INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2022-2024

SSG13-TD37/PLEN

STUDY GROUP 13

Original: English

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

TD

Source:	Editors
Title:	Draft new Recommendation ITU-T Y.3810 (formerly Y.QKDN-iwfr): “Quantum key distribution network interworking - framework” – for consent

Contact:	Yasuhiro Fujiyoshi Toshiba corporation Japan	Tel: Fax: E-mail: yasuhiro.fujiyoshi@toshiba.co.jp
Contact:	Zhao Yongli BUPT China	Tel: Fax: E-mail: yonglizhao@bupt.edu.cn
Contact:	Hyungsoo Kim KT Korea (Rep. of)	Tel: Fax: E-mail: hans9@kt.com
Contact:	Taesang Choi ETRI Korea (Rep. of)	Tel: Fax: E-mail: choits@etri.re.kr

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

Abstract: This is the final draft Recommendation Y.3810 (formerly Y.QKDN-iwfr) “Quantum key distribution network interworking - framework” for consent (output of SG13 meeting, 4 -15 July 2022)

Summary

This output document is the draft of Y.QKDN-iwfr for consent, updated based on the discussion results of C40 in the SG13 meeting (4 – 15 July 2022).

The attached Annex A is the final draft Recommendation ITU T X.QKDN-iwfr “Quantum key distribution network interworking - framework” for consent.

Annex

Draft new Recommendation ITU-T Y.3810 (formerly Y.QKDN-iwfr)

Quantum key distribution network interworking - framework

Summary

For quantum key distribution networks (QKDN), Recommendation ITU-T Y.QKDN-iwfr specifies framework of QKDN interworking (QKDNi). This Recommendation describes the overview of interworking QKDNs, the reference models, and the functional models of gateway functions (GWFs) and interworking functions (IWFs). The configurations for QKDNi are specified. Appendix I includes QKDNi with different key relay schemes.

Keywords
Quantum key distribution (QKD), QKD network (QKDN), QKDN interworking (QKDNi)

Table of Contents

Draft new Recommendation Y.3810 (formerly Y.QKDN-iwfr)

Quantum key distribution network interworking - framework

1. Scope

This Recommendation specifies a framework for QKDN interworking (QKDNi).

In particular, this Recommendation includes:

- Reference models for QKDNi;
- Functional models for QKDNi;
- Configurations 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.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 management agent (KMA)** [ITU-T Y.3802]: A functional element to manage keys generated by one or multiple quantum key distribution (QKD) modules in a QKD node (trusted node).

NOTE – KMA acquires keys from one or multiple QKD modules, synchronizes, resizes, formats, and stores them. It also relays keys through key management agent (KMA) links.

3.1.2 **key management agent link (KMA link)** [ITU-T Y.3802]: A communication link connecting key management agents (KMAs) to perform key relay and communications for key management.

3.1.3 **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.

3.1.4 **key supply agent (KSA)** [ITU-T Y.3802]: A functional element to supply keys to a cryptographic application, being located between a key management agent (KMA) and the cryptographic application.

NOTE – Application interfaces for cryptographic applications are installed into the key supply agent (KSA). The KSA synchronizes keys, and verifies their integrity via a KSA link before supplying them to the cryptographic application.

3.1.5 **key supply agent link (KSA link)** [ITU-T Y.3802]: A communication link connecting key supply agents (KSAs) to perform key synchronization and integrity verification.

3.1.6 **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.

3.1.7 **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.

3.1.8 **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).

3.1.9 **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.

3.1.10 **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.

3.1.11 **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.

3.1.12 **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

IWF	InterWorking Function
IWN	InterWorking Node
KM	Key Manager
KMA	Key Management Agent
KSA	Key Supply Agent
OTP	One-Time Pad
QKD	Quantum Key Distribution
QKDN	QKD Network
QKDNi	QKDN interworking

5. Conventions

None.

6. Overview of QKDNi

Quantum key distribution network (QKDN) [ITU-T Y.3800] 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.

The functional requirements and architecture of single QKDN are specified based on the functional requirements of QKDN in [ITU-T Y.3801], functional architecture and operational procedures of QKDN in [ITU-T Y.3802].

This Recommendation considers the QKDN interworking (QKDNi) supporting multiple QKDN providers.

NOTE 1 - QKDN provider is specified in [ITU-T Y.3809].

