ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T Q.4161 (12/2023)

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

Protocols and signalling for Quantum key distribution networks

Protocols for Ak 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.4161

Protocols for Ak interfaces for quantum key distribution networks

Summary

Recommendation ITU-T Q.4161 specifies protocols for Ak interfaces in quantum key distribution networks.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T Q.4161	2023-12-14	11	11.1002/1000/15755

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.4161

Protocols for Ak interfaces for quantum key distribution networks

1 Scope

This Recommendation specifies protocols for Ak 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).

3.1.3 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.

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

3.1.5 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.

3.1.6 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.

3.1.7 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.

3.1.8 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.

3.1.9 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).

3.1.10 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.

3.1.11 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
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 Ak interface

Reference point Ak connects a cryptographic application and a key supply function in a KSA. It is responsible for sending key requests from the cryptographic application to the KSA, performing authentication between the cryptographic application and the KSA, and supplying keys from the KSA to the cryptographic application.

7 Signalling procedure

The following two modes are specified for key request and key supply at the Ak interface.

1) Key supply upon request mode: Both KMs on the source and destination sides initiate key supplies after receiving key requests from the corresponding cryptographic applications.

2) Proactive key supply mode: The KM on the source side initiates key supply upon request, and then instructs the KM on the destination side to supply a key proactively.

NOTE – The proactive key supply mode can be adopted in scenarios where the cryptographic applications on both sides are restricted to have no direct communication before they have KSA-keys.

Examples of signalling procedure of key request, key relay, and key supply in QKDN are described in 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 procedure for key supply upon request mode

7.1.1 Key request on the source side

When a cryptographic application needs keys for encryption, it sends a key request to the KM, which then supplies keys. If the KM does not have a sufficient number of keys in storage, it initiates key generation or key relay to share the necessary number, and supplies them to the cryptographic applications when their generation or relay is completed.

Figure 1 shows signalling procedures for key request at the Ak interface on the source side.

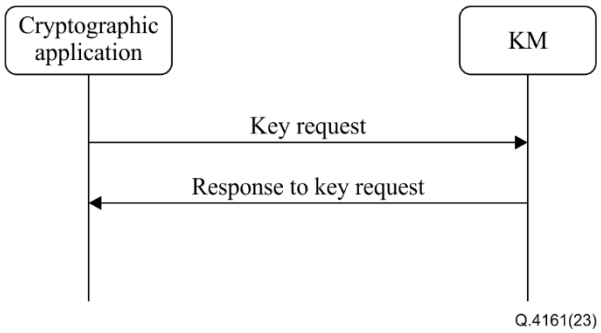

Figure 1 – Signalling procedures for key request at the Ak interface on the source side

7.1.2 Key request with identifier on the destination side

The destination cryptographic application requests a key from the KM to which it is connected. The destination cryptographic application sends a request with the key identifier (ID) that is received from the source cryptographic application in order to specify the key.

Figure 2 shows signalling procedures for a key request with ID at the Ak interface on the destination side.

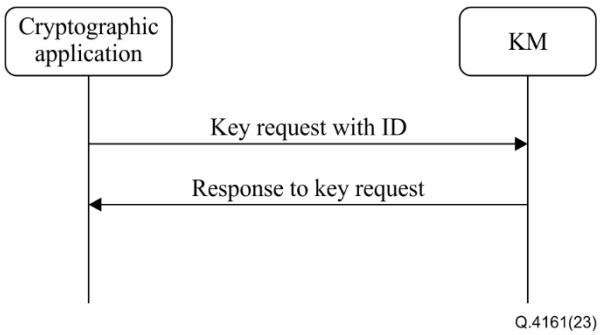

Figure 2 – Signalling procedures for a key request with identifier at the Ak interface on the destination side

7.2 Signalling procedure for proactive key supply mode

7.2.1 Session creation on the source side

When a cryptographic application needs keys for encryption, it first sends a session creation request to the KM on the source side. The source KM then notifies the KM on the destination side to create a session and responds with a session ID to the source cryptographic application when the session is successfully created. Based on the session created, the source cryptographic application can request keys from the source KM.

Figure 3 shows signalling procedures for a session creation at the Ak interface on the source side.

