ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

# ITU-T Q.4163 (12/2023)

SERIES Q: Switching and signalling, and associated measurements and tests

Protocols and signalling for Quantum key distribution networks

# Protocols for Kx interfaces for quantum key distribution networks

ITU-T Q-SERIES RECOMMENDATIONS

**Switching and signalling, and associated measurements and tests**

| | |
|---|---|
| SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE | Q.1-Q.3 |
| INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING | Q.4-Q.59 |
| FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN | Q.60-Q.99 |
| CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS | Q.100-Q.119 |
| SPECIFICATIONS OF SIGNALLING SYSTEMS NO. 4, 5, 6, R1 AND R2 | Q.120-Q.499 |
| DIGITAL EXCHANGES | Q.500-Q.599 |
| INTERWORKING OF SIGNALLING SYSTEMS | Q.600-Q.699 |
| SPECIFICATIONS OF SIGNALLING SYSTEM NO. 7 | Q.700-Q.799 |
| Q3 INTERFACE | Q.800-Q.849 |
| DIGITAL SUBSCRIBER SIGNALLING SYSTEM NO. 1 | Q.850-Q.999 |
| PUBLIC LAND MOBILE NETWORK | Q.1000-Q.1099 |
| INTERWORKING WITH SATELLITE MOBILE SYSTEMS | Q.1100-Q.1199 |
| INTELLIGENT NETWORK | Q.1200-Q.1699 |
| SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000 | Q.1700-Q.1799 |
| SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC) | Q.1900-Q.1999 |
| BROADBAND ISDN | Q.2000-Q.2999 |
| SIGNALLING REQUIREMENTS AND PROTOCOLS FOR THE NGN | Q.3000-Q.3709 |
| SIGNALLING REQUIREMENTS AND PROTOCOLS FOR SDN | Q.3710-Q.3899 |
| TESTING SPECIFICATIONS | Q.3900-Q.4099 |
| PROTOCOLS AND SIGNALLING FOR PEER-TO-PEER COMMUNICATIONS | Q.4100-Q.4139 |
| PROTOCOLS AND SIGNALLING FOR COMPUTING POWER NETWORKS | Q.4140-Q.4159 |
| **PROTOCOLS AND SIGNALLING FOR QUANTUM KEY DISTRIBUTION NETWORKS** | **Q.4160-Q.4179** |
| SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2020 | Q.5000-Q.5049 |
| COMBATING COUNTERFEITING AND STOLEN ICT DEVICES | Q.5050-Q.5069 |

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

# Recommendation ITU-T Q.4163

## Protocols for Kx interfaces for quantum key distribution networks


### Summary

Recommendation ITU-T Q.4163 specifies protocols for Kx interfaces for quantum key distribution networks.


### History *

| Edition | Recommendation | Approval | Study Group | Unique ID |
|---|---|---|---|---|
| 1.0 | ITU-T Q.4163 | 2023-12-14 | 11 | 11.1002/1000/15727 |


### Keywords

Message parameters, protocol, QKD (quantum key distribution), QKDN (QKD network), signalling procedure.


* To access the Recommendation, type the URL https://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID.

## 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


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

# Recommendation ITU-T Q.4163

## Protocols for Kx interfaces for quantum key distribution networks

### 1 Scope

This Recommendation specifies protocols for Kx interfaces for quantum key distribution networks (QKDNs) especially in the following areas:

– signalling procedures;

– signalling messages and parameters;

– 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), *Security requirements and measures for QKD networks – Key management*.

### 3 Definitions

#### 3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

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

**3.1.2 key management agent (KMA)** [b-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.

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

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

**3.1.7 key relay** [b-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)** [b-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.

**3.1.9 key supply agent-key (KSA-key)** [b-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** [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** [b-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** [b-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)** [b-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** [b-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** [b-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

Rx Receiver

TCP Transmission Control Protocol

TLS Transport Layer Security

Tx Transmitter

## 5 Conventions

None.

## 6 Kx interface

A Kx interface is a reference point connecting two KMs in each QKD node via a KM link. A Kx interface provides a means for exchanging information and operations required for key relay, key synchronization and authentication between KMs.

## 7 Signalling procedure

Examples of signalling procedure for key request, key relay and key supply in QKDN are described in Appendix I of [ITU-T Q.4160]. The protocol suites applied for signalling are specified in clause 7 of [ITU-T Q.4160].

### 7.1 Signalling procedures for key relay

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

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

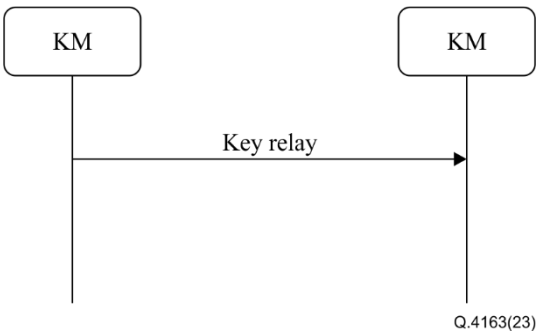


**Figure 1 – Signal ling procedures for key relay at the Kx interface**

On receipt of the key, 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 that has been completed.

