Draft A.1 justification for a work item and proposed initial texts are attached as Annex A and B respectively.

Annex A

A.1 justification for proposed draft new Recommendation Y.QKDN_rsfr

Question:	16/13	**Proposed new ITU-T Recommendation**	E-Meeting, 5-16 July 2021
Reference and title:	ITU-T Y.QKDN_rsfr "Quantum key distribution networks - resilience framework"		
Base text:		**Timing:**	2022-12
Editor(s):	Xiaosong Yu, Yongli Zhao, Yuhang Liu, Zhangchao Ma	**Approval process:**	AAP

Scope (defines the intent or object of the Recommendation and the aspects covered, thereby indicating the limits of its applicability):

This recommendation describes the framework for resilience in QKDN.

In particular, the contribution includes:

- Overview of resilience in QKDN
- Roles of resilience in QKDN
- Requirements of quantum layer for resilience in QKDN
- Requirements of KM layer for resilience in QKDN
- Requirements of CM layer for resilience in QKDN
- Use cases of resilience scheme in QKDN

Summary (provides a brief overview of the purpose and contents of the Recommendation, thus permitting readers to judge its usefulness for their work):

Resilience is necessary to be introduced into QKDN to guarantee stable running of QKDN and the continuous key supply. Based on the functional requirements of QKDN in [ITU-T Y.3801] and functional architecture of QKDN in [ITU-T Y.3802], this recommendation is to specify the framework of resilience in QKDN including typical scenarios of resilience as well as requirements of resilience supported in quantum layer, key management layer, and control and management layer, respectively.

QKDN resilience use cases considered in this recommendation include network resources reservation, network resources recovery and alternative schemes such as re-routing.

Relations to ITU-T Recommendations or to other standards (approved or under development):

This work item will refer to the QKDN Recommendations such as ITU-T Recommendation Y.3800, Y.3801, Y.3802, Y.3803, Y.3804, G.808, and X.1710.

This work item will collaborate with related recommendations such as Y.QKDN_qos_req, Y.QKDN_qos_gen, and Y.supp.QKDN-mla.

The proposed new WI will be studied in a harmonious manner with existing and ongoing works in ITU-T and other SDOs but there are no duplications identified so far.

Liaisons with other study groups or with other standards bodies:

ITU-T SG15, ITU-T QIT4N.

Supporting members that are committing to contributing actively to the work item:

Beijing University of Posts and Telecommunications, China; CAS Quantum Network Co. Ltd., China; China Academy of Information and Communication Technology (CAICT), MIIT. P.R. China; QuantumCTek Co., Ltd., China.

Annex B

Draft new Recommendation ITU-T Y.QKDN_rsfr

Quantum key distribution networks - resilience framework

Summary

For resilience in quantum key distribution network (QKDN), the recommendation specifies the framework of resilience in QKDN including the conceptual models of QKDN protection and recovery. It also provides typical cases of resilience and related requirements of resilience supported by quantum layer, key management layer, and control and management layer, respectively.

Keywords

QKD; QKDN; resilience; framework; requirement.

Table of Contents

Draft new Recommendation ITU-T Y.QKDN_rsfr

Quantum key distribution networks - resilience framework

1. Scope

This Recommendation illustrates the framework for resilience in QKDN. It gives an overview on resilience in QKDN with its related conceptual models. And it provides requirements of QKDN multiple layers to support resilience in QKDN as well as the use cases.

In particular, the recommendation includes:

- Overview of resilience in QKDN
- Roles of resilience in QKDN
- Requirements of quantum layer for resilience in QKDN
- Requirements of KM layer for resilience in QKDN
- Requirements of CM layer for resilience in QKDN
- Use cases of resilience in QKDN

2. References

[ITU-T X.1701] Recommendation ITU-T Y.1701 (2020), *Security framework for quantum key distribution networks*.

[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_qos_req] Draft Recommendation ITU-T Y.QKDN_qos_req (2020), *Requirements of QoS assurance for quantum key distribution networks*

[ITU-T G.808] Recommendation ITU-T G.808 (2016), *Terms and definitions for network protection and restoration*.

< 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 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.

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

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

3.1.7 Key service recovery ratio [ITU-T Y.QKDN_qos_req]: the ratio of the number of successfully recovered key provisioning services to the total number of failed key provisioning services.

3.1.8 Wavelength consumption ratio [ITU-T Y.QKDN_qos_req]: the ratio of the consumed wavelength resource for the delivery of QKD keys to the consumed wavelength resource for the recovery of the failed QKD keys.

-TBD

3.2 Terms defined in this Recommendation

This chapter defines all the terms used in this recommendation.

