International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3810

(09/2022)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Quantum key distribution networks

Quantum key distribution network interworking – Framework

Recommendation ITU-T Y.3810

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Computing power networks	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3599
BIG DATA	Y.3600–Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	**Y.3800–Y.3999**
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.3810

Quantum key distribution network interworking – Framework

Summary

For quantum key distribution networks (QKDN), Recommendation ITU-T Y.3810 specifies the 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.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3810	2022-09-29	13	11.1002/1000/15063

Keywords

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

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.3810

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), *Overview on networks supporting quantum key distribution.*

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

[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

None.

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

QKD-Rx QKD Receiver

QKD-Tx QKD Transmitter

5 Conventions

None.

6 Overview of QKDNi

A quantum key distribution network (QKDN) [ITU-T Y.3800] is a cryptographic infrastructure to provide secure symmetric keys to cryptographic applications in user networks. When constructing a large scale QKDN which covers a wide area, it may consist of multiple QKDNs interworking each other.

The functional requirements and architecture of a 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 – QKDN provider is specified in [ITU-T Y.3809].

QKDN providers may have their own policies for such as service in terms of charging, routing and security. Network topologies and technology which are used in QKDN are confidential information. They do not 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 from transferring 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.

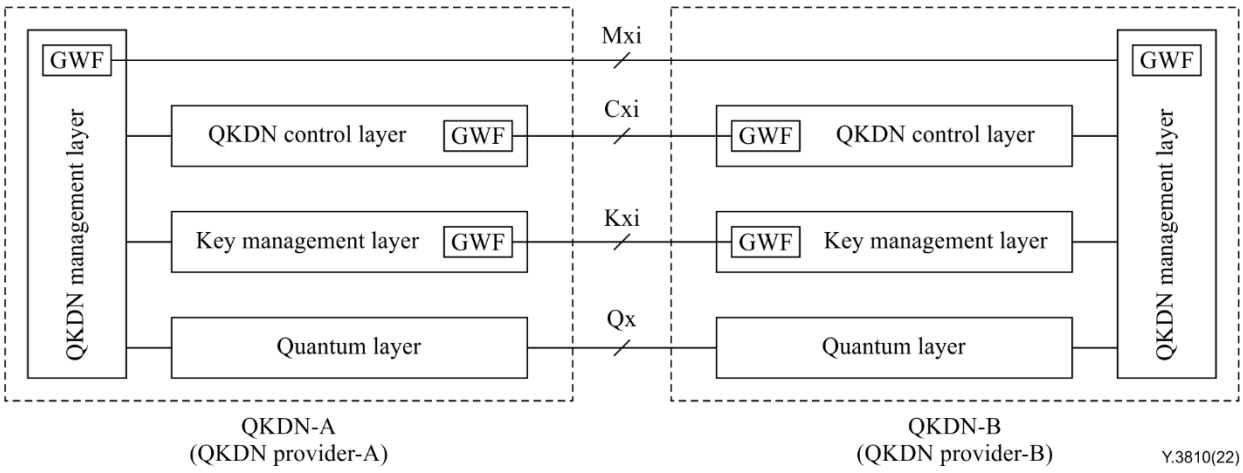

Figure 1 – Reference model for QKDNi with GWFs

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 where standardized protocols are used in a QKDN internally, the GWF conducts protocol conversion that gets into alignment with the 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 layers: When keys are relayed between QKDN providers through the 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 layers: QKDN control information can be shared between QKDN providers through the 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 layers: QKDN management information can be shared between QKDN providers through the 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 connected between service providers. Customer control and fault, configuration, accounting, performance, security (FCAPS) should be managed by each provider.

NOTE 3 – Qx is a reference point for interworking of quantum layers without GWFs. When QKD-keys are shared between QKDN providers through the 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 layers 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 layers, QKDN control layers and QKDN management layers. 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 interworking functions (IWFs).

