Draft new Recommendation ITU-T Y.QKDN-rsrq

Requirements for quantum key distribution network resilience

Summary

For quantum key distribution networks (QKDN), Recommendation ITU-T Y.QKDN-rsrq specifies the general requirements for resilience, and separately specifies the supporting requirements for protection and recovery.

Keywords

Quantum key distribution (QKD); QKD network (QKDN); resilience; requirement; protection; recovery

Table of Contents

Draft new Recommendation ITU-T Y.QKDN-rsrq

Requirements for quantum key distribution network resilience

1. Scope

This recommendation specifies the general requirements for QKDN resilience, as well as the supporting requirements for protection and recovery.

In particular, the Recommendation covers:

- Introduction
- General requirements for QKDN resilience
- Requirements of protection to support resilience
- Requirements of recovery to support resilience

The appendix describes examples of resilience.

2. References

[ITU-T Y.3800] Recommendation ITU-T Y.3800 (2019), *Framework for Networks to support Quantum Key Distribution*.

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

[ITU-T Y.3802] Recommendation ITU-T Y.3802 (2020), *Functional architecture of the Quantum Key Distribution network*.

[ITU-T Y.3803] Recommendation ITU-T Y.3803 (2020), *Key management for quantum key distribution network*.

[ITU-T Y.3804] Recommendation ITU-T Y.3804 (2020), *Control and Management for Quantum Key Distribution Network*.

[ITU-T Y.~~QKDN-rsfr~~3815] Recommendation ITU-T Y.~~QKDN-rsfr~~3815 (2023~~1~~), *Quantum key distribution networks – overview of resilience.*

< Others to be added>

3. Terms and definitions

3.1. Terms defined elsewhere

This recommendation uses the following terms defined elsewhere:

3.1.1 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.

3.1.2 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.

3.1.3 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.

3.1.4 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 and the receivers.

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 user network [ITU-T Y.3800]: A network in which cryptographic applications consume keys supplied by a quantum key distribution (QKD) network.

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

3.1.8 key supply [ITU-T Y.3800]: A function providing keys to cryptographic applications.

3.1.9 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.

3.1.10 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.

3.1.11 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).

-TBD

3.2 Terms defined in this Recommendation

This chapter defines all the terms used in this recommendation.

-TBD

4 Abbreviations and acronyms

This chapters describes all the abbreviations and acronyms used in the recommendation.

QKD	Quantum Key Distribution
QKDN	Quantum Key Distribution Network
KM	Key Manager
QoS	Quality of Service

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 document is to be claimed.

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

The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Introduction

This Recommendation specifies the general requirements for QKDN resilience. Based on the models of protection and recovery identified in Y.3815, clauses 8 and 9 specify the requirements for protection and recovery to support resilience.

7 General requirements for QKDN resilience

7.1 Requirements for quantum layer to support resilience

Req_Qr 1 Additional QKD modules and links are recommended to be pre-set in advance to prevent the interruption of key supply caused by failures in working QKD modules and links.

7.2 Requirements for key management layer to support resilience

Req_KMr 1 ~~The~~ A KM is recommended to switch to the available key relay route allocated by control and management functions in case of failures of the working key relay route.

7.3 Requirements for control layer to support resilience

Req_Cr 1 ~~The~~ A QKDN controller is recommended to provide resilience-oriented routing control of key relay.

NOTE 1 – In some cases, multiple key relay routes may be allocated for resilience.

Req_Cr 2 ~~The~~ A QKDN controller is recommended to provide resilience-oriented charging policy control.

Req_Cr 3 ~~The~~ A QKDN controller is recommended to provide resilience-oriented session control.

Req_Cr 4 ~~The~~ A QKDN controller is recommended to provide resilience information to a QKDN manager.

7.4 Requirements for management layer to support resilience

Req_Mr 1 ~~The~~ A QKDN manager is recommended to provide resilience management to support:

– collecting/receiving status information of resilience-oriented functional components;

– management of resilience policies, and interactions with relevant functional components for resilience actions.

