INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2022-2024

SG13-TD301/WP3

STUDY GROUP 13

Original: English

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

TD

Source: Editors

Title: Draft new Recommendation ITU-T Y.3815 (formerly Y.QKDN-rsfr) "Quantum key distribution networks – overview of resilience" - for consent

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

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

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

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

Abstract: This TD includes the draft output of Recommendation ITU-T Y.QKDN-rsfr "Quantum key distribution networks – overview of resilience" for consent.

Summary

This TD is the output document for draft Recommendation ITU-T Y.QKDN-rsfr "Quantum key distribution networks – overview of resilience" based on the following input contribution and the discussion during the Q16/13 meeting, 17 - 21 July 2023.

C-125	BUPT, USTB	Draft Recommendation ITU-T Y.QKDN-rsfr "Quantum key distribution networks – overview of resilience" (for consent)	Q16/13

- Proposal of contribution

– This document includes the draft of Recommendation ITU-T Y.QKDN-rsfr "Quantum key distribution networks – overview of resilience" for consent.

- Meeting result

– The meeting raised the comment that the key words regarding "QKDN resilience" and "QKDN recovery" needs some explanation in the main text.

- The meeting raised the comment that the colors and arrows in the diagrams should be unified.

Attachments:

Annex I: Draft Recommendation ITU-T Y.QKDN-rsfr "Quantum key distribution networks – overview of resilience" (output of Q16/13, 17 - 21 July 2023)

Annex I:

Draft Recommendation ITU-T Y.3815 (formerly Y.QKDN-rsfr)

Quantum key distribution networks – overview of resilience

Summary

For seamless key supply even in the case of network failures, this Recommendation describes an overview of resilience and conceptual models of protection and recovery for Quantum key distribution network (QKDN).

Keywords

Quantum key distribution (QKD); QKD network (QKDN); resilience; overview; conceptual model.

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 6

7 Protection of key supply in QKDN 7

7.1 Protection in quantum layer 8

7.2 Protection in key management layer 10

8 Recovery of key supply in QKDN 10

Draft Recommendation ITU-T Y.3815 (formerly Y.QKDN-rsfr)

Quantum key distribution networks – overview of resilience

1. Scope

This Recommendation describes an overview of resilience and the conceptual models of protection and recovery for Quantum key distribution network (QKDN).

In particular, the Recommendation includes:

- Introduction;
- Protection of key supply in QKDN;
- Recovery of key supply in QKDN.

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), *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.*

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-key (QKD-key) [ITU-T Y.3802]: A pair of symmetric random bit strings generated by a pair of quantum key distribution (QKD) modules, particularly referring to random bit strings before being resized and formatted in a key manager (KM).

3.1.5 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.

3.1.6 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.

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

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

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

3.1.10 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.

3.1.11 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.

3.1.12 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).

3.1.13 key supply agent-key (KSA-key) [ITU-T Y.3803]: Key data stored and processed in a key supply agent (KSA), and securely shared between a KSA and a matching KSA.

3.2. **Terms defined in this Recommendation**

None.

4 Abbreviations and acronyms

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

QKD	Quantum Key Distribution
QKDN	QKD Network
KM	Key Manager
KSA	Key Supply Agent

5 Conventions

None.

6 Introduction

The capability against failures, be commonly referred to as resilience, is of positive significance for the construction of QKDN as described in [ITU-T Y.3800]. Resilience for QKDN, called “QKDN resilience” in this document, is the ability to provide and maintain an acceptable service level in the face of failures based on prepared facilities, which can be supported by protection and recovery of key supply in QKDN, thereby maintaining the seamless key supply even in the case of network failures. This Recommendation describes an overview of resilience in QKDN, mainly from the aspects of protection and recovery of key supply, which is supported by functions specified in [ITU-T Y.3801-3804].

NOTE 1 – Beyond protection/recovery specified in this Recommendation, there are other options to support resilience.

