INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2022-2024

SG11-TD457/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_Ck: Protocols for Ck interface for QKDN (Geneva, 10-19 May 2023)

Contact:	Kaoru KENYOSHI NICT Japan	Tel: +81 50 3566 5852 E-mail: kaoru.kenyoshi@nict.go.jp
Contact:	Mariko Honda NICT Japan	E-mail: mariko.honda@ntt-at.co.jp
Contact:	Xuefu Wang QuantumCTek Co., Ltd. China	E-mail: xuefu.wang@quantum-info.com
Contact:	Zhangchao Ma CAS Quantum Network Co., Ltd. China	E-mail: mazhangchao@qtict.com
Contact:	Junsen Lai CAICT, Ministry of Industry and Information Technology (MIIT) China	E-mail: laijunsen@caict.ac.cn

Abstract: This TD is the output of draft Recommendation Q.QKDN_Ck: Protocols for Ck interface for QKDN (Geneva, 10-19 May 2023).

Summary

This is the output of draft Recommendation ITU-T Q.QKDN_Ck: Protocols for Ck interface for QKDN, based on the discussion results on C204 with modifications at the Q2/11 meeting (Geneva, 10-19 May 2023).

Draft Recommendation ITU-T Q.QKDN_Ck

Protocols for Ck interface for QKDN

Summary

Recommendation ITU-T Q.QKDN_Ck specifies protocols for Ck interface in quantum key distribution networks (QKDN).

Keywords

Protocol, QKD (quantum key distribution), QKDN (QKD network), signalling procedure, message parameters

Table of Contents

Draft new Recommendation ITU-T Q.QKDN_Ck

Protocols for Ck interface for QKDN

1. Scope

This Recommendation specifies protocols at Ck interface for quantum key distribution network (QKDN) especially the following areas.

- signalling procedures for Ck interface for QKDN;
- signalling messages and parameters for Ck interface for QKDN;
- security considerations

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.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.3802] Recommendation ITU-T Y.3802 (2020)/Cor.1 (04/2021), *Quantum key distribution networks - Functional architecture*.

[ITU-T Q.QKDN_profr] draft Recommendation Q.QKDN_profr, *Quantum key distribution networks - Protocol framework.*

3. Definitions

3.1.Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 **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.

3.1.2 **key management agent (KMA)** [ITU-T Y.3802]**:** A functional element to manage keys generated by a quantum key distribution (QKD) module/QKD modules in a QKD node (trusted node).

NOTE - KMA acquires keys from a QKD module/QKD modules, synchronizes, resize, formats, and stores them. It also relays keys through key management agent (KMA) links.

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

3.1.4 **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.

~~3.1.5 **key manager link (KM link)** [ITU-T Y.3800]: A communication link connecting key managers (KMs) to perform key management.~~

~~3.1.6~~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).

~~3.1.7~~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.

~~3.1.8~~3.1.7 **key supply agent link (KSA link)** [ITU-T Y.3802]: A communication link connecting KSAs to perform key synchronization and integrity verification.

~~3.1.9~~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.

~~3.1.10~~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.

~~3.1.11~~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).

~~3.1.12~~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.

~~3.1.13~~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.

~~3.1.14 **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.~~

~~3.1.15~~3.1.13 **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).

~~This Recommendation uses the following terms defined elsewhere:~~

3.2.Terms defined in this Recommendation

None.

4. Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ID	Identifier
KM	Key manager
KMA	Key Management Agent
KSA	Key Supply Agent
QKD	Quantum Key Distribution
QKDN	QKD Network
TCP	Transmission Control Protocol

5. Conventions

None.

6. Ck interface

Ck is a reference point connecting a QKDN controller control and management function in a QKDN controller and a KM control and management function in a key manager (KM). It is responsible for the QKDN controller to communicate control information with a key management agent (KMA) and a key supply agent (KSA).

7. Signalling procedure

Examples of signalling procedure of key request, key relay, and key supply in QKDN are described in the Appendix I of [ITU-T Q.QKDN_profr]. The protocol suites applied for the signalling are specified in clause 8 of [ITU-T Q.QKDN_profr]. Two kinds of signalling procedures are defined depending on the network architecture of distributed QKDN and centralized QKDN.

7.1. Signalling procedures at the Ck interface for a distributed QKDN

The distributed QKDN performs key relay with a series of hops between KMs to the destination KM. At the Ck interface of the distributed QKDN, a KM requests a QKDN controller for the information of the KM of neighbours for the next hop for key relay and the KM relays the key to the next KM based on the controller’s response. Then the next KM requests again to the controller for the next hop. This request and hop procedure repeats until the key relay is completed to the destination.

Figures 1 shows signalling procedures at the Ck interface for key relay request in a distributed QKDN.

