INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2022-2024

SG13-TD37/WP3

STUDY GROUP 13

Original: English

Question(s): 16/13 Geneva, 4 - 15 July 2022

TD

Source: Editors

Title: Draft Recommendation ITU-T Y.QKDN-iwrq: "Quantum key distribution networks interworking – functional requirements"

Contact:	Yazi Wang Beijing University of Posts and Telecommunications. China	Tel: +86-19800372862 E-mail: yazi_wang@bupt.edu.cn
Contact:	Yongli Zhao Beijing University of Posts and Telecommunications. China	Tel: +86-10-61198108 E-mail: yonglizhao@bupt.edu.cn
Contact:	Xiaosong Yu Beijing University of Posts and Telecommunications. China	Tel: +86-10-61198108 E-mail: xiaosongyu@bupt.edu.cn
Contact:	Zhangchao Ma CAS Quantum Network Co., Ltd. China	Tel: +86-10-83057625 E-mail: mazhangchao@casquantumnet.com
Contact:	Junsen Lai China Academy of Information and Communication Technology (CAICT), Ministry of Industry and Information Technology (MIIT), China	Tel: +86-10-62300592 E-mail: laijunsen@caict.ac.cn

Abstract: This is the revised draft Recommendation Y.QKDN-iwrq "Quantum key distribution network interworking – functional requirements" (output of SG13 meeting, 4 -15 July 2022)

Summary

This TD is the output document for the draft Recommendation ITU-T Y.QKDN-iwrq "Quantum key distribution networks interworking – functional requirements" based on the following input contributions and the discussion during the Q16/13 meeting, 4 – 15 July 2022. As the discussion results, contents should be further improved.

C-0044	BUPT, CAS Quantum Network Co. Ltd., MIIT	Proposed improvements to ITU-T Y.QKDN-iwrq: "Quantum key distribution networks - interworking requirements"	Q16/13

- Proposal of contribution

- This contribution includes the revised contents based on discussion results for the draft Recommendation ITU-T Y.QKDN-iwrq “Quantum key distribution networks interworking – functional requirements” based on the results of SG13 Q16 meeting (7 – 9 June 2022).

- Meeting result

- According to the discussion results, the document is preparing to be consented in November meeting, and the title, summary, scope, references, conventions, introduction and main clauses (i.e., clauses 7, 8 and 9) were revised based on the discussion results of C44 in the SG13 meeting (4 – 15 July 2022).
- According to the discussion suggestions, the Yellow parts represent the contents should be further discussed in September meeting, and this document still needs further improvement for consent in November meeting.
- About Appendix I in this document, it was removed from this document to the NWI Y.QKDN-iwac.

Attachments:

Annex I: Draft Recommendation ITU-T Y.QKDN-iwrq: “Quantum key distribution networks interworking – functional requirements” (output of Q16/13, 4 – 15 July 2022)

Annex I

Draft Recommendation ITU-T Y.QKDN-iwrq

Quantum key distribution networks interworking – functional requirements

Summary

For quantum key distribution networks (QKDN), Recommendation ITU-T Y.QKDN_iwrq specifies functional requirements for QKDNi. This Recommendation describes the general requirements, the functional requirements for QKDNi with GWNs and the functional requirements for QKDNi with IWNs.

Keywords
QKD, QKDN (QKD network), interworking;

Table of Contents

Draft Recommendation Y.QKDN-iwrq

Quantum key distribution networks interworking - functional requirements

1. Scope

This Recommendation specifies the functional requirements for QKDNi as follows.

- General requirements for QKDNi;
- Functional requirements for QKDNi with GWNs;
- Functional requirements for QKDNi with IWNs.

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 Y.QKDN-iwfr] Draft Recommendation ITU-T Y.QKDN-iwfr, Quantum key distribution networks - interworking framework.

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

[ITU-T Y.3801] Recommendation ITU-T Y.3801 (2020) Functional requirements for quantum key distribution network.

[ITU-T Y.3802] Recommendation ITU-T Y.3802 (2020), Quantum key distribution networks – Functional architecture.

[ITU-T Y.3809] Recommendation ITU-T Y.3809 (2022), A role-based model in quantum key distribution networks deployment

3. Definitions

3.1. Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 **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.

3.1.2 **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.

3.1.3 **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.

3.1.4 **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).

3.1.5 **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.

3.1.6 **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.

3.1.7 **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.

3.1.8 **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).

3.2. Terms defined in this Recommendation

This Recommendation defines no term.

4. Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AES	Advanced Encryption Standard
FCAPS	Fault, Configuration, Accounting, Performance, Security
GWF	GateWay Function
GWN	GateWay Node
IT-secure	Information-theoretically secure
IWF	InterWorking Function
IWN	InterWorking Node
KM	Key manager
OTP	One-time pad encryption
QKD	Quantum Key Distribution
QKDN	QKD Network
QKDNi	QKDN interworking

5. Conventions

In this Recommendation:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

6. Introduction

The functional requirements for QKDNi are specified in order to meet the QKDNi capabilities and the layer structure in [ITU-T Y.QKDN-iwfr].