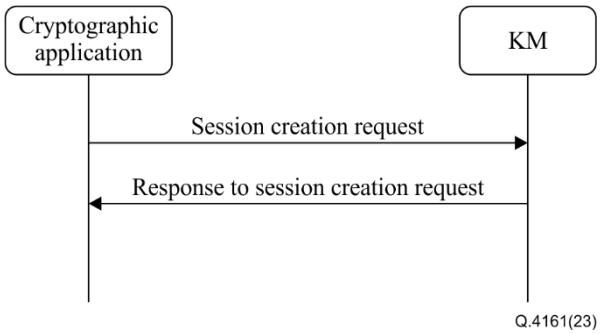

Figure 3 – Signalling procedures for session creation at the Ak interface on the source side

7.2.2 Session creation on the destination side

The destination cryptographic application receives a session creation notification from the KM to which it is connected. The destination KM sends the notification with the session ID that is received from the source KM in order to specify the session.

Figure 4 shows signalling procedures for session creation at the Ak interface on the destination side.

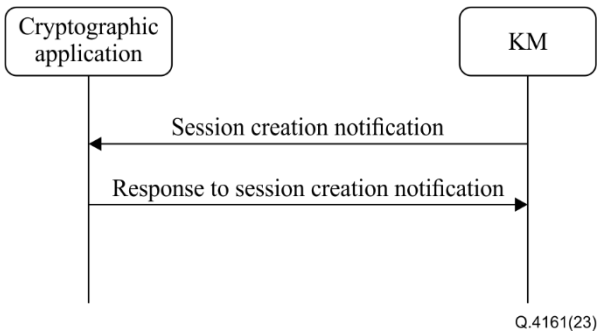

Figure 4 – Signalling procedures for session creation at the Ak interface on the destination side

7.2.3 Key request with session identifier on the source side

With a created session, the KM on the source side supplies KSA-keys on request from the source cryptographic application.

Figure 5 shows signalling procedure for a key request with a session ID at the Ak interface on the source side.

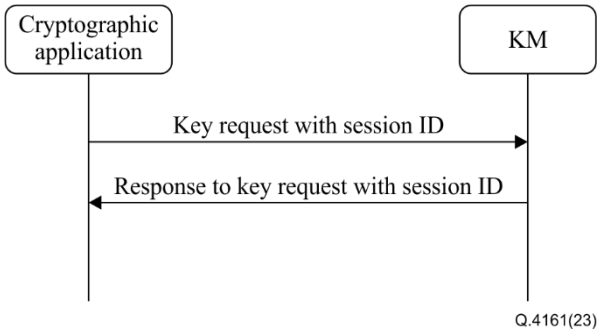

Figure 5 – Signalling procedures for key request with session identifier at the Ak interface on the source side

7.2.4 Proactive key supply on the destination side

The KM on the destination side proactively supplies KSA-keys to the destination cryptographic application to which it is connected. This scheme is applicable when the key request from the source cryptographic application is received by the source KM, which then instructs the destination KM to supply a key proactively.

Figure 6 shows signalling procedures for proactive key supply at the Ak interface on the destination side.

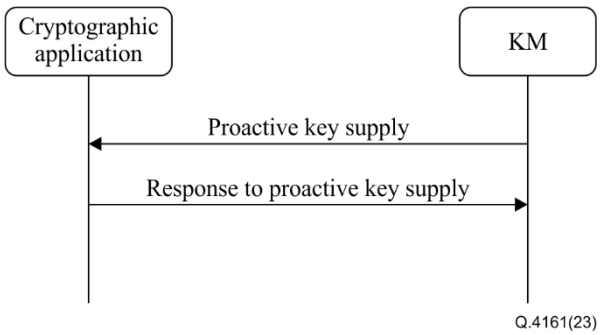

Figure 6 – Signalling procedures for proactive key supply at the Ak interface on the destination side

8 Signalling messages and parameters

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

The M/O columns of Tables 1 to 11 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 11 is not necessarily mapped to a field in the message payload and might be part of the control parameters of a specific protocol. The data type listed in columns 3 of tables 1 to 11 may vary with specific protocols.

8.1 Messages and parameters for key supply upon request mode

8.1.1 Key request message

A message is sent from the cryptographic application to the KM on the source side to request keys.

Table 1 lists the parameters of a key request message.

Table 1 – Parameters of key request message

Parameter	Description	Data type	M/O	Remarks
Application source ID	ID of the source cryptographic application (i.e., the application that sends this message)	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	M	
Application name	Name of the cryptographic application	String	O	
Number of keys	Number of KSA-keys requested	Integer	O	A default value is applied if omitted
Size of key	Length of each KSA-key requested	Integer	O	A default value is applied if omitted
Extension	Array of extension parameters	Array of objects	O	

8.1.2 Key request with identifier message

On receipt of the KSA-key, the source cryptographic application sends the corresponding key ID to the destination cryptographic application. The destination cryptographic application sends a request to the destination KM with the key ID. The destination cryptographic application then receives the key that has been shared between the source and destination KMs.

