INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2022-2024

SG11-TD453/GEN

STUDY GROUP 11

Original: English

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

TD

Source: Editors

Title: Output – draft baseline text of draft Recommendation ITU-T Q.QKDN_profr "Quantum key distribution networks - Protocol framework" (Geneva, 10-19 May 2023)

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

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

Contact: Taesang Choi
ETRI
Korea (Rep. of)
E-mail: choits@etri.re.kr

Abstract: This document contains output baseline text of draft Recommendation Q.QKDN_profr "Quantum key distribution networks - Protocol framework".

Summary

This TD is the outcome of revised draft Recommendation ITU-T Q.QKDN_profr "Quantum key distribution networks - Protocol framework" based on the discussion results on input documents C197 with modifications at the Q2/11 meetings (Geneva, 10-19 2023).

Annex I

Draft Recommendation ITU-T Q.QKDN_profr

Quantum key distribution networks – Protocol framework

Summary

Recommendation ITU-T Q.QKDN_profr specifies a framework for signalling requirements and protocols for quantum key distribution networks (QKDN).

Keywords

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

Table of Contents

Draft new Recommendation ITU-T Q.QKDN_profr

Quantum key distribution networks - Protocol framework

1 Scope

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

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

NOTE – QKD protocols which perform between a pair of QKD modules 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*

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:

IT-secure	Information-theoretically secure
KM	Key Manager
KSA	Key Supply Agent
QKD	Quantum Key Distribution
QKDN	QKD Network

5 Conventions

None.

6 Overview

Basic functions and layered structures of the QKDN are defined in [ITU-T Y.3800]. Functional requirements and architectures are specified in [ITU-T Y.3801] and [ITU-T Y.3802], respectively. A security framework for the QKDN is specified in [ITU-T X.1710], by addressing the security threats against the QKDN, and deriving the general security requirements and the security measures for the QKDN. Representative signalling procedures and corresponding message parameters are given as protocol examples for some QKDN reference points in [b-ITU-T FG QIT4N D2.3.2].

This Recommendation describes a framework of signalling requirements and protocols for QKDN. Various kinds of protocols can be used in a QKDN. 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.

Figure 1 shows the functional architecture of QKDN which is defined in [ITU-T Y.3802].

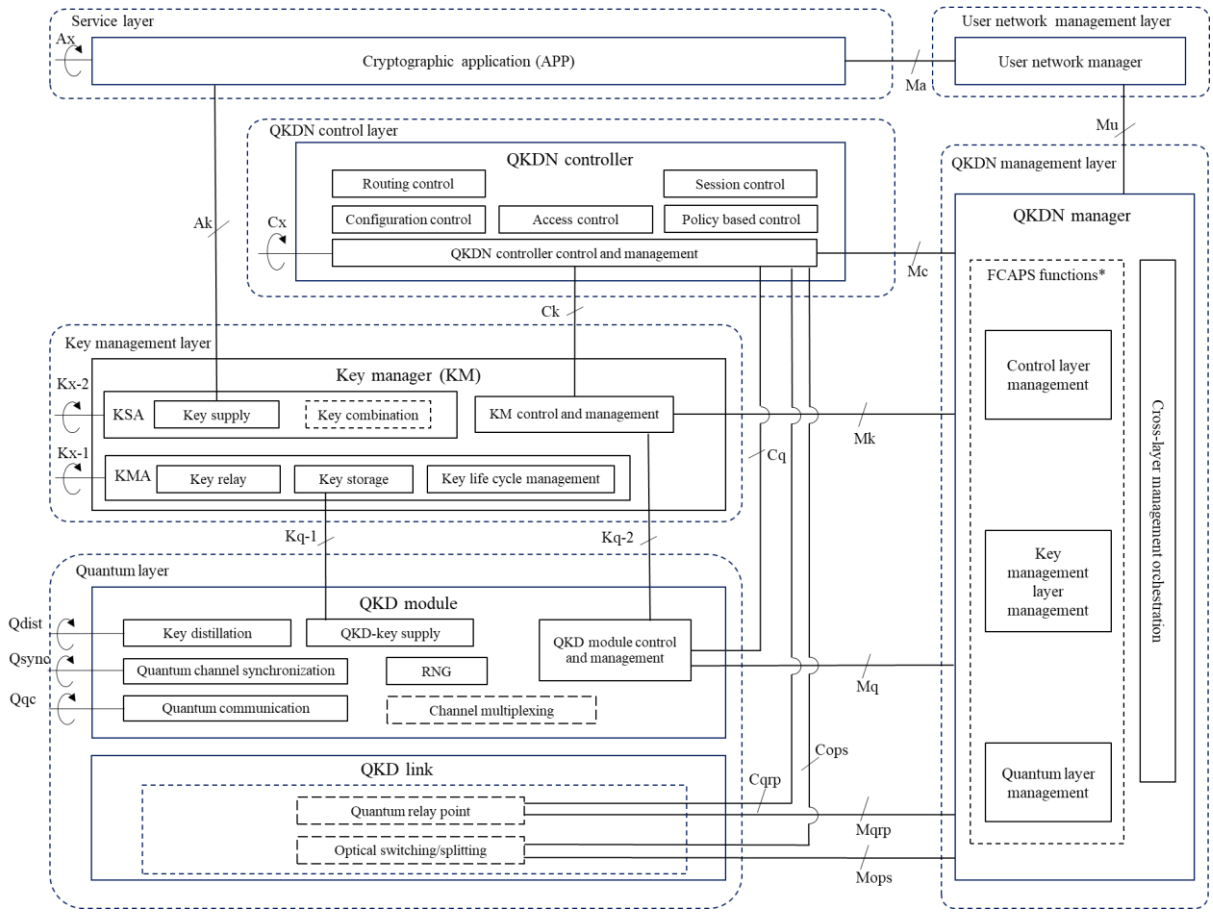

Figure 1 – A functional architecture model of QKDN defined in [ITU-T Y.3802]

The following reference points are defined in [ITU-T Y.3802].

