ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T Q.4164 (12/2023)

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

Protocols and signalling for Quantum key distribution networks

Protocols for Ck 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.4164

Protocols for Ck interfaces for quantum key distribution networks

Summary

Recommendation ITU-T Q.4164 specifies protocols for Ck interfaces in quantum key distribution networks.

History*

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T Q.4164	2023-12-14	11	11.1002/1000/15728

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.4164

Protocols for Ck interfaces for quantum key distribution networks

1 Scope

This Recommendation specifies protocols for Ck 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 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 [b-ITU-T Y.3802]: A communication link connecting key management agents (KMAs) to perform key relay and communications for key management.

3.1.4 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.

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

3.1.6 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.

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

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 [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.

3.1.10 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).

3.1.11 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.

3.1.12 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.

3.1.13 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

RPC Remote Procedure Call

Rx Receiver

TCP Transmission Control Protocol

TLS Transport Layer Security

Tx Transmitter

5 Conventions

None.

6 Ck interface

A Ck interface is a reference point connecting a control and management functions in both a QKDN controller and a key manager (KM). A Ck interface provides a means for a QKDN controller to communicate control information with a key management agent (KMA) and a key supply agent (KSA).

7 Signalling procedure

Examples of signalling procedures 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]. Two kinds of signalling procedures can be distinguished according to whether the QKDN network architecture is distributed or centralized.

7.1 Signalling procedures for key relay request in a distributed QKDN

A distributed QKDN performs key relay with a series of hops between KMs to the destination KM. At the Ck interface of a distributed QKDN, a KM requests a QKDN controller for information about the KMs of neighbours for the next hop for key relay. The KM then relays the key to the next KM based on the controller's response. The next KM in turn requests the next hop from the controller. This request and hop procedure repeats until the key relay is completed at the destination.

Figure 1 shows signalling procedures for a key relay request in a distributed QKDN.

The KM sends a key relay next hop request to the QKDN controller for the KM identifier (ID) of the next hop. The QKDN controller responds with possible KM IDs to hop to the next KM.

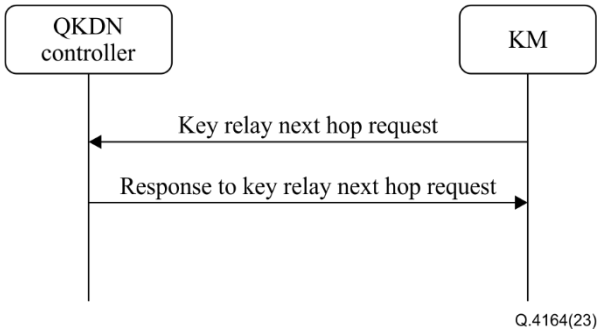

Figure 1 – Signalling procedures for key relay request in a distributed QKDN

7.2 Signalling procedures for key relay request in a centralized QKDN

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

Figure 2 shows signalling procedures for a key relay request in a centralized QKDN.

After the cryptographic application sends a key request to the KM, if a key relay is needed and there is none available, the KM requests one from the QKDN controller with a notification. The QKDN

controller specifies the whole route for the key relay 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 the completion by a response to key relay request.

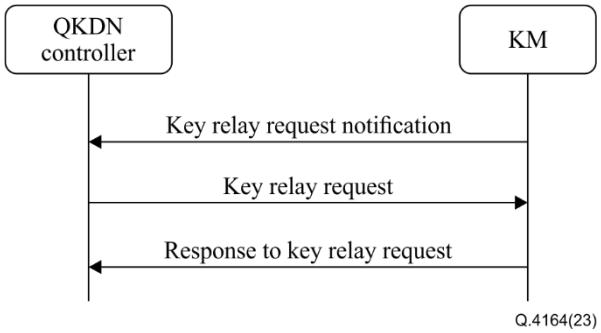

Figure 2 – Signalling procedures for key relay request in a centralized QKDN

7.3 Signalling procedures for session creation request

To facilitate key supply between cryptographic applications and the KMs on both sides, the source KM can send a session creation request to the corresponding QKDN controller, which then generates a session ID and notifies the destination KM with the session ID to create a session. After receiving the session creation result, the QKDN controller responds to the source KM with the session ID.

