INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2022-2024

SG11-TD713-R1/GEN

STUDY GROUP 11

Original: English

Question(s): 2/11 Geneva, 10-20 October 2023

TD

Source: Editors

Title: Output – Revised baseline text of draft Recommendation ITU-T Q.QKDN_Mk "Protocols for interfaces on quantum key distribution network manager" (Geneva, 10-20 October 2023)

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

Contact: Jeongyun Kim
ETRI
Korea (Rep. of)
Tel: + 82-42-860-5311
Fax:
E-mail: jykim@etri.re.kr

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

Abstract: This TD includes the output - baseline text of the draft ITU-T Q.QKDN_Mk "Protocols for interfaces on quantum key distribution network manager" (Geneva, 10-20 October 2023).

Summary

This TD is the outcome of initial draft Recommendation ITU-T Q.QKDN_Mk "Protocols for interfaces on quantum key distribution network manager " (Geneva, 10 - 20 May 2023) based on the discussion results on contribution C230 and C308 with modifications at the Q2/11 meetings (Geneva, 10-20 October 2023).

Attachments:

Annex A: Draft Recommendation ITU T Q.QKDN_Mk "Protocols for interfaces on quantum key distribution network manager".

Annex A
Draft Recommendation ITU-T Q.QKDN_Mk

Protocols for interfaces on quantum key distribution network manager

Summary

Recommendation ITU-T Q.QKDN_Mk specifies protocols for interfaces on a quantum key distribution network manager (QKDN manager) in quantum key distribution networks (QKDN). Reference points on a QKDN manager are defined in [ITU-T Y.3802] which are Mq, Mqrp, Mops, Mk, Mc, Mu and Mx. A QKDN manager performs FCAPS functions through these interfaces to QKD modules, KMs, QKDN controllers, QKD links, user network managers and corresponding QKDN managers.

Keywords

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

Table of Contents

Draft Recommendation ITU-T Q.QKDN_Mk

Protocols for interfaces on quantum key distribution network manager

1. Scope

This Recommendation specifies protocols at interfaces on a quantum key distribution network manager (QKDN manager) for quantum key distribution network (QKDN) especially the following areas.

- signalling procedures for interfaces on a QKDN manager for QKDN;
- signalling messages and parameters for interfaces on a QKDN manager for QKDN;
- 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)/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.3804] Recommendation ITU-T Y.3804 (2020) (09/2020), *Quantum key distribution networks – Control and management*.

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 management agent (KMA)** [ITU-T Y.3802]**:** A functional element to manage keys generated by a quantum key distribution (QKD) module/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 (KMA link)** [ITU-T Y.3802]**:** A communication link connecting KMAs to perform key relay and communications for key management.

3.1.4 **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.

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

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

3.1.7 **key supply agent (KSA)** [ITU-T Y.3802]: A functional element to supply keys to a cryptographic application, being located between a key management agent (KMA) and the client.

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 client.

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

3.1.9 **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.

3.1.10 **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.

3.1.11 **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).

3.1.12 **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.

3.1.13 **quantum key distribution network controller (QKDN controller)** [ITU-T Y.3800]: A functional module, which is located in a quantum key distribution (QKD) network control layer to control a QKD network.

3.1.14 **quantum key distribution network manager (QKDN manager)** [ITU-T Y.3800]: A functional module, which is located in a quantum key distribution (QKD) network management layer to monitor and manage a QKD network.

3.1.15 **quantum key distribution node (QKD node)** [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).

This Recommendation uses the following terms defined elsewhere:

3.2.Terms defined in this Recommendation

None

4. Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

FCAPS	Fault, Configuration, Accounting, Performance and Security
ID	IDentifier
KM	Key Manager
KMA	Key Management Agent
KSA	Key Supply Agent
QKD	Quantum Key Distribution
QKDN	Quantum Key Distribution Network
TCP	Transmission Control Protocol

5. Conventions

None.

6. Interfaces on a QKDN manager

Reference points on a QKDN manager are defined in [ITU-T Y.3802] as follows.

- Mq: a reference point connecting the QKDN manager with a QKD module control and management function in a QKD module. It is responsible for the QKDN manager to communicate management information with the QKD module.
- Mops: a reference point connecting the QKDN manager and an optical switching/splitting function in a QKD link. It is responsible for the QKDN manager to communicate management information with the QKD link.
- Mqrp: a reference point connecting the QKDN manager and a quantum relay point function in a QKD link. It is responsible for the QKDN manager to communicate management information on the quantum relay point with the QKD link.
- Mk: a reference point connecting the QKDN manager and a KM control and management function in a KM. It is responsible for the QKDN manager to communicate management information with a KMA and a KSA.
- Mc: a reference point connecting the QKDN manager and a QKDN controller control and management function in a QKDN controller. It is responsible for the QKDN manager to communicate management information with the QKDN controller.

- Mu: a reference point connecting a user network manager in a user network and the QKDN manger in the QKDN. It is responsible for the QKDN manager to communicate management information with the user network manager.
- Mx: a reference point connecting two QKDN managers. It is responsible for the QKDN manager to communicate management information with other QKDN manager.

Reference points Mq, Mqrp, Mops, Mk, Mc, Mu and Mx are defined as interfaces between the QKDN manager and the functional components. A QKDN manager performs FCAPS functions through these interfaces to QKD modules, KMs, QKDN controllers, QKD links, user network managers and corresponding QKDN managers.