- reference points of QKD modules: Qqc, Qsync, Qdist
- reference points of KMs: Kq-1, Kq-2, Kx-1, Kx-2
- reference points of QKDN controllers: Ck, Cq, Cops, Cqrp, Cx
- reference points of QKDN managers: Mq, Mops, Mqrp, Mk, Mc, Mu
- reference points of user network managers: Ma
- reference points of cryptographic applications: Ak, Ax

The functional architecture model in figure 1 and the above reference points defined in [ITU-T Y.3802] are the references of this Recommendation.

Reference points of Qqc, Qsync, Qdist in the quantum layer, and reference points of Ma, and Ax in the user network are outside the scope of this Recommendation.

7 Signalling requirements

This clause specifies signalling requirements of each reference points. Key file format and metadata are defined in [ITU-T Y.3803]. Control and management information is discussed in [ITU-T Y.3804]. Security requirements and measures on key data, metadata and control and management information are specified in [ITU-T X.1712].

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

Table 1 – transferred information at reference points

reference points	Transferred information	

	key data	metadata	Control and management information	Note
Kq-1	✓	✓	✓	
Kq-2		✓	✓	
Kx-1	✓	✓	✓	IT-secure encryption for key relay such as OTP is highly recommended.
Kx-2		✓	✓	
Ck		✓	✓	
Cq		✓	✓	
Cops			✓	
Cqrp			✓	
Cx		✓	✓	
Mq			✓	
Mops			✓	
Mqrp			✓	
Mk			✓	
Mc			✓	
Mu			✓	
Ak	✓	✓		

8 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 9110~~7231~~ [b-IETF RFC 9110~~7231~~:*	
L4 protocols	TLS TCP UDP	*RFC 5246 [b-IETF RFC 5246]* *RFC 9293~~793~~ [b-IETF RFC 9293~~793~~]* *RFC 768 [b-IETF RFC 768]*	
L3 protocols	IPv4 IPv6	*RFC 791 [b-IETF RFC 791]* *RFC 8200~~2460~~ [b-IETF RFC 8200~~2460~~]*	
L2 protocols	Ethernet	*IEEE 802.3 [b-IEEE 802.3]*	

Figure 2 illustrates protocol stacks between cryptographic applications and KMs and between QKDN controllers in QKDN.

