ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T Y.3815 (09/2023)

SERIES Y: Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities

Quantum key distribution networks

Quantum key distribution networks – Overview of resilience

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	Y.100-Y.999
General	Y.100-Y.199
Services, applications and middleware	Y.200-Y.299
Network aspects	Y.300-Y.399
Interfaces and protocols	Y.400-Y.499
Numbering, addressing and naming	Y.500-Y.599
Operation, administration and maintenance	Y.600-Y.699
Security	Y.700-Y.799
Performances	Y.800-Y.899
INTERNET PROTOCOL ASPECTS	Y.1000-Y.1999
General	Y.1000-Y.1099
Services and applications	Y.1100-Y.1199
Architecture, access, network capabilities and resource management	Y.1200-Y.1299
Transport	Y.1300-Y.1399
Interworking	Y.1400-Y.1499
Quality of service and network performance	Y.1500-Y.1599
Signalling	Y.1600-Y.1699
Operation, administration and maintenance	Y.1700-Y.1799
Charging	Y.1800-Y.1899
IPTV over NGN	Y.1900-Y.1999
NEXT GENERATION NETWORKS	Y.2000-Y.2999
Frameworks and functional architecture models	Y.2000-Y.2099
Quality of Service and performance	Y.2100-Y.2199
Service aspects: Service capabilities and service architecture	Y.2200-Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250-Y.2299
Enhancements to NGN	Y.2300-Y.2399
Network management	Y.2400-Y.2499
Computing power networks	Y.2500-Y.2599
Packet-based Networks	Y.2600-Y.2699
Security	Y.2700-Y.2799
Generalized mobility	Y.2800-Y.2899
Carrier grade open environment	Y.2900-Y.2999
FUTURE NETWORKS	Y.3000-Y.3499
CLOUD COMPUTING	Y.3500-Y.3599
BIG DATA	Y.3600-Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	**Y.3800-Y.3999**
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	Y.4000-Y.4999
General	Y.4000-Y.4049
Definitions and terminologies	Y.4050-Y.4099
Requirements and use cases	Y.4100-Y.4249
Infrastructure, connectivity and networks	Y.4250-Y.4399
Frameworks, architectures and protocols	Y.4400-Y.4549
Services, applications, computation and data processing	Y.4550-Y.4699
Management, control and performance	Y.4700-Y.4799
Identification and security	Y.4800-Y.4899
Evaluation and assessment	Y.4900-Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.3815

Quantum key distribution networks – Overview of resilience

Summary

Recommendation ITU-T Y.3815 gives an overview of resilience and conceptual models of protection and recovery for quantum key distribution networks for seamless key supply even in the case of network failure.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T Y.3815	2023-09-29	13	11.1002/1000/15643

Keywords

Conceptual model, overview, QKD network (QKDN), quantum key distribution (QKD), resilience.

* To access the Recommendation, type the URL https://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

© ITU 2023

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

Recommendation ITU-T Y.3815

Quantum key distribution networks – Overview of resilience

1 Scope

This Recommendation gives an overview of resilience and the conceptual models of protection and recovery for quantum key distribution networks (QKDNs).

This Recommendation includes the following:

– an introduction to resilience in QKDNs;

– protection of key supply in QKDNs;

– recovery of key supply in QKDNs.

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), *Overview on networks supporting 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), *Quantum key distribution networks – Functional architecture*.

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

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

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

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

3.1.4 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.

3.1.5 quantum key distribution [b-ETSI GR QKD 007]: Procedure or method for generating and distributing symmetrical cryptographic keys with information theoretical security based on quantum information theory.

3.1.6 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).

3.1.7 quantum key distribution 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.

3.1.8 quantum key distribution 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).

3.1.9 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.

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

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

KM Key Manager

KML Key Management Layer

KSA Key Supply Agent

QKD Quantum Key Distribution

QKDN Quantum Key Distribution Network

QL Quantum Layer

5 Conventions

None.

6 Introduction

The capability against failures, 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 Recommendation, 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 seamless key supply even in the case of network failures. This Recommendation gives 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], [ITU-T Y.3802], [ITU-T Y.3803] and [ITU-T Y.3804].

