



**Question(s):** 2/11

Geneva, 10-20 October 2023

**TD**

**Source:** Editors

**Title:** Consent – Revised baseline text of draft Recommendation ITU-T Q.4163 (ex. Q.QKDN\_Kx): Protocols for Kx interface for quantum key distribution network

---

**Contact:** Kaoru KENYOSHI  
NICT  
Japan  
Tel: +81 50 3566 5852  
E-mail: [kaoru.kenyoshi@nict.go.jp](mailto:kaoru.kenyoshi@nict.go.jp)

---

**Contact:** Mariko Honda  
NICT  
Japan  
E-mail: [mariko.honda@ntt-at.co.jp](mailto:mariko.honda@ntt-at.co.jp)

---

**Contact:** Lei Zhou  
QuantumCTek Co., Ltd.  
China  
E-mail: [lei.zhou@quantum-info.com](mailto:lei.zhou@quantum-info.com)

---

**Contact:** Zhangchao Ma  
CAS Quantum Network Co., Ltd.  
China  
E-mail: [mazhangchao@qtict.com](mailto:mazhangchao@qtict.com)

---

**Contact:** Junsen Lai  
CAICT, Ministry of Industry and  
Information Technology (MIIT)  
China  
E-mail: [laijunsen@caict.ac.cn](mailto:laijunsen@caict.ac.cn)

---

**Abstract:** This TD is the output of draft Recommendation ITU-T Q.4163 (ex. Q.QKDN\_Kx): Protocols for Kx interface for quantum key distribution network (for consent) at the Q2/11 meeting (Geneva, 10-20 October 2023).

**Summary**

This is the output of draft Recommendation ITU-T Q.4163 (ex. Q.QKDN\_Kx): Protocols for Kx interface for quantum key distribution network (for consent), based on the discussion results on C228 and C336 with modifications at the Q2/11 meeting (Geneva, 10-20 October 2023).

## **Draft Recommendation ITU-T Q.4163 (ex. QKDN\_Kx)**

### **Protocols for Kx interface for quantum key distribution network**

#### **Summary**

Recommendation ITU-T Q.4163 specifies protocols for Kx interface in quantum key distribution network (QKDN).

#### **Keywords**

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

## Table of Contents

1.	Scope.....	4
2.	References.....	4
3.	Definitions .....	4
3.1.	Terms defined elsewhere .....	4
3.2.	Terms defined in this Recommendation .....	6
4.	Abbreviations and acronyms .....	6
5.	Conventions .....	6
6.	Kx interface .....	6
7.	Signalling procedure .....	6
7.1.	Signalling procedures for key relay .....	6
7.2.	Signalling procedures for key supply notification.....	7
8.	Signalling messages and parameters .....	8
8.1.	Key relay message .....	8
8.2.	Key relay completion notification message.....	8
8.3.	Key supply notification message .....	9
8.4.	Response to key supply notification message .....	9
9.	Security considerations .....	10
	Appendix I Protocol implementation using TCP.....	11
	Bibliography.....	12

## Draft Recommendation ITU-T Q.4163

### Protocols for Kx interface for quantum key distribution network

#### 1. Scope

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

- signalling procedures for Kx interface for QKDN;
- signalling messages and parameters for Kx 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 Q.4160] Recommendation ITU-T Q.4160 (2023), *Quantum key distribution networks - Protocol framework*.
- [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 Y.3803] Recommendation ITU-T Y.3803 (2020), *Quantum key distribution networks - Key management*.

#### 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-key (KMA-key)** [ITU-T Y.3803]: Key data stored and processed in a key management agent (KMA), and securely shared between a KMA and a matching KMA.
- 3.1.4 **key management agent link (KMA link)** [ITU-T Y.3802]: A communication link connecting KMAs to perform key relay and communications for key management.
- 3.1.5 **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.
- 3.1.6 **key manager link (KM link)** [ITU-T Y.3800]: A communication link connecting key managers (KMs) to perform key management.
- 3.1.7 **key relay** [ITU-T Y.3800]: A method to share keys between arbitrary quantum key distribution (QKD) nodes via intermediate QKD node(s).
- 3.1.8 **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.

- 3.1.9 **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.
- 3.1.10 **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.
- 3.1.11 **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.

- 3.1.12 **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).

- 3.1.13 **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.

- 3.1.14 **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.
- 3.1.15 **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:

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

### **5. Conventions**

None.

### **6. Kx interface**

Kx interface is at a reference point connecting two key managers (KMs) in each quantum key distribution (QKD) node via a KM link. It is responsible for exchanging information and operations required for key relay, key synchronization and authentication between KMs.

### **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.4160]. The protocol suites applied for the signalling are specified in clause 7 of [ITU-T Q.4160].

#### **7.1. Signalling procedures for key relay**

The key is relayed at Kx interface from the source to the destination. A KM sends the key to the KM which is specified in the message from a QKDN controller.

Figure 1 shows signalling procedures for key relay at the Kx interface.

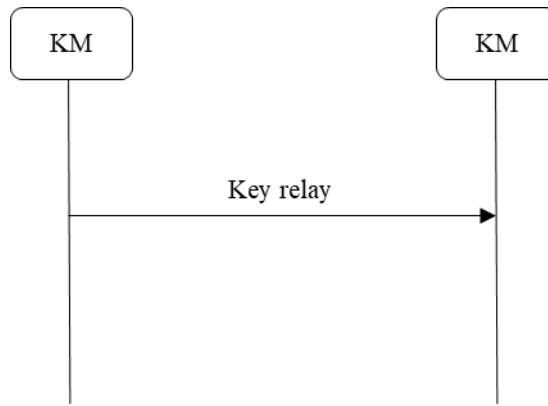


Figure 1 - Signalling procedures for key relay at the Kx interface

When the key is received by the destination KM, the destination KM notifies the completion of key relay to the source KM. The notification is sent with the information to specify the transaction linked to the key relay which has been completed.