Providing the seamless key supply for user network is important. Different kinds of failures in QKDN can affect or even interrupt the key supply. This Recommendation describes how to protect the QKDN from key supply interruption and how to recover the key supply. For example, if the communication on quantum channels is interrupted for reasons such as optical fibre cut, interruption of key supply can occur. Thus, this Recommendation describes an overview of resilience in QKDN to support the seamless key supply even in the case of network failures.

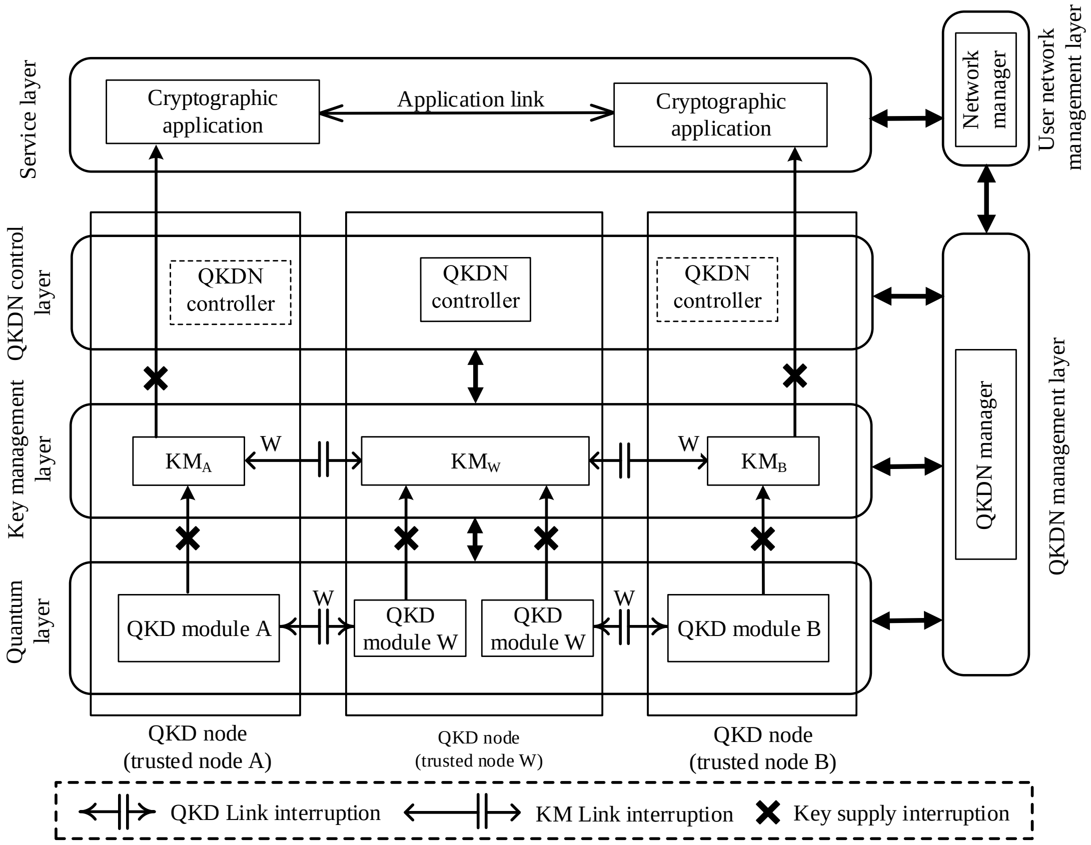

Figure 1 – Illustration of key-supply failures in QKDN

As shown in Fig. 1, the key supply to the cryptographic applications can be interrupted by potential failures occurring in either the key management layer or the quantum layer. This Recommendation considers the following conceptual models of QKDN resilience.

