ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T Q.4162 (12/2023)

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

Protocols and signalling for Quantum key distribution networks

---

Protocols for Kq-1 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.4162

Protocols for Kq-1 interfaces for quantum key distribution networks

Summary

Recommendation ITU-T Q.4162 specifies protocols for Kq-1 interfaces in quantum key distribution networks.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T Q.4162	2023-12-14	11	11.1002/1000/15726

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

Recommendation ITU-T Q.4162

Protocols for Kq-1 interfaces for quantum key distribution networks

1 Scope

This Recommendation specifies protocols for Kq-1 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 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.

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

3.1.4 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.

3.1.5 quantum key distribution key [b-ITU-T Y.3802]: A pair of symmetric random bit strings generated by a pair of quantum key distribution (QKD) modules, particularly referring to random bit strings before being resized and formatted in a key manager.

3.1.6 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.

3.1.7 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).

3.1.8 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.

3.1.9 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.

3.1.10 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:

HTTPS	Hypertext Transfer Protocol Secure
ID	Identifier
KM	Key Manager
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 Kq-1 interface

A Kq-1 interface is established between a KM and a QKD module. The Kq-1 interface is used for key acquisition between the key storage function in the KM and the quantum key distribution key (QKD-key) supply function in the QKD module.

7 Signalling procedure

The following two modes are specified for key supply at the Kq-1 interface.

1) Proactive key supply mode: QKD module initiates the supply of QKD-keys to KM.
2) Key supply upon request mode: KM initiates the procedure by requesting QKD module to supply QKD-keys and QKD module supplies QKD-keys to the KM in response to the request.

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

7.1 Signalling procedure for proactive key supply mode

This procedure is initiated when the QKD-keys are generated in the QKD module. The number of QKD-keys supplied mainly depends on the key generation request from the QKDN controller.

Figure 1 shows signalling procedures for proactive key supply mode at the Kq-1 interface.

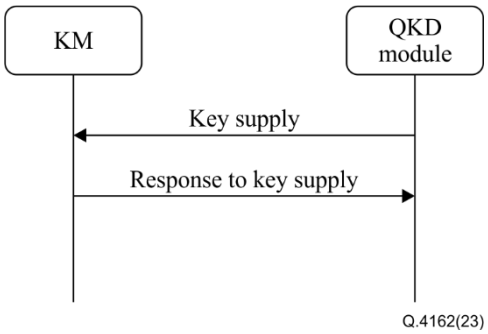

Figure 1 – Signalling procedures for proactive key supply mode at the Kq-1 interface

7.2 Signalling procedure for key supply upon request mode

In this procedure, the KM sends a key request to the QKD module when the KM needs QKD-keys. The QKD module supplies QKD-keys to the KM in response to the request.

Figure 2 shows signalling procedures for key supply upon request mode at the Kq-1 interface.

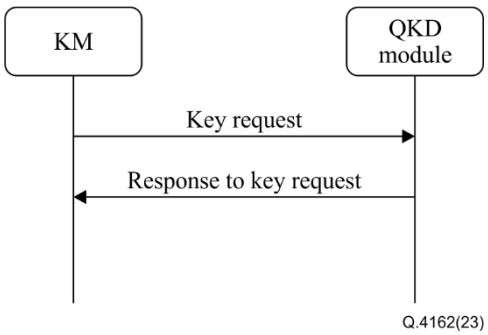

Figure 2 – Signalling procedures for key supply upon request mode at the Kq-1 interface

8 Signalling messages and parameters

This clause specifies messages and their parameters for the Kq-1 interface.

The M/O columns of Tables 1 to 4 relate to signalling of the parameter 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 Appendices I and II.

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 of Tables 1 to 4 may vary with specific protocols.

8.1 Messages and parameters for proactive key supply mode

8.1.1 Key supply message

A key supply message is sent from the QKD module to the KM in the same QKD node. The QKD module supplies the QKD-key with a unique QKD-key identifier (ID) to the KM.

Table 1 lists parameters of key supply message.

Table 1 – Parameters of key supply message

Parameter	Description	Data type	M/O	Remarks
Key	QKD-key data supplied	String	M	
Key ID	ID of the QKD-key supplied	String	M	
QKD module ID	ID of the QKD module (Alice or Bob) that supplies the QKD-key	String	O	
Matching QKD module ID	ID to identify the matching QKD module that constitutes the pair of Alice and Bob	String	O	
Key length	Length of each QKD-key supplied	Integer	O	A default value is applied if omitted
Generation time stamp	Time stamp of QKD-key generation at the pair of QKD modules	String	O	
Hash value	Hash value of the QKD-key data.	String	O	
Extension	Array of extension parameters	Array of objects	O	For future use

8.1.2 Response to key supply message

A response to a key supply message is sent from the KM to the QKD module in response to the key supply. The KM notifies the results of the receipt of the QKD-keys to the QKD module.

Table 2 lists parameters of a response to key supply message.