Figure 2 shows signalling procedures for Key relay completion notification at the Kx interface.

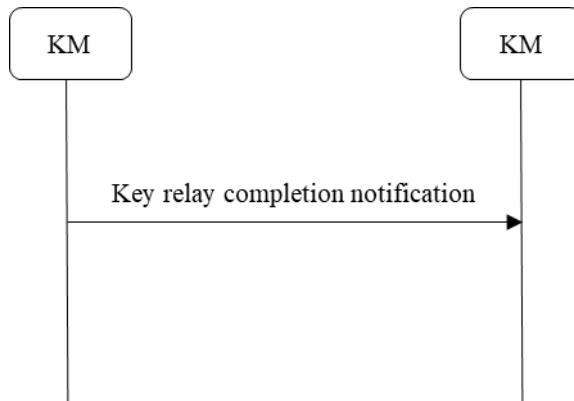


Figure 2 - Signalling procedures for Key relay completion notification at the Kx interface

## 7.2. Signalling procedures for key supply notification

When the key request from the source cryptographic application is received by the source KM, the source KM can notify the destination KM to make a proactive key supply. Then the destination KM proactively supplies KSA-keys to the destination cryptographic application and responds to the source KM with key IDs of the KSA-keys supplied.

Figure 3 shows signalling procedures for key supply notification at the Kx interface.

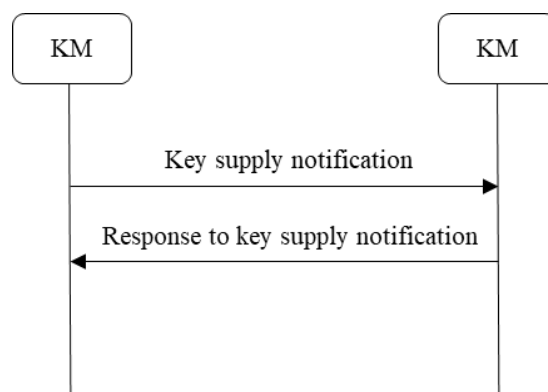


Figure 3 - Signalling procedures for key supply notification at the Kx interface

## 8. Signalling messages and parameters

This clause specifies messages and their parameters for the Kx 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.

The messages and parameters defined in this clause are independent of a specific protocol and can have different implementations. The recommended protocol implementations are described in Appendix I.

NOTE – 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 message

Key relay message conveys the key from the source KM to the destination KM.

Table 1 shows parameters of Key relay message.

Table 1 - Parameters of Key relay 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	M	
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	O	
Keys	Key file consists of key data and metadata.	Array of objects	M	
	Key ID	ID of the KMA-key relayed	string	M
	Key	KMA-key data relayed	string	M
	Key extension	Extensions to key file	object	O
Key relay request ID	ID of key relay request	string	O	
Extension	Array of extension parameters	Array of objects	O	

### 8.2. Key relay completion notification message

When the key reaches the destination KM, the KM notifies the completion of the key relay to the source KM. The notification is sent with the information to specify the transaction linked to the key relay which has been completed.

Table 2 shows parameters of Key relay completion notification message.

Table 2 - Parameters of Key relay completion notification message



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

### 8.3. Key supply notification message

When the key request from the source cryptographic application is received by the source KM, the source KM can notify the destination KM to make a proactive key supply. The notification is sent with the information to specify the session created for key supply and the number of KSA-keys to be supplied.

Table 3 shows parameters of Key supply notification message.

Table 3 - Parameters of Key supply notification message

Parameter	Description	Data type	M/O	Remarks
Session ID	ID of the session created for key supply	string	M	
Number of keys	Number of KSA-keys to be supplied	integer	O	A default value is applied if omitted.
Size of key	Length of each KSA-key to be supplied	integer	O	A default value is applied if omitted.
Extension	Array of extension parameters	Array of objects	O	

### 8.4. Response to key supply notification message

The destination KM responds to the source KM with key IDs of the KSA-keys received by the destination cryptographic application during the created session.

Table 4 shows parameters of Response to key supply notification message.

Table 4 - Parameters of Response to key supply notification message

Parameter	Description	Data type	M/O	Remarks
Session ID	ID of the session created for key supply	string	M	
Key ID	ID of the KSA-key received by the destination cryptographic application	string	M	
Response	Result of key supply	string	M	Success or failure reason
Extension	Array of extension parameters	Array of objects	O	

## **9. Security considerations**

Key data, metadata and control and management information are transferred through Kx reference point. Security requirements and measures to protect them are specified in [ITU-T X.1712].

## Appendix I

### Protocol implementation using TCP

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

This appendix describes a protocol implementation for messages and parameters 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.

One KM can connect to another KM using TCP protocol [b-IETF RFC 9293]. The corresponding message format over TCP is as follows.

Version	MessageID	CommandCode	Length	Payload
---------	-----------	-------------	--------	---------

Figure I.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 Kx 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.

At the connection establishment, mutual authentication between the KMs shall be performed. After the mutual authentication, a Command/Response message can be transferred at the Kx interface for key relay.

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

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

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

CommandCode	Command/Response message name
0x1101	Key relay
0x1102	Key relay completion notification
0x1103	Key supply notification
0x1104	Response to key supply notification

The first two digits “11” in a CommandCode indicates that the corresponding message is sent from one KM to another.

## **Bibliography**

- [b-ETSI GR QKD 007] ETSI GR QKD 007 (2018), *Quantum Key Distribution (QKD); Vocabulary*.
- [b-IETF RFC 9293] IETF RFC 9293, *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*.
-