1) QKDN resilience supported by protection of key supply;

2) QKDN resilience supported by recovery of key supply;

7 Protection of key supply in QKDN

Protection of key supply in QKDN aims to provide additional QKD modules /QKD links /key relay routes for stable key supply, such as the allocation of backup resources before the failure occurs. Functional enhancement could be supported in QKDN. In this Recommendation, protection of QKD-key supply and KSA-key supply are described to support resilience. These protection methods could support the prevention of potential key supply interruptions. And the following terms represent the status of QKD modules, QKD links and key relay routes in quantum layer and key management layer for protection.

- Working (W) QKD module /QKD link /key relay route: a QKD module /QKD link /key relay route that normally works for key supply.
- Protection (P) QKD module /QKD link /key relay route: an alternative QKD module /QKD link /key relay route that pre-set for protection.
- Protected QKD module /QKD link /key relay route: a working QKD module /QKD link /key relay route that matched with a protection QKD module /QKD link /key relay route. When the failure occurs on the protected QKD module /QKD link /key relay route, it would be replaced with the protection QKD module /QKD link /key relay route.

7.1 Protection in quantum layer

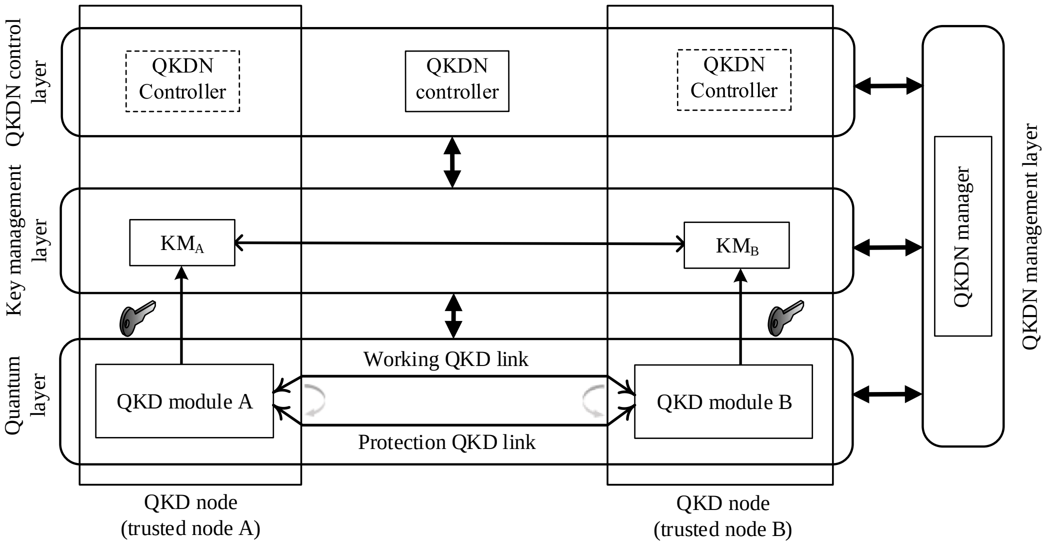

Figure 2 – A conceptual model of protection of QKD link for QKD-key supply in quantum layer

As shown in Fig. 2, a conceptual model of protection of QKD link in quantum layer is provided. The protection QKD link can be pre-set to support resilience. When failure occurs on the working QKD link, the protection QKD link can be enabled for seamless QKD-key supply.