Figure 3 shows signalling procedures for a session creation request.

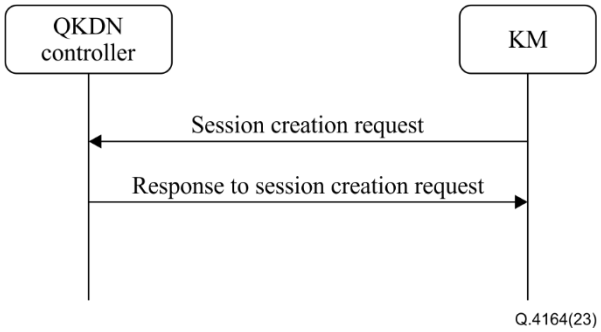

Figure 3 – Signalling procedures for session creation request

7.4 Signalling procedures for session creation notification

The corresponding QKDN controller can send a session creation notification with the session ID to the destination KM, which then notifies the destination cryptographic application. After receiving the session creation result from the destination cryptographic application, the destination KM responds to the corresponding QKDN controller with the session ID.

Figure 4 shows signalling procedures for a session creation notification.

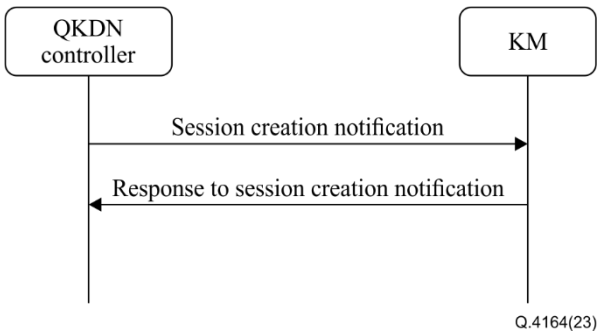

Figure 4 – Signalling procedures for session creation notification

7.5 Signalling procedures for key reservation request

The QKDN controller can send a key reservation request to the KM with KMA ID to reserve the key that will be relayed to destination KM. After receiving the key reservation request, the KM responds to the corresponding QKDN controller with a response to the key reservation request with KMA-key ID reserved and result code.

Figure 5 shows signalling procedures for a key reservation request.

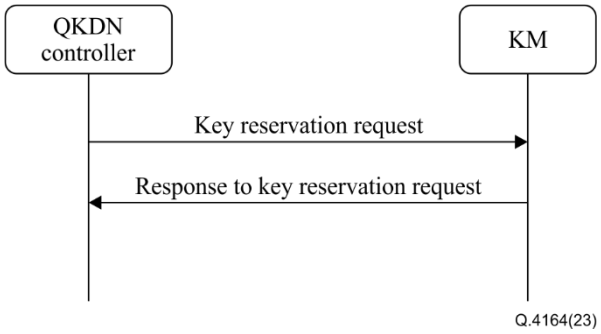

Figure 5 – Signalling procedures for key reservation request

7.6 Signalling procedures for key allocation request

The corresponding QKDN controller can send a key allocation request with KMA ID, KMA-key IDs to allocate the key resource that has been reserved. After receiving the key allocation request, the KM responds to the corresponding QKDN controller with a result code.

Figure 6 shows signalling procedures for a key allocation request.

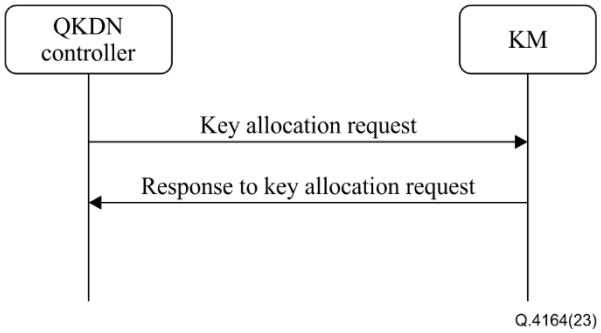

Figure 6 – Signalling procedures for key allocation request

8 Signalling messages and parameters

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

The M/O columns of Tables 1 to 13 relate to signalling of the parameters 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 13 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 13 may vary with specific protocols.