This Recommendation specifies the general and functional requirements for QKDNi. The functional requirements with GWNs and IWNs consider key management layer, QKDN control layer and QKDN management layer.

NOTE 1 - GWFs and IWFs are assumed to perform the following functions such as:

- Charging settlement between different charging policies;
- Terminal mobility (e.g., roaming of cryptographic applications);
- Number portability (e.g., subscribers move to other QKDN providers with same IDs);
- Security demarcation.

7. General requirements for QKDNi

- QKDNi is recommended to be compatible with various kinds of providers which implement different protocols.
- QKDNi is recommended to receive status information of different QKD module(s) and QKD link(s) from the different QKDN providers.
- QKDNi is recommended to receive operators' policy from the QKDN control layer to enforce it.
- QKDNi is recommended to protect any information on the key data from being leaked.
- QKDNi is recommended to contain different policies may be defined for different classes of providers.
- QKDNi is recommended to provide different protocol conversion.
- QKDNi is recommended to provide quality of service (QoS) policy control among different QKDN providers.
- QKDNi is recommended to enforce different QKDN providers' policies to key management layer.
- QKDNi is recommended to provide security configuration control information among multiple QKDN providers, which includes control related configuration, state of components (in service, out of service, standby, or reserved), alarm or failure diagnosis, and status of QBER.
- QKDNi is required to provide configuration management to support multiple management of resource provisioning among multiple QKDN providers.
- QKDNi is recommended to provide configuration management to support routing and rerouting of key relay among multiple QKDN providers.
- QKDNi is recommended to receive status information of different QKD module(s) and QKD link(s) from different QKDN providers.
- QKDNi is recommended to provide security management information from different QKDN providers, which includes management information for security (metadata, event logs, audit trail data), log database (key life cycle, traceability data of key), root certification authority, key management policy.

8. Functional requirements for QKDNi with GWNs

NOTE 1 – A functional entity (i.e., GWF) and reference model for QKDNi with GWFs has been defied in [ITU-T Y.QKDN-iwfr], and QKDN A and QKDN B are connecting at Qx, Kxi, and optionally Cxi.

8.1. Key management layer requirements for QKDNi

Req_KM 1. The key management layer is recommended to receive keys from a QKD module(s), and to relay them via Kxi with OTP encryption between QKD provider A and QKD provider B.

Req_KM 2. The key management layer is recommended to receive status information of different QKD module(s) and QKD link(s) from different QKDN providers, and to relay them via Kxi with OTP encryption.

8.2. QKDN control layer for QKDNi

Req_C 1. The QKDN control layer is recommended to share QKDN control information via Cxi between QKD provider A and QKD provider B.

Req_C 2. The QKDN control layer is recommended to provide mutual information control via Cxi between QKD provider A and QKD provider B.

8.3. QKDN management layer requirements for QKDNi

[Editors' Note: Consider whether QKDN management layer requirements for QKDNi is necessary, which should be discussed in this July meeting. Since reference model for QKDNi with GWFs mainly consider Kxi and Cxi.]

Req_M 1. The QKDN management layer is required to share performance management message to support:

- collecting/receiving performance information from respective quantum layer, the key management layer and the QKDN control layer;
- analyzing respective QKDN performance information collected/received.

9. Functional requirements for QKDNi with IWNs

NOTE 1 – A functional entity (i.e., IWF) and reference model for QKDNi with IWFs has been defied in [ITU-T Y.QKDN-iwfr], and QKDN A and QKDN B are connecting at Kxi' and optionally Cxi'.

9.1. Key management layer requirements for QKDNi

Req_KM 1. The key management layer is required to receive keys from a QKD module(s), and to transfer them via Kxi' between two internal KMs in IWN.

Req_KM 2. The key management layer is recommended to receive status information of different QKD module(s) and QKD link(s) from different QKDN providers, and to transfer them via Kxi' between two internal KMs in IWN.

Req_KM 3. The key management layer is recommended to receive relative information, such as key ID, QKD module ID, key generation date, and to transfer them via Kxi' between two internal KMs in IWN.

9.2. QKDN control layer requirements for QKDNi

Req_C 1. The control layer is recommended to share QKDN control information between QKDN providers via Qxi'.

NOTE 2 - QKDN control information can include routing control, session control, authentication and authorization control and QoS policy control, etc.

9.3. QKDN management layer requirements for QKDNi

[Editors' Note: Consider whether QKDN management layer requirements for QKDNi is necessary, which should be discussed in this July meeting. Since reference model for QKDNi with IWFs mainly consider Kxi' and Cxi'.]

Req_M 1. The QKDN management layer is recommended to share fault management message to respective IWF to support:

- collecting/receiving status information provided by respective quantum, key management, and control layers;

Req_M 2. The QKDN management layer is recommended to share fault management message to respective IWF.

10. Security consideration

To be added.

Bibliography

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

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

[b-ITU-T Y.3804] Recommendation ITU-T Y.3804 (2020), *Quantum key distribution networks – Control and management*

_____