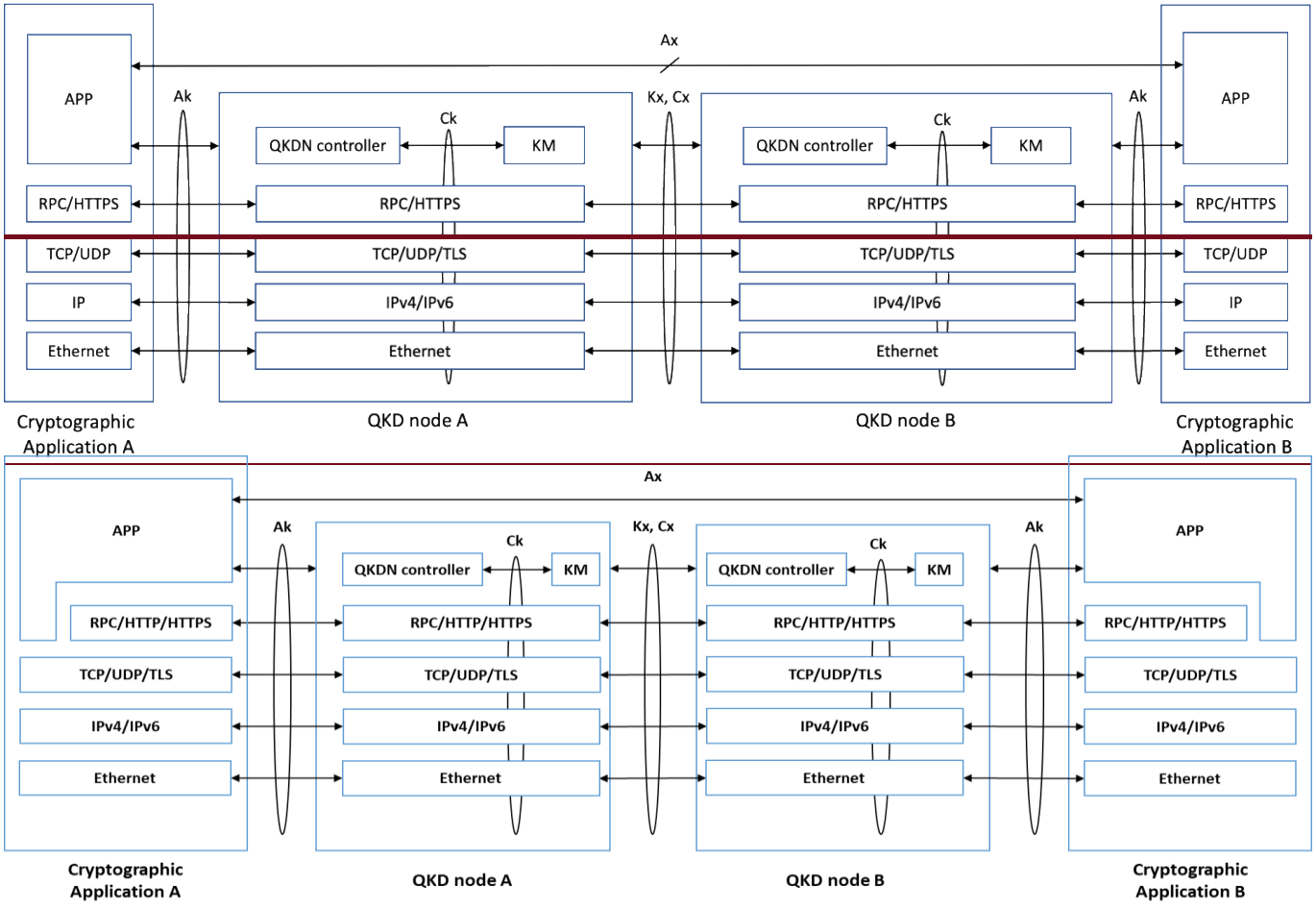

Figure 2 - Protocol stacks between cryptographic applications and KMs and between QKDN controllers in QKDN

Figure 3 illustrates protocol stacks between QKDN controller, KM, QKD module, QKD link and QKDN manager in QKDN.

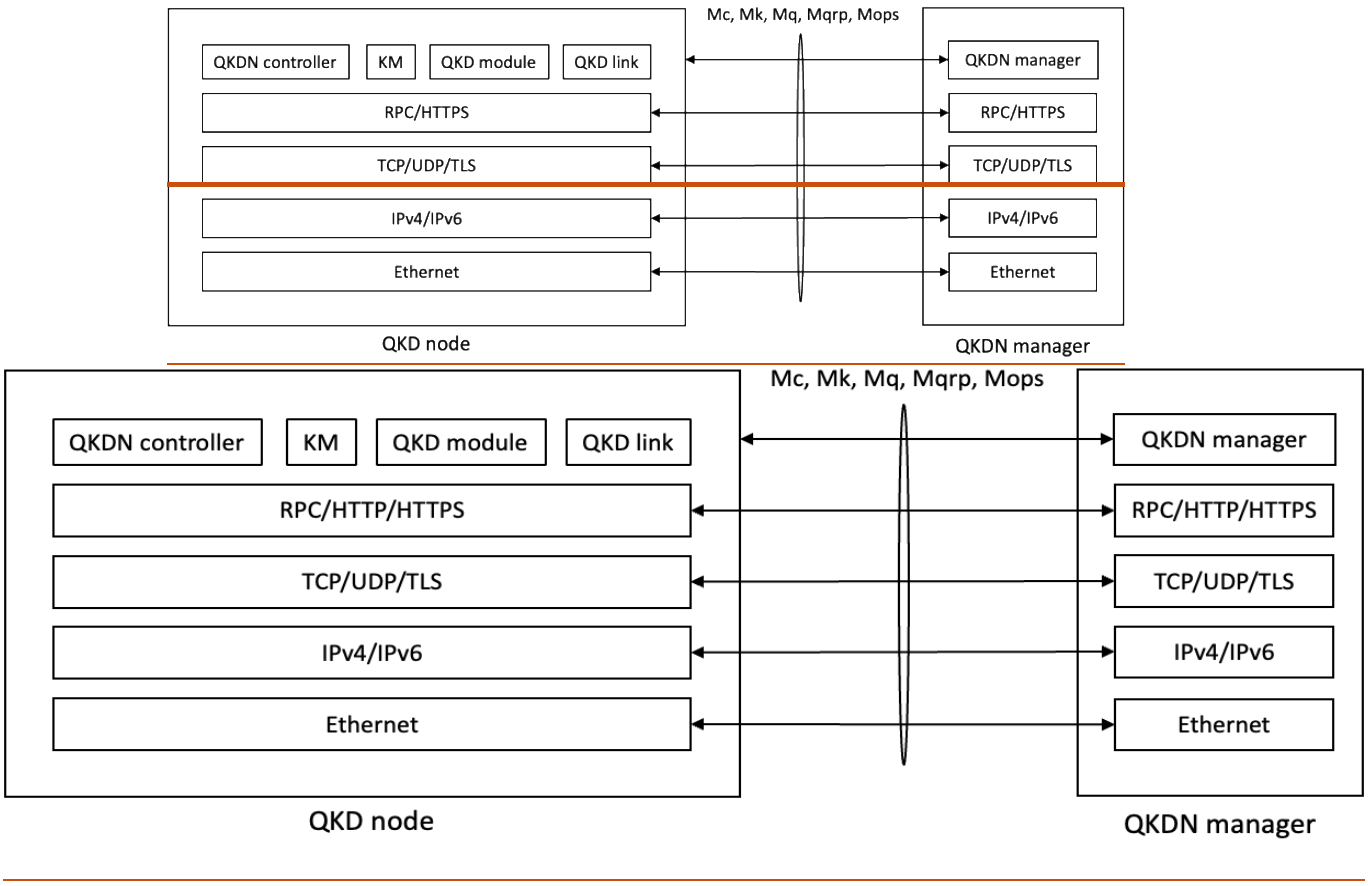

Figure 3 – Protocol stacks between QKDN controller, KM, QKD module, QKD link and QKDN manager in QKDN.

