Annex

Draft new 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 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*

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

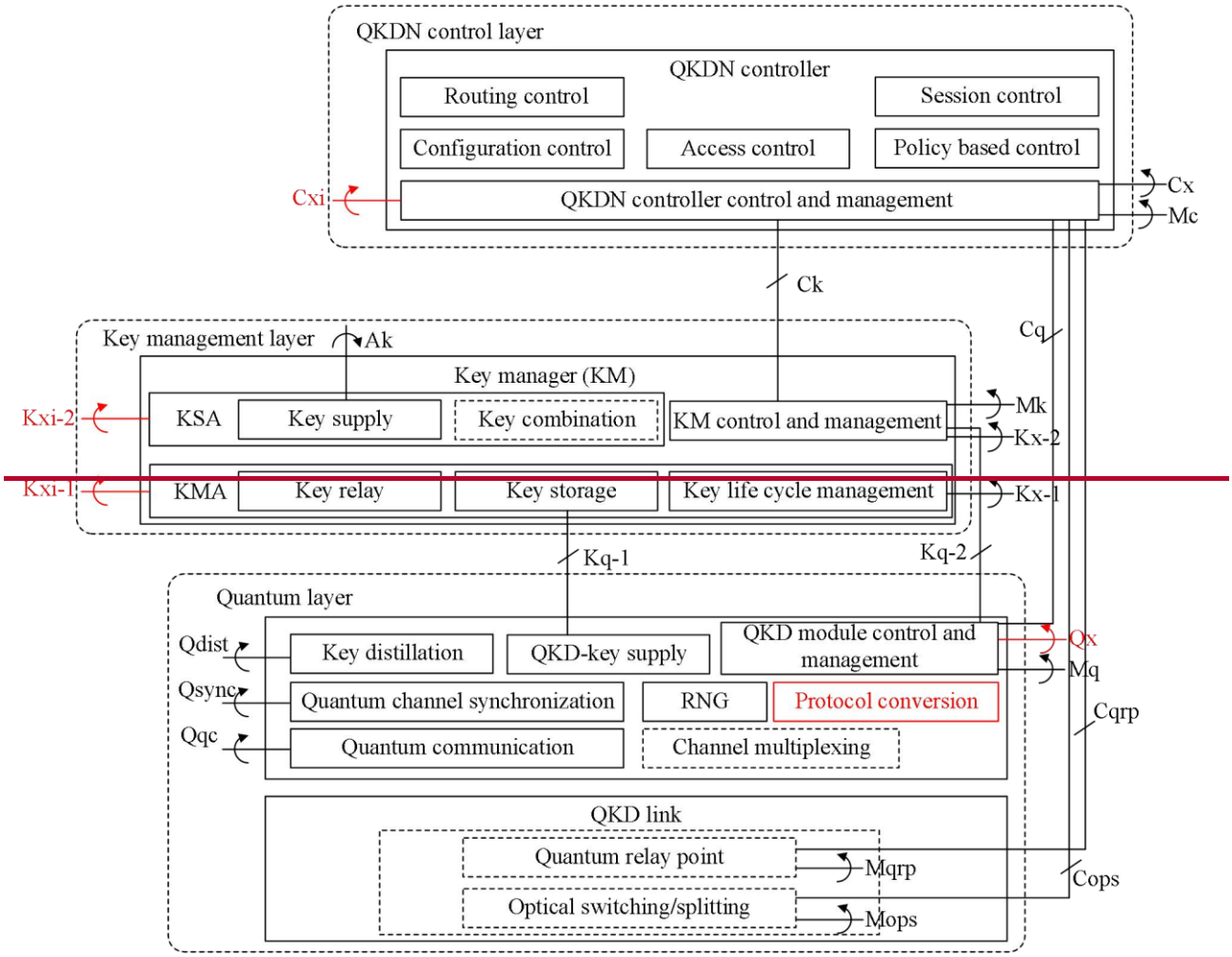
Quantum key distribution network (QKDN) is a cryptographic infrastructure to provide secure symmetric keys to cryptographic applications in user networks. Constructing a large scale QKDN which covers wide area, it may consist of multiple QKDNs and they are interworking each other.

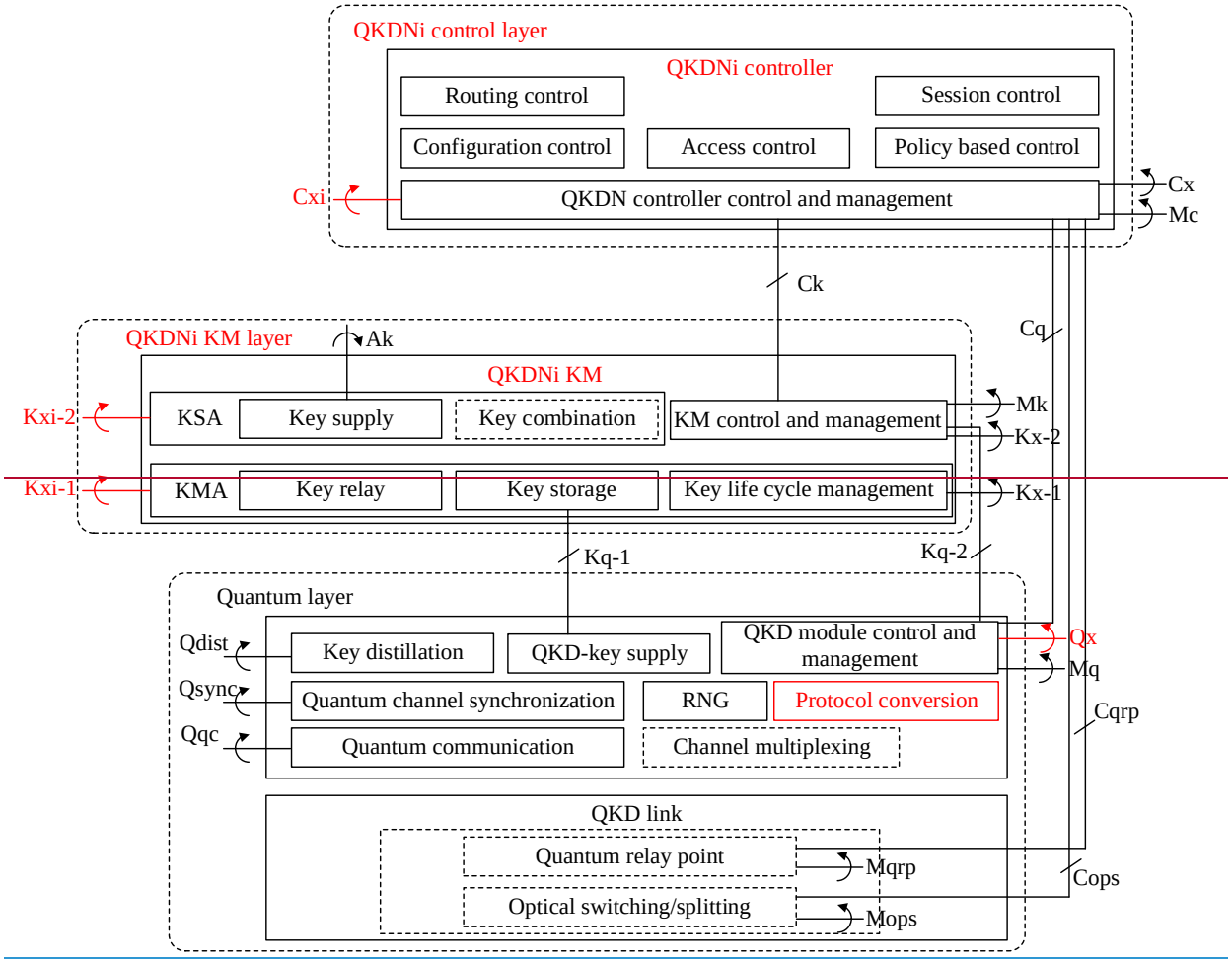
An overview on QKDNi including the overview of interworking QKDNs, the reference models, and the functional models of ~~Gateway Functions (~~GWFs~~)~~ and ~~Inter Working Functions (~~IWFs~~)~~ for QKDNi is addressed in [ITU-T Y.3810]. Moreover, QKDN interworking functional requirements are identified in [ITU-T Y.QKDN-iwrq].