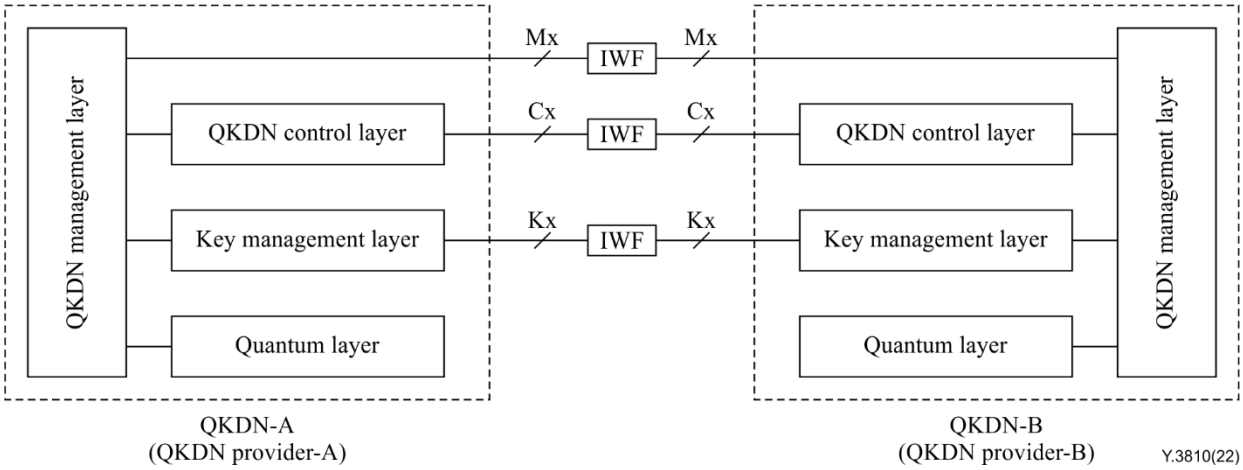

Figure 2 – Reference model for QKDNi with IWFs

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 the QKDN which is interworking. 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 gateway nodes (GWNs)

QKDN-A and QKDN-B connect at Qx, Kxi, and optionally at Cxi. Qx and Kxi can be used to perform secure key relay with one-time pad (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 nodes 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 the 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.