Appendix I

Signalling procedures

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

A.1. Key supply upon request mode

Figure I-1 shows typical signalling procedures for key supply upon request mode implemented by two QKD nodes.

The typical signalling procedures shown in Figure I-1 are briefly described as follows:

1) The source cryptographic application sends "Key request" message to the source KM at the source QKD node.
2) The source KM responds "Response to key request" message to the source cryptographic application with keys requested and the corresponding key IDs.
3) The source cryptographic application sends "Notify key ID" message to the destination cryptographic application with the key IDs.
4) The destination cryptographic application sends "Key request with ID" message with the received key IDs to the destination KM at the destination QKD node.
5) The destination KM responds "Response to key request" message to the destination cryptographic application with keys requested.

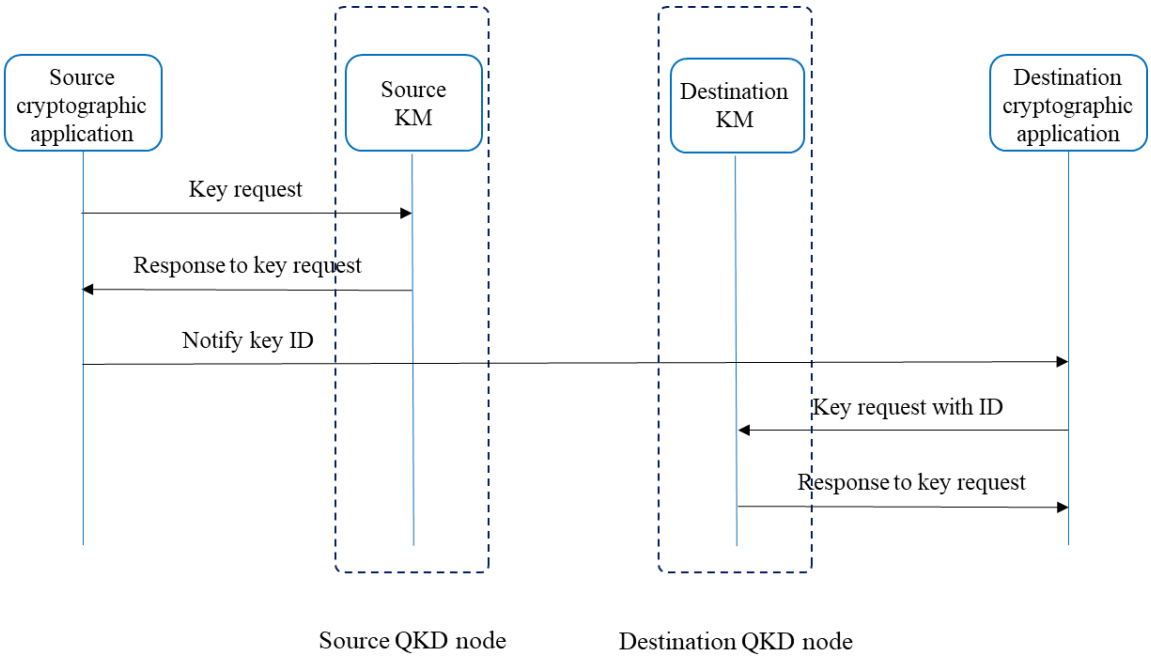

Figure I-1 – Typical signalling procedures for key supply upon request mode implemented by two QKD nodes

NOTE1 – Notify key ID message is transmitted through the Ax reference point between two cryptographic applications. This signalling message is outside the scope of this Recommendation.

A.2. Proactive key supply mode

Beside the procedure of key supply upon key request as described in A.1, there is another mode at the Ak interface to supply keys proactively. In the mode, the KM at the source QKD node initiates a key supply upon request, and then instructs the KM at the destination QKD node to make a proactive key supply. The proactive key supply mode can be adopted in scenarios where the cryptographic applications at both sides are restricted to have no direct communication before they have KSA-keys.

Figure I-2 shows typical signalling procedures for proactive key supply mode implemented by two QKD nodes.

The typical signalling procedures shown in Figure I-3 are briefly described as follows:

1) The source cryptographic application sends “Session creation request” message to the source KM at the source QKD node.

2) The source KM sends “Session creation request” message to the corresponding QKDN controller.

3) The QKDN controller generates a session ID and sends “Session creation notification” message with the session ID to the destination KM at the destination QKD node. If there are distributed QKDN controllers, the “Session creation notification” message will be sent from the QKDN controller at the source QKD node to the QKDN controller at the destination QKD node, and then relayed to the destination KM.

4) The destination KM sends “Session creation notification” message with the received session ID to the destination cryptographic application.

5) The destination cryptographic application responds “Response to session creation notification” message to the destination KM with the session creation result.

6) The destination KM responds “Response to session creation notification” message to the corresponding QKDN controller with the received session creation result. If there are distributed QKDN controllers, the “Response to session creation notification” message will be sent from the destination KM to the QKDN controller at the destination QKD node, and then relayed to the QKDN controller at the source QKD node.

7) As the session is successfully created, the QKDN controller responds “Response to session creation request” message to the source KM with the session ID.

8) The source KM responds “Response to session creation request” message to the source cryptographic application with the received session ID.

9) The source cryptographic application sends “Key request with session ID” message to the source KM with the received session ID.