Based on the conceptual models on QKDNi illustrated in [ITU-T Y.3810] and the QKDNi functional requirements identified in [ITU-T Y.QKDN-iwrq], two functional architectures ~~of~~ for QKDNi ~~in two functions~~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].~~*Editor's note – The majority of the architecture elements should be improved further.*~~


QKDN control layer
QKDN controller
Routing control
Session control
Configuration control
Access control
Policy based control
Cxi
QKDN controller control and management
Cx
Mc
Ck
Cq
Key management layer
Ak
Key manager (KM)
Kxi-2
KSA
Key supply
Key combination
KM control and management
Mk
Kx-2
Kxi-1
KMA
Key relay
Key storage
Key life cycle management
Kx-1
Kq-1
Kq-2
Quantum layer
Qdist
Key distillation
QKD-key supply
QKD module control and management
Qx
Mq
Qsync
Quantum channel synchronization
RNG
Protocol conversion
Cqrp
Qqc
Quantum communication
Channel multiplexing
QKD link
Quantum relay point
Mqrp
Cops
Optical switching/splitting
Mops


QKDNi control layer
QKDNi controller
Routing control
Session control
Configuration control
Access control
Policy based control
Cxi
QKDN controller control and management
Cx
Mc
Ck
Cq
QKDNi KM layer
Ak
QKDNi KM
Kxi-2
KSA
Key supply
Key combination
KM control and management
Mk
Kx-2
Kxi-1
KMA
Key relay
Key storage
Key life cycle management
Kx-1
Kq-1
Kq-2
Quantum layer
Qdist
Key distillation
QKD-key supply
QKD module control and management
Qx
Mq
Qsync
Quantum channel synchronization
RNG
Protocol conversion
Cqrp
Qqc
Quantum communication
Channel multiplexing
QKD link
Quantum relay point
Mqrp
Cops
Optical switching/splitting
Mops