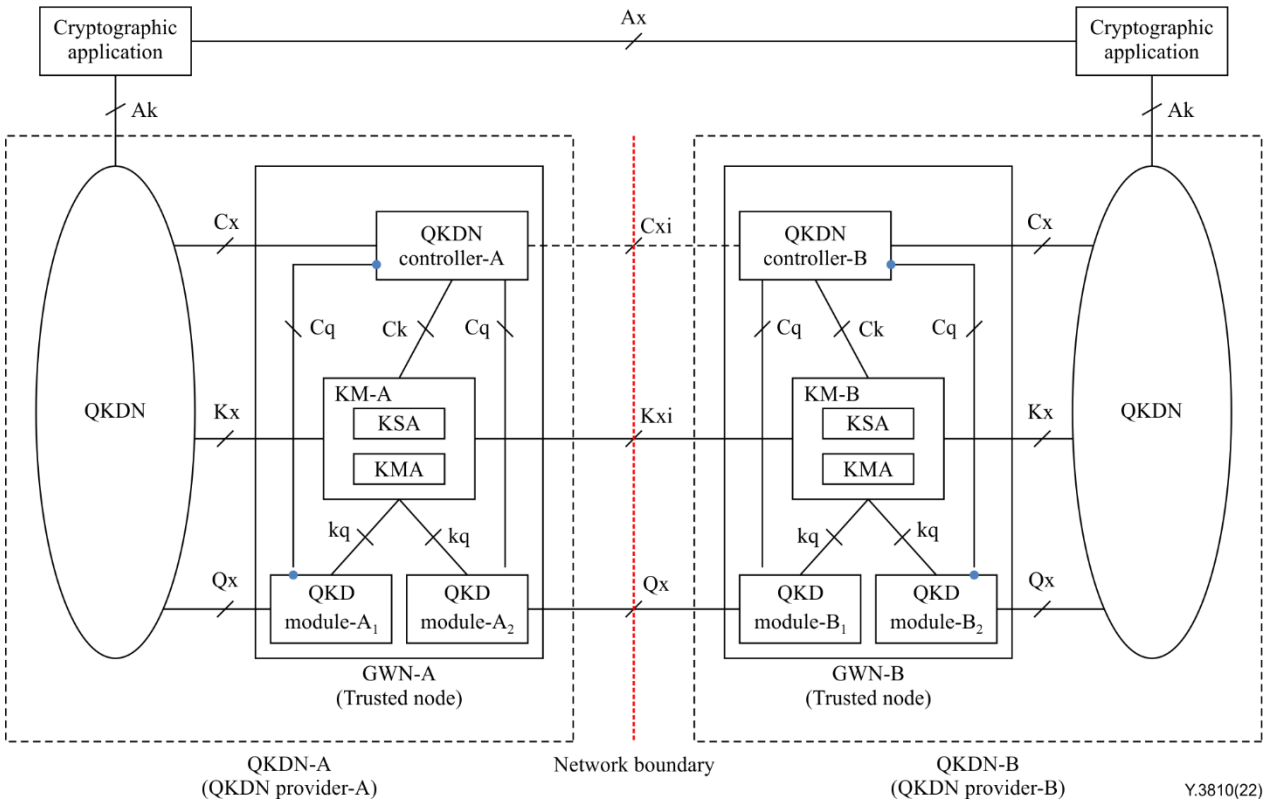

Figure 3 – Functional model for QKDNi with GWNs

8.2 Functional model for QKDNi with interworking nodes (IWNs)

QKDN-A and QKDN-B connect at Kxi' and optionally at 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 as 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.

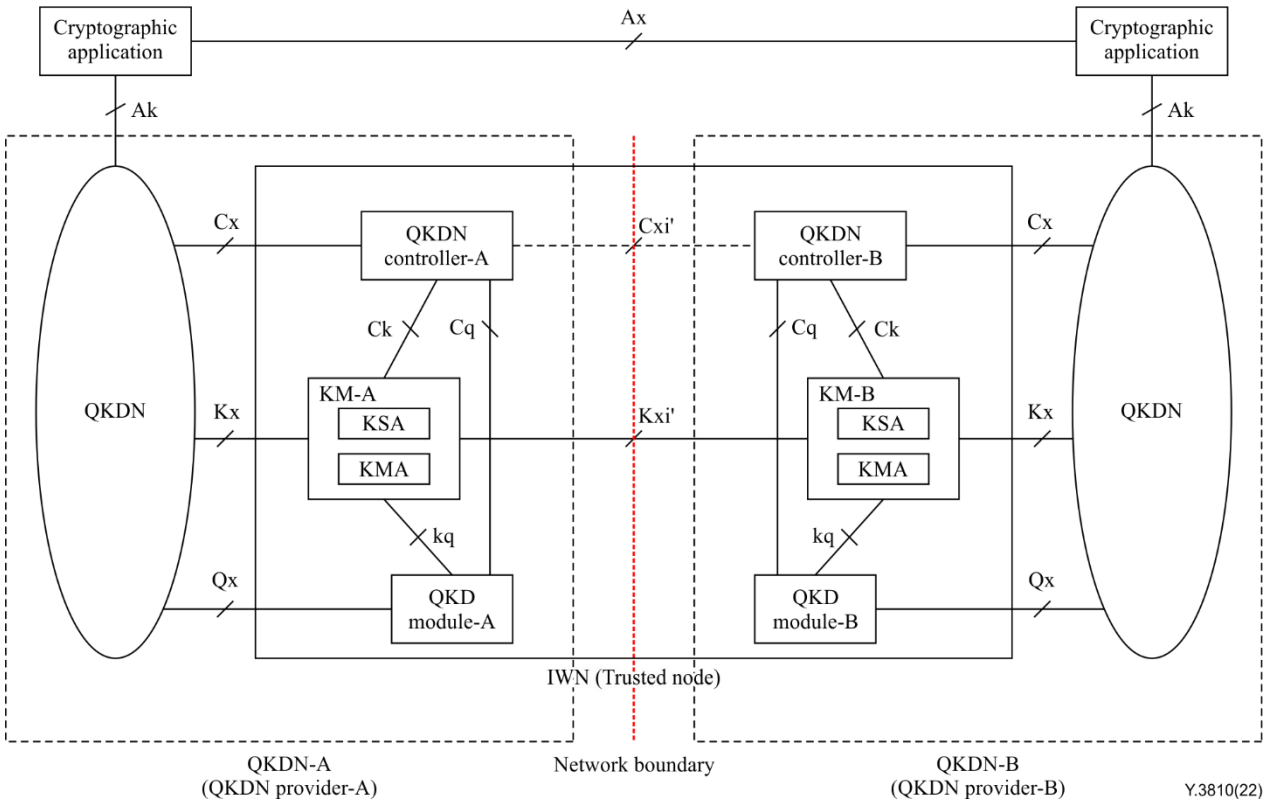

Figure 4 – Functional model for QKDNi with IWN

9 Configurations for QKDNi

9.1 Configuration for QKDNi with gateway functions (GWFs)

Figure 5 illustrates a configuration for QKDNi with GWFs.

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 connect via Qx, Kxi and optionally Cxi.

