INTERNATIONAL TELECOMMUNICATION UNION
**TELECOMMUNICATION STANDARDIZATION SECTOR**
STUDY PERIOD 2022-2024

**SG13-TD309/WP3**
**STUDY GROUP 13**
**Original: English**

**Question(s):** 16/13 Geneva, 26 July 2023

**TD**

**Source:** Editors

**Title:** Draft Recommendation ITU-T Y.QKDN-rsrq "Requirements for quantum key distribution network resilience" (output of interim meeting, 17 - 21 July 2023)

**Contact:** Xiaosong Yu
Beijing University of Posts and Telecommunications.
China
Tel: +86-10-61198108
E-mail:xiaosongyu@bupt.edu.cn

**Contact:** Yuhang Liu
Beijing University of Posts and Telecommunications.
China
Tel: +86-15998440173
E-mail:yuhangliu@bupt.edu.cn

**Contact:** Yongli Zhao
Beijing University of Posts and Telecommunications.
China
Tel: +86-10-61198108
E-mail:yonglizhao@bupt.edu.cn

**Contact:** Zhangchao Ma
University of Science and Technology Beijing (USTB)
China
Tel: +86-10-62332374
E-mail:mazhangchao@ustb.edu.cn

**Contact:** Junsen Lai
CAICT, Ministry of Industry and Information Technology (MIIT)
China
Tel: +86-10-62300592
E-mail: laijunsen@caict.ac.cn

**Abstract:** This TD includes the draft output of Recommendation ITU-T Y.QKDN-rsrq "Requirements for quantum key distribution network resilience" (output of Q16/13 meeting, 17 - 21 July 2023).

**Summary**

This TD is the output document for draft Recommendation ITU-T Y.QKDN-rsrq "Requirements for quantum key distribution network resilience" based on the following input contribution and the discussion during the Q16/13 meeting, 17 - 21 July 2023.

| | | | |
|---|---|---|---|
| C-136 | BUPT, MIIT | Y.QKDN-rsrq "Requirements for quantum key distribution network resilience": Proposed updates for general requirements. | Q16/13 |

- Proposal of contribution

- This proposal includes the updates to draft Recommendation ITU-T Y.QKDN-rsrq "Requirements for quantum key distribution network resilience".

- Meeting result

- The proposal is accepted. The meeting also raised the comment that the requirements can be formulated according to specific resilience mechanism from the perspective of overall QKDN.
- The meeting raised the comment that some of the proposed requirements are not general, which should be clarified.

**Attachments:**

**Annex I:** Draft Recommendation ITU-T Y.QKDN-rsrq "Requirements for quantum key distribution network resilience" (output of Q16/13, 17 - 21 July 2023)

**Annex I:**

## Draft 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

1. Scope ..... 5
2. References ..... 5
3. Terms and definitions ..... 5
3.1. Terms defined elsewhere ..... 5
3.2 Terms defined in this Recommendation ..... 6
4 Abbreviations and acronyms ..... 6
5 Conventions ..... 6
6 Introduction ..... 7
7 General requirements for QKDN resilience ..... 7
8 Requirements of protection to support resilience ..... 7
9 Requirements of recovery to support resilience ..... 9

# Draft 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] Recommendation ITU-T Y.QKDN-rsfr (2021), *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

## 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

*Editor's note: some of the requirements are limited to the specific use cases, which are not general and should be clarified.*

~~7~~

### 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.

Req_Qr 2 The QKD module for resilience is required to be contained within the defined cryptographic boundary along with the working QKD module.

Req_Qr 3 The QKD module for resilience is recommended to implement functions that are necessary for executing the same QKD protocol as the working QKD module.

~~1~~Req_Qr 4 The QKD link for resilience is recommended to be deployed in separated optical fiber from the working QKD link.

~~TBD~~

### 7.2 Requirements for key management layer to support resilience

Req_KMr 1 The KM~~s~~ is ~~are~~ recommended to switch to the available key relay route allocated by control and management functions when failures occurred in working key relay route.