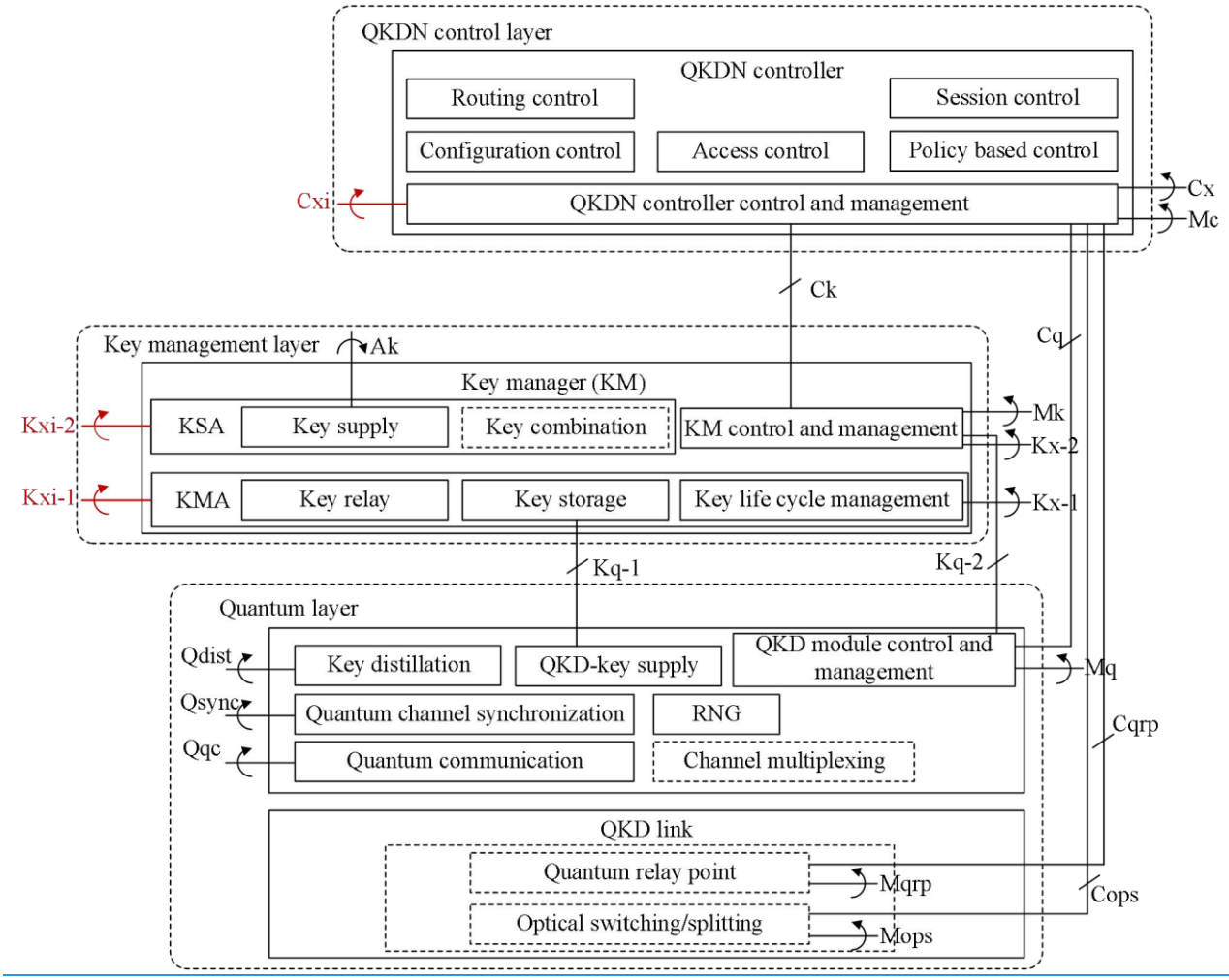


Figure 1 - A functional architecture for QKDNi with GWNs

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].~~the functional elements in the quantum layer including the QKD link and QKD module are defined in [ITU-T Y.3802]. The parameters of the QKD link and QKD module such as protocol conversion aiming at involving interoperability between QKD modules with different QKD protocols and implementations.~~

– 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.~~the functional elements in the key management layer including key management agent (KMA) and key supply agent (KSA) 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. ~~the functional element in the QKDN control layer is the QKDN controller. It supports interworking of key relay routing. 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].

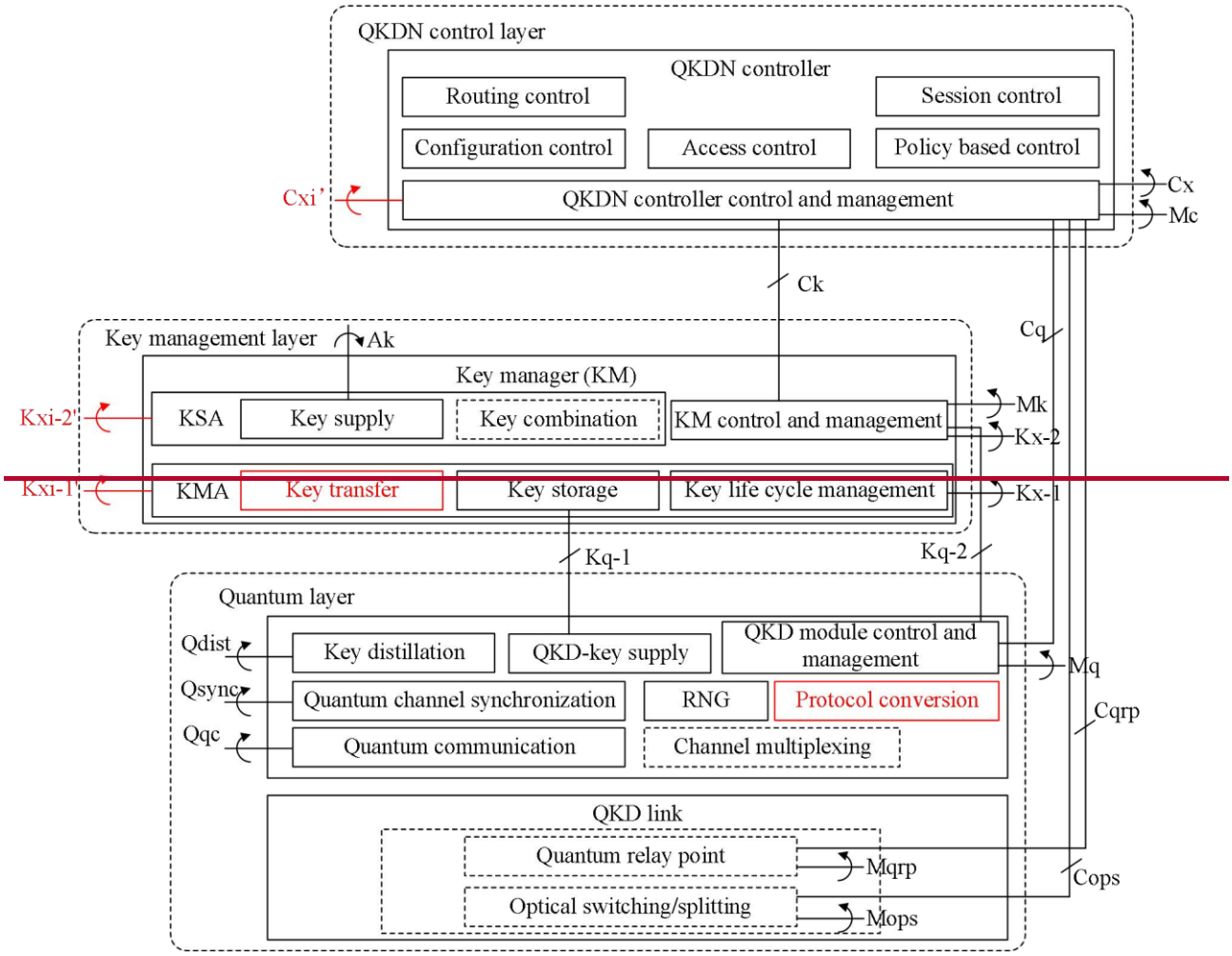
Most of the reference points in Figure 1 have been defined in [ITU-T Y.3802], some reference points for QKDNi with GWF have been defined in [ITU-T Y.3810], and this Recommendation defines the newly added one and presents the existing ones related to QKDNi with GWNs.