10) The source KM sends “Key supply notification” message to the destination KM with the number of keys to be supplied.

11) The destination KM sends “Proactive key supply” message to the destination cryptographic application with the notified number of keys.

12) The destination cryptographic application responds “Response to proactive key supply” message to the destination KM with key IDs of the received keys.

13) The destination KM responds “Response to key supply notification” message to the source KM with the received key IDs.

14) The source KM responds “Response to key request with session ID” message to the source cryptographic application with keys corresponding to the received key IDs.

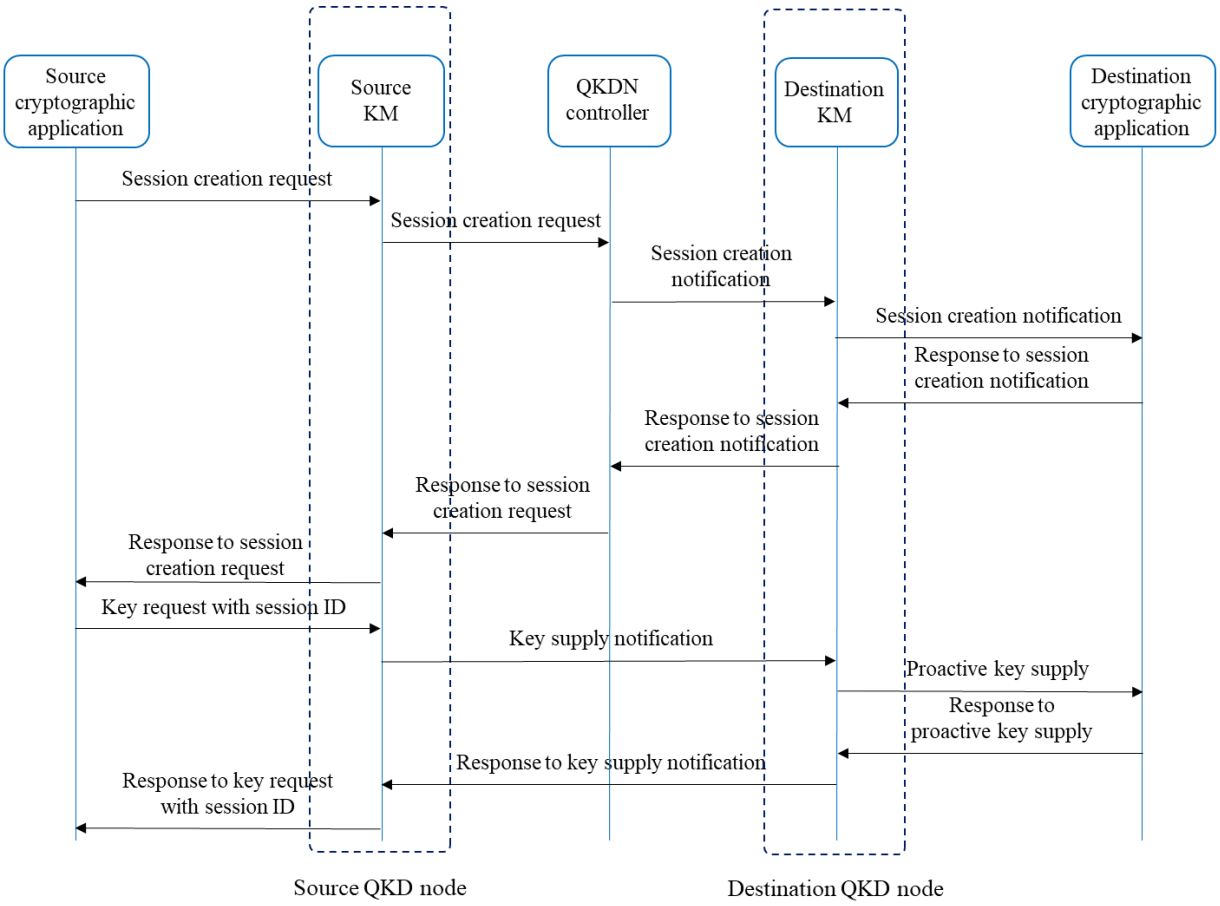

Figure I-2 – Typical signalling procedures for proactive key supply mode implemented by two QKD nodes

A.3. Key relay for a distributed QKDN

Figure I-3a shows typical signalling procedures for key relay for a distributed QKDN which is defined in [ITU-T Y.3802].

1) The KM1 sends “Key replay next hop request” message to the QKDN controller in the QKD node 1, and the QKDN controller responds “Response to key relay next hop request” message with the next hop destination for key relay, then the KM1 relays key along with the response.

2) The KM2 and the QKDN controller in the QKD node 2 performs the same procedures as the KM1 of the QKDN node 1.

3) When the key reaches the destination QKD node which is the nearest node to the destination cryptographic application, the KM (shown as KM3 in the figure) sends “Notify completion of key relay” message to the source KM (shown as the KM1 in the figure).

4) The nearest KM (shown as KM3 in the figure) responds “Response to key request” message with keys.