Table 2 lists the parameters of a key request with an ID message.

Table 2 – Parameters of a key request with identifier message

Parameter	Description	Data type	M/O	Remarks
Application source ID	ID of the source cryptographic application	String	M	
Application destination ID	ID of the destination cryptographic application (i.e., the application that sends this message)	String	O	
Application name	Name of the cryptographic application	String	O	
Key IDs	IDs of the KSA-keys requested	Array of objects	M	These IDs are notified from the source cryptographic application
Key ID	ID of the KSA-key requested	String	M	
Key ID extension	Extensions to key ID	Object	O	
Extension	Array of extension parameters	Array of objects	O	

8.1.3 Response to key request message

A response to a key request message is sent from the KM to the cryptographic application in response to the key request or the key request with ID from the cryptographic application. The KM supplies the requested KSA-keys to the cryptographic application. There is no difference between the source side and the destination side for the response to the key request.

Table 3 lists the parameters of a response to a key request message.

Table 3 – 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	KSA-key data provided for the request	String	M	
Key ID	ID of the KSA-key provided	String	M	
Key extension	Extensions to key file	Object	O	Hash value, etc.
Response	Result of key supply	String	M	Reason for success or failure
Extension	Array of extension parameters	Array of objects	O	

8.2 Messages and parameters for proactive key supply mode

8.2.1 Session creation request message

A session creation request message is sent from the cryptographic application to the KM on the source side. A session is created to facilitate key supply between the cryptographic applications and the KMs on both sides.

Table 4 lists the parameters of a session creation request message.

Table 4 – 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 sends this message)	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	
Application name	Name of the source cryptographic application	String	O	
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	

8.2.2 Response to session creation request message

The response to a session creation request message is sent from the KM to the cryptographic application on the source side. On receipt of a session creation request, the source KM notifies the KM on the destination side to create a session and responds with a session ID to the source cryptographic application when the session is successfully created.

Table 5 lists the parameters of a response to a session creation request message.

Table 5 – Parameters of response to session creation request message

Parameter	Description	Data type	M/O	Remarks
Session ID	ID of the session created	String	M	
Response	Result of the creation of the session	String	M	Success, failure reason, or status table of key supply
Source KM ID	ID of the source KM	String	O	
Extension	Array of extension parameters	Array of objects	O	

8.2.3 Session creation notification message

A session creation notification message is sent from the KM to the cryptographic application on the destination side. The destination KM proactively sends the session ID to the destination cryptographic application and notifies it with the ID of the source cryptographic application requesting to communicate with it.

Table 6 lists the parameters of a session creation notification message.

Table 6 – 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 receives this message)	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	
Application name	Name of the source cryptographic application	String	O	
Session ID	ID of the session created	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	

8.2.4 Response to session creation notification message

A response to a session creation notification message is sent from the cryptographic application to the KM in response to the session creation notification on the destination side. The destination cryptographic application notifies the result of the creation of the session to the destination KM.

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

Table 7 – Parameters of response to session creation notification message

Parameter	Description	Data type	M/O	Remarks
Session ID	ID of the session created	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	

8.2.5 Key request with session identifier message

With a created session, the cryptographic application sends a key request with session ID message to the KM on the source side. The source KM then supplies the requested KSA-keys to the source cryptographic application during the session.

Table 8 lists the parameters of a key request with a session ID message.

Table 8 – Parameters of key request with session identifier message

Parameter	Description	Data type	M/O	Remarks
Session ID	ID of the session created	String	M	
Number of keys	Number of KSA-keys requested	Integer	O	A default value is applied if omitted
Size of key	Length of each KSA-key requested	Integer	O	A default value is applied if omitted
Extension	Array of extension parameters	Array of objects	O	

8.2.6 Response to key request with session identifier message

A response to a key request with a session ID message is sent from the KM to the cryptographic application on the source side. The source KM then supplies the requested KSA-keys to the source cryptographic application during the created session.

Table 9 lists the parameters of a response to a key request with a session ID message.

Table 9 – Parameters of response to key request with session identifier message

Parameter	Description	Data type	M/O	Remarks
Session ID	ID of the session created	String	M	
Keys	Key file consists of key data and metadata	Array of objects	M	
Key	KSA-key data provided for the request	String	M	
Key ID	ID of the KSA-key provided	String	M	
Key extension	Extensions to key file	Object	O	Hash value, etc.
Response	Result of key supply	String	M	Reason for success or failure
Extension	Array of extension parameters	Array of objects	O	

8.2.7 Proactive key supply message

A proactive key supply message is sent from the KM to the cryptographic application on the destination side. The destination KM proactively supplies the KSA-key to the destination cryptographic application during the created session.