QKDN providers may have their own policies for such as service, charging, routing and security. Network topologies and technology which are used in QKDN are confidential information. They don’t usually disclose them to other QKDN providers even in interworking cases. QKDNs should be demarcated at a network boundary and connect through interworking interfaces. Interworking interfaces are strictly prohibited to transfer unauthorized information. Gateway functions (GWFs) and interworking functions (IWFs) support interworking interfaces.

7. Reference models for QKDNi

7.1. Reference model for QKDNi with GWFs

Figure 1 shows a reference model for QKDNi with GWFs.

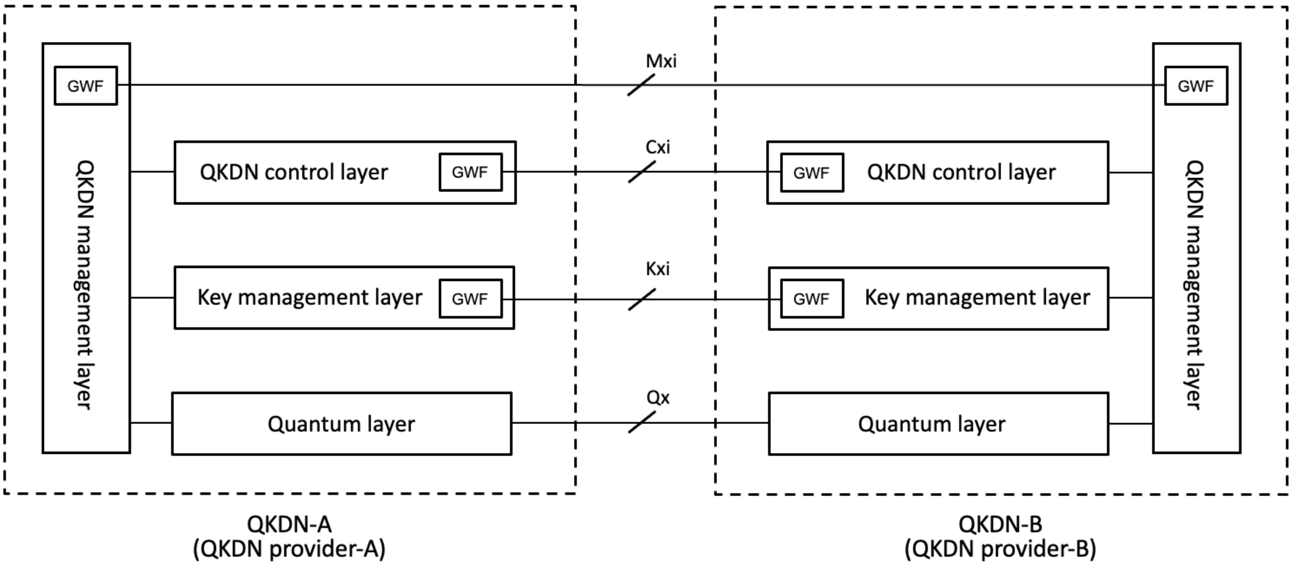

Figure 1. Reference model for QKDNi with GWFs

The GWF is located at the border of each QKDN provider. The GWF is a functional entity to support interworking interfaces between two different QKDN providers. The GWF may perform to convert internal protocols in a QKDN to other protocols for QKDNi. Even in a case that standardized protocols are used in a QKDN internally, the GWF conducts protocol conversion that gets into alignment with inconsistency of the parameters used in the internal protocol and the interworking protocol such as filtering of confidential parameters.

The following three reference points are identified between GWFs.

- Kxi is a reference point for interworking of key management layer: When keys are relayed between QKDN providers through key management layer, relative information for this purpose should be communicated, such as key ID, QKD module ID, key generation date, etc.
- Cxi is a reference point for interworking of QKDN control layer: QKDN control information can be shared between QKDN providers through QKDN control layer, such as routing control, session control, authentication and authorization control and QoS policy control, etc.
- Mxi is a reference point for interworking of QKDN management layer: QKDN management information can be shared between QKDN providers through QKDN management layer, such as charging information.

NOTE 1 - Cxi interface optionally supports interworking of key relay routing. Key relay routing will perform independently in each QKDN according to policies of each service provider.

NOTE 2 - Management functions are not usually connecting between service providers. Customer control and FCAPS should be managed by each provider.