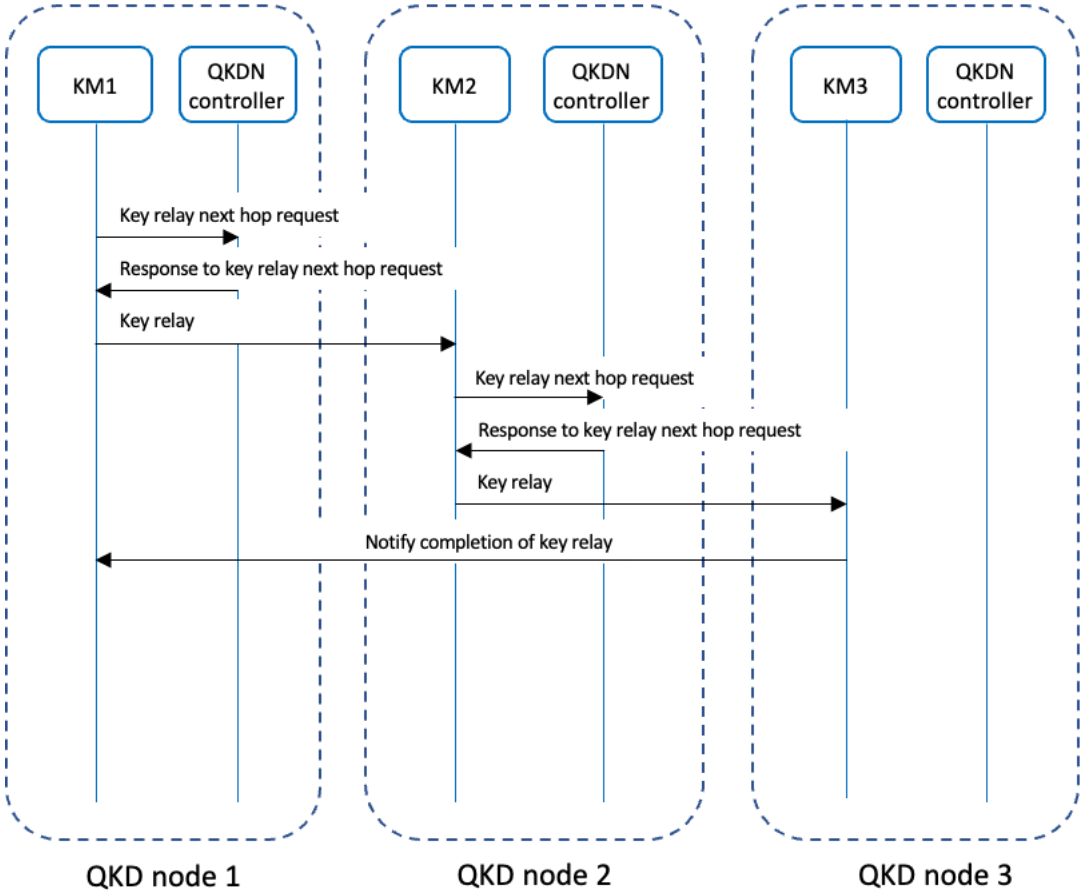

Figure I-3a – Typical signalling procedures for key relay for a distributed QKDN

A.4. Key relay for a centralized QKDN

Figure I-3b shows typical signalling procedures for key relay for a centralized QKDN which is defined in [ITU-T Y.3802].

1) The KM1 sends “Notify key replay request” message to the QKDN controller, and the QKDN controller responds “Key relay request” message with the full key relay route to the destination node.

2) The KM1 starts key relay along with the key relay route. The KM2 in QKD node 2 performs key relay according with the key relay route.

3) When the key reaches the destination QKD node which is the nearest node to the destination cryptographic application, the KM (shown as KM3 in the figure) sends “Notify completion of key relay” message to the source KM (shown as KM1 in the figure), then the KM 1 sends “Response to key relay request” message to the QKDN controller.

4) The nearest KM (shown as KM3 in the figure) responds “Response to key relay” message with keys.