The KM sends Key relay next hop request to the QKDN controller in order to request the KM identifier (ID) of the next hop. The QKDN controller responds possible KMs with the KM IDs to hop to the next KM.

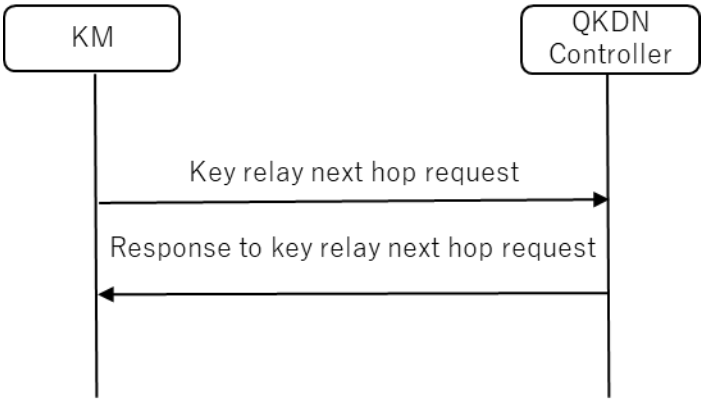
KM
QKDN Controller
Key relay next hop request
Response to key relay next hop request

Figure 1 - Signalling procedures at the Ck interface in a distributed QKDN

7.2. Signalling procedures at the Ck interface for a centralized QKDN

In a centralized QKDN, the request from the cryptographic application to the KM is transmitted to the QKDN controller, and the QKDN controller returns the whole route to the destination KM (list of KMs to be passed) to the requesting KM. When all the key relays are completed, the source KM returns notification that the key relay is completed.

Figures 2 shows signalling procedures at the Ck interface for key relay request in a centralized QKDN.

After the cryptographic application sends a key request to the KM, the KM sends notification of receipt of a key request to the QKDN controller with Notify key relay request. The QKDN controller specifies the whole route for the key transfer to the destination KM and notifies the requesting KM of the list of transit KMs by a Key relay request. The source KM starts the key relay according to the list of transit KMs. When the key relay completes at the KM to which the destination cryptographic application is connected, the source KM notifies the QKDN controller of completion of key relay by Response to key replay request.

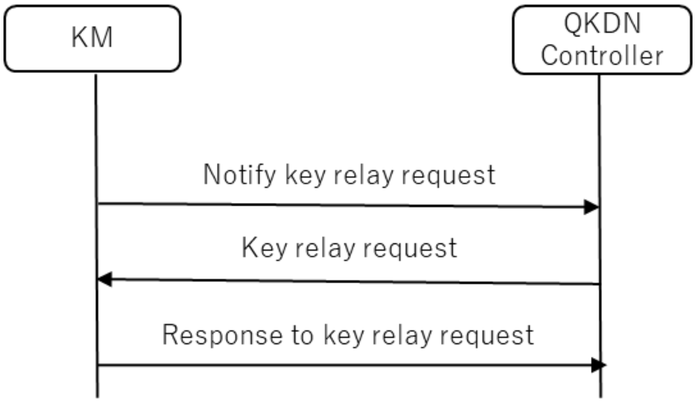

Figure 2 - Signalling procedures at the Ck interface in a centralized QKDN

8. Signalling messages and parameters

This clause specifies messages and their parameters for the Ck interface.

In the M/O column of the tables in this clause, M indicates that the parameter is mandatory for signalling, and O indicates that the parameter is optional for signalling.

NOTE – The messages and parameters defined in this clause are independent of a specific protocol. Different protocols can have different implementations of these messages and parameters. The recommended protocol implementations are described in Annex A. A message parameter described in the following tables is not necessarily mapped to a field in the message payload and might be a part of control parameters of one specific protocol. The Data type column of the tables may vary with specific protocols.

8.1. Key relay next hop request message

Table 1 shows parameters of Key relay next hop request message. Either Destination KMA ID or Application destination ID is mandatory to specify the destination.

Table 1 - Parameters of Key relay next hop request message

Parameter	Description	Data type	M/O	Remarks
Source KMA ID	ID of KMA that is the source in the entire key relay route	string	O	
Destination KMA ID	ID of KMA that is the destination in the entire key relay route	string	Either Destination KMA ID or Application destination ID is mandatory	
Application destination ID	ID of the cryptographic application with which the source cryptographic application (i.e. source application) requests to communicate	string	Either Destination KMA ID or Application destination ID is mandatory	
Extension	Array of extension parameters	Array of objects	O	

8.2. Response to key relay next hop request message

Table 2 shows parameters of Response to key relay next hop request message. For a distributed QKDN, the QKDN controller returns the IDs of the possible KMs to reach the destination KMA or the destination KMA ID.