8.1 Key relay next hop request message

Table 1 lists parameters of a key relay next hop request message. Either a 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 a 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 a 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 lists parameters of a 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, with or without 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 an 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 Key relay request notification message

Table 3 lists parameters of a key relay request notification message. In a centralized QKDN, after receiving a key request sent by a cryptographic application, if a key relay is needed, the KM can request the whole route of the key relay from the QKDN controller. At this time, as in the case of a 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 key relay request notification 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 a 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 a 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 lists parameters of a key relay request message. The QKDN controller returns all KMs in the route (transit KMA IDs) to reach the destination KMA, with or without 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	Mandatory if an application destination ID is contained in the key relay request notification message.	
Transit KMA IDs	List of IDs of KMAs that are the transition nodes of key relay route	String	M	
Key relay request ID	ID of key relay request	String	O	
Extension	Array of extension parameters	Array of objects	O	

8.5 Response to key relay request message

Table 5 lists parameters of a 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	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	

8.6 Session creation request message

A session creation request message is sent from the source KM to the corresponding QKDN controller. A session can be created to facilitate key supply between cryptographic applications and KMs on both sides.

Table 6 lists parameters of a session creation request message.

Table 6 – Parameters of session creation request message

Parameter	Description	Data type	M/O	Remarks
Application source ID	ID of the source cryptographic application (i.e., the application that connects to the source KM to receive KSA-keys)	String	M	
Application destination ID	ID of the destination cryptographic application (i.e., the application with which the source cryptographic application requests to communicate)	String	M	
Number of keys	Number of KSA-keys requested	Integer	O	A default value is applied if omitted. This parameter can be used as the maximum number of KSA-keys requested during one session
Extension	Array of extension parameters	Array of objects	O	

8.7 Response to session creation request message

A response to a session creation request message is sent from the corresponding QKDN controller to the source KM. After receiving a session creation request, the QKDN controller generates a session ID and notifies the destination KM of the session ID to create a session. After receiving the session creation result, the QKDN controller responds to the source KM with the session ID.

Table 7 lists parameters of a response to a session creation request message.

Table 7 – Parameters of response to session creation request message

Parameter	Description	Data type	M/O	Remarks
Session ID	ID of the session created for key supply	String	M	
Response	Result of the creation of the session	String	M	Reason for success or failure
Destination KM ID	ID of the destination KM	String	M	
Extension	Array of extension parameters	Array of objects	O	

8.8 Session creation notification message

A session creation notification message is sent from the corresponding QKDN controller to the destination KM. The destination KM can notify the destination cryptographic application of the received session ID for a session creation.

Table 8 lists parameters of a session creation notification message.

Table 8 – Parameters of session creation notification message

Parameter	Description	Data type	M/O	Remarks
Application source ID	ID of the source cryptographic application (i.e., the application that connects to the source KM to receive KSA-keys)	String	M	
Application destination ID	ID of the destination cryptographic application (i.e., the application with which the source cryptographic application requests to communicate)	String	M	
Session ID	ID of the session created for key supply	String	M	
Source KM ID	ID of the source KM	String	M	
Number of keys	Number of KSA-keys requested	Integer	O	A default value is applied if omitted. This parameter can be used as the maximum number of KSA-keys requested during one session
Extension	Array of extension parameters	Array of objects	O	

8.9 Response to session creation notification message

A response to a session creation notification message is sent from the destination KM to the corresponding QKDN controller. The destination KM responds to the corresponding QKDN controller with the session creation result.

Table 9 lists parameters of a response to a session creation notification message.