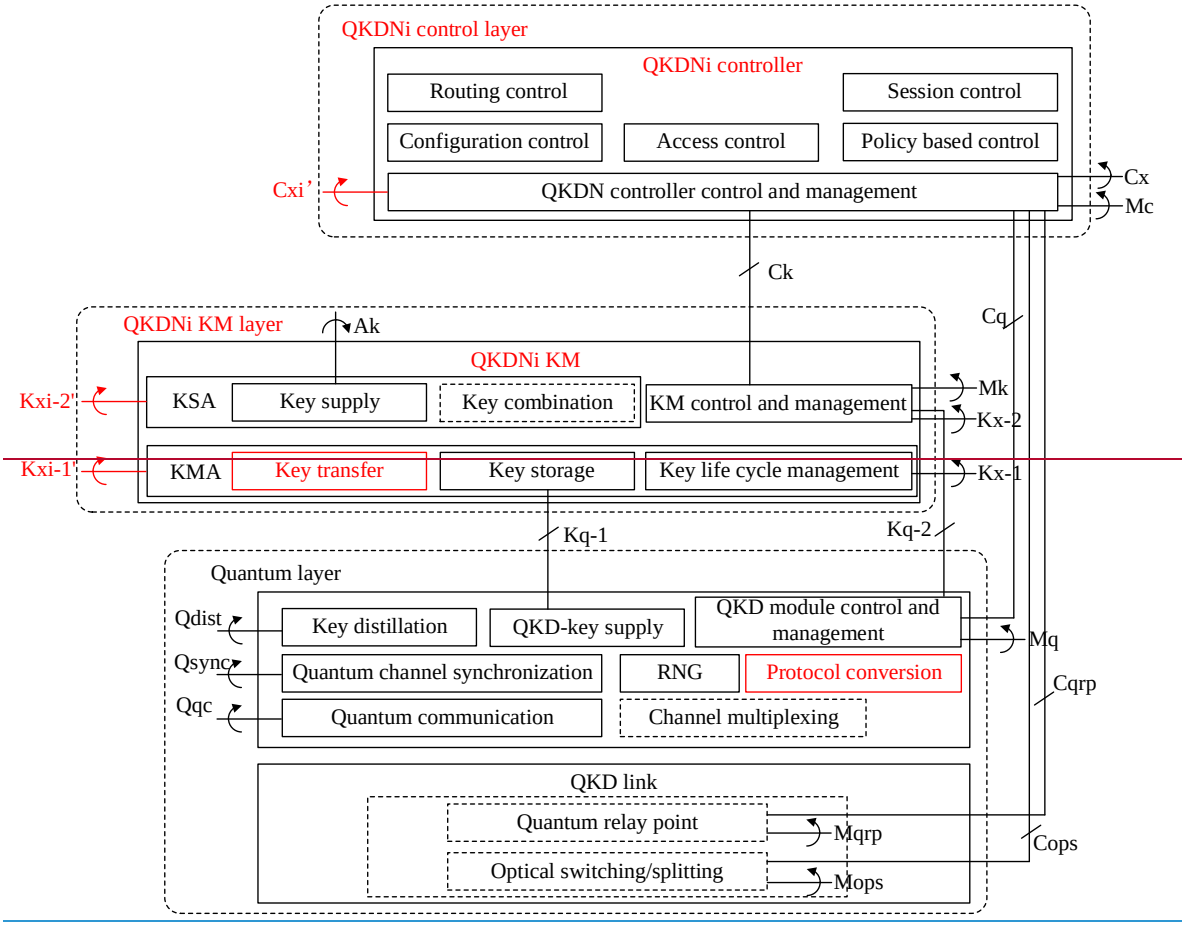
The newly added reference point is:

– **Kx-1**: a reference point connecting two KMAs in each 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


QKDN control layer
QKDN controller
Routing control
Session control
Configuration control
Access control
Policy based control
Cxi'
QKDN controller control and management
Cx
Mc
Ck
Cq
Key management layer
Ak
Key manager (KM)
Kxi-2'
KSA
Key supply
Key combination
KM control and management
Mk
Kx-2
Kxi-1'
KMA
Key transfer
Key storage
Key life cycle management
Kx-1
Kq-1
Kq-2
Quantum layer
Qdist
Key distillation
QKD-key supply
QKD module control and management
Mq
Qsync
Quantum channel synchronization
RNG
Protocol conversion
Cqrp
Qqc
Quantum communication
Channel multiplexing
QKD link
Quantum relay point
Mqrp
Cops
Optical switching/splitting
Mops


QKDNi control layer
QKDNi controller
Routing control
Session control
Configuration control
Access control
Policy based control
Cxi'
QKDN controller control and management
Cx
Mc
Ck
Cq
QKDNi KM layer
Ak
QKDNi KM
Kxi-2'
KSA
Key supply
Key combination
KM control and management
Mk
Kx-2
Kxi-1'
KMA
Key transfer
Key storage
Key life cycle management
Kx-1
Kq-1
Kq-2
Quantum layer
Qdist
Key distillation
QKD-key supply
QKD module control and management
Mq
Qsync
Quantum channel synchronization
RNG
Protocol conversion
Cqrp
Qqc
Quantum communication
Channel multiplexing
QKD link
Quantum relay point
Mqrp
Cops
Optical switching/splitting
Mops