NOTE 3 - Qx is a reference point for interworking of quantum layer without GWFs. When QKD-keys are shared between QKDN providers through quantum layer, a QKD protocol such as BB84 will be performed through Qx interface. This reference point is defined in [ITU-T Y.3802].

NOTE 4 – Interworking of quantum layer might involve interoperability between QKD modules with different QKD protocols and implementations, which still need further study. The details are outside the scope of this Recommendation.

The GWF mainly has basic functions among multiple QKDNs, including functions for interworking of key management layer, QKDN control layer and QKDN management layer. These functions are accommodated at interworking points of QKDNs. A gateway node (GWN) is a kind of a QKD node including a GWF.

7.2. Reference model for QKDNi with IWFs

Figure 2 shows a reference model for QKDNi with IWFs.

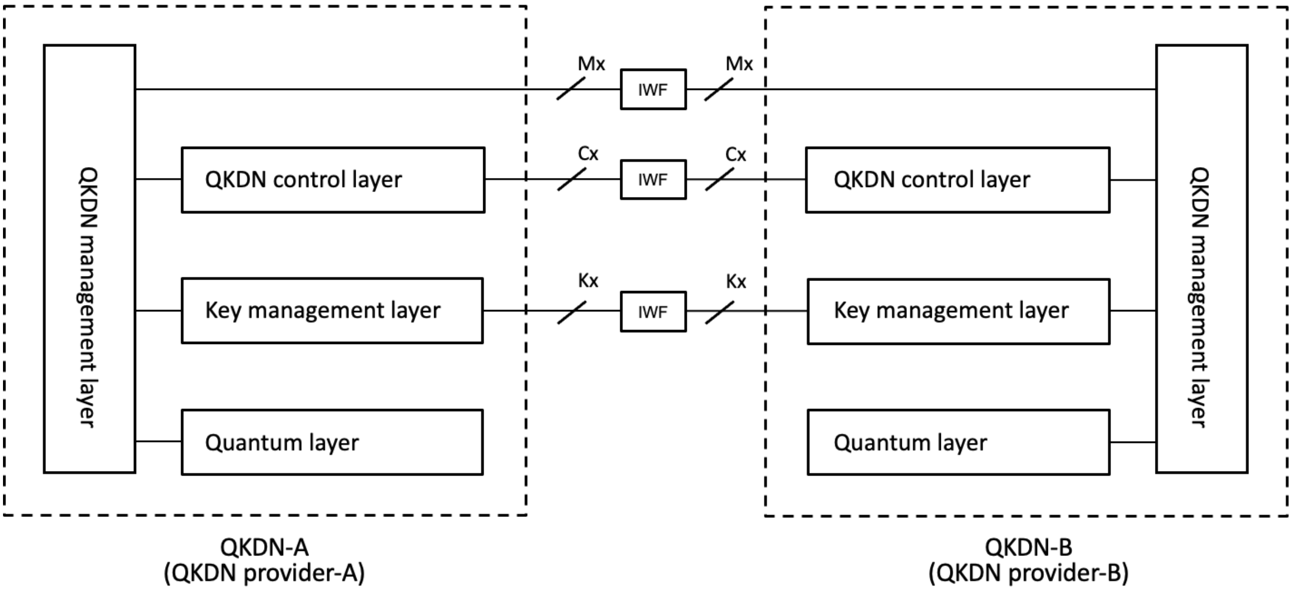

Figure 2. Reference model for QKDNi with IWFs

The IWF might be used for connecting QKDNs, as shown in Figure. 2. The IWF can be installed in a trusted node other than inside of the QKDN which interworks. The interworking structure with the IWF is one of the variations of the structure using the GWFs for interworking, considering the IWF consists of two GWFs.

IWF and GWF have the same functions but these functions are accommodated in an interworking node (IWN), which is a kind of QKD node including an IWF.

8. Functional models for QKDNi

8.1. Functional model for QKDNi with GWNs

QKDN-A and QKDN-B are connecting at Qx, Kxi, and optionally Cxi. Qx and Kxi can be used to perform secure key relay with OTP encryption between QKDN provider-A and QKDN provider-B.

Figure 3 illustrates a functional model for QKDNi with GWNs.

This model shows both QKDNs are distributed QKDN, and QKDN controllers are accommodated in the QKD node A and B to control KMs and QKDN modules. When QKDNs are centralized QKDNs, KMs and QKD modules in the QKDN-A and QKDN-B are controlled by the centralized QKDN controller in each QKDN.

