INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2022-2024

SG11-TD459/GEN

STUDY GROUP 11

Original: English

Question(s): 2/11 Geneva, 10-19 May 2023

TD

Source: Editors

Title: Output – initial baseline text of draft Recommendation ITU-T Q.QKDNi_profr "QKDNi - Protocol framework" (Geneva, 10-19 May 2023)

Contact: Kaoru Kenyoshi
NICT
Japan
Tel :
Fax :
E-mail: kaoru.kenyoshi@nict.go.jp

Contact: Jeongyun Kim
ETRI
Korea (Rep. of)
Tel: + 82-42-860-5311
Fax:
E-mail: jykim@etri.re.kr

Contact: Hongyu Wu
QuantumCTek Co., Ltd.
China
Tel :
Fax :
E-mail: hongyu.wu@quantum-info.com

Abstract: This TD includes the output - baseline text of a new work item Q.QKDNi_profr "QKDNi - Protocol framework" (Geneva, 10-19 May 2023)

Summary

This TD is the outcome of initial draft Recommendation ITU-T Q.QKDNi_profr "QKDNi - Protocol framework" based on the discussion results on contribution C125R1 and C132 with modifications at the Q2/11 meetings (Geneva, 10-19 May 2023).

Attachments:

Annex A: Draft Recommendation ITU T Y.QKDNi_profr "QKDN Interworking- Protocol framework"

Annex A: Proposed initial draft of Q.QKDNi_profr

Initial draft Recommendation ITU-T Q.QKDNi_profr

Quantum key distribution networks Interworking - Protocol framework

Summary

Recommendation ITU-T Q.QKDNi_profr specifies protocol framework including signalling requirements and protocols for quantum key distribution networks Interworking (QKDNi).

Keywords

Protocol, QKD (quantum key distribution), QKDN (QKD network), QKDNi (QKDN interworking), signalling requirement.

Table of Contents

Initial Draft Recommendation ITU-T Q.QKDNi_profr

Quantum key distribution networks Interworking- Protocol framework

1 Scope

This Recommendation specifies a protocol framework for signalling aspects of a quantum key distribution network interworking (QKDNi), especially the following areas:

- Overview of signalling and protocols for QKDN interworking
- Signalling requirements for QKDN interworking
- Protocol suites for QKDN interworking.

NOTE – QKD protocols which perform between QKD modules of interworking QKDN through QKD links are outside the scope of this Recommendation.

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 X.1710] Recommendation ITU-T X.1710 (2020), *Security framework for quantum key distribution networks*

[ITU-T X.1712] Recommendation ITU-T X.1712 (2021)/Cor.1 (02/2022), *Security requirements and measures for quantum key distribution networks - key management*

[ITU-T Y.3800] Recommendation ITU-T Y.3800 (2019)/Cor.1 (04/2020), *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) /Cor.1 (04/2021), *Quantum key distribution networks - Functional architecture*

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

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

[ITU-T Y.3810] Recommendation ITU-T Y.3810 (2022), *Quantum key distribution networks - Quantum key distribution network interworking – Framework*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 **information theoretically secure (IT-secure)** [ITU-T Y.3800]: Secure against any deciphering attack with unbounded computational resources.

3.1.2 **key management** [ITU-T Y.3800]: All activities performed on keys during their life cycle starting from their reception from the quantum layer, the storage, formatting, relay, synchronization, authentication, to supply to cryptographic application and delete or preserve depending on the key management policy.

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 manager link (KM link)** [ITU-T Y.3800]: A communication link connecting key managers (KMs) to perform key management.

3.1.5 **key relay** [ITU-T Y.3800]: A method to share keys between arbitrary quantum key distribution (QKD) nodes via intermediate QKD node(s).

3.1.6 **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 client.

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 client.

3.1.7 **key supply agent-key (KSA-key)** [ITU-T Y.3803]: Key data stored and processed in a key supply agent (KSA), and securely shared between a KSA and a matching KSA.

3.1.8 **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.

3.1.9 **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.

3.1.10 **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).

3.1.11 **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.

3.1.12 **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.

3.1.13 **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.