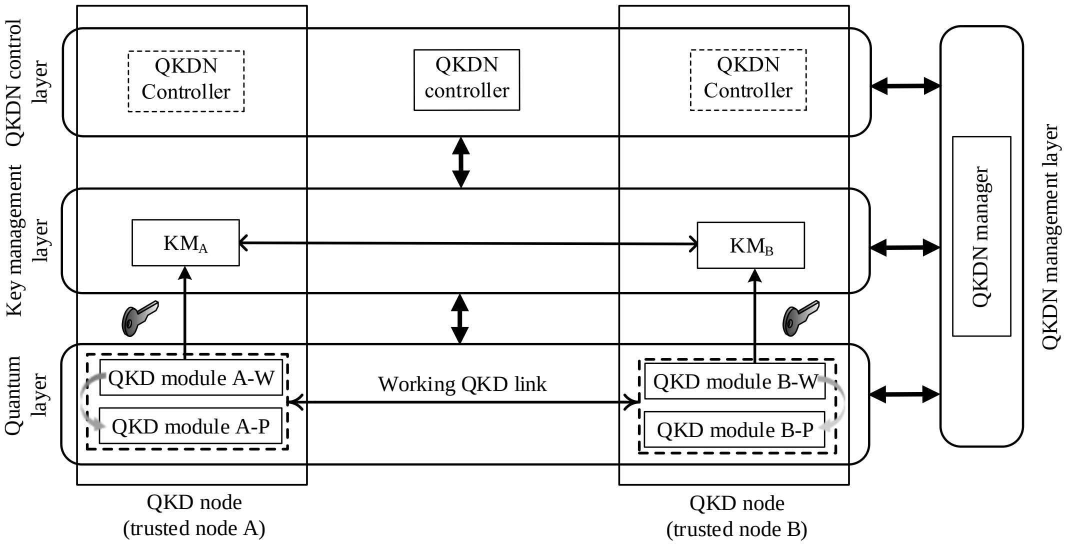

Figure 3 – A conceptual model of protection of QKD modules for QKD-key supply in quantum layer

As shown in Fig. 3, a conceptual model of protection of QKD modules in quantum layer is provided. The protection QKD modules can also be pre-set in QKD nodes to support resilience. When failure occurs on the working QKD module, the protection QKD module can be enabled for seamless QKD-key supply.

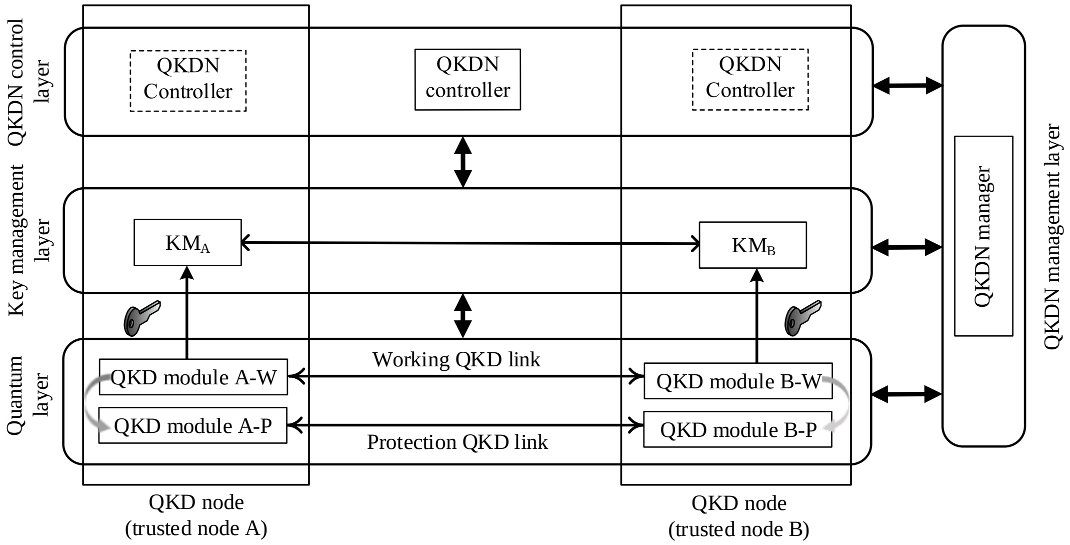

Figure 4 – A conceptual model of protection of both QKD modules and QKD link for QKD-key supply in quantum layer

As shown in Fig. 4, a conceptual model of higher-level protection of both QKD modules and QKD link in quantum layer is provided. Protection QKD link and modules can both be pre-set to support resilience.

NOTE 1 – Generally, a working QKD link refers to the link between a pair of QKD modules for QKD-key supply. To support QKDN resilience, the QKDN controller can enable multiple QKD modules and links for simultaneous key supply.