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

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

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

1) protection of key supply;

2) recovery of key supply.

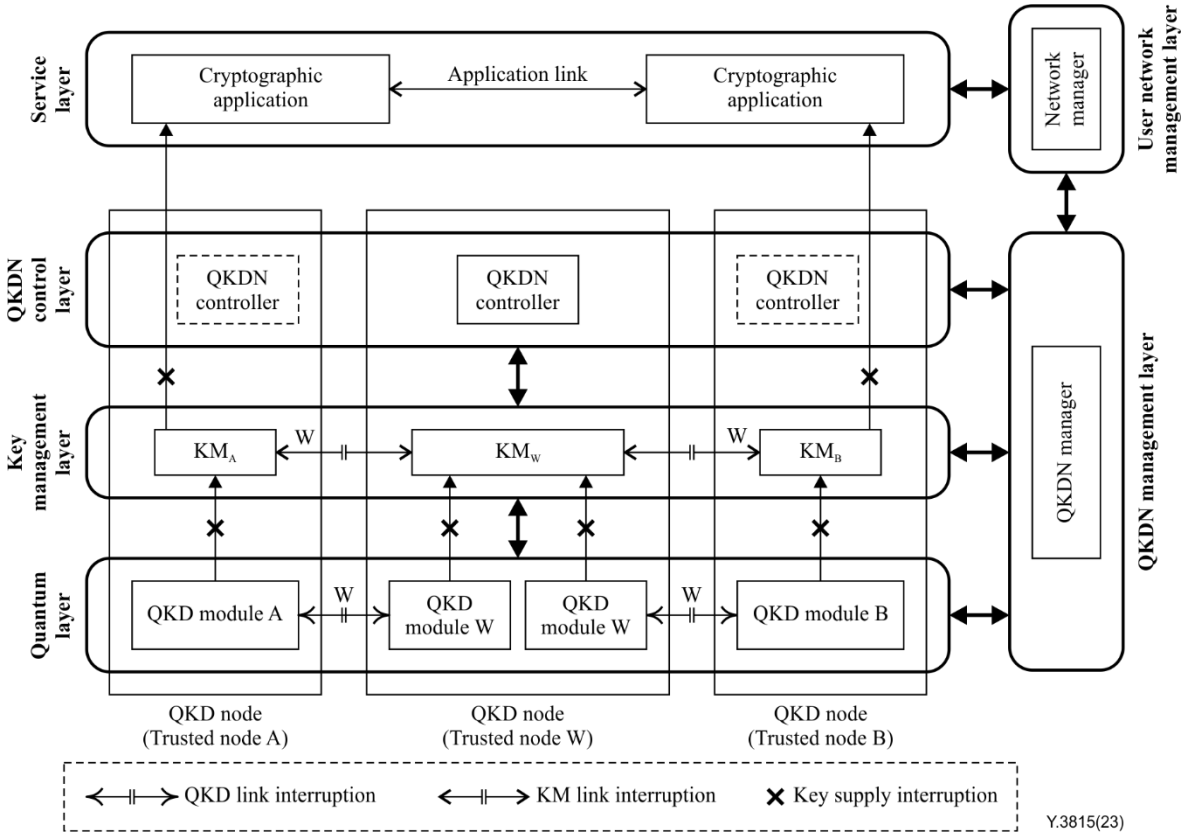

Figure 1 – Illustration of key supply failures in a QKDN

7 Protection of key supply in QKDN

Protection of key supply in QKDN aims to provide additional QKD modules, QKD links or key relay routes for stability, such as the allocation of backup resources before a failure occurs. Functional enhancement can be supported in QKDNs. In this Recommendation, protection of QKD-key supply and KSA-key supply are described to support resilience. These protection methods can support the prevention of potential key supply interruptions. In addition, the following terms represent the status of QKD modules, QKD links and key relay routes in the QL and KML for protection.

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

7.1 Protection in quantum layer

A conceptual model for protection of a QKD link in a QL is shown in Figure 2. The protection QKD link can be pre-set to support resilience. When a failure occurs in a working QKD link, the protection QKD link can be enabled for seamless QKD-key supply.