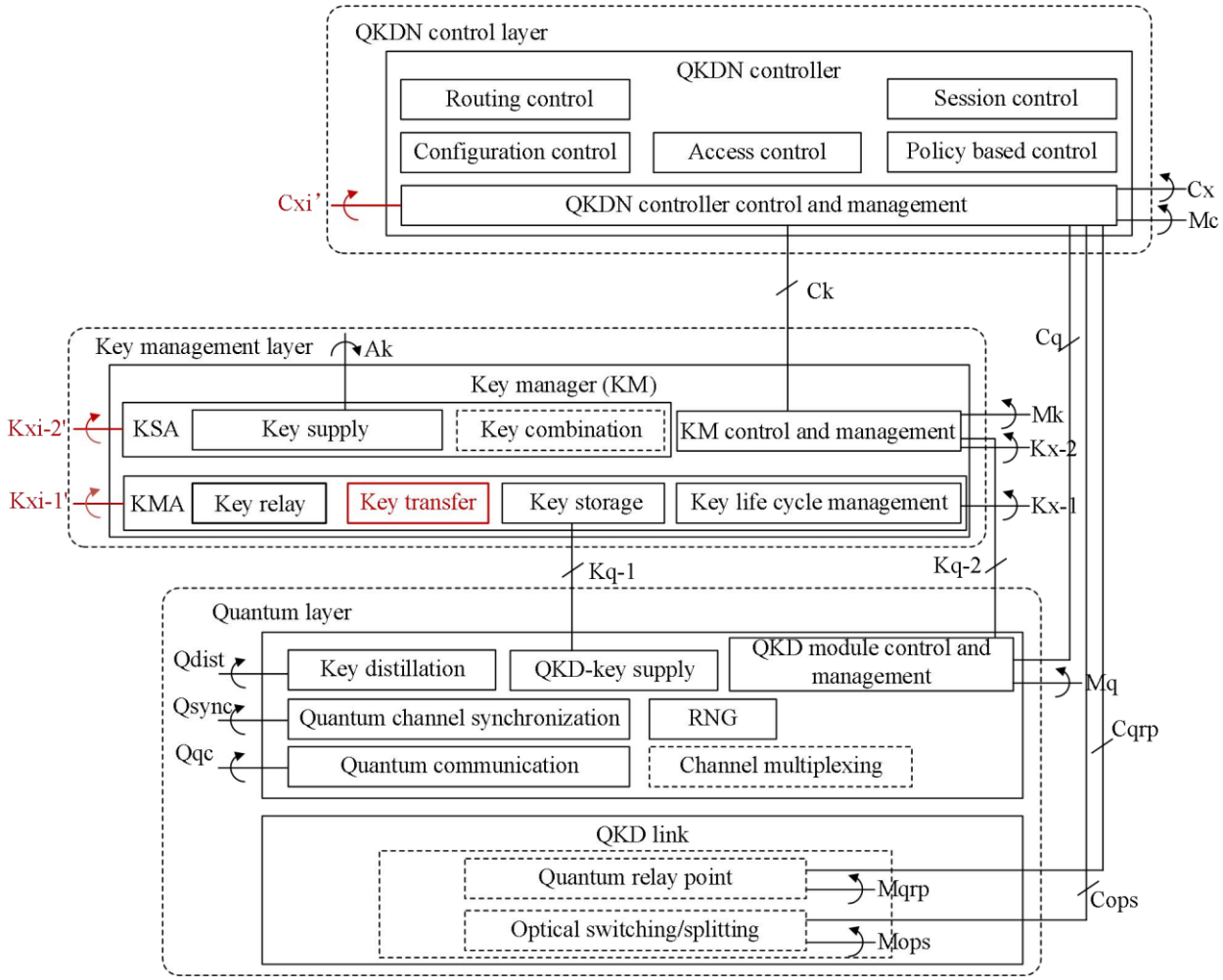


Figure 2 - A functional architecture for QKDNi with IWNs

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 ~~at the next meeting~~further.

7.1. Functional elements in GWFs

A GWF is to support interworking interfaces between two different QKDN ~~providerss~~, 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. Interworking architectural configurations

~~*Editor's note – This clause is moved from the appendix to the main body according to the meeting result in August meeting.*~~

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

9.1. Configuration 1: Interworking of distributed QKDNs

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

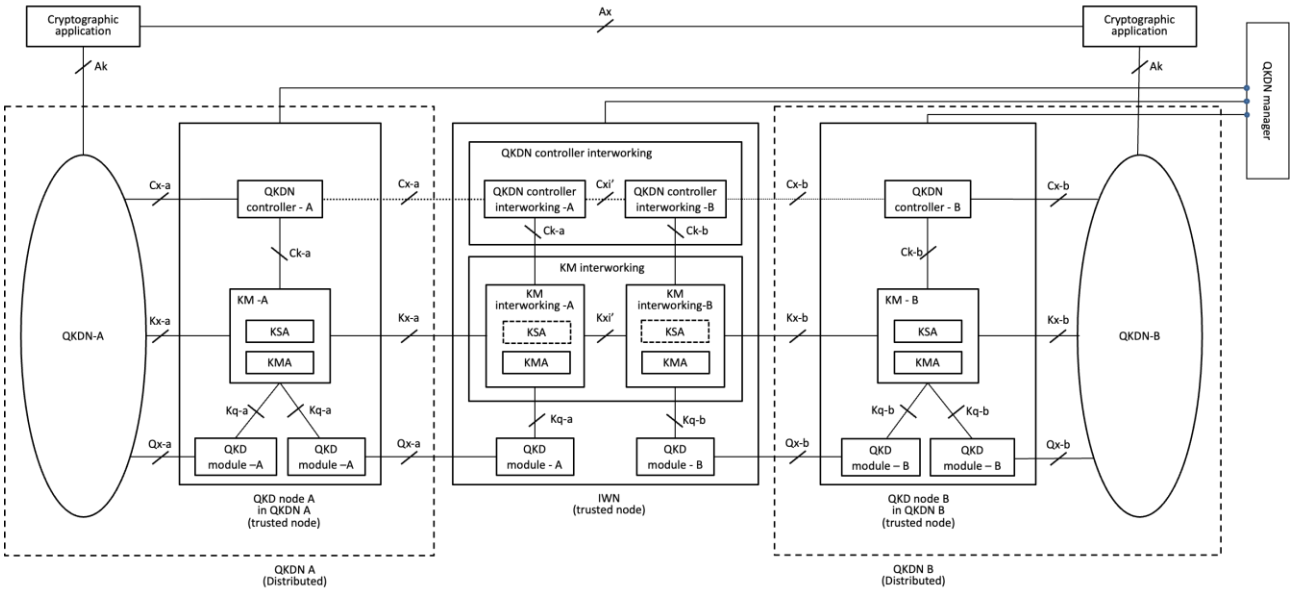


Figure 3 - Interworking of distributed QKDNs ~~(Scenario I-1)~~

~~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 4.