~~Req_KMr 1~~

~~TBD~~

### 7.3 Requirements for control layer to support resilience

Req_Cr 1 The 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 QKDN controller is recommended to provide resilience-oriented charging policy control.

~~Req_M 1 A QKDN controller is recommended to pre-set additional key relay route in advance to support seamless key supply under failures.~~The QKDN controller is recommended to provide resilience-oriented session control.

Req_Cr 3

**Formatted:** English (United States)
**Formatted:** English (United States)
**Formatted:** Normal, Justified, No bullets or numbering
**Formatted:** English (United States)
**Formatted:** English (United States)
**Formatted:** Font: Not Italic
**Formatted:** Space Before: 3 pt, Add space between paragraphs of the same style, Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0 cm + Indent at: 0 cm
**Formatted:** Font: English (United Kingdom)
**Formatted:** Font: English (United Kingdom)
**Formatted:** Font: English (United Kingdom)
**Formatted:** Font: Not Italic, (Asian) Chinese (Simplified, Mainland China)
**Formatted:** Font: Not Italic
**Formatted:** Font: Not Italic
**Formatted:** Space Before: 3 pt, Add space between paragraphs of the same style, Outline numbered + Level: 4 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0 cm + Indent at: 0 cm
**Formatted:** Font: Not Italic, Highlight
**Formatted:** Space Before: 3 pt, Add space between paragraphs of the same style, Outline numbered + Level: 4 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0 cm + Indent at: 0 cm
**Formatted:** Space Before: 3 pt, No bullets or numbering
**Formatted:** Space Before: 3 pt, Add space between paragraphs of the same style, Outline numbered + Level: 4 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0 cm + Indent at: 0 cm
**Formatted:** Font: Not Italic

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

~~TBD~~

### 7.4 Requirements for management layer to support resilience

~~*Req_C-P 1* A QKDN manager is required to record and update the status of QKD modules and links that pre-set for resilience;~~

Req_Mr 1 ~~A QKDN manager is required to monitor the status of key supply and respond to the failures.~~The 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.

~~*Req_M 2*~~

~~TBD~~

## 8 Requirements of protection to support resilience

*Editor's note: the requirements should be further identified as work progresses.*

### 8.1 Requirements of protection in quantum layer

*Req_Q-P 1. Additional QKD links are recommended to be pre-set as the protection QKD links for protection of key supply;*

*Req_Q-P 2. Additional QKD modules are recommended to be pre-set as the protection QKD modules for protection of key supply;*

*Req_Q-P 3. A protection QKD link is recommended to have an equivalent QKD ability with the QKD protected link(s).*

TBD

### 8.2 Requirements of protection in key management layer

*Req_KM-P 1. When failure occurs, the KMs are recommended to switch to the protection key relay route(s) for continuous key supply.*

TBD

### 8.3 Requirements of protection in control layer

~~*Req_C-P 2*~~*Req_C-P 1 A QKDN controller is recommended to allocate protection key relay route to enable seamless key supply under failures.*

TBD

### 8.4 Requirements of protection in management layer

*Req_M-P 1. A QKDN manager is required to record the matchup between working QKD modules and protection QKD modules;*

*Req_M-P 2. A QKDN manager is required to record the matchup between working QKD links and protection QKD links.*

TBD

**Formatted:** Font: Not Italic

**Formatted:** Add space between paragraphs of the same style, Outline numbered + Level: 4 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0 cm + Indent at: 0 cm, Allow hanging punctuation, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers, Font Alignment: Auto, Tab stops: Not at 1.4 cm + 2.1 cm + 2.8 cm + 3.5 cm

**Formatted:** Font: Not Italic

**Formatted:** Space Before: 3 pt, Add space between paragraphs of the same style, Outline numbered + Level: 4 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0 cm + Indent at: 0 cm

**Formatted:** Space Before: 3 pt, Add space between paragraphs of the same style, Outline numbered + Level: 4 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0 cm + Indent at: 0 cm