3.2.1 Resilience in QKDN: The set of capabilities that allow a QKDN to protect or recover the QKD key supply within a threshold in the event of a QKD impairment.

NOTE – In general, the resilience schemes will involve re-routing. When resilience progress such as re-routing is performed, a percentage of the QKDN resources will be aggregated for the re-routing of impaired QKD-key services.

3.2.2 Failure: The fault cause of interrupted key supply persisted long enough to consider the ability of a QKD-key service to perform a required function to be terminated.

-TBD

4 Abbreviations and acronyms

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

-TBD

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 prohibited from” 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” indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords “is not recommended” indicate a requirement which is not recommended but which is not specifically prohibited. Thus, conformance with this specification can still be claimed even if this requirement is present.

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 Overview of resilience in QKDN

Resilience is necessary to be introduced into QKDN to guarantee stable running of QKDN and the continuous key supply. The framework for resilience in QKDN as well as requirements of resilience in QKDN supported by multi-layer functions is specified based on the functional requirements of QKDN in [ITU-T Y.3801] and functional architecture of QKDN in [ITU-T Y.3802]. The consideration on multi-layer QKDN resilience is based on the multi-layer functions in [ITU-T Y.3803] and [ITU-T Y.3804]. Expected effects on resilience in QKDN are based on descriptions in QoS related documents such as [ITU-T Y.QKDN_qos_req]. This recommendation is to specify resilience framework for QKDN supported by functions and requirements of QKDN layers.

Keep QKD running normally to provide the continuous protection of targeted traffic in the user network with stable key supply is an important issue in QKDN. When a QKDN failure such as key supply interruption or QKD link impairment occurs, the security of the services will be impaired. Also, when such failure accumulates, obvious impairment such as QoS degradation will occur for the user network services, while for QKDN, it can be a systematic interruption that a QKDN cannot work normally. Thus, a framework for resilience is needed for stable running of QKDN, it should be supported by multi-layer requirements to guarantee the continuous key supply.

This Recommendation will consider the following use cases of resilience in QKDN.

1) Resilience in QKDN supported by network resources reservation;

2) Resilience in QKDN supported by network resources recovery;

3) Resilience in QKDN supported by alternative schemes such as re-routing.

In the following clauses, the recommendation specifies conceptual models of resilience in QKDN. Use cases of resilience in QKDN are included, and the resilience should also be supported by multiple layers with related requirements of resilience in quantum layer, key management (KM) layer, and control and management (CM) layer, respectively.

7 Roles of resilience in QKDN

7.1 Protection of key supply in QKDN

QKDN protection needs to reserve pre-assigned network resources to guarantee the continuous key supply of QKD-key services. Functional enhancement could be supported by multi-layer entities in QKDN.

-TBD

7.2 Recovery of key supply in QKDN

QKDN recovery needs collaborative operations to recover or stabilize QKD-key services. Functional enhancement could be supported by multi-layer entities in QKDN.

-TBD

8 Requirements of quantum layer for resilience in QKDN

[Note: contributions on quantum layer requirements for resilience in QKDN are invited. Some of the important requirements to be considered are tolerance on QKD parameters, recovery time limit of QKD links. These requirements will provide architectural functional enhancement to quantum layer for resilience in QKDN.]

-TBD

9 Requirements of KM layer for resilience in QKDN

[Note: contributions on KM layer requirements for resilience in QKDN are invited. Some of the important requirements to be considered are threshold of key storage, threshold of key-supply rates, required key update period, required key service recovery ratio, and required synchronous frequency. These requirements will provide architectural functional enhancement to KM layer for resilience in QKDN.]

-TBD

10 Requirements of CM layer for resilience in QKDN

[Note: contributions on CM layer requirements for resilience in QKDN are invited. Some of the important requirements to be considered are requirements of selective QKD routing paths, requirements of QKDN response to recovery, and required wavelength consumption ratio. These requirements will provide architectural functional enhancement to CM layer for resilience in QKDN.]

-TBD

11 Use cases of resilience in QKDN

How to recover the QKDN resources under a QKD impairment is an important issue to be solved for resilience in QKDN. With multi-layer functional requirements and architecture descripted in Y.3801 to 3804, the resilience in QKDN requires collaborative operations among QKDN layers. Figures 1-3 show several conceptual models of typical resilience cases in QKDN as well as corresponding operations with the support of QKDN layers.