Table 2 - Parameters of Response to key relay next hop request message

Parameter	Description	Data type	M/O	Remarks
Source KMA ID	ID of KMA that is the source in the entire key relay route	string	O	
Destination KMA ID	ID of KMA that is the destination in the entire key relay route	string	Mandatory if application destination ID is contained in the key relay next hop request message.	

Next KMA IDs	IDs of KMAs available as a next relay hop to relay the keys to the destination KMA	Array of string	M	
Extension	Array of extension parameters	Array of objects	O	

8.3. Notify key relay request message

Table 3 shows parameters of Notify key relay request message. In a centralized QKDN, when a key request is sent by a cryptographic application, the KM notifies the QKDN controller the receipt of a key request and requests the whole route of the key relay. At this time, as same in the case of the distributed QKDN, information is required for either the Destination KMA ID or the Application destination ID in order to specify the destination of the key relay.

Table 3 - Parameters of Notify key relay request message

Parameter	Description	Data type	M/O	Remarks
Source KMA ID	ID of KMA that is the source in the entire key relay route	string	O	
Destination KMA ID	ID of KMA that is the destination in the entire key relay route	string	Either Destination KMA ID or Application destination ID is mandatory	
Application destination ID	ID of the cryptographic application with which the source cryptographic application (i.e. source application) requests to communicate	string	Either Destination KMA ID or Application destination ID is mandatory	
Extension	Array of extension parameters	Array of objects	O	

8.4. Key relay request message

Table 4 shows parameters of Key relay request message. The QKDN controller returns all KMs in the route (Transit KMA IDs) to reach the destination KMA or the destination KMA ID.

Table 4 - Parameters of Key relay request message

Parameter	Description	Data type	M/O	Remarks
Source KMA ID	ID of KMA that is the source in the entire key relay route	string	O	
Destination KMA ID	ID of KMA that is the destination in the entire key relay route	string	M	
Transit KMA IDs	List of IDs of KMAs that are the transition nodes of key relay route	string	M	
Key relay request ID			O	

Extension	Array of extension parameters	Array of objects	O	

8.5. Response to key relay request message

Table 5 shows parameters of Response to key relay request message.

Table 5 - Parameters of Response to key relay request message

Parameter	Description	Data type	M/O	Remarks
Response	Result of key relay	string	M	Success or failure reason
Key relay request ID			O	

Editor’s note: The corresponding description and data type of “Key relay request ID” needs to be addressed.

9. Security considerations

Control and management information is transferred through Ck reference point. Security requirements and measures to protect it are specified in [ITU-T X.1712].

Annex A

Protocol implementation ~~for~~using TCP

(This annex forms an integral part of this Recommendation.)

This annex describes a protocol implementation for messages and parameters ~~for~~using TCP which are described in clause 8.

NOTE 1 - Some of the parameters are mapped to a part of control information of the protocol instead of being mapped to a field in the data payload.

The KM can connect to the QKDN controller using TCP protocol [b-IETF RFC 9293~~793~~]. The corresponding message format over TCP is as follows.

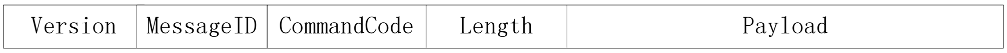

Figure A.1 – Message format over TCP

Version: the current version of the protocol format adopted, 2 bytes;

MessageID: the unique identifier of each message, 4 bytes;

CommandCode: a unique code that denotes different Command/Response messages transferred at the Ck interface, 2 bytes;

Length: the length of the message payload, 2 bytes;

Payload: the message parameters of a specific Command/Response message, JSON data format [b-IETF RFC 8259].

NOTE 2 – TLS protocol [b-IETF RFC 5246] can be implemented with TCP protocol for enhanced security.

~~*Editor's note - Detail implementation of TLS protocol needs to be addressed.*~~

At the connection establishment, mutual authentication between the KM and the QKDN controller shall be performed. After the mutual authentication, a Command/Response message can be transferred at the Ck interface for key relay request.

NOTE 3 – When applying TLS protocol, the KM can verify the validity of a certificate the QKDN controller possesses and confirm the ID of the QKDN controller it is connecting to, based on the certificate. Similarly, the QKDN controller can verify the validity of a certificate the KM possesses and confirm the ID of the connecting KM based on the certificate.

Table A.1 shows a list of CommandCode vs. Command/Response message name.

Table A.1 – CommandCode vs. Command/Response message name

CommandCode	Command/Response message name
0x01	Key relay next hop request
0x02	Response to key relay next hop request
0x03	Notify key relay request
0x04	Key relay request
0x05	Response to key relay request

Bibliography

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

[b-IETF RFC 9293~~793~~] IETF RFC 9293~~793~~, ~~*TRANSMISSION CONTROL PROTOCOL*~~ *Transmission Control Protocol (TCP)*.

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

[b-IETF RFC 8259] IETF RFC 8259, *The JavaScript Object Notation (JSON) Data Interchange Format*.