**Formatted:** Font:

**Formatted:** Normal, Space Before: 3 pt

**Formatted:** Font: (Asian) Japanese, (Other) English (United Kingdom)

**Formatted:** Space Before: 3 pt, No bullets or numbering

**Formatted:** Font: (Asian) Japanese

**Formatted:** Font: Not Italic, (Asian) Japanese, (Other) English (United Kingdom)

# 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_C-R 1. A QKDN controller can optionally enable multiple key relay routes for recovery of key supply;*

*Req_C-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.*

TBD

# 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

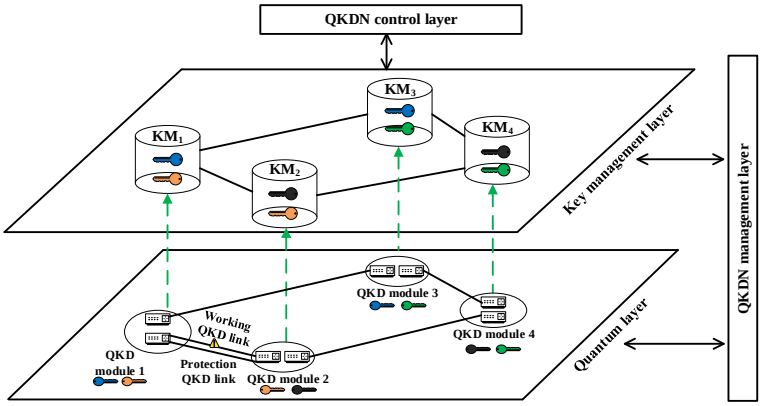


Figure 1 – Example 1.1 for QKDN resilience with protection of QKD-key supply

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.

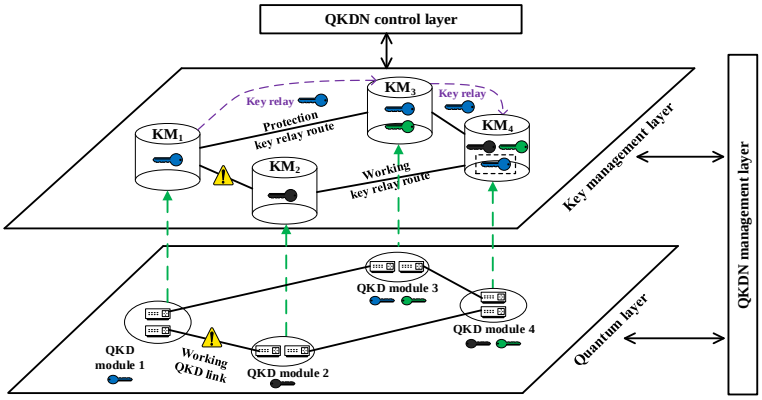


Figure 2 – Example 1.2 for QKDN resilience with protection of KSA-key supply

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

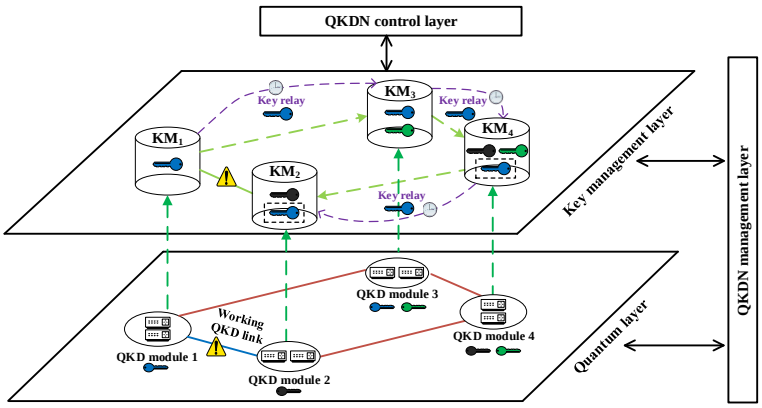


Figure 3 – Example 2.1 for QKDN resilience with recovery

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