NOTE 1 – A centralized QKDN and a distributed QKDN are specified in [ITU-T Y.3802].

NOTE 2 – Since a pair of QKD modules (sender and receiver) works with single technology (e.g., using the same QKD protocol, restriction of hardware and strict security requirements etc.), the QKD modules connecting at network boundary (QKD module-A_2 and QKD module-B_1 in figure 3) can be operated by different QKDN providers. In many cases using single technology, the modules are provided by the same vender.

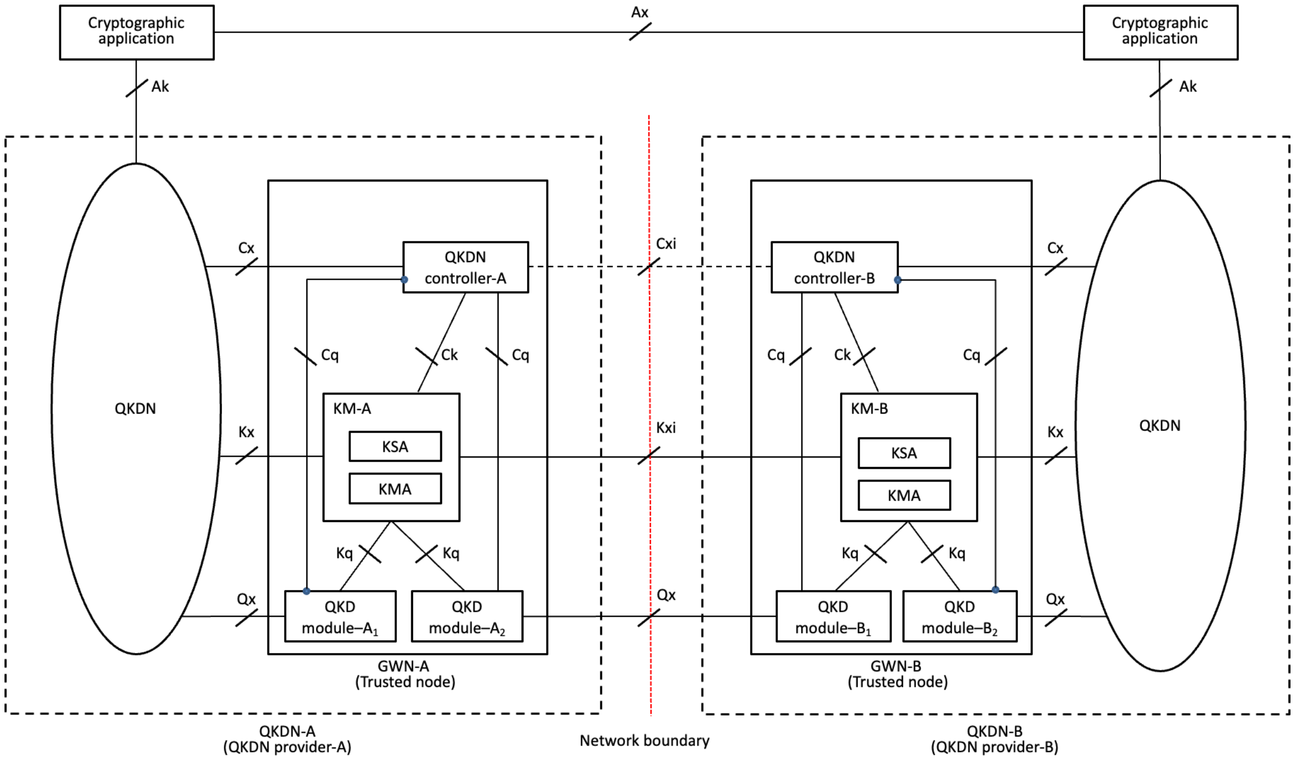

Figure 3 - Functional model for QKDNi with GWNs

8.2. Functional model for QKDNi with IWNs

QKDN-A and QKDN-B are connecting at Kxi’ and optionally Cxi’. Where there are no QKD links between the QKDN-A and QKDN-B, KM-A and KM-B should be located within the same QKD node. Keys can then be transferred between KM-A and KM-B through Kxi' within the secure operational environment of the IWN (trusted node).

Information which is transferred at Kxi’ and Cxi’ is the same with it at the Kxi and Cxi but Kxi’ and Cxi’ are internal interfaces within a trusted node.