3.1.14 **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:

GWF	Gateway Function
GWN	Gateway Node
IT-secure	Information-theoretically secure
IWF	Interworking Function
IWN	Interworking Node
KM	Key Manager
KSA	Key Supply Agent
QKD	Quantum Key Distribution
QKDN	QKD Network
QKDNi	QKDN interworking
QKD-Rx	QKD Receiver
QKD-Tx	QKD Transmitter

5 Conventions

None.

6 Overview

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. 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 procedure of QKDN in [ITU-T Y.3802].

When constructing a large scale QKDN which covers a wide area, it may consist of multiple QKDNs interworking each other. In this regard, the overview of QKDN interworking (QKDNi), the reference models, and the functional models of gateway functions (GWFs) and interworking functions (IWFs) are described in [ITU-T Y.3810]. [ITU-T Y.3813] describes the functional requirements for key management layer, QKDN control layer, and QKDN management layer, for interworking using gateway nodes (GWNs) and/or interworking nodes (IWNs). Furthermore, [ITU-T Y.QKDN-iwac] specifies functional architecture as well as operational procedure for QKDNi.

This Recommendation describes a framework of signalling requirements and protocols for QKDNi. Various kinds of protocols can be used in a QKDNi. This Recommendation specifies a framework of signalling requirements and protocols for key management layer, QKDN control layer and QKDN management layer. Protocols for quantum layer which are performed between two QKD modules are outside the scope of this Recommendation.

Based on the conceptual models on QKDNi illustrated in [ITU-T Y.3810] and the QKDNi functional requirements identified in [ITU-T Y.3813], two functional architectures for QKDNi with GWNs and IWNs are specified in [ITU-T Y.QKDN-iwac].

7 Reference models for QKDNi

7.1 Reference model for QKDNi with GWFs

Figure 1 shows a reference model for QKDNi with GWFs which is defined in [ITU-T Y.3810].

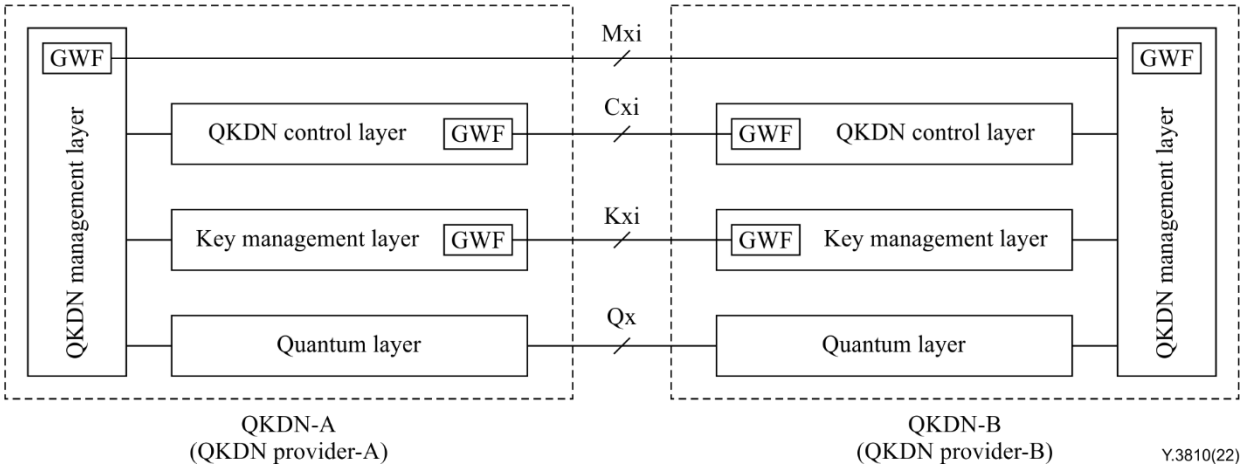

Figure 1 – Reference model for QKDNi with GWFs defined in [ITU-T Y.3810]

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.

7.2 Reference model for QKDNi with IWFs

Figure 2 shows a reference model for QKDNi with interworking functions (IWFs) which is defined in [ITU-T Y.3810].