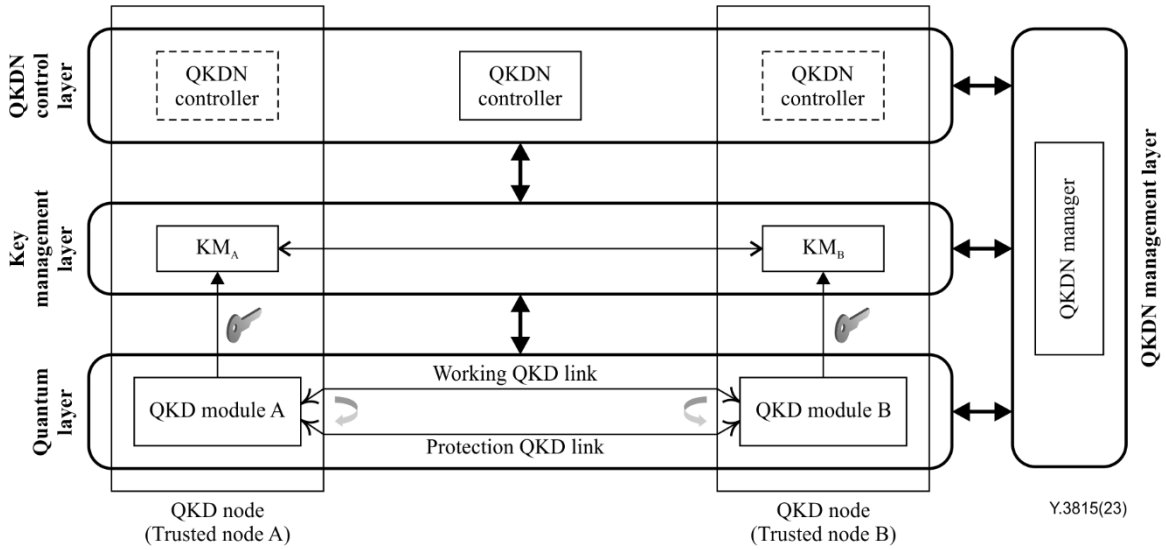

Figure 2 – A conceptual model of protection of QKD link for QKD-key supply in quantum layer