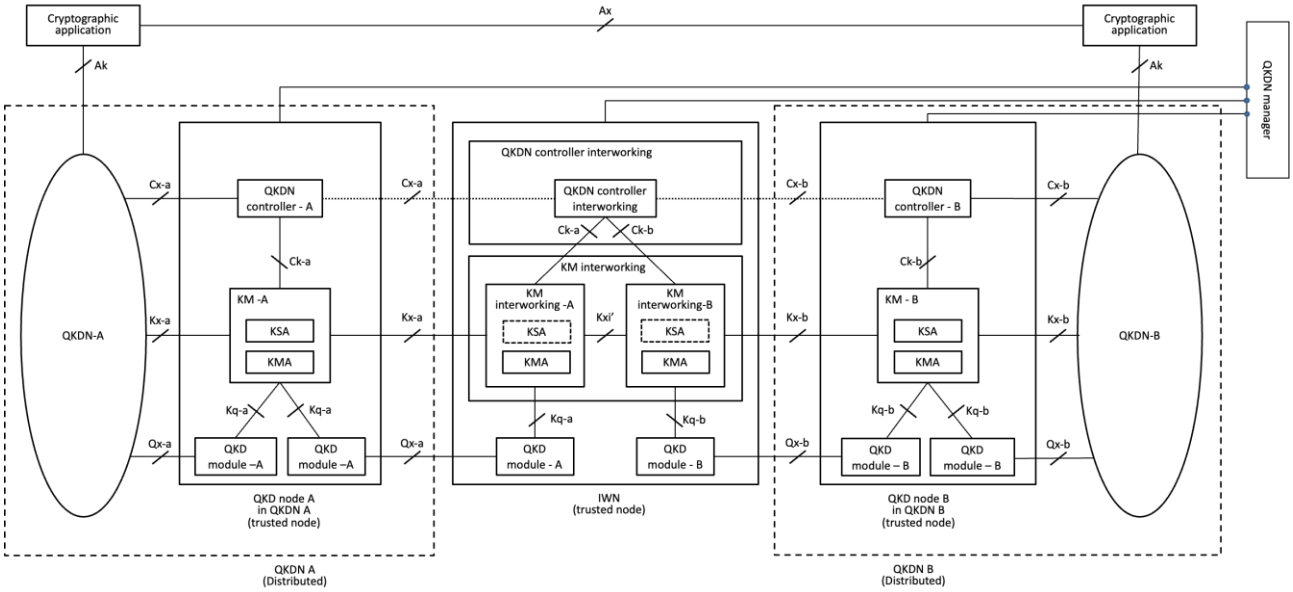


Figure 4 - Interworking of distributed QKDNs with unified QKDNi controller ~~(Scenario I-2)~~

In ~~Scenario~~ figure 5~~I-3~~, a single KM interworking function interacts with both QKD module-A and QKD module-B for key relay, while in scenario Figure 4~~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 5.

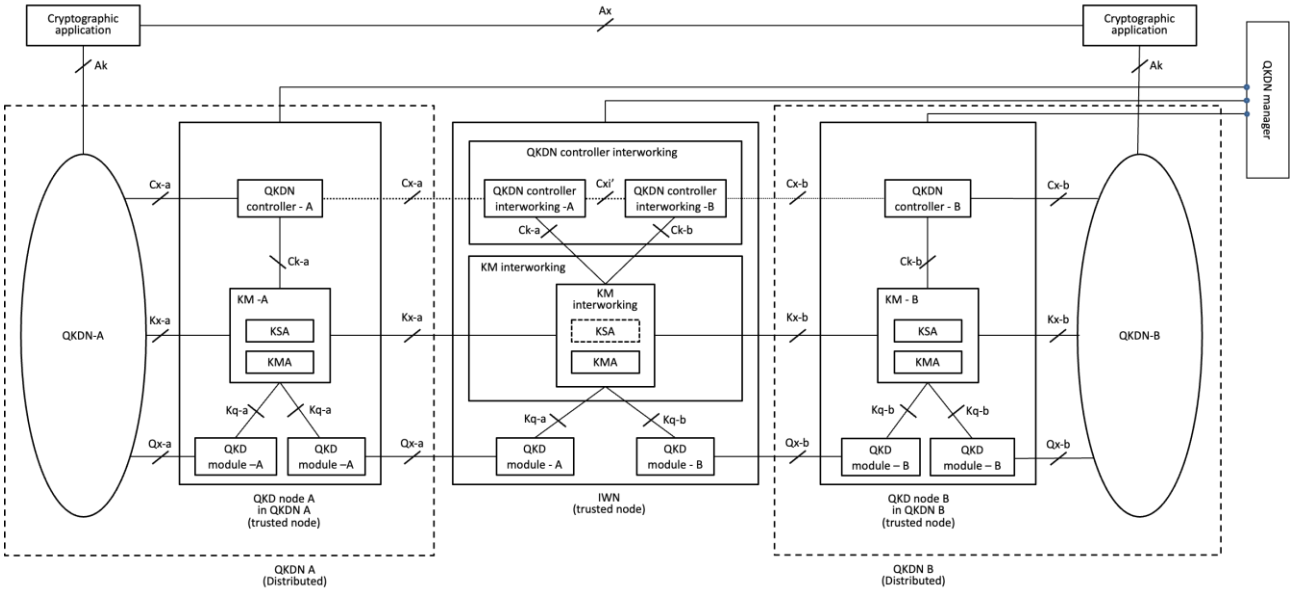


Figure 5 - Interworking of distributed QKDNs with unified QKDNi KM ~~(Scenario I-3)~~