Table 10 lists the parameters of a proactive key supply message.

Table 10 – Parameters of proactive key supply message

Parameter	Description	Data type	M/O	Remarks
Session ID	ID of the session created	String	M	
Keys	Key file consists of key data and metadata	Array of objects	M	
Key	KSA-key data supplied	String	M	
Key ID	ID of the KSA-key supplied	String	M	
Key extension	Extensions to key file	Object	O	Hash value, etc.
Extension	Array of extension parameters	Array of objects	O	

8.2.8 Response to proactive key supply message

A response to a proactive key supply message is sent from the cryptographic application to the KM in response to proactive key supply on the destination side. The destination cryptographic application notifies the receipt of the KSA-key to the destination KM.

Table 11 lists the parameters of a response to proactive key supply message.

Table 11 – Parameters of response to proactive key supply message

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

9 Security considerations

Key data and associated metadata are transferred through an Ak reference point. 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 cryptographic application can connect to the KM using the TCP [b-IETF RFC 9293]. The corresponding message format over the TCP is shown in Figure I.1.

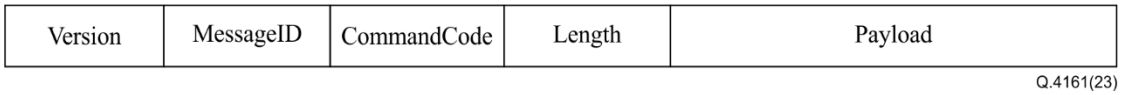

Figure I.1 – Message format over the transmission control protocol

In Figure I.1:

Version: the current version of the 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 Ak 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 cryptographic application and the KM is performed. After mutual authentication, a command/response message can be transferred via the Ak interface for key request and key supply.

NOTE 3 – When applying the TLS protocol, the cryptographic application 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 cryptographic application possesses and based on that confirm the ID of the connecting cryptographic application.

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

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

CommandCode	Command/response message name
0x2101	Key request
0x2102	Key request with ID
0x1203	Response to key request
0x2104	Session creation request
0x1205	Response to session creation request
0x1206	Session creation notification
0x2107	Response to session creation notification

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

CommandCode	Command/response message name
0x2108	Key request with session ID
0x1209	Response to key request with session ID
0x120A	Proactive key supply
0x210B	Response to proactive key supply

The first two digits "12" in a CommandCode indicate that the corresponding message is sent from the KM to the cryptographic application; "21" indicate that the corresponding message is sent from the cryptographic application 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 8.1 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 8.1 to the corresponding data format specified in [b-ETSI GS QKD 014].

NOTE – In this implementation, the cryptographic application and the KM correspond to the secure application entity (SAE) 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 8.1.1 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
Application source ID	O	String	None
Application destination ID	M	String	"{target_SAE_ID}" part of the access URL
Application name	O	String	None
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 Key request with identifier message

In this implementation, the key request with ID message specified in clause 8.1.2 corresponds to the HTTPS request of the HTTPS transaction performed as the Get Key with ID method specified in [b-ETSI GS QKD 014]. Table II.2 lists the mapping of the key request with ID message to the Get Key with ID method.

Table II.2 – Mapping of key request with identifier message to Get Key with ID method

Parameter	M/O	Data type	Implementation in Get Key with ID method
Application source ID	M	String	"{initiator_SAE_ID}" part of the access URL
Application destination ID	O	String	None
Application name	O	String	None
Key IDs	M	Array of objects	The "key_IDs" item in the key ID data format

Table II.2 – Mapping of key request with identifier message to Get Key with ID method

Parameter	M/O	Data type	Implementation in Get Key with ID method
Key ID	M	String	The "key_ID" item in the key ID data format
Key ID extension	O	Object	The "key_ID_extension" item in the key ID data format
Extension	O	Array of objects	The "key_IDs_extension" item in the key ID data format

II.3 Response to key request message

In this implementation, the response to a key request message specified in clause 8.1.3 corresponds to the HTTPS response of the HTTPS transaction performed as the Get Key method or the Get Key with ID method. Table II.3 lists the mapping of the response to a key request message to the Get Key method or the Get Key with ID method.

Table II.3 – Mapping of response to key request message to Get Key/Get Key with ID method

Parameter	M/O	Data type	Implementation in Get Key or Get Key with ID 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 or Get Key with ID 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), *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-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