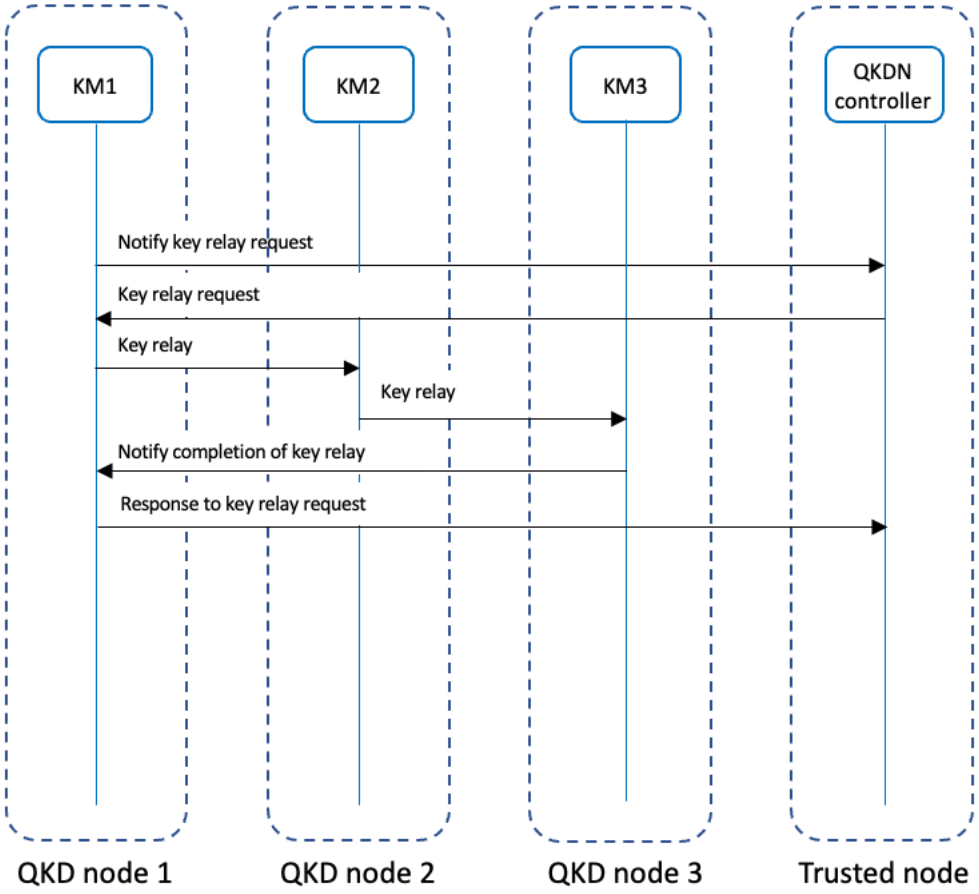

Figure I-3b – Typical signalling procedures for key relay for a centralized QKDN

A.5. Key request, key relay, and key supply

Figure I-4a shows typical signalling procedures for key request, key relay, and key supply for a distributed QKDN which is defined in [ITU-T Y.3802].

1) The source cryptographic application sends “Key request” message to the KM1 in the QKD node 1, where is the nearest node of the source cryptographic application.
2) The KM1 sends “Key replay next hop request” message to the QKDN controller in the QKD node 1, and the QKDN controller responds “Response to key relay next hop request” message with the next hop destination for key relay, then the KM1 relays key along with the response.
3) The KM2 and the QKDN controller in the QKD node 2 performs the same procedures as the KM1 of the QKDN node 1.
4) When the key reaches the destination QKD node which is the nearest node to the destination cryptographic application, the KM (shown as KM3 in the figure) sends “Notify completion of key relay” message to the source KM (shown as the KM1 in the figure), then the KM 1 responds “Response to key request” message to the source cryptographic application with keys.
5) The source cryptographic application sends “Notify key ID” message to the destination cryptographic application with key ID.
6) The destination cryptographic application sends “Key request with ID” message with key ID which is received from the source cryptographic application.
7) The nearest KM (shown as KM3 in the figure) responds “Response to key request” message with keys.

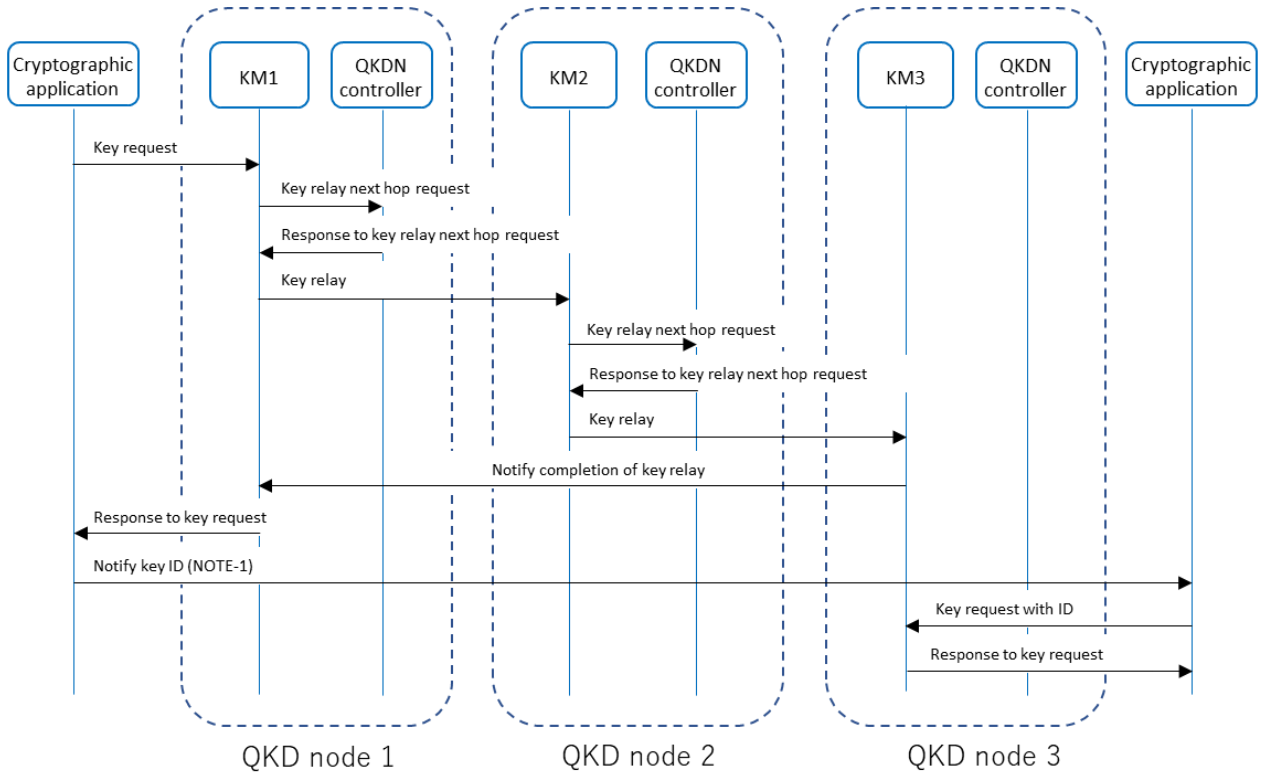

Figure I-4a– Typical signalling procedures for key request, ~~and~~ key relay, and key supply for distributed QKDNs

Figure I-4b shows typical signalling procedures for key request, key relay, and key supply~~relay~~ for a centralized QKDN which is defined in [ITU-T Y.3802].