7. Signalling procedures

Editor's note – Contributions are invited on signalling procedures for subscribe and unsubscribe (Reference: 3GPP TS 23.288 Architecture enhancements for 5G System (5GS) to support network data analytics services).

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

Two kinds of signalling procedures are defined depending on the initiation from functional components and from a QKDN manager. Functional components refer QKD modules, KMs, QKDN controllers, QKD links, user network managers and corresponding QKDN managers in this clause.

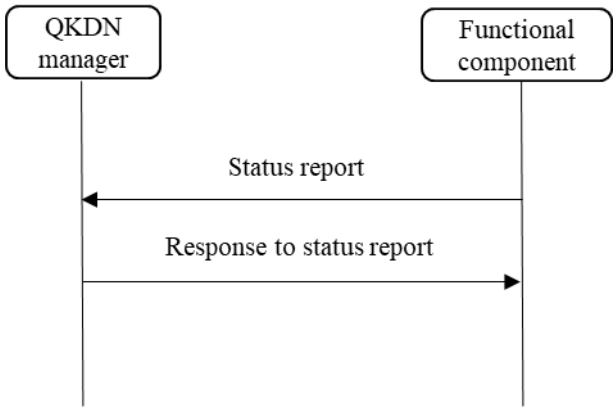

Figure - 1 Signalling procedure at the interfaces between functional components and the QKDN manager for status report.

Editor's note – It is further study that what condition triggers for the functional component to request status report to QKDN manager.

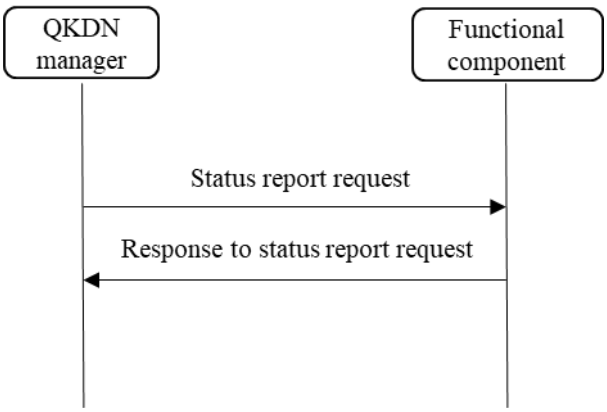

Figure -2 Signalling procedure at the interfaces between functional components and the QKDN manager for status report request

8. Signalling messages and parameters

This clause specifies messages and their parameters for the interfaces on a QKDN manager.

Table 1 is a reference table of component ID in messages at each interface.

Table 1 - Reference table of component ID in messages at each interface

Interface	Component ID
Mq	QKD module ID
Mops and Mqrp	QKD link ID
Mk	KM ID
Mc	QKD controller ID
Mu	User network manager ID
Mx	Corresponding QKDN manager ID

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.

NOTE – The messages and parameters defined in this clause are independent of a specific protocol. Different protocols can have different implementations of these messages and parameters. The recommended protocol implementations are described in Annex A. 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. Status report message

A status report message is sent from the functional component to the QKD manager to report status.

Table 2 shows message format and parameters of status report message.

Table 2 - Message format and parameters of status report message

Parameter	Description	Data type	M/O	Remarks
Component ID	ID of the functional component that sends a status report to the QKDN manager	string	M	
Extension	Array of extension parameters	Array of objects	O	Status information of the functional component

NOTE 1 – The extension in Table 2 includes the performance data and status of the functional component at least, which are sent from the functional component to the QKDN manager. For more information on the parameter, refer to [ITU-T Y.3804].

8.2. Response to status report message

A response to status report message is sent from the QKDN manager to the functional component in response to the status report message.

Table 3 shows parameters of response to status report message.

Table 3 – Parameters of response to status report message

Parameter	Description	Data type	M/O	Remarks
Component ID	ID of the functional component that sends a status report to the QKDN manager	string	M	
Response	Result of the receipt of the status report	string	M	Success or failure reason
Extension	Array of extension parameters	Array of objects	O	For future use

8.3. Status report request message

A status report request message is sent from the QKD manager to the functional component to request status information.

Table 4 shows message format and parameters of status report request.

Table 4 - Message format and parameters of status report request

Parameter	Description	Data type	M/O	Remarks
Component ID	ID of the functional component that is required to send a status report to the QKDN manager	string	O	
Extension	Array of extension parameters	Array of objects	O	

8.4. Response to status report request message

A response to status report request message is sent from the functional component to the QKDN manager in response to the status report request message.

Table 5 shows parameters of response to status report request message.

Table 5 – Parameters of response to status report request message

Parameter	Description	Data type	M/O	Remarks
Component ID	ID of the functional component that is required to send a status report to the QKDN manager	string	M	
Response	Result of the receipt of the status report	string	M	Success or failure reason
Extension	Array of extension parameters	Array of objects	O	Status information of the functional component

NOTE 1 – The extension in Table 5 includes the performance data and status of the functional component at least, which QKDN manager requests to receive from the functional component. For more information on the parameter, refer to [ITU-T Y.3804].

9. Security considerations

Management information is transferred through Mk reference point. Security requirements and measures to protect it are specified in [ITU-T X.1712].

Appendix I

Bibliography

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

[b-IETF RFC 793] IETF RFC 793, *TRANSMISSION CONTROL PROTOCOL.*

[b-IETF RFC 5246] IETF RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2.*

[b-IETF RFC 8259] IETF RFC 8259, *The JavaScript Object Notation (JSON) Data Interchange Format.*

_____