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

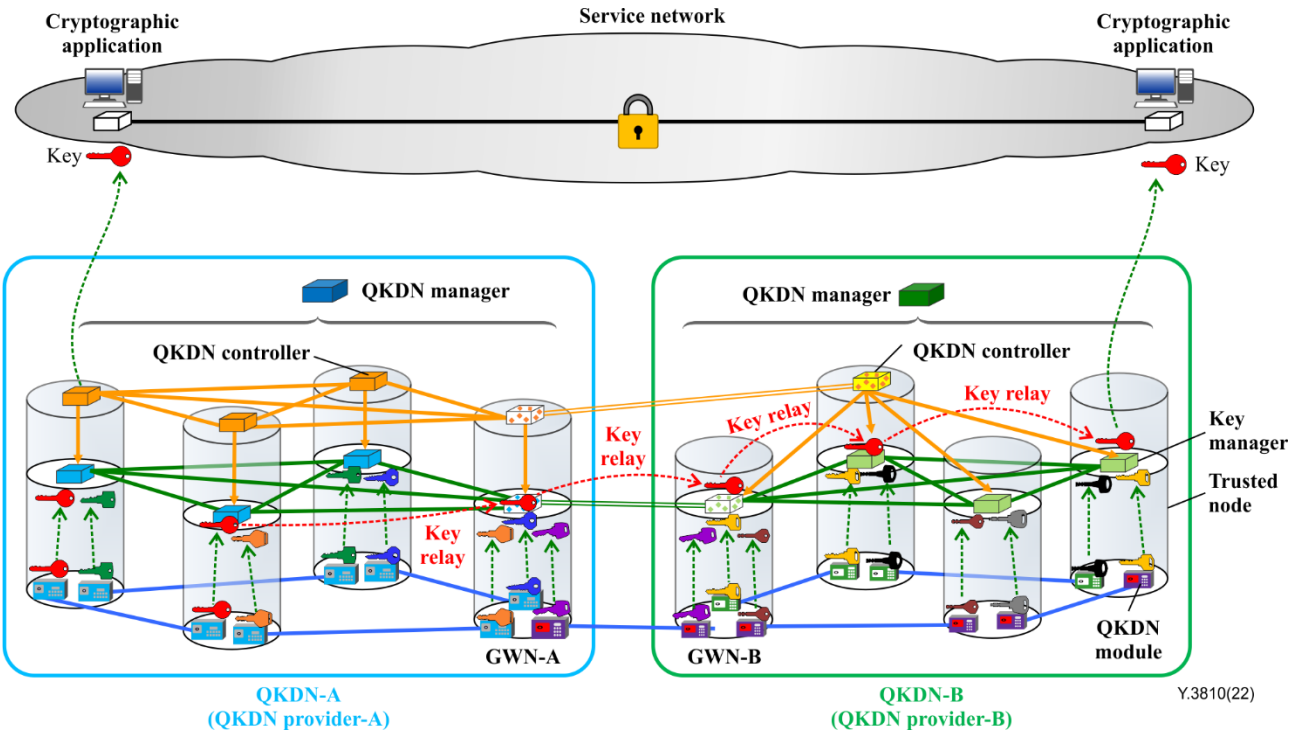

Figure 5 – Configuration for QKDNi with GWFs

9.2 Configuration for QKDNi with interworking functions (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 connect via an IWN. The IWN might be accommodated in common premises of two QKDN providers or may belong to one of them.