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

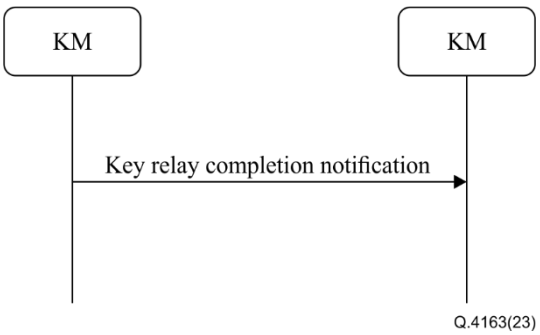


**Figure 2 – Signalling procedures for key relay completion notification at the Kx interface**

## 7.2 Signalling procedures for key supply notification

On receipt of the key request from the source cryptographic application, the source KM can notify the destination KM to supply a key proactively. The destination KM then 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.

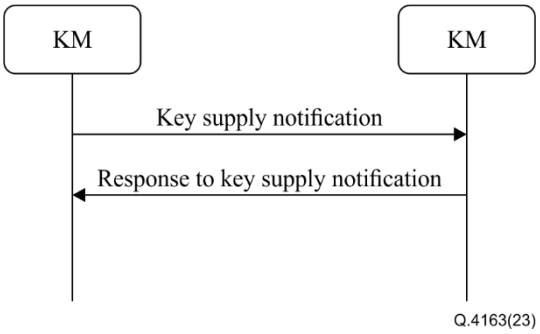


**Figure 3 – Signalling procedures for key supply notification at the Kx interface**

# 8 Signalling messages and parameters

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

The M/O columns of Tables 1 to 4 relate to signalling of the parameters specified in columns 1; M indicates mandatory and O indicates optional.

The messages and parameters specified 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 Tables 1 to 4 is not necessarily mapped to a field in the message payload and might be a part of the control parameters of a specific protocol. The data type listed in columns 3 in Tables 1 to 4 may vary with specific protocols.

## 8.1 Key relay message

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

Table 1 lists parameters of a key relay message.

**Table 1 – Parameters of key relay message**

| Parameter | Description | Data type | M/O | Remarks |
|---|---|---|---|---|
| Source KMA ID | Identifier (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 | Hash value, etc. |
| 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 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 that has been completed.

Table 2 lists parameters of a 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 | Reason for success or failure |
| 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

On receipt of the key request from the source cryptographic application, the source KM can notify the destination KM to supply a key proactively. 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 lists parameters of a 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 lists parameters of a response to a 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 | Reason for success or failure |
| Extension | Array of extension parameters | Array of objects | O | |

# 9 Security considerations

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

# Appendix I

## Protocol implementation using the transmission control protocol

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

This appendix describes an implementation for messages and parameters described in clause 8 using the transmission control protocol (TCP).

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

One KM can connect to another KM using the TCP protocol [b-IETF RFC 9293]. The corresponding message format over the TCP is shown in Figure I.1.

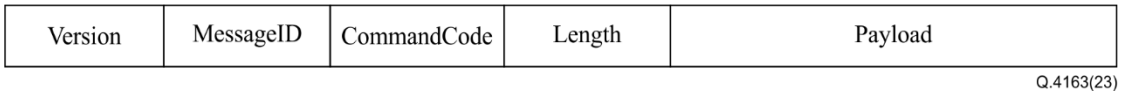


**Figure I.1 – Message format over the transmission control protocol**

In Figure I.1:

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

MessageID: the unique ID 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, JavaScript object notation data format [b-IETF RFC 8259].

NOTE 2 – The transport layer security (TLS) protocol [b-IETF RFC 5246] can be implemented with the TCP for enhanced security.

On establishment of the connection, mutual authentication between the KMs is performed. After mutual authentication, a command/response message can be transferred at the Kx interface for key relay.

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

Table I.1 lists 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 indicate that the corresponding message is sent from one KM to another.

# Bibliography


[b-ITU-T Y.3800] Recommendation ITU-T Y.3800 (2019), *Overview on networks supporting quantum key distribution*.

[b-ITU-T Y.3802] Recommendation ITU-T Y.3802 (2020), *Quantum key distribution networks –- Functional architecture*.

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

[b-ETSI GR QKD 007] Group Report ETSI GR QKD 007 V1.1.1 (2018), *Quantum key distribution (QKD); Vocabulary*.

[b-IETF RFC 5246] IETF RFC 5246 (2008), *The transport layer security (TLS) protocol – Version 1.2*.

[b-IETF RFC 8259] IETF RFC 8259 (2017), *The JavaScript object notation (JSON) data interchange format.*

[b-IETF RFC 9293] IETF RFC 9293 (2022), *Transmission control protocol (TCP).*

# 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 |

Published in Switzerland
Geneva, 2024