8 Requirements of protection to support resilience

Req_P 1. Protection QKD links are recommended to be pre-set for protection of key supply;

Req_P 2. Protection QKD modules are recommended to be pre-set for protection of key supply;

Req_P 3. A protection QKD module is required to be contained within the defined cryptographic boundary along with the working QKD module;

Req_P 4. A protection QKD module is recommended to support the same QKD protocol as the working QKD module;

Req_P 5. A protection QKD link is recommended to provide equivalent QKD capability as the protected QKD link(s);

Req_P 6. A protection QKD link is recommended to be deployed in separate optical fiber from the working QKD link;

Req_P 7. A protection QKD module /link is recommended to be pre-configured, and automatically switch to the protection QKD module /link in case of failures of the working QKD module /link;

Req_P 8. A KM is recommended to switch to the protection key relay route(s) for seamless key supply in case of failures of the working key relay route(s);

Req_P 9. A protection key relay route is recommended to provide equivalent capability for KSA-key delivery as the protected key relay route(s);

Req_P 10. A QKDN controller is recommended to allocate protection key relay route to enable seamless key supply under failures;

Req_P 11. A QKDN controller is recommended to provide updated fault, performance, accounting, and configuration information to a QKDN manager after protection switching;

Req_P 12. A QKDN manager is required to record the correspondence between working QKD modules /links /key relay routes, and their respective protection QKD modules /links /key relay routes;

Req_P 13. A QKDN manager is recommended to establish and maintain protection-oriented network topology and resource information to support routing calculation for protection switching;

Req_P 14. A QKDN manager is recommended to record logs for protection switching related events to support post-event analysis;

Req_P 15. A QKDN is required to support coordinated protection switching across quantum layer and key management layer, over QKD modules, QKD links, and key relay routes.

9 Requirements of recovery to support resilience

~~9.1 Requirements of recovery in quantum layer~~

~~TBD~~

~~9.2 Requirements of recovery in key management layer~~

~~TBD~~

~~9.3 Requirements of recovery in control layer~~

~~*Req_R 1. A QKDN controller can optionally enable multiple key relay routes for recovery of key supply;*~~

~~*Req_R 2. A QKDN controller is recommended to search for the key relay route for recovery within the toleration time of the cryptographic application.*~~
~~TBD~~

~~9.4 Requirements of recovery in management layer~~

~~*Req_M-R 1.A QKDN manager is required to record the operations for recovery to update the status of key relay routes.*~~

Req_R 1. A KM is recommended to balance key supply rates between working and recovery key relay routes according to QoS considerations and security requirements of cryptographic applications;

Req_R 2. A KM is recommended to ensure seamless key supply to cryptographic applications when switching key supply to a key relay route for recovery;

Req_R 3. A QKDN controller is recommended to dynamically recalculate and establish key relay routes to recover interrupted key supply based on network conditions;

Req_R 4. A QKDN controller can optionally enable multiple key relay routes for recovery of key supply;

Req_R 5. A QKDN controller is recommended to recalculate the key relay route for recovery within the toleration time of the cryptographic application;

Req_R 6. A QKDN manager is required to record the operations for recovery to update the status of key relay routes;

Req_R 7. A QKDN manager is recommended to retain diagnostic information and records related to alarms for the purpose of analyzing the root cause of disruptions in key relay routes that trigger recovery.

~~TBD~~

Formatted: Not Highlight

Appendix I

Examples of QKDN resilience

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

The continuous key supply under failures is important in QKDN. With functional requirements and architecture specified in Y.3800 to 3804, the QKDN resilience can be supported by protection and recovery. Figures 1-3 show several examples of protection and recovery as well as corresponding operations.