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

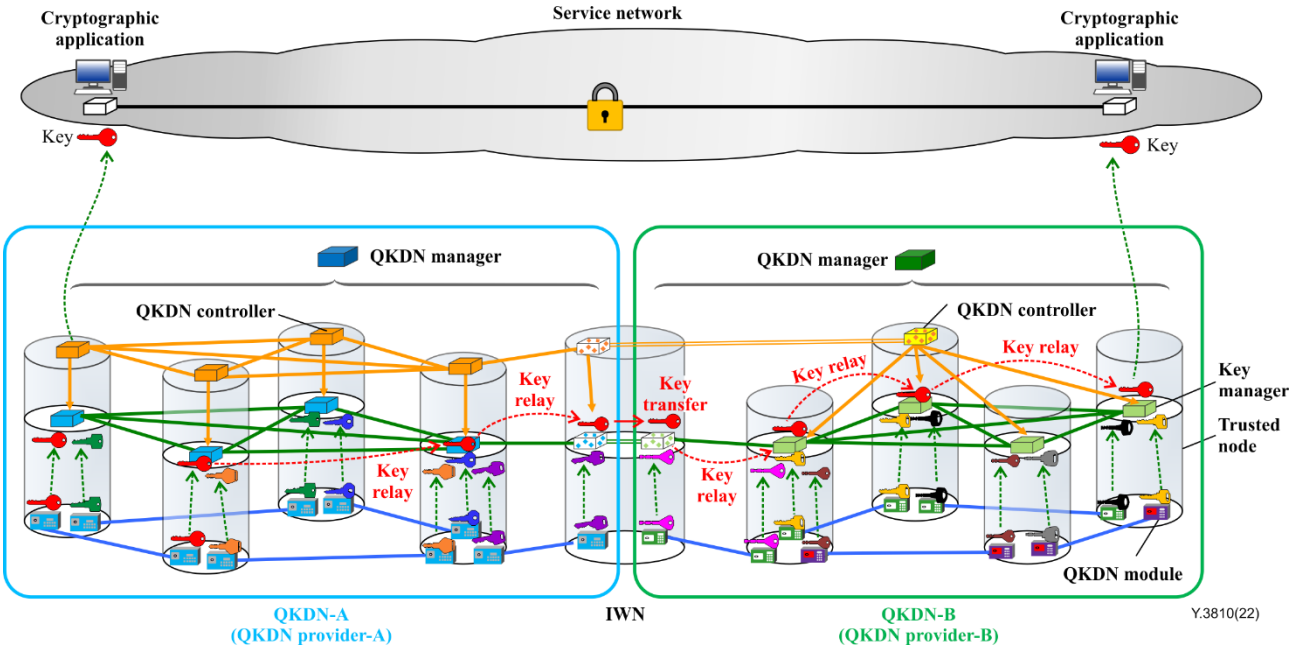

Figure 6 – Configuration for QKDNi with IWFs

10 Security considerations

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}.

