Annex

Draft new Recommendation ITU-T Y.3813 (ex. 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 QKDN interworking (QKDNi). This Recommendation describes the functional requirements for key management layer, QKDN control layer, and QKDN management layer, for interworking using gateway nodes (GWNs) and/or interworking nodes (IWNs).

Keywords
Quantum key distribution (QKD), QKD network (QKDN), QKDN interworking (QKDNi)

Table of Contents

Draft new Recommendation Y.3813 (ex. Y.QKDN-iwrq)

Quantum key distribution networks interworking - functional requirements

1. Scope

This Recommendation specifies the functional requirements for QKDN interworking (QKDNi) as follows.

- Functional requirements for key management layer;
- Functional requirements for QKDN control layer;
- Functional requirements for QKDN management layer.

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.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.3810] Recommendation ITU-T Y.3810 (2022), Quantum key distribution networks - interworking framework.

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:

GWF GateWay Function

GWN GateWay Node

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.3810].

This Recommendation specifies the functional requirements for QKDNi using gateway nodes (GWNs) and interworking nodes (IWNs) specified in [ITU-T Y.3810]. The functional requirements are defined for key management layer, QKDN control layer and QKDN management layer.

Based on the functions (i.e., gateway function (GWF) and interworking function (IWF)) and the reference models for QKDNi specified in [ITU-T Y.3810], keys can be relayed between GWNs, and keys can be transferred in the IWN.

7. Functional requirements for key management layer

7.1. Key management layer requirements for QKDNi

Req_KM 1. The key management layers of interworking QKDNs are required to receive keys from their own QKD module(s).

Req_KM 2. The key management layers of interworking QKDNs are recommended to receive status information of the interworking QKD module(s) .

Req_KM 3. The key management layers of interworking QKDNs are recommended to exchange key metadata between QKDNs, such as key ID, QKD module ID, key generation date, etc.

Req_KM 4. The key management layers of interworking QKDNs are recommended to share key management information between QKDNs.

NOTE - Information on key management may include information such as which KM the key is transferred to, timestamp, the cryptographic application to which the key is supplied, shared key number of a KM link, key consumption rate, KM link status, accounting and alarm on fault.

7.2. Key management layer requirements for QKDNi with GWNs

Req_KM 5. The key management layers of interworking QKDNs are required to support key relays between GWNs.

NOTE - Secure key relay with OTP encryption between GWNs is defined in [ITU-T Y.3810].

7.3. Key management layer requirements for QKDNi with IWNs

Req_KM 6. The key management layers of interworking QKDNs are required to support key transfers in the IWN.

NOTE - Secure key transfer in the IWN is defined in [ITU-T Y.3810].

8. Functional requirements for QKDN control layer

8.1. QKDN control layer for QKDNi

Req_C 1. The QKDN control layers of interworking QKDNs are recommended to share QKDN control information between QKDNs.

NOTE - QKDN control information on QKDN control layer may include routing control information, session control information, authentication control information and quality of service (QoS) policy control information, etc.

Req_C 2. The QKDN control layers of interworking QKDNs are recommended to provide charging policy control between QKDNs.

Req_C 3. The QKDN control layers of interworking QKDNs are recommended to support access control to perform authentication.

NOTE - The authentication between QKDNs can be based on their certificates.

Req_C 4. The QKDN control layers of interworking QKDNs are recommended to exchange QKDN routing control information to support interworking route.

NOTE - QKDN routing control information may include QKD node addresses, KM IDs, key consumption rate, residual number of keys from the KMs, etc.

Req_C 5. The QKDN control layers of interworking QKDNs are recommended to work together to provide routing control for interworking.

8.2. QKDN control layer for QKDNi with GWNs

Req_C 6. The QKDN control layers of interworking QKDNs are recommended to provide session control to relay the key between GWNs.

NOTE – The session in GWN is the communicate to relay the key between QKDNs.

8.3. QKDN control layer for QKDNi with IWNs

Req_C 7. The QKDN control layers of interworking QKDNs are recommended to provide session control to transfer the key in the IWN.

NOTE - Keys can then be transferred between two KMs through Kxi' within the secure operational environment of the IWN, and an IWN might contain multiple KMs.

9. Functional requirements for QKDN management layer

NOTE - [ITU-T Y.3810] has defined that network topologies and technology are not usually disclosed to other QKDN providers even in interworking cases, and that interworking interfaces are strictly prohibited to transfer unauthorized information.

9.1. QKDN management layer for QKDNi

Req_M 1. The QKDN management layers of interworking QKDNs are recommended to provide configuration management to support:

- managing of resource provisioning between QKDNs;

Req_M 2. The QKDN management layers of interworking QKDNs are recommended to provide fault management to support:

- capabilities of monitoring, detecting, diagnosing between QKDNs;
- management of failure resolving policies, and interactions with relevant functional components for healing actions between QKDNs.

Req_M 3. The QKDN management layers of interworking QKDNs are recommended to provide accounting management to support:

- key supply services and their policies between QKDNs;
- costs determination of key usage between QKDNs.

Req_M 4. The QKDN management layers of interworking QKDNs are recommended to provide performance management to support:

- monitoring and analyzing the performance status of QKDNi;
- analyzing the QKDN performance information collected/received from QKDNi;
- quality of service (QoS) of key supply between QKDNs.

Req_M 5. The QKDN management layers of interworking QKDNs are recommended to provide security management to support:

- collecting/receiving security related management information between QKDNs;
- management of authentication and authorization between QKDNs;
- the key life cycle management between QKDNs.

Req_M 6. The QKDN management layers of interworking QKDNs can optionally share status information.

NOTE - Status information shared between QKDNs may include information such as QBER, key rate, QKD link status, etc.

Req_M 7. The QKDN management layers of interworking QKDNs are recommended to provide configuration management to support:

- routing and rerouting for interworking.

Req_M 8. The QKDN management layers of interworking QKDNs are recommended to provide fault management to support:

- routing and rerouting for interworking as needed in case of the faults.

10. Security consideration

In order to mitigate security threats and potential attacks, for example, issues of confidentiality, integrity, authenticity, non-repudiation, availability and traceability need to be addressed, and appropriate security and privacy protection schemes should be considered in the QKDN, the user network and interfaces between the two networks. Details are outside the scope of this Recommendation.

Bibliography

[b-ETSI GR QKD 007] ETSI GR 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.*

_____