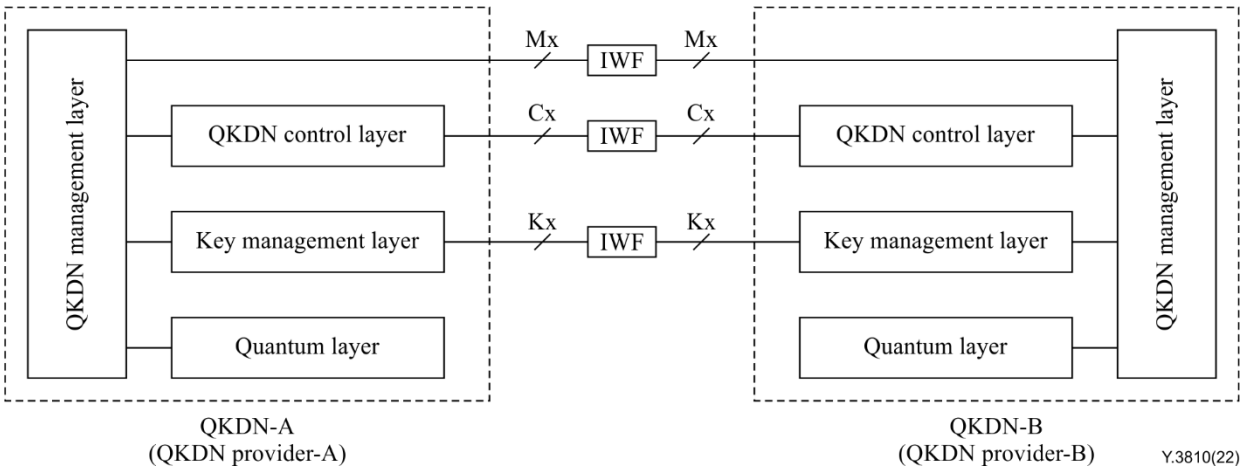

Figure 2 – Reference model for QKDNi with IWFs defined in [ITU-T Y.3810]

Figure 3 shows a functional model for QKDNi with interworking functions (IWFs) which is defined in [ITU-T Y.3810].