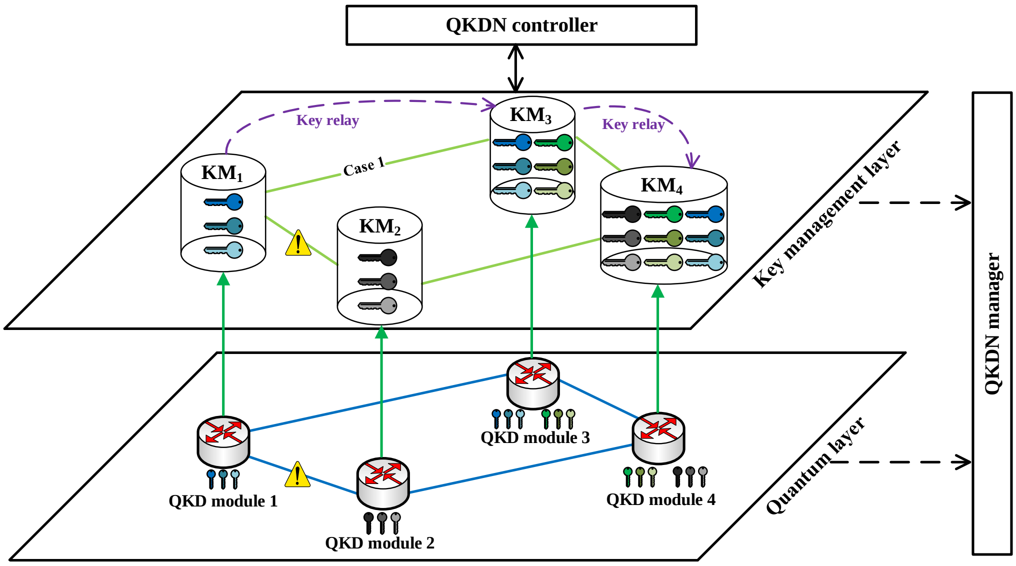

Figure 1 – Case 1 of resilience in QKDN with network resource reservation

Case 1) When QKDN failures happen such as the interrupted key supply, resource reservation such as a selective QKD path is prepared to keep the key supply without affecting security of services, while additional QKD overhead should be considered. This process is supported by QKDN multi-layer functions and architecture. There should be requirements of QKDN entities in multiple layers such as an acceptable threshold for a key storage as well as key service recovery ratio.

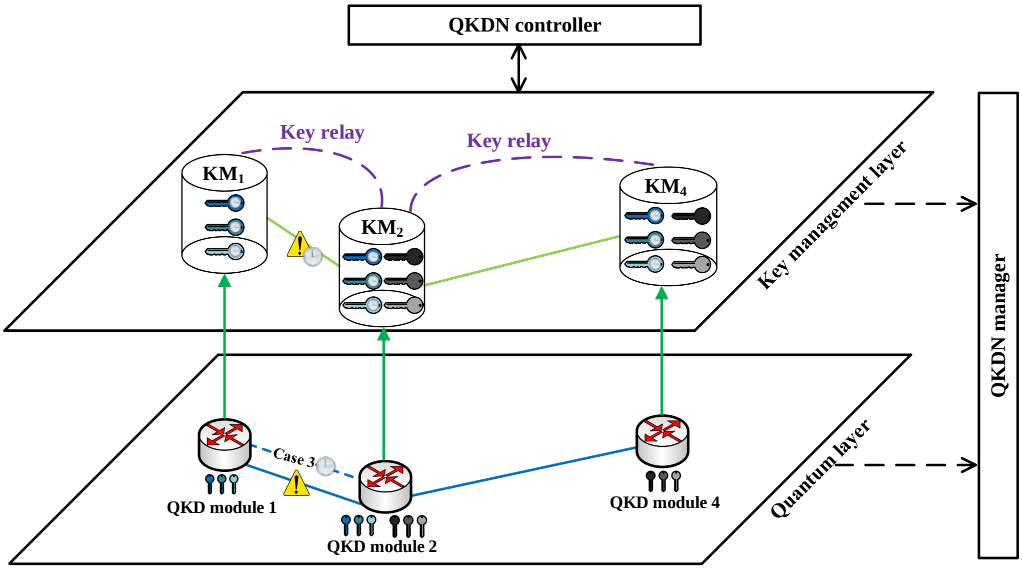

Figure 2 – Case 2 of resilience in QKDN with network resource recovery

Case 2) When QKDN failures happen such as interrupted key supply caused by rising QBER in a QKD link, resilience operations should be adopted to recover the impaired QKD link within services tolerance, while the additional operations overhead should be considered. This process is supported by QKDN multi-layer functions and architecture. There should be requirements of QKDN entities in multiple layers such as an acceptable time threshold for the recovery.