Table 9 – Parameters of response to session creation notification message

Parameter	Description	Data type	M/O	Remarks
Session ID	ID of the session created for key supply	String	M	
Response	Result of the creation of the session	String	M	Reason for success or failure
Extension	Array of extension parameters	Array of objects	O	

8.10 Key reservation request

Table 10 lists parameters of a key reservation request.

Table 10 – Parameters of key reservation 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	M	
Destination KMA ID	ID of KMA that is the destination in the entire key relay route	String	M	
Application destination ID	ID of the destination cryptographic application (i.e., the application with which the source cryptographic application requests to communicate)	String	O	
Extension	Array of extension parameters	Array of objects	O	

8.11 Response to key reservation request

Table 11 lists parameters of a response to a key reservation request message.

Table 11 – Parameters of response to key reservation 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	O	
Application destination ID	ID of the destination cryptographic application (i.e., the application with which the source cryptographic application requests to communicate)	String	O	
Key IDs	IDs of KMA-keys reserved	String	M	
Response	Result of key reservation request	Integer	M	
Extension	Array of extension parameters	Array of objects	O	

8.12 Key allocation request

Table 12 lists parameters of a key allocation request.

Table 12 – Parameters of key allocation 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	M	
Destination KMA ID	ID of KMA that is the destination in the entire key relay route	String	M	
Application destination ID	ID of the destination cryptographic application (i.e., the application with which the source cryptographic application requests to communicate)	String	O	
Key IDs	IDs of KMA-keys reserved	Array of objects	M	
Extension	Array of extension parameters	Array of objects	O	

8.13 Response to key allocation request

Table 13 lists parameters of a response to a key allocation request message.

Table 13 – Parameters of response to key allocation 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	O	
Application destination ID	ID of the destination cryptographic application (i.e., the application with which the source cryptographic application requests to communicate)	String	O	
Key IDs	IDs of KMA-keys reserved	Array of objects	O	
Response	Result of key allocation request	Integer	M	
Extension	Array of extension parameters	Array of objects	O	

9 Security considerations

Control and management information is transferred through a Ck reference point. Security requirements and measures to protect it 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 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.

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

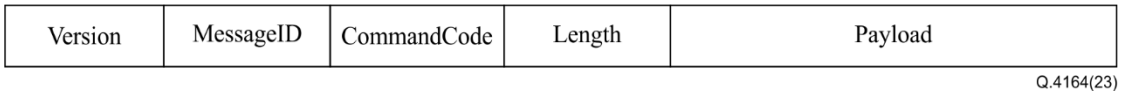

Figure I.1 – Message format over the transmission control protocol

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 Ck 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 or enhanced security.

On establishment of the connection, mutual authentication between the KM and the QKDN controller is performed. After mutual authentication, a command/response message can be transferred at the Ck interface for key relay request.

NOTE 3 – When applying the TLS protocol, the KM can verify the validity of a certificate the QKDN controller possesses and based in that confirm the ID of the QKDN controller it is connecting to. Similarly, the QKDN controller can verify the validity of a certificate the KM possesses and based in that confirm the ID of the connecting 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
0x1401	Key relay next hop request
0x4102	Response to key relay next hop request
0x1403	Key relay request notification
0x4104	Key relay request
0x1405	Response to key relay request
0x1406	Session creation request
0x4107	Response to session creation request

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

CommandCode	Command/response message name
0x4108	Session creation notification
0x1409	Response to session creation notification
0x410A	Key reservation request
0x140B	Response to key reservation request
0x410C	Key allocation request
0x140D	Response to key allocation request

The first two digits "14" in a CommandCode indicate that the corresponding message is sent from the KM to the QKDN controller; "41" indicate that the corresponding message is sent from the QKDN controller to the KM.

Appendix II

Protocol implementation using gRPC

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

This appendix describes a protocol implementation for messages and parameters that are described in clause 8 using gRPC.

II.1 Mapping of signalling messages to gRPC messages

gRPC is a cross-platform open source high-performance remote procedure call (RPC) framework. It is currently being developed under the Cloud Native Computing Foundation (CNCF) under the Linux Foundation. It uses HTTP 2.0 and supports multiple programming languages [b-CNCF gRPC].