1) The source cryptographic application sends “Key request” message to the KM1 in the QKD node 1, where is the nearest node of the source cryptographic application.
2) The KM1 sends “Notify key replay request” message to the QKDN controller, and the QKDN controller responds “Key relay request” message with the full key relay route to the destination node.
3) The KM1 starts key relay along with the key relay route. The KM2 in QKD node 2 performs key relay according with the key relay route.
4) When the key reaches the destination QKD node which is the nearest node to the destination cryptographic application, the KM (shown as KM3 in the figure) sends “Notify completion of key relay” message to the source KM (shown as KM1 in the figure), then the KM 1 sends “Response to key relay request” message to the QKDN controller, and also responds “Response to key request” message to the source cryptographic application with keys.
5) The source cryptographic application sends “Notify key ID” message to the destination cryptographic application with key ID.
6) The destination cryptographic application sends “Key request with ID” message with key ID which is received from the source cryptographic application.
7) The nearest KM (shown as KM3 in the figure) responds “Response to key relay” message with keys.

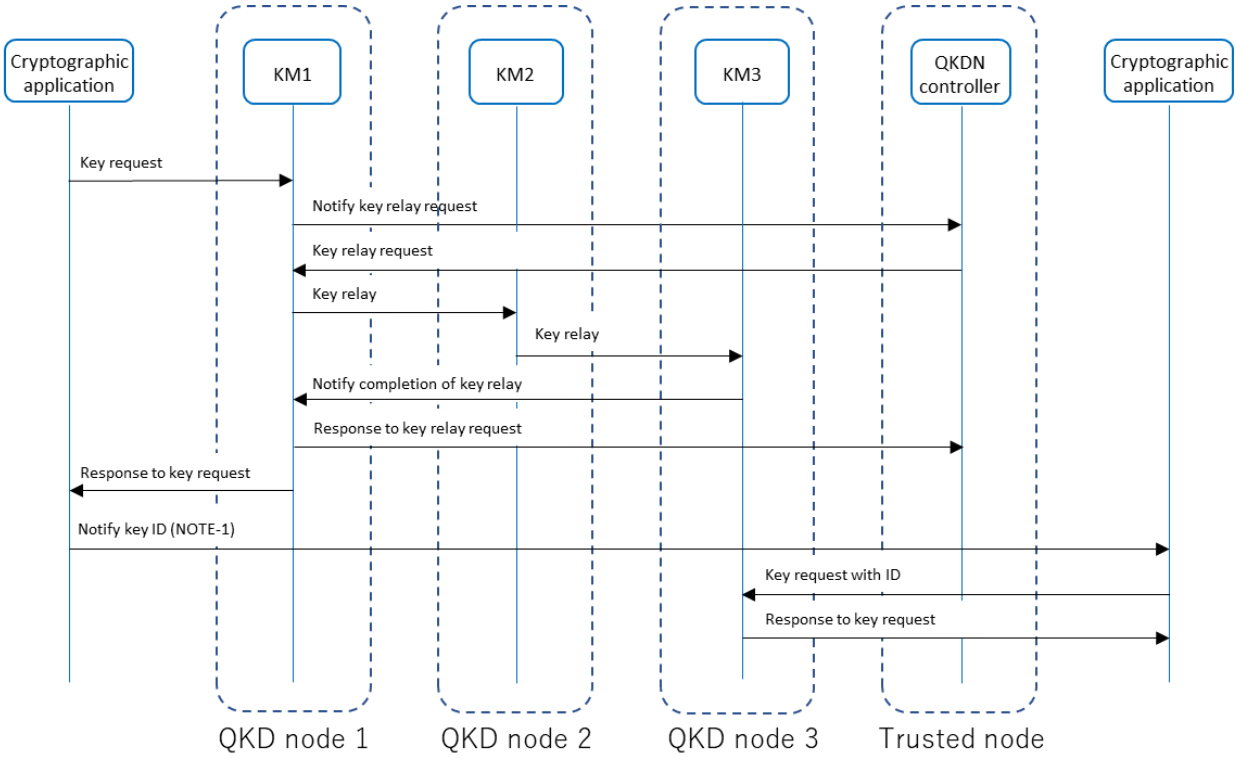

Figure I-4b – Typical signalling procedures for key request, ~~and~~ key relay, and key supply for centralized QKDNs

NOTE 1 – Notify key ID message is transmitted through the Ax reference point between two cryptographic applications. This signalling message is outside the scope of this Recommendation.

NOTE 2 – Figure I-4a and I-4b illustrate signalling procedures for the case 2 of key relay which is specified in [ITU-T Y.3800].

Bibliography

[b-ETSI GR QKD 007] ~~Group Report~~ ETSI G~~R~~S~~~~ 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~~9110] IETF RFC 9110~~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 9293~~793~~] IETF RFC 9293~~793~~, ~~*TRANSMISSION CONTROL PROTOCOL*~~*Transmission Control Protocol (TCP)*.

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

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

[b-IETF RFC 8200~~2460~~] IETF RFC 8200~~2460~~, *Internet Protocol, Version 6 (IPv6) Specification.*

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

_____