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

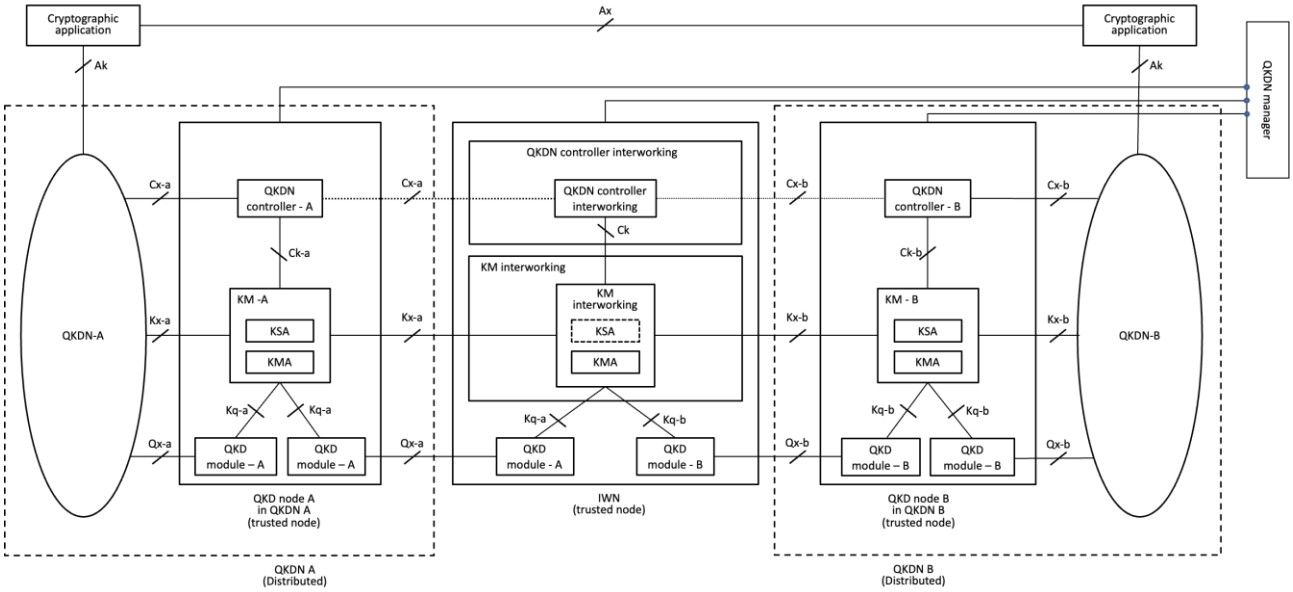


Figure 6 - Interworking of distributed QKDNs with unified QKDNi controller and QKDNi KM ~~(Scenario I-4)~~

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

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

Figure 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.

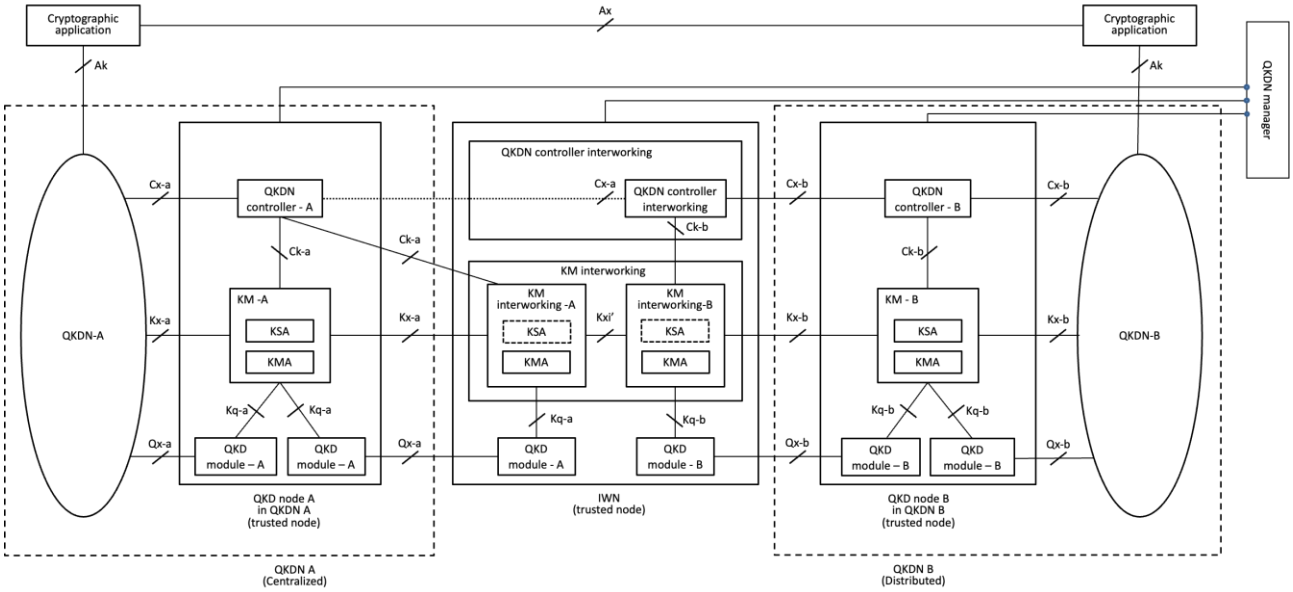


Figure 7 - Interworking of a distributed QKDN and a centralized QKDN ~~(Scenario I-5)~~

~~Scenario I-6 in f~~Figure 8 illustrate the model with unified ~~KM interworking~~QKDNi KM function and with centralized QKDN A which has sole control of QKDN controller. As shown in the figure, ~~KM interworking~~QKDNi KM function in the IWN is controlled only by QKDN A.

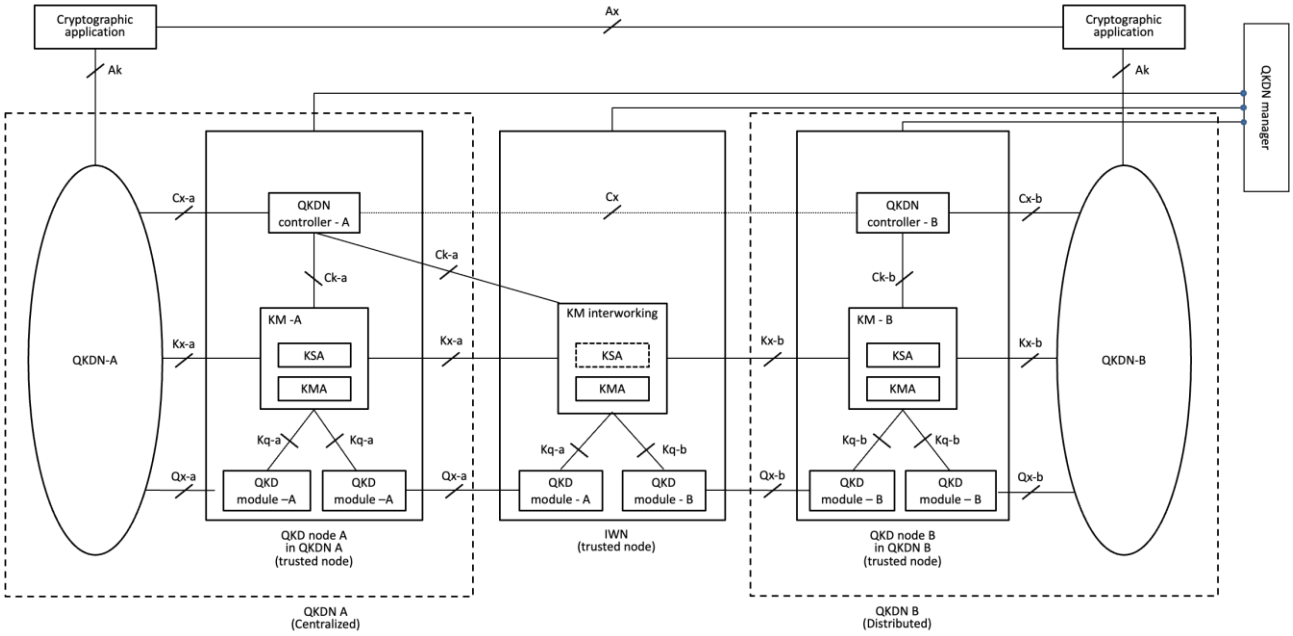


Figure 8 - Interworking of a distributed QKDN and a centralized QKDN ~~(Scenario I-6)~~

9.3. Configuration 3: Interworking of centralized QKDNs

~~For interworking of centralized QKDNs, scenario I-7 is the model of Key relay performed in an IWN.~~ Figure 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.