Table II.1-1 – Example mapping of signalling messages to gRPC messages

Signalling messages	gRPC message name
Key relay request notification	KeyRelayRequestNotification
Key relay request	KeyRelayRequest
Response to key relay request	KeyRelayResponse
Key reservation request	KeyReservationRequest
Response to key reservation request	KeyReservationResponse
Key allocation request	KeyAllocationRequest
Response to key allocation request	KeyAllocationResponse

II.2 Key relay request notification

Table II.2-1 shows gRPC profiles for a key relay request notification message mapping example.

Table II.2-1 – gRPC profiles for key relay request notification message mapping example

Parameter	Mapped to	Data type
Source KMA ID	gRPC 'start_km'	String
Destination KMA ID	gRPC 'end_km'	String
Application destination ID	not mapped	
Extension	not mapped	

II.3 Key relay request and response message

Table II.3-1 lists gRPC profiles for a key relay request message mapping example. Table II.3-2 lists an example of response message mapping.

Table II.3-1 – gRPC profiles for key relay request message mapping example

Parameter	Mapped to	Data type
Source KMA ID	gRPC 'start_km'	String
Destination KMA ID	gRPC 'end_km'	String
Transit KMA IDs	gRPC 'kma_id'	String
Key relay request ID	gRPC 'keyrelayrequest_id'	String

Table II.3-1 – gRPC profiles for key relay request message mapping example

Parameter	Mapped to	Data type
Extension	not mapped	

Table II.3-2 – gRPC profiles for response to key relay request message mapping example

Parameter	Mapped to	Data type
Response	gRPC 'result_code' ex) 0: OK, 1: NG	Integer
Key relay request ID	gRPC 'keyrelayrequest_id'	String
Extension	gRPC 'error_message'	String

II.4 Key reservation request and response message

Table II.4-1 lists gRPC profiles for a key reservation request message mapping example. Table II.4-2 lists an example of response message mapping.

Table II.4-1 – gRPC profiles for key reservation request message mapping example

Parameter	Mapped to	Data type
Source KMA ID	gRPC 'start_km'	String
Destination KMA ID	gRPC 'end_km'	String
Application destination ID	not mapped	
Extension	not mapped	

Table II.4-2 – gRPC profiles for response to key reservation request message mapping example

Parameter	Mapped to	Data type
Source KMA ID	gRPC 'start_km'	String
Destination KMA ID	gRPC 'end_km'	String
Application destination ID	not mapped	
Key IDs	gRPC 'key_id'	String
Response	gRPC 'result_code' ex) 0: OK, 1: NG	Integer
Extension	gRPC 'error_message'	String

II.5 Key allocation request and response message

Table II.5-1 lists gRPC profiles for a key allocation request message mapping example. Table II.5-2 lists an example of response message mapping.

Table II.5-1 – gRPC profiles for key allocation request message mapping example

Parameter	Mapped to	Data type
Source KMA ID	gRPC 'start_km'	String
Destination KMA ID	gRPC 'end_km'	String
Application destination ID	not mapped	
Key IDs	gRPC 'key_id'	String
Extension	not mapped	

Table II.5-2 – gRPC profiles for response to key allocation request message mapping example

Parameter	Mapped to	Data type
Source KMA ID	gRPC 'start_km'	String
Destination KMA ID	gRPC 'end_km'	String
Application destination ID	not mapped	
Key IDs	gRPC 'key_id'	String
Response	gRPC 'result_code' ex) 0: OK, 1: NG	Integer
Extension	gRPC 'error_message'	String

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-CNCF gRPC] Cloud Native Computing Foundation (2024). *What is gRPC?* Mountain View, CA: gPRC authors. Available [viewed 2023-03-03] at; https://grpc.io/docs/what-is-grpc/ See also [viewed 2023-03-03]: https://www.cncf.io/projects/grpc/

[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