Figure 4 illustrates a functional model for QKDNi with IWN.

This model shows both QKDNs are distributed QKDN, and QKDN controllers are accommodated in the IWN to control KMs and QKDN modules. When QKDNs are centralized QKDNs, KMs and QKD modules in the IWN are controlled by the centralized QKDN controller in each QKDN.

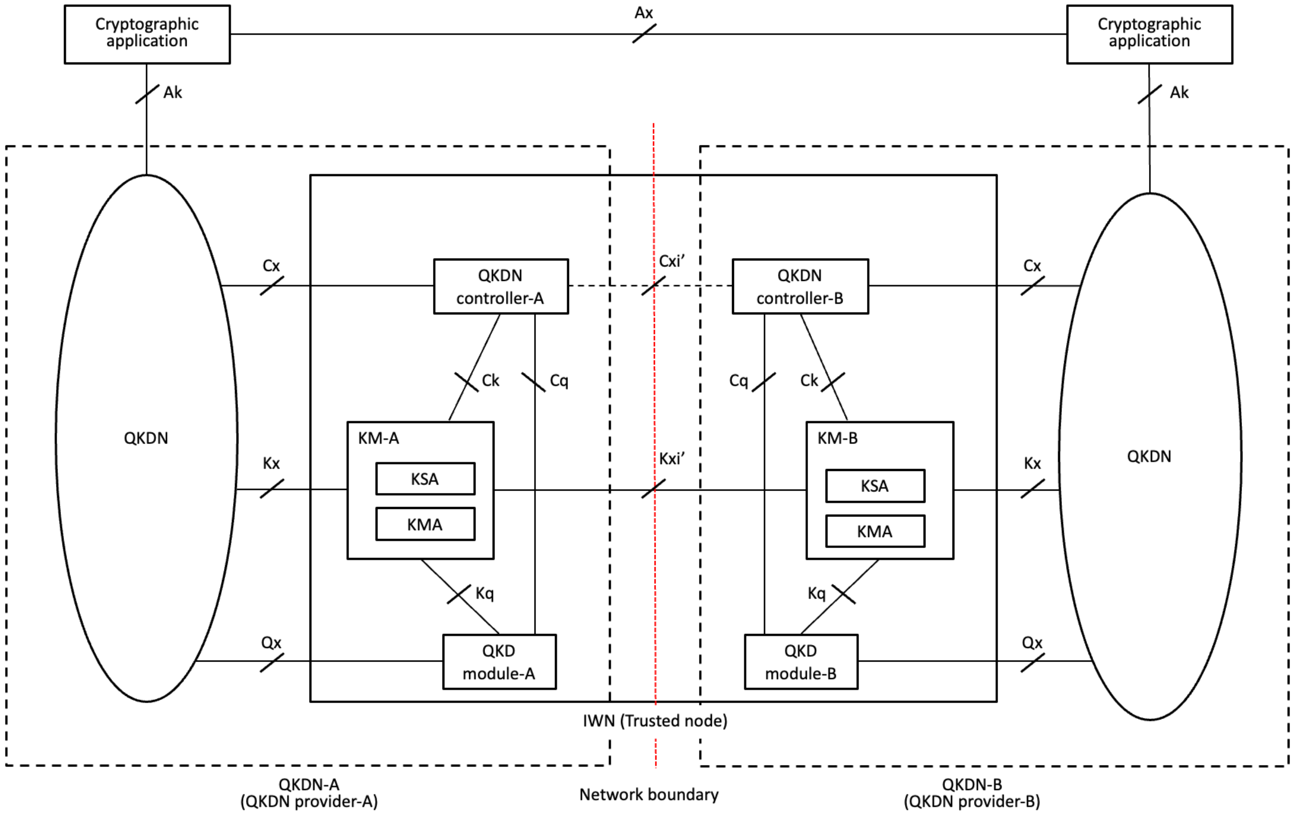

Figure 4 – Functional model for QKDNi with IWN

9. Configurations for QKDNi

9.1. Configuration for QKDNi with GWFs

Figure 5 illustrates a configuration for QKDNi with GWNs.

This configuration shows the QKDN-A is a distributed QKDN and the QKDN-B is a centralized QKDN. QKDN-A and QKDN-B are interworking with GWFs which are accommodated in each GWN. GWN are connecting via Qx, Kxi and optionally Cxi.