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

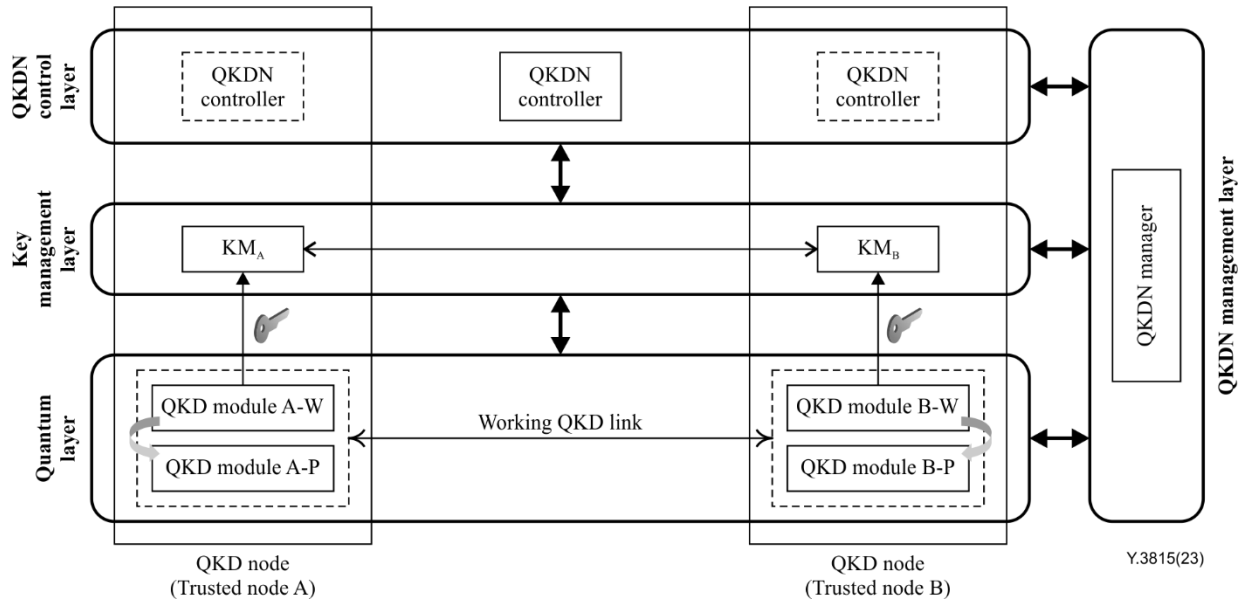

Figure 3 – A conceptual model of protection of QKD modules for QKD-key supply in quantum layer

A conceptual model for higher-level protection of both QKD modules and a QKD link in a QL is shown in Figure 4. Protection QKD link and modules can both be pre-set to support resilience.

NOTE 1 – Generally, a working QKD link is one 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 or splitting functions with available QKD modules.

NOTE 3 – The interruption of QKD can be caused by failures in QKD modules or QKD links, including an increase in quantum bit error rate or interruption in key generation. The occurrence of these failures can be monitored through control and management functions in a QL.

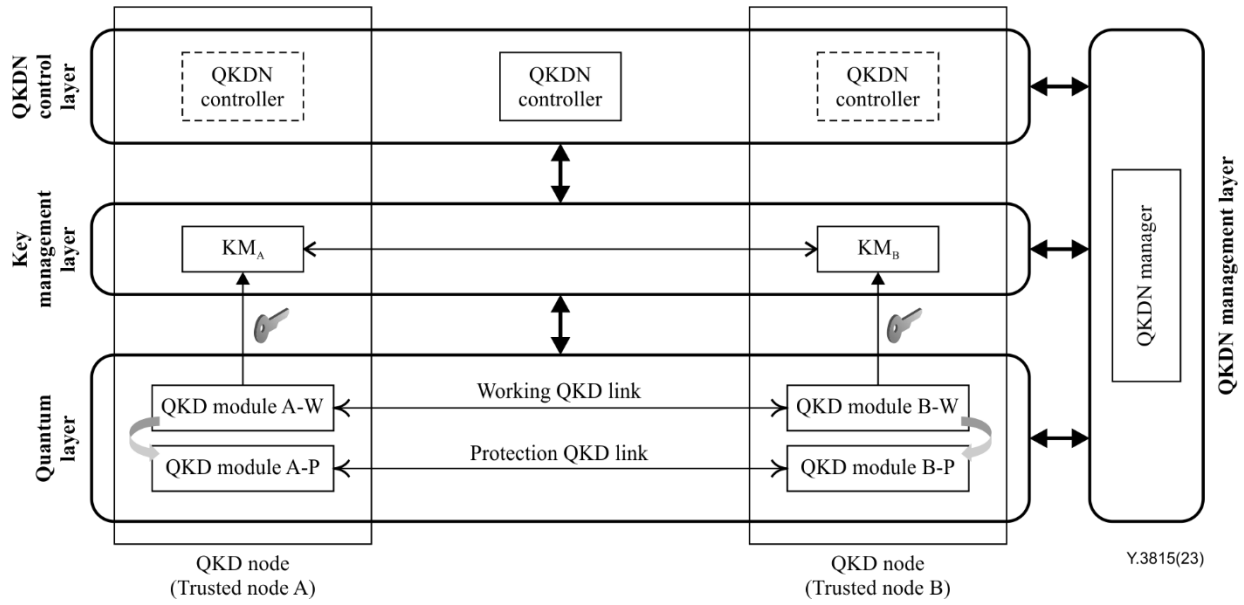

Figure 4 – A conceptual model of protection of both QKD modules and a QKD link for QKD-key supply in quantum layer

7.2 Protection in key management layer

In a KML, 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.

A conceptual model for protection in a KML is shown in Figure 5. 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.

