INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2022-2024

SG11-TD714/GEN

STUDY GROUP 11

Original: English

Question(s): Q2/11 Geneva, 10-20 October 2023

TD

Source: Editors

Title: Output – initial draft for Q.QKDNi_KM: Protocols for interfaces between key managers for quantum key distribution network interworking

Contact: Kaoru Kenyoshi E-mail: kaoru.kenyoshi@nict.go.jp
NICT
Japan

Contact: Hongyu Wu E-mail: hongyu.wu@quantum-info.com
QuantumCTek Co., Ltd.
China

Contact: Jeong Yun KIM E-mail: jykim@etri.re.kr
ETRI
Korea (Rep. of)

Abstract: This document contains the initial draft for Q.QKDNi_KM: Protocols for interfaces between key managers for quantum key distribution network interworking.

Summary

This TD is the outcome of the initial draft Recommendation ITU-T Q.QKDNi_KM: "Protocols for interfaces between key managers for quantum key distribution network interworking" based on the discussion results on the input document C244 with modifications at the Q2/11 meetings (Geneva, 10-20 October 2023).

Draft Recommendation ITU-T Q.QKDNi_KM

Protocols for interfaces between key managers for quantum key distribution network interworking

Summary

Recommendation ITU-T Q.QKDNi_KM specifies protocols for Kxi and Kxi' interfaces in quantum key distribution networks interworking (QKDNi).

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

Table of Contents

Draft Recommendation ITU-T Q.QKDNi_KM

Protocols for interfaces between key managers for quantum key distribution network interworking

1. Scope

This Recommendation specifies protocols at Kxi and Kxi' interfaces for quantum key distribution network interworking (QKDNi) especially the following areas.

- Signalling procedures for Kxi and Kxi' interfaces for QKDNi;
- Signalling messages and parameters for Kxi and Kxi' interfaces for QKDNi;
- 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 X.1710] Recommendation ITU-T X.1710 (2020), *Security framework for quantum key distribution networks*

[ITU-T X.1712] Recommendation ITU-T X.1712 (2021)/Cor.1 (02/2022), Security requirements and measures for quantum key distribution networks - key management.

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

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

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

[ITU-T Y.3810] Recommendation ITU-T Y.3810 (2022), Quantum key distribution networks - Quantum key distribution network interworking – Framework

[ITU-T Q.QKDNi_profr] draft Recommendation Q.QKDNi_profr, Quantum key distribution networks Interworking - Protocol framework.

3. Definitions

3.1. Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

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

3.1.2 **key manager (KM)** [ITU-T Y.3800]: A functional module located in a quantum key distribution (QKD) node to perform key management in the key management layer.

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

3.1.4 **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.

3.1.5 **quantum key distribution link (QKD link)** [ITU-T Y.3800]: A communication link between two quantum key distribution (QKD) modules to operate the QKD.

NOTE – A QKD link consists of a quantum channel for the transmission of quantum signals, and a classical channel used to exchange information for synchronization and key distillation.

3.1.6 **quantum key distribution module (QKD module)** [ITU-T Y.3800]: A set of hardware and software components that implements cryptographic functions and quantum optical processes, including quantum key distribution (QKD) protocols, synchronization, distillation for key generation, and is contained within a defined cryptographic boundary.

NOTE – A QKD module is connected to a QKD link, acting as an endpoint module in which a key is generated. These are two types of QKD modules, namely, the transmitters (QKD-Tx) and the receivers (QKD-Rx).

3.1.7 **quantum key distribution network (QKDN)** [ITU-T Y.3800]: A network comprised of two or more quantum key distribution (QKD) nodes connected through QKD links.

NOTE – A QKDN allows sharing keys between the QKD nodes by key relay when they are not directly connected by a QKD link.

3.2. Terms defined in this Recommendation

None.

4. Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

GWF GateWay Function

GWN GateWay Node

HTTPS HyperText Transfer Protocol Secure

ID IDentifier

IWF InterWorking Function

IWN InterWorking Node

KM Key Manager

QKD Quantum Key Distribution

QKDN Quantum Key Distribution Network

QKDNi Quantum Key Distribution Network Interworking

5. Conventions

None.

6. Interfaces for interworking of key management layers in QKDNs

Kx and Kxi interfaces are defined for interworking of key management layers in [ITU-T Y.3810].

- Kxi is a reference point connecting two KMs between the QKDNs via an interworking KM link. It is responsible for exchanging information and operations required for key relay, key synchronization and authentication between QKDNs.
- Kxi' is a reference point connecting two KMs in the IWN via an interworking KM link. It is responsible for exchanging information and operations required for key transfer, key synchronization and authentication between QKDNs.

The signalling procedure and the message parameters specified in the clause 7 and 8 can be used both for Kxi and Kxi' interfaces.

7. Signalling procedure

Examples of signalling procedure of key request, key relay, and key transfer in interworking QKDNs are described in Appendix I of [ITU-T Q.QKDNi_profr]. The protocol suites applied for the signalling are specified in clause 9 of [ITU-T Q.QKDNi_profr].

Editor's note – key relay message and parameters will be included for Kxi interface.

7.1. Signalling procedure for key transfer

To share keys between two interworking QKDNs, the keys are relayed at Kxi interface or transferred at Kxi' interface. Figure 1 shows the signalling procedure of the key transfer at the Kxi'.