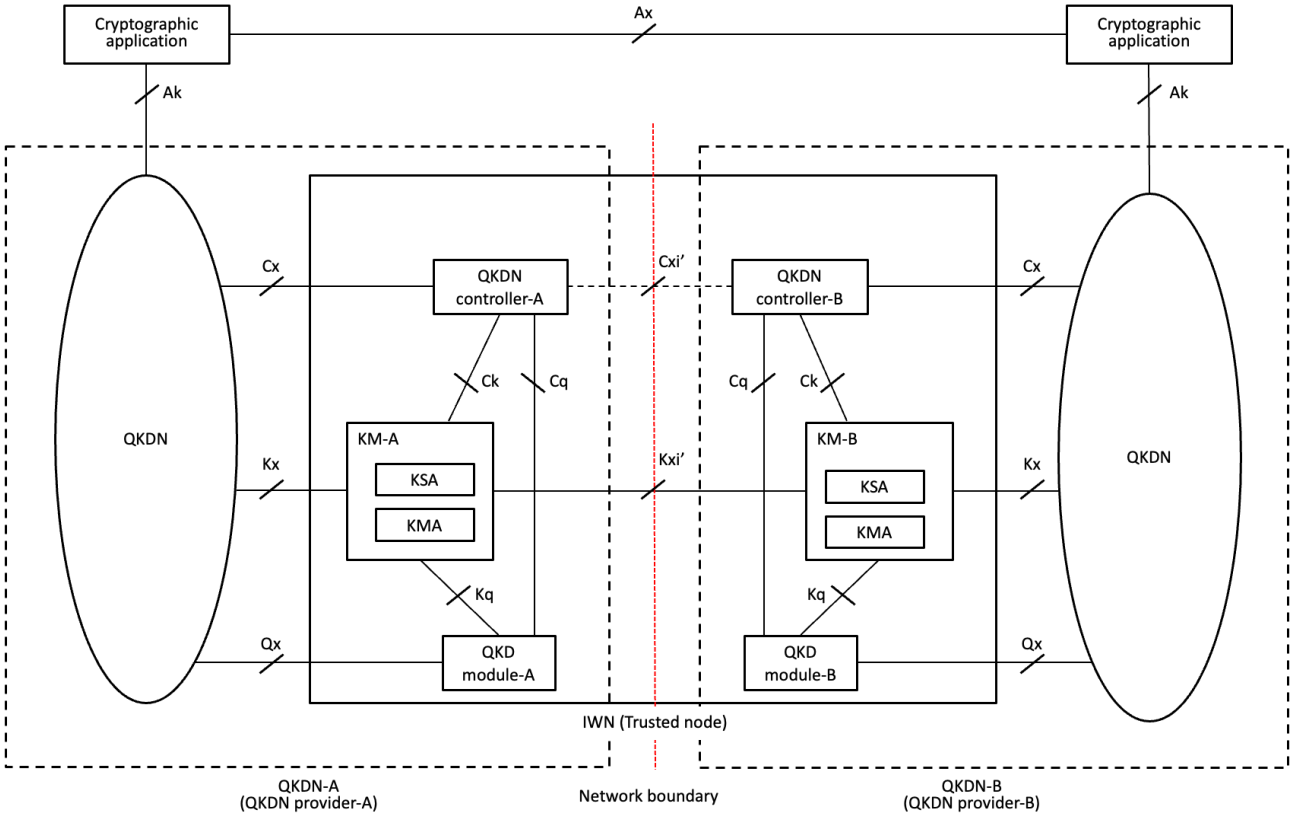

Figure 3 – Functional model for QKDNi with IWFs defined in [ITU-T Y.3810]The following two reference points are identified in IWN.

- Kxi' is a reference point for interworking of key management layers in IWN.

NOTE 1 - Keys can be transferred between KM-A and KM-B through Kxi' within the secure operational environment of the IWN (trusted node).

- Cxi' is a reference point for interworking of QKDN control layers in IWN.

NOTE 2 - 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. Protocols at Kxi' and Cxi' might be different from them at Kxi and Cxi.

8 Signalling requirements

This clause specifies signalling requirements of each reference points specified in [ITU-T Y.3813].

Table 1 summarises information which is transferred at each reference point.

Table 1 – transferred information at reference points

reference points	Transferred information			Note
	key data	metadata	Control and management information	
Kxi, Kxi'	✓	✓	✓	
Cxi, Cxi'		✓	✓	
Mxi			✓	

9 Protocol suites and stacks

This clause specifies protocol suites in QKDN. Appropriate protocols can be selected for each reference points and network interfaces.

Table 2 includes list of protocols which can be applied at each reference point.

Table 2 – protocol suites

		reference	Note
High layer protocols	RPC HTTP/HTTPS	*RFC 5531 [b-IETF RFC 5531]* *RFC 7231 [b-IETF RFC 7231:*	
L4 protocols	TLS TCP UDP	*RFC 5246 [b-IETF RFC 5246]* *RFC 793 [b-IETF RFC793]* *RFC 768 [b-IETF 768]*	
L3 protocols	IP	*RFC 791 [b-IETF 791]* *RFC2460 [b-IETF 2460]*	
L2 protocols	Ethernet	*IEEE 802.3 [b-IEEE 802.3]*	