When keys are relayed from QKDN-A to QKDN-B via Kxi interface, they can be encrypted with OTP encryption.

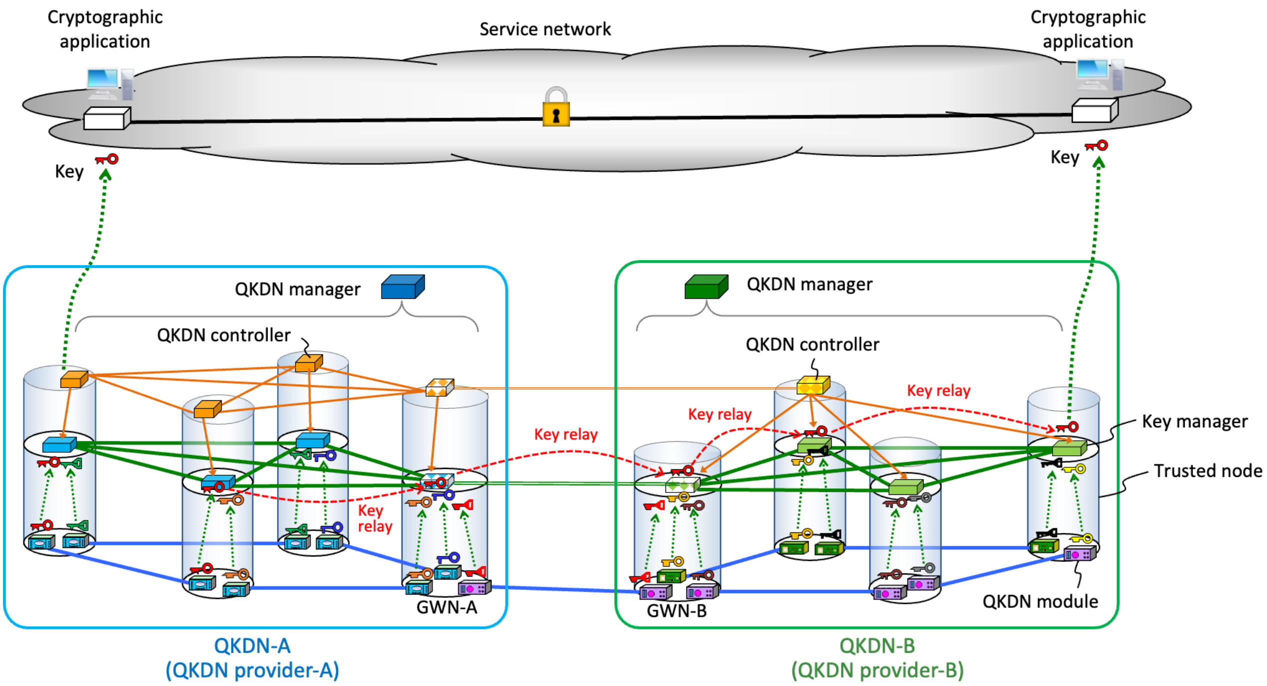

Figure 5 - Configuration for QKDNi with GWFs

9.2. Configuration for QKDNi with IWFs

Figure 6 illustrates a configuration for QKDNi with IWFs.

This configuration shows the QKDN-A is a distributed QKDN and the QKDN-B is a centralized QKDN. QKDN-A and QKDN-B are connecting via an IWN. The IWN might be accommodated in common premises of two QKDN providers or belong to one of them.

Keys are transferred between two QKDN providers within the secure operational environment of the IWN (trusted node).