NOTE 2 – The protection QKD link can be enabled through optical switching /splitting functions with available QKD modules.

NOTE 3 – The interruption of QKD can be caused by failures in QKD modules /QKD links, including QBER increase, key generation interruption, etc. The occurrence of these failures can be monitored through control and management functions in quantum layer.

7.2 Protection in key management layer

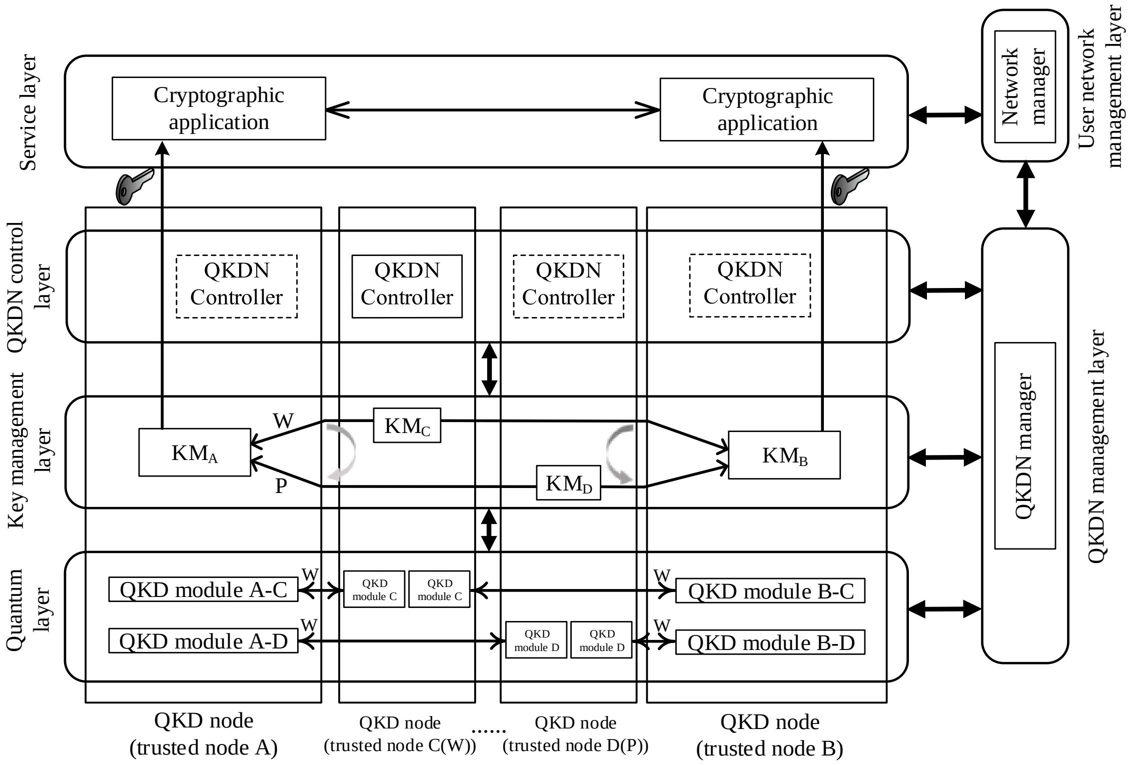

Figure 5 – A conceptual model of protection in key management layer

In key management layer, a protection key relay route can be pre-set, which can be enabled to support seamless key supply for the interrupted working key relay route.

As shown in Fig. 5, a conceptual model of protection in key management layer is provided. A key relay route A-D-B is pre-set for protection of key relay route A-C-B, while the key supply over QKD links A-D and D-B is normal for key relay route A-D-B. When the key relay route A-C-B is interrupted, it can switch to the key supply of key relay route A-D-B when A-D-B is available with enough keys.

NOTE 4 – To support QKDN resilience with protection, relevant key-supply interruption and switching overheads should be taken into consideration.