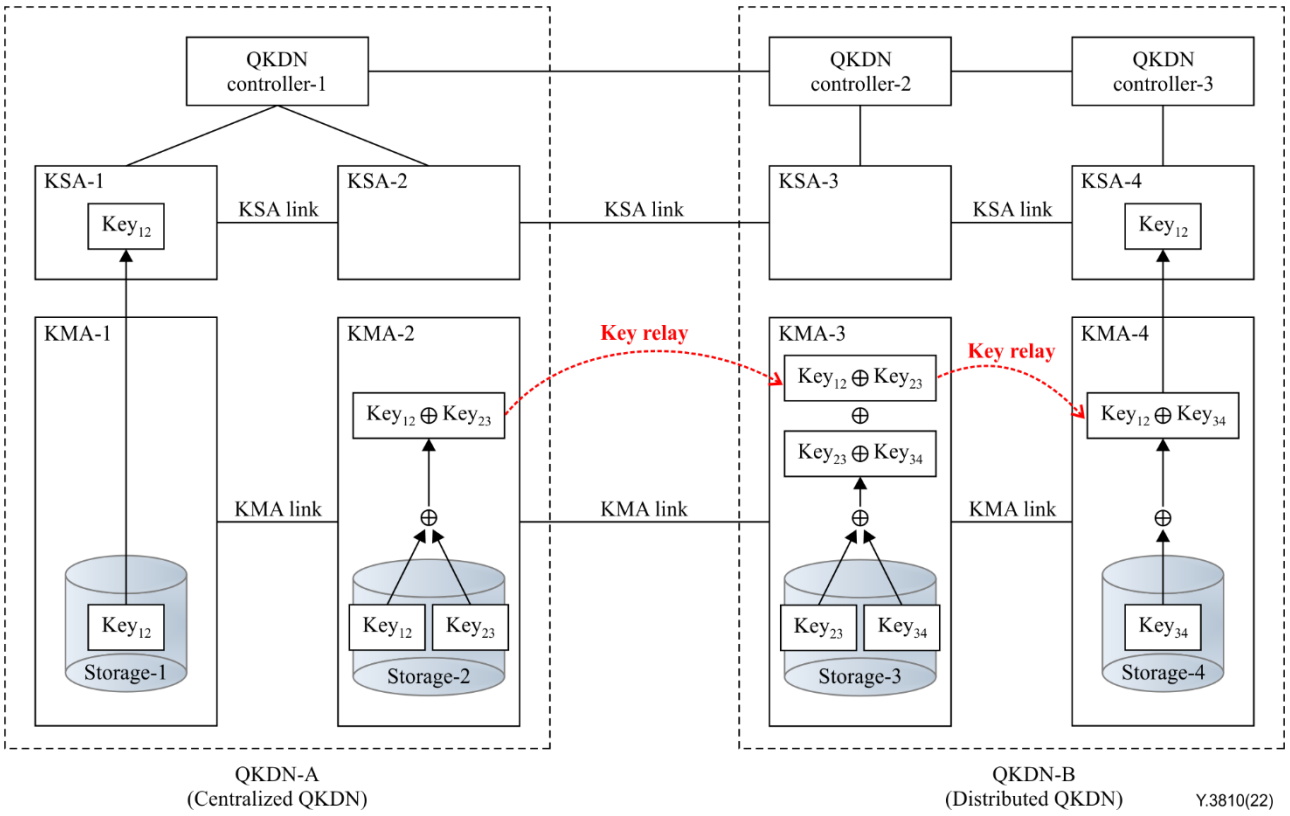

Figure I.1 – QKDNi key relay scheme - case 1

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.

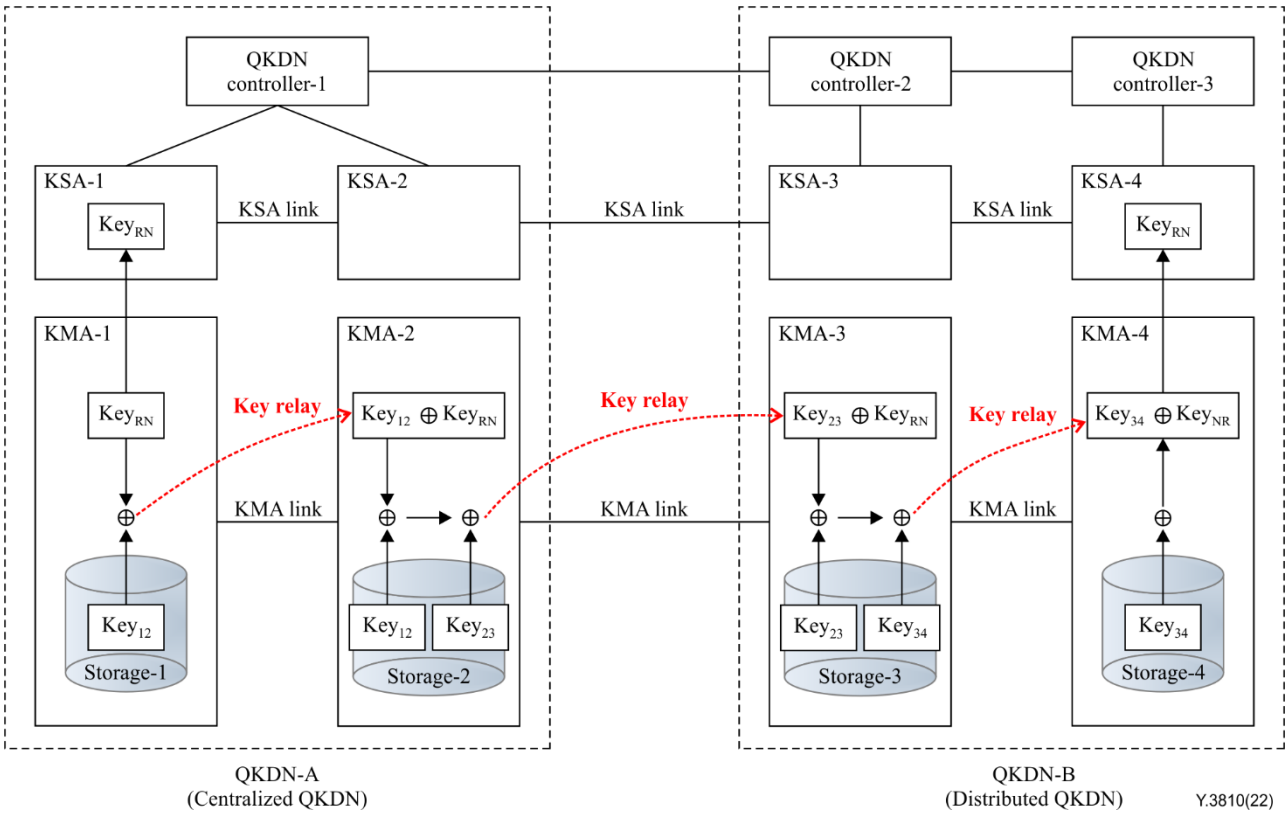

Figure I.2 – QKDNi key relay scheme - case 2

Bibliography

[b-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*.

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

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2022