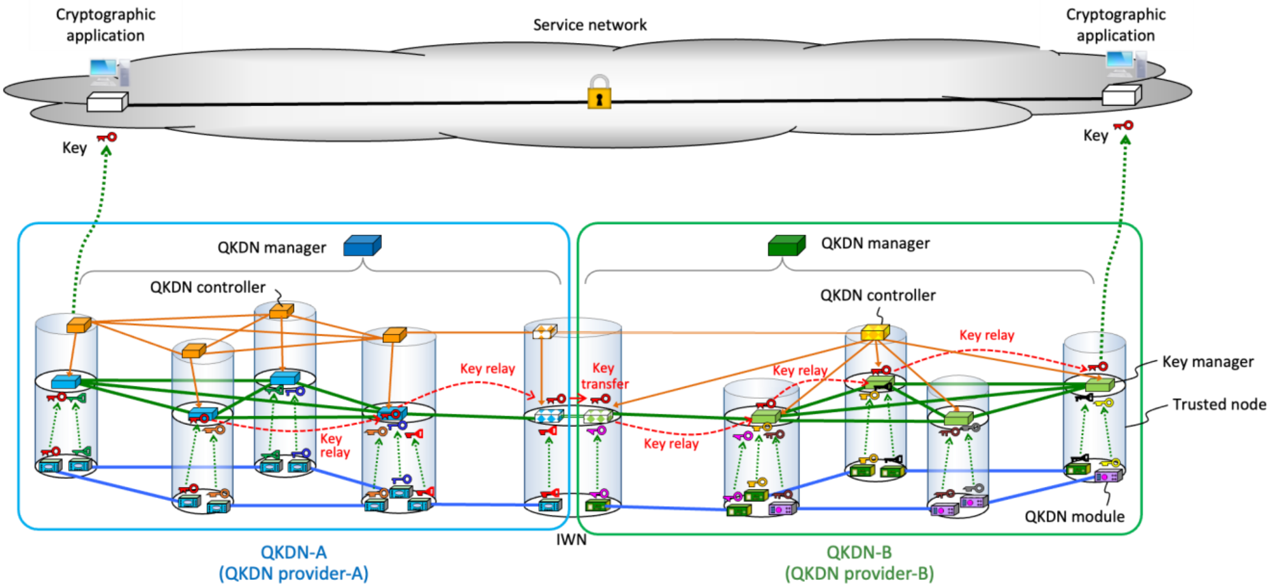

Figure 6 - Configuration for QKDNi with IWFs

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.

Appendix I

QKDNi with different key relay schemes

(This appendix does not form an integral part of this Recommendation.)

This appendix provides two cases to support QKDNi with different key relay schemes.

NOTE - Key relay schemes case 1 and case 2 are specified in [ITU-T Y.3800].

I.1 QKDNi key relay **scheme - case 1**

A key relay scheme in QKDNi to share a key between the source node and destination node is illustrated in Figure I-1. Meanwhile, the source node in QKDN-A, the destination node in QKDN-B. The Key_{12} is generated between KMA-1 and KMA-2. The Key_{12} is relayed from KMA-2 to KMA-3 by OTP encryption with the Key_{23}. It is relayed from KMA-3 to KMA-4 by OTP encryption with the Key_{34}.