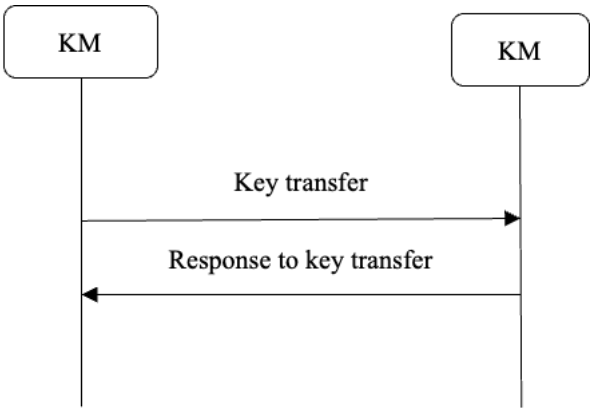

Figure 1 – Signalling procedures for key transfer

8. Signalling messages and parameters

This clause specifies messages and their parameters for the Kxi and Kxi' interface.

In the M/O column of the tables in this clause, M indicates that the parameter is mandatory for signalling, and O indicates that the parameter is optional for signalling.

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

NOTE – A message parameter described in the following tables is not necessarily mapped to a field in the message payload and might be a part of control parameters of one specific protocol. The Data type column of the tables may vary with specific protocols.

8.1. Key transfer message

Key transfer message is sent from one KM to the corresponding KM which is connected via Kxi or Kxi', for sharing the keys between two interworking QKDNs.

Table 1 shows parameters of key transfer message.

Table 1 – Parameters of key transfer message

Parameter		Description	Data type	M/O	Remarks
Keys		Key file consists of key data and metadata to be transferred.	Array of objects	M	
	Key	key value	string	M	
	Key ID	ID of the key	string	M	
	Key extension	Extensions to key file	object	O	
Application source ID		ID of the cryptographic application for which the transferred keys are shared, in the QKDN of the sender side of this message	string	O	Either of the Application ID pair or the KM ID pair is mandatory
Application destination ID		ID of the cryptographic application for which the transferred keys are shared, in the QKDN of the receiver side of this message	string	O	
Source KM ID		ID of the KM for which the keys are shared, in the QKDN of the sender side of this message	string	O	
Destination KM ID		ID of the KM for which the keys are shared, in the QKDN of the receiver side of this message	string	O	
Extension		Array of extension parameters	Array of objects	O	

8.2. Response to key transfer message

Response to key transfer message is sent from the KM that received the key transfer message as the response to the KM that sent the key transfer message.

Table 2 shows parameters of response to key transfer message.

Table 2 – Parameters of response to key transfer message

Parameter	Description	Data type	M/O	Remarks
Response	Response text to key transfer message	string	M	
Extension	Array of extension parameters	Array of objects	O	

9. Security considerations

(Texts to be added)

Appendix I

Protocol implementation using HTTPS

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

The signalling messages and parameters specified in clause 8 can be implemented using HTTPS according to the protocol and data format of REST-based key delivery API specified in [b-ETSI GS QKD 020]. This appendix describes the mapping of the messages and parameters specified in clause 8 to the corresponding data format specified in [b-ETSI GS QKD 020].

NOTE – In this implementation, the cryptographic application and the KM correspond to the SAE (Secure Application Entity) and the KME (Key Management Entity) defined in [b-ETSI GS QKD 020] respectively.

I.1 Key transfer message

In this implementation, the key transfer message specified in clause 8.1 corresponds to the HTTPS request of the HTTPS transaction performed as the 'ext_keys' method specified in [b-ETSI GS QKD 020]. Table I.1 shows the mapping of the key transfer message to the 'ext_keys' method.

Table I.1 – Mapping of key transfer message to ext_keys method

Parameter		M/O	Data type	Implementation in 'ext_keys' method
Keys		M	array of objects	The 'Keys' item in the 'ext_key_container' data format
	Key	M	string	The 'value' item in the 'ext_key_container' data format
	Key ID	M	string	The 'key_id' item in the 'ext_key_container' data format
	Key extension	O	object	The 'extension' item in the 'ext_key_container' data format
Application source ID		O	string	'{initiator_SAE_ID}' part of the Access URL
Application destination ID		O	string	'{target_SAE_ID}' part of the Access URL
Source KM ID		O	string	None
Destination KM ID		O	string	None
Extension		O	array of objects	'extension_optional' item in the 'ext_key_container' data format

I.2 Response to key transfer message

In this implementation, the Response to key transfer message specified in clause 8.2 corresponds to the HTTPS response of the HTTPS transaction performed as the 'ext_keys' method. Table I.2 shows the mapping of the response to key transfer message to the 'ext_keys' method.

Table I.2 – Mapping of response to key transfer message to ext_keys method

Parameter	M/O	Data type	Implementation in 'ext_keys' method
Response	M	string	'message' item in the 'message_data' data format

Extension	O	array of objects	‘details’ item in the ‘message_data’ data format

Bibliography

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

[b-ETSI GS QKD 020] Draft ETSI GS QKD 020 V0.2.1(2023-05), *Quantum Key Distribution (QKD); Protocol and data format of REST-based interoperable Key management System API.*