay performed in an IWN same as interworking of distributed QKDNs shown in I.2.1. Figure I-9 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.

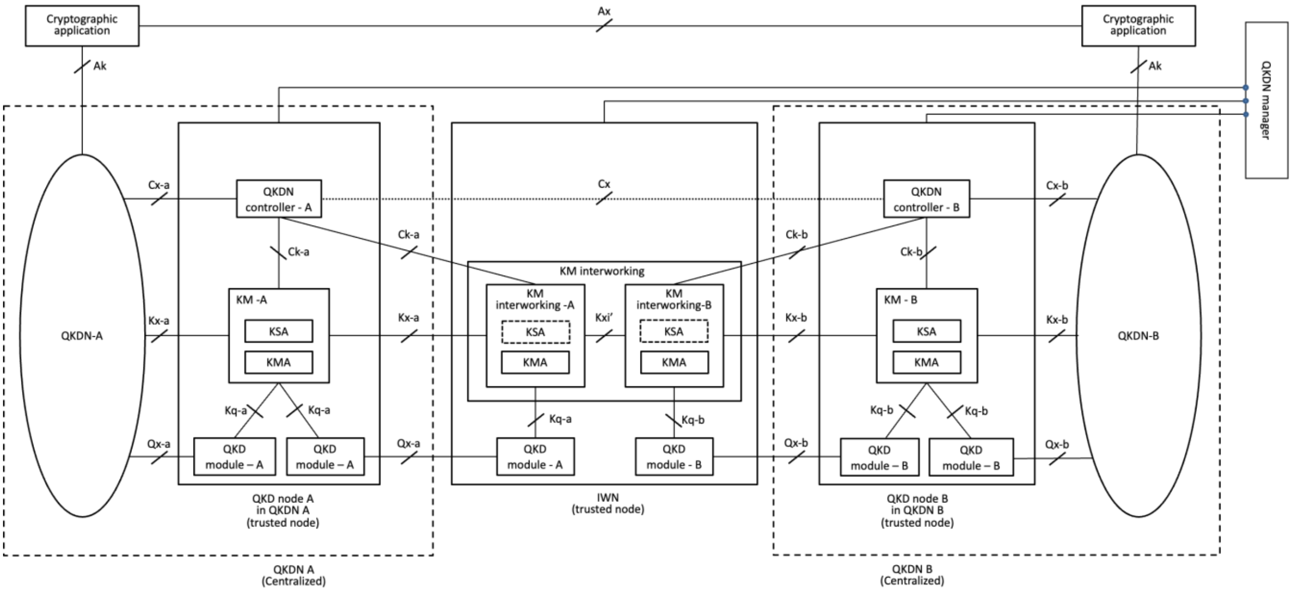

Figure I-9 – Interworking of centralized QKDNs (Scenario I-7)

Scenario I-8 in figure I-10 illustrates the model with unified KM interworking function and with centralized QKDN A which has sole control of QKDN controller. This scenario is the same as scenario I-6. As shown in the figure, KM interworking function in the IWN is controlled only by QKDN A.

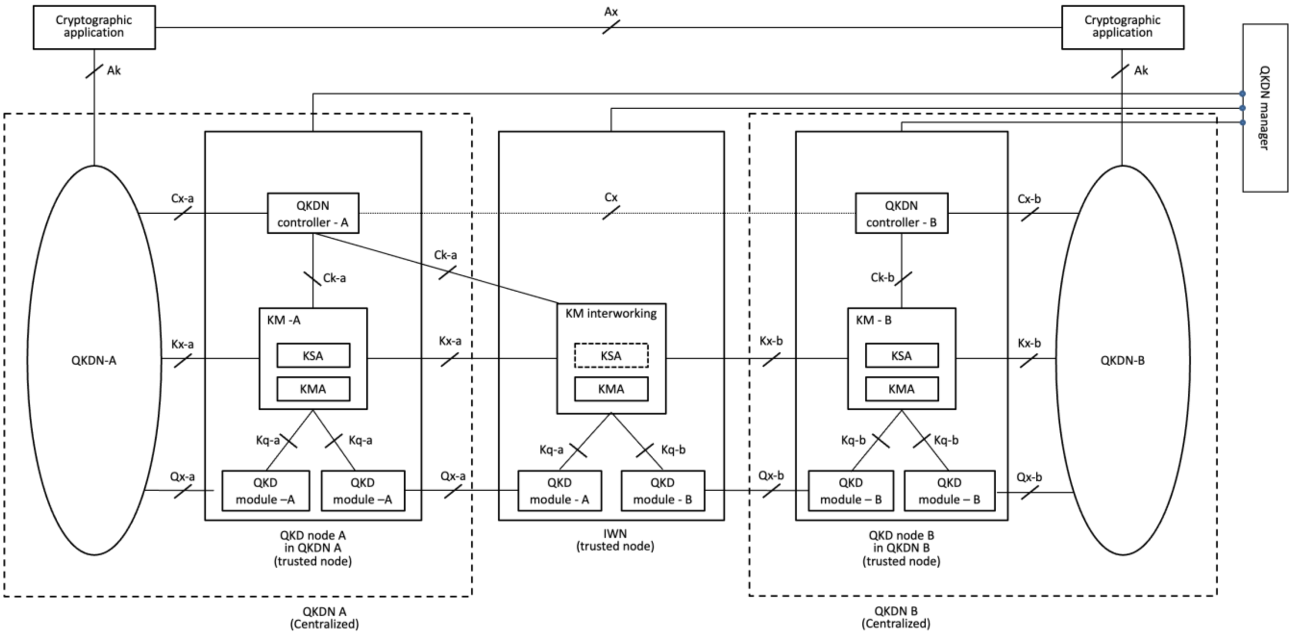

Figure I-10 – Interworking of centralized QKDNs (Scenario I-8)

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*