Table 2 – Parameters of response to key supply message

Parameter	Description	Data type	M/O	Remarks
Key ID	ID of the QKD-key received.	String	M	
QKD module ID	ID of the QKD module (Alice or Bob) that supplies the QKD-key	String	O	
Matching QKD module ID	ID to identify the matching QKD module that constitutes the pair of Alice and Bob	String	O	
Response	Result of the receipt of the QKD-key	String	M	Reason for success or failure
Extension	Array of extension parameters	Array of objects	O	For future use

8.2 Messages and parameters for key supply upon request mode

8.2.1 Key request message

A key request message is sent from the KM to the QKD module to request QKD-keys.

Table 3 lists parameters of a key request message.

Table 3 – Parameters of key request message

Parameter	Description	Data type	M/O	Remarks
Number of keys	Number of QKD-keys requested	Integer	O	A default value is applied if omitted
Size of key	Length of each QKD-key requested	Integer	O	A default value is applied if omitted
Extension	Array of extension parameters	Array of objects	O	

8.2.2 Response to key request message

A response to a key request message is sent from the QKD module to the KM in response to the key request from the cryptographic application. The QKD module supplies the requested QKD-keys to the cryptographic application.

Table 4 lists parameters of a response to key request message.

Table 4 – Parameters of response to key request message

Parameter	Description	Data type	M/O	Remarks
Keys	Key file consists of key data and metadata.	Array of objects	M	
Key	QKD-key data provided for the request	String	M	
Key ID	ID of the QKD-key provided	String	M	
Key extension	Extensions to key file	Object	O	
Response	Result of key supply	String	M	
Extension	Array of extension parameters	Array of objects	O	

9 Security considerations

Key data and associated metadata are transferred through a Kq-1 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 using the transmission control protocol (TCP) for messages and parameters that are described in clause 8.

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.

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

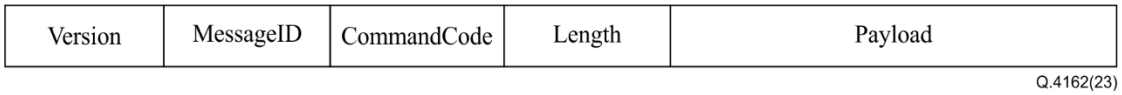

Figure I.1 – Message format over the transmission control protocol

In Figure I.1:

Version: the current version of the message 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 Kq-1 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 QKD module and the KM is performed. After mutual authentication, a command/response message can be transferred via the Kq-1 interface for key supply from the QKD module to the KM.

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

Table I.1 lists CommandCode vs. command/response message name.

Table I.1 – CommandCode vs. command/response message name

CommandCode	Command/response message name
0x3101	Key supply
0x1302	Response to key supply
0x1303	Key request
0x3104	Response to key request

The first two digits "13" in a CommandCode indicate that the corresponding message is sent from the KM to the QKD module; "31" indicate that the corresponding message is sent from the QKD module to the KM.

Appendix II

Protocol implementation for key supply upon request mode using hypertext transfer protocol secure

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

The signalling messages and parameters for key supply upon request mode specified in clause 8.2 can be implemented using hypertext transfer protocol secure (HTTPS) according to the protocol and data format of the representational state transfer-based key delivery application programming interface specified in [b-ETSI GS QKD 014]. This appendix describes the mapping of the messages and parameters specified in clause 8.2 to the corresponding data format specified in [b-ETSI GS QKD 014].

NOTE – In this implementation, the KM and the QKD module play the roles of secure application entity and the key management entity defined in [b-ETSI GS QKD 014], respectively.

II.1 Key request message

In this implementation, the key request message specified in clause 8.2.1 corresponds to the HTTPS request of the HTTPS transaction performed as the Get Key method specified in [b-ETSI GS QKD 014]. Table II.1 lists the mapping of the key request message to the Get Key method.

Table II.1 – Mapping of key request message to Get Key method

Parameter	M/O	Data type	Implementation in Get Key method
Number of keys	O	Integer	The "number" item in the key request data format
Size of key	O	Integer	The "size" item in the key request data format
Extension	O	Array of objects	The "extension_mandatory" or "extension_optional" item in the Key request data format

II.2 Response to key request message

In this implementation, the response to key request message specified in clause 8.2.2 corresponds to the HTTPS response of the HTTPS transaction performed as the Get Key method specified in [b-ETSI GS QKD 014]. Table II.2 lists the mapping of the response to a key request message to the Get Key method.

Table II.2 – Mapping of response to key request message to Get Key method

Parameter	M/O	Data type	Implementation in Get Key method
Keys	M	Array of objects	The "keys" item in the key container data format
Key	M	String	The "key" item in the key container data format
Key ID	M	String	The 'key_ID' item in the key container data format
Key extension	O	Object	The "key_ID_extension" item in the key container data format
Response	M	String	The status code of HTTPS transaction performed as Get Key method
Extension	O	Array of objects	The "key_container_extension" item in the key container data format

Bibliography

[b-ITU-T Y.3800] Recommendation ITU-T Y.3800 (2019)/Cor.1 (04/2020), *Overview on networks supporting quantum key distribution*.

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

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

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

[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