I.1 Example of protection in QKDN

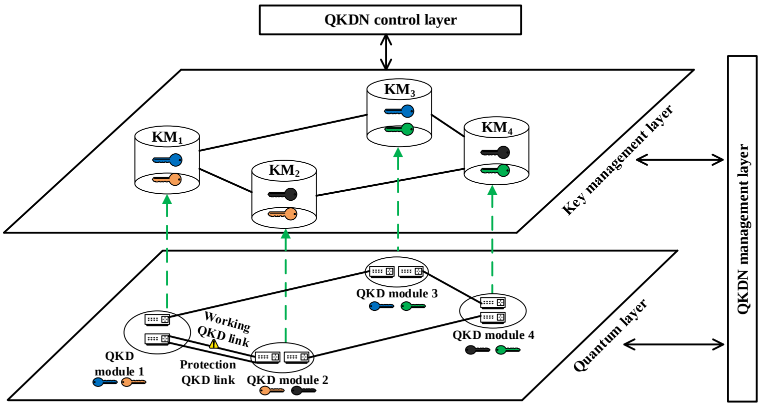

Figure 1 – Example 1.1 for QKDN resilience with protection of QKD-key supply

Example 1.1) To avoid the interruption of QKD caused by the failure in QKD link 1-2, an additional QKD link can be pre-set as protection QKD link. When the failure occurs, the working QKD link can be replaced by the protection QKD link through optical switching.

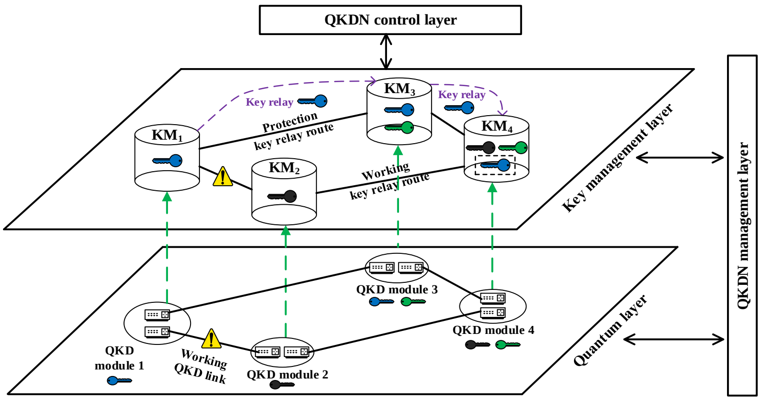

Figure 2 – Example 1.2 for QKDN resilience with protection of KSA-key supply

Example 1.2) The KMs over key relay route 1-2-4 through QKD modules 1, 2 and 4 supply keys to cryptographic application A. To avoid the interruption of QKD caused by the failure in QKD link 1-2 or 2-4, an alternative key relay route 1-3-4 (i.e., the key relay route goes through QKD modules 1, 3 and 4) is pre-set, which is available to other cryptographic applications when there are no failures. When the key relay route 1-2-4 is impaired, leading to the interruption of KSA-key supply, protection is enabled for application A. The key relay route 1-2-4 switches to the key relay route 1-3-4, and the KM initiates the key supply for cryptographic application A with the keys over key relay route 1-3-4.

I.2 Examples of recovery in QKDN

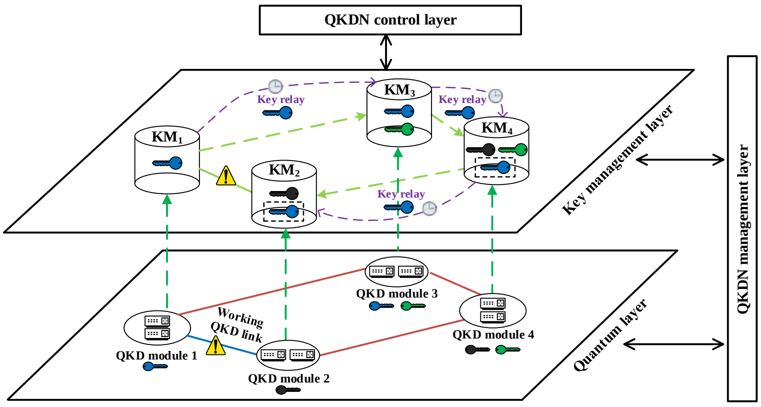

Figure 3 – Example 2.1 for QKDN resilience with recovery

Example 2.1) The KM over working QKD link between QKD module 1 and QKD module 2 supplies keys to cryptographic application A. If the working QKD link 1-2 is impaired, the related QKD process could be interrupted. For the recovery of single failure, a re-routing key relay route will be searched for synchronized keys to recover the impaired key supply of application A, i.e., the key relay route which goes through KM 1, 3, 4, and 2. The time delay and other overheads caused by recovery should be considered.

Bibliography

TBD