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

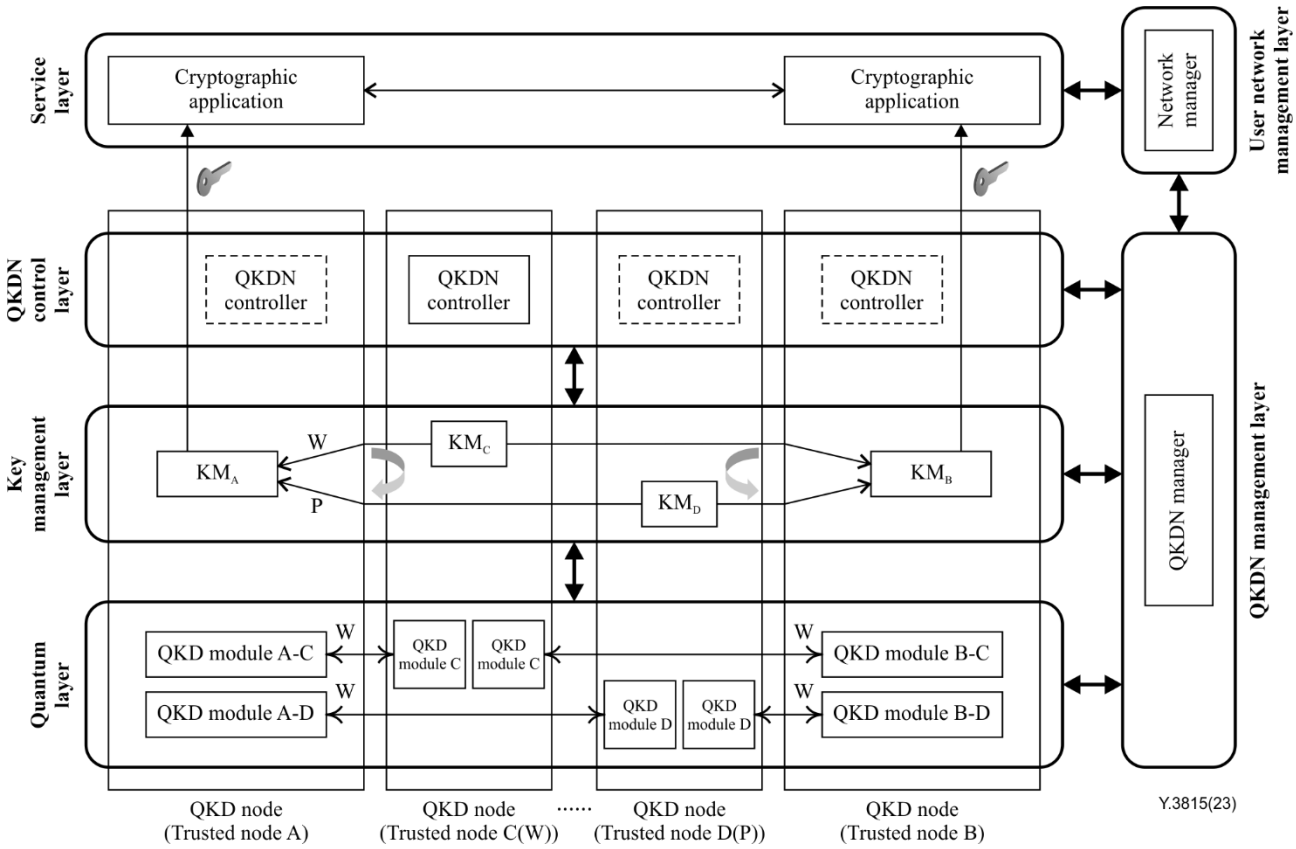

Figure 5 – A conceptual model of protection in key management layer

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 can be supported in a QKDN control layer and management layer. Specifically, a QKDN provides the function of re-routing for recovery as shown in Figure 6. The mechanism of re-routing for a key relay route is similar to the case of protection in a KML as shown in Figure 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.