8 Recovery of key supply in QKDN

Recovery of key supply in QKDN aims to recover the interrupted key supply through control and management functions. Functional enhancement could be supported in QKDN control layer and management layer. Specifically, QKDN provides the function of re-routing for recovery as shown in Fig. 6. The mechanism of re-routing for key relay route is similar to the case of protection in key management layer as shown in Fig. 5. The difference is that the key relay route for protection is pre-set, while the key relay route for recovery can be automatically calculated.

- Key relay route for recovery (R): a new key relay route allocated by control and management functions to support key supply when impairment occurs to the working key relay route.

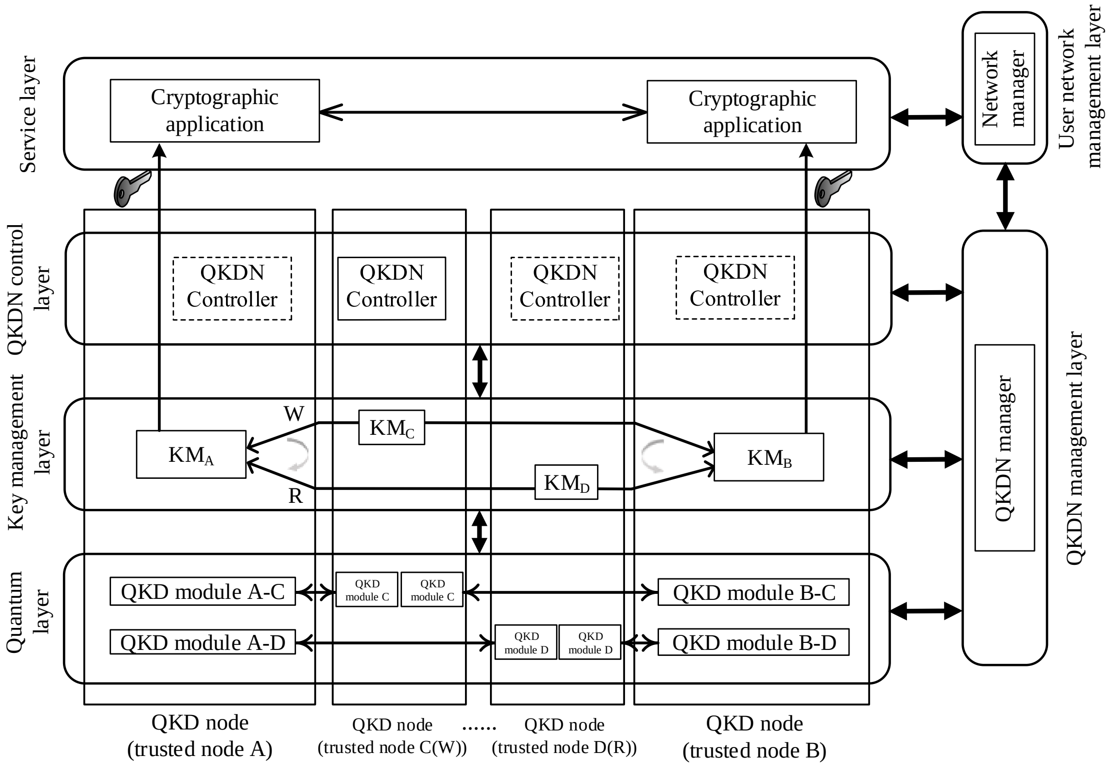

Figure 6 – A conceptual model of re-routing for QKDN resilience

When there occurs the key-supply failure in QKDN, recovery tries to support the key supply through control and management functions. In key management layer, it can replace the impaired key relay route with other available key relay routes. As a result, the interrupted key supply to cryptographic application can be recovered. Based on the scale of key-supply failure(s), the overheads for recovery can be different.

NOTE 5 – To support QKDN resilience with recovery, the overhead including time delay with re-routing should be taken into consideration.