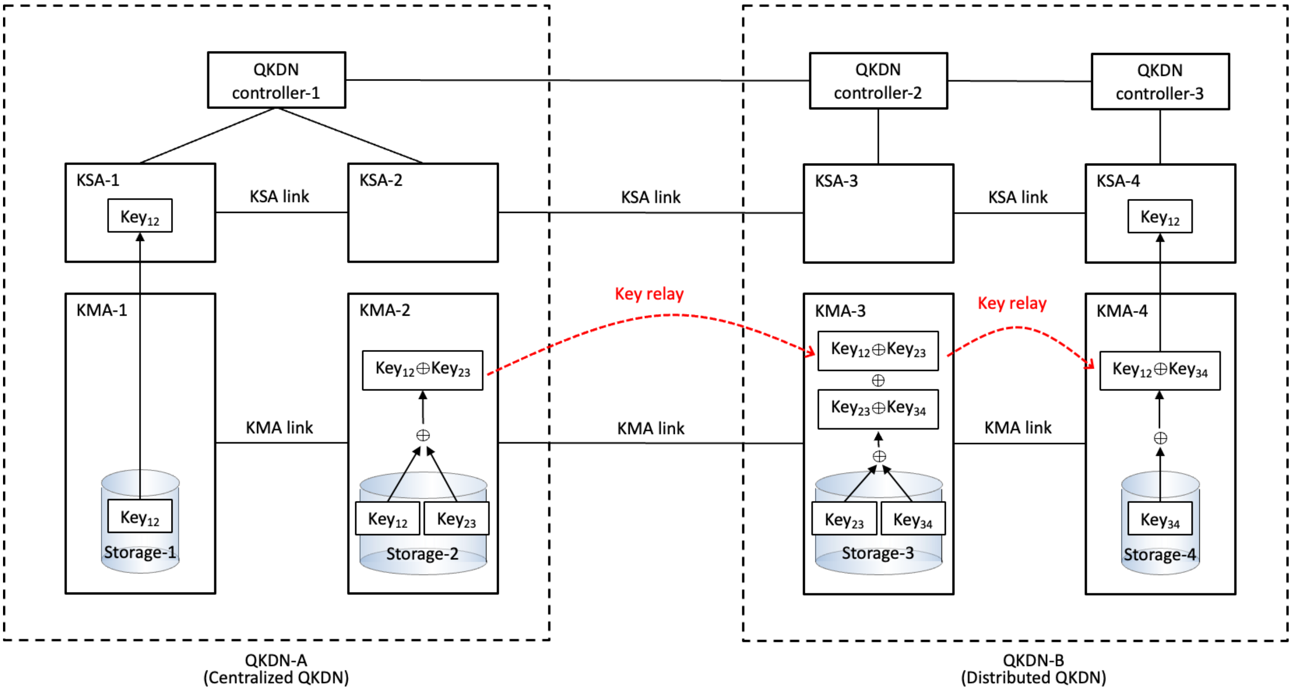

Figure I-1 – QKDNi key relay scheme - case 1

I.2 QKDNi key relay scheme - case 2

In case 2, which is illustrated in Figure I-2, a random bit string Key_{RN} which is generated locally at KMA-1 in QKDN-A is used for key relay from KMA-1 to KMA-4.

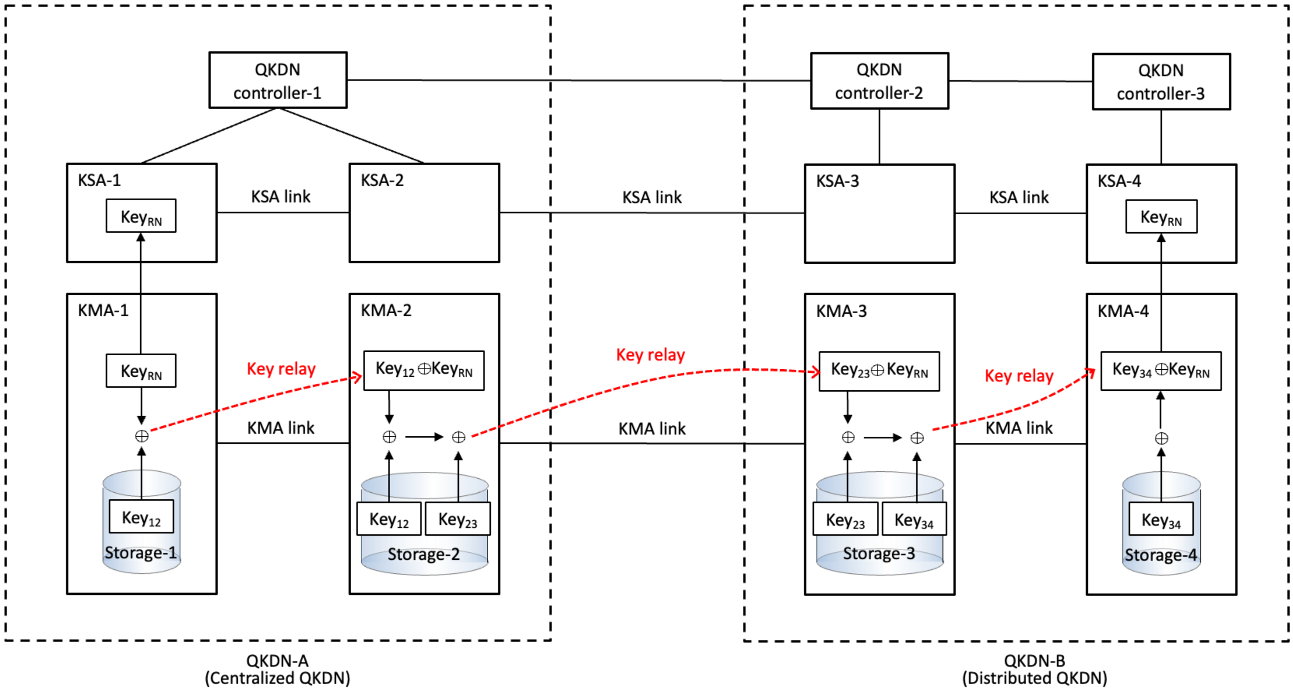

Figure I-2 – QKDNi key relay scheme - case 2

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.*

____