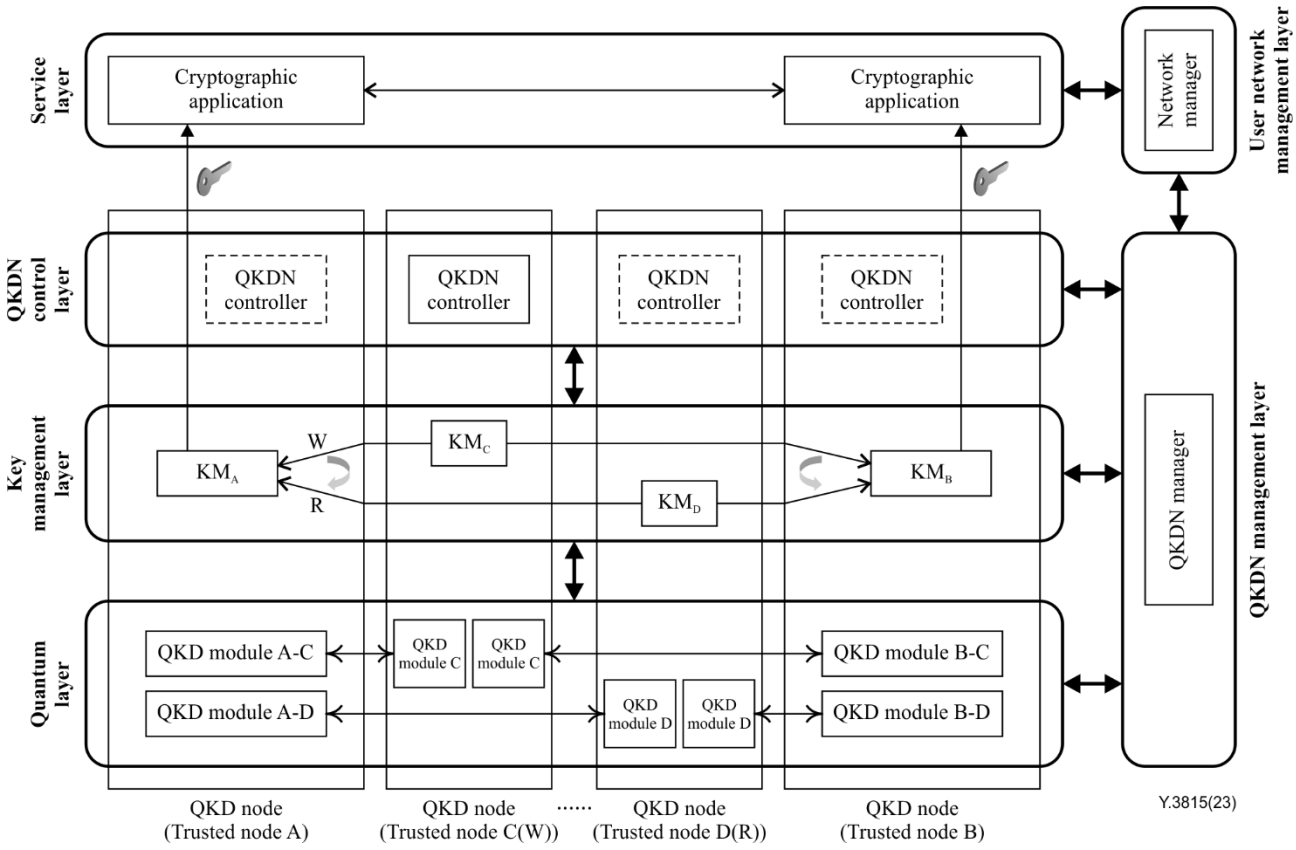

Figure 6 – A conceptual model of re-routing for QKDN resilience

When a key-supply failure occurs in a QKDN, recovery tries to support key supply through control and management functions. In a KML, it can replace the impaired key relay route by another that is available. As a result, the interrupted key supply to a cryptographic application can be recovered. Based on the scale of key-supply failure(s), the overheads for recovery can differ.

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

Bibliography

[b-ETSI GR QKD 007] Group Report ETSI GR QKD 007 V1.1.1 (2018), *Quantum key distribution (QKD); Vocabulary*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2023