Figure 3 illustrates protocol stacks between …

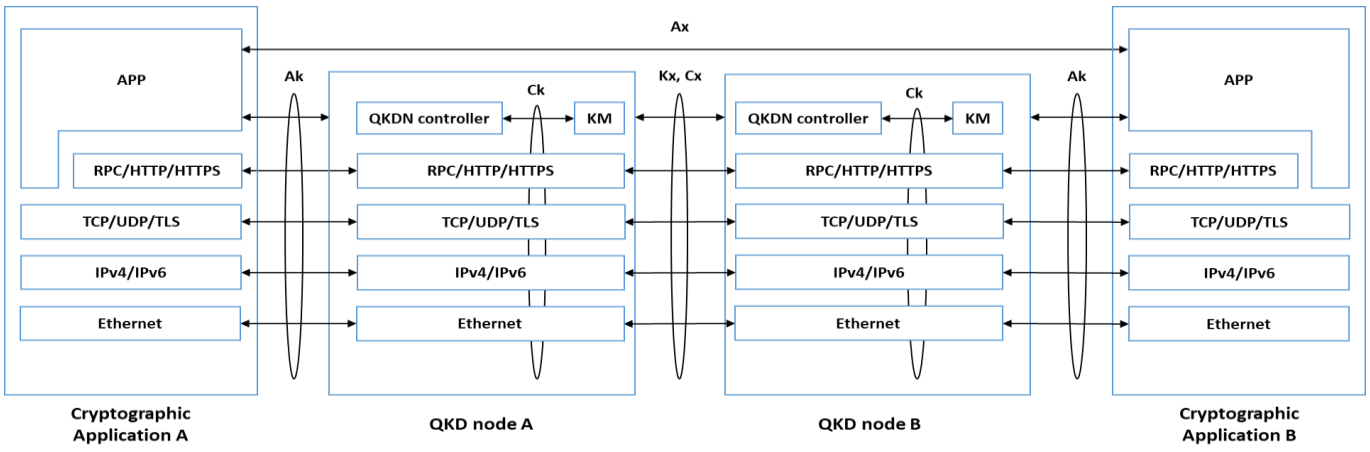

Figure 3 - Protocol stacks between KMs and between QKDN controllers in QKDN interworking

Figure 4 illustrates protocol stacks between QKDN managers in QKDN interworking.

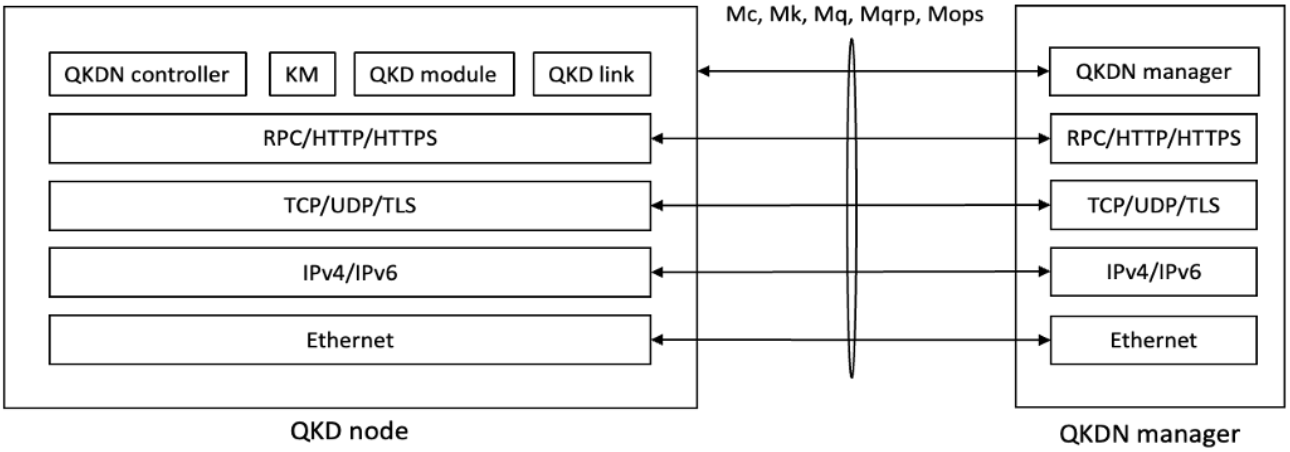

Figure 4 – Protocol stacks between QKDN managers in QKDN interworking.

Bibliography

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

[b-ETSI GS QKD 014] ETSI GS QKD 014 V1.1.1 (2019-02), *Protocol and data format of REST-based key delivery API.*

[b-ITU-T FG-QIT4N D2.3] D2.3 *Technical Report on quantum key distribution network (QKDN) protocols part 2: Key management layer, QKDN control layer, and QKDN management layer*.

[b-IETF RFC 5531] IETF RFC 5531, *RPC: Remote Procedure Call Protocol Specification Version 2.*

[b-IETF RFC 7231] IETF RFC 7321, *Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content.*

[b-IETF RFC 5246] IETF RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2.*

[b-IETF RFC 793] IETF RFC 793, *TRANSMISSION CONTROL PROTOCOL*.

[b-IETF RFC 768] IETF RFC 768, *User Datagram Protocol*.

[b-IETF RFC 791] IETF RFC 791, *INTERNET PROTOCOL*.

[b-IETF RFC 2460] IETF RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification.*

[b-IEEE 802.3] IEEE 802.3-2018, IEEE Standard for Ethernet.

Appendix I

Signalling procedures

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

Editor's note – This appendix will include signalling procedures for QKDN interworking.