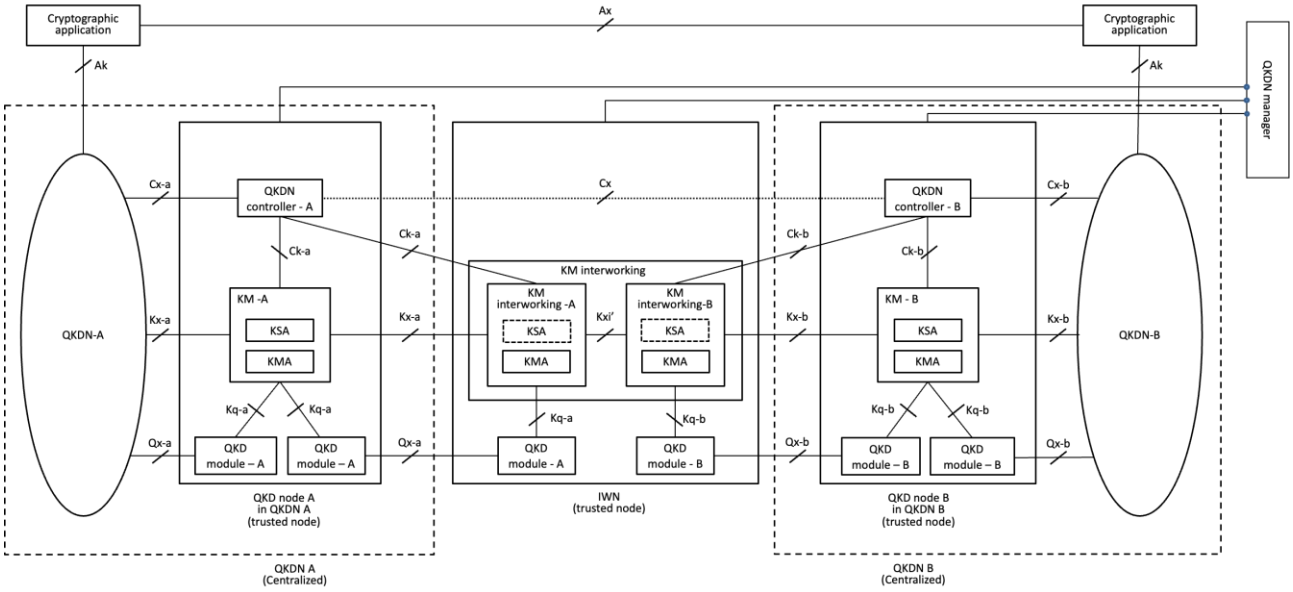


Figure 9 - Interworking of centralized QKDNs ~~(Scenario I-7)~~

Figure 10~~Scenario I-8 in figure 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.

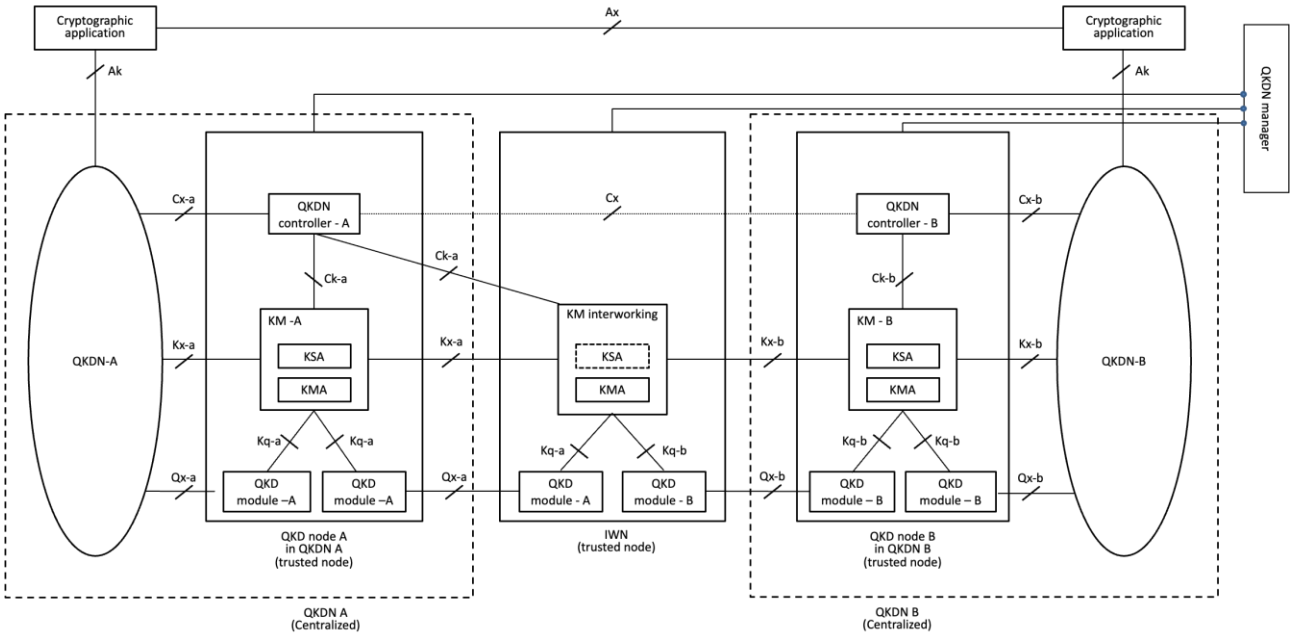


Figure 10 - Interworking of centralized QKDNs ~~(Scenario I-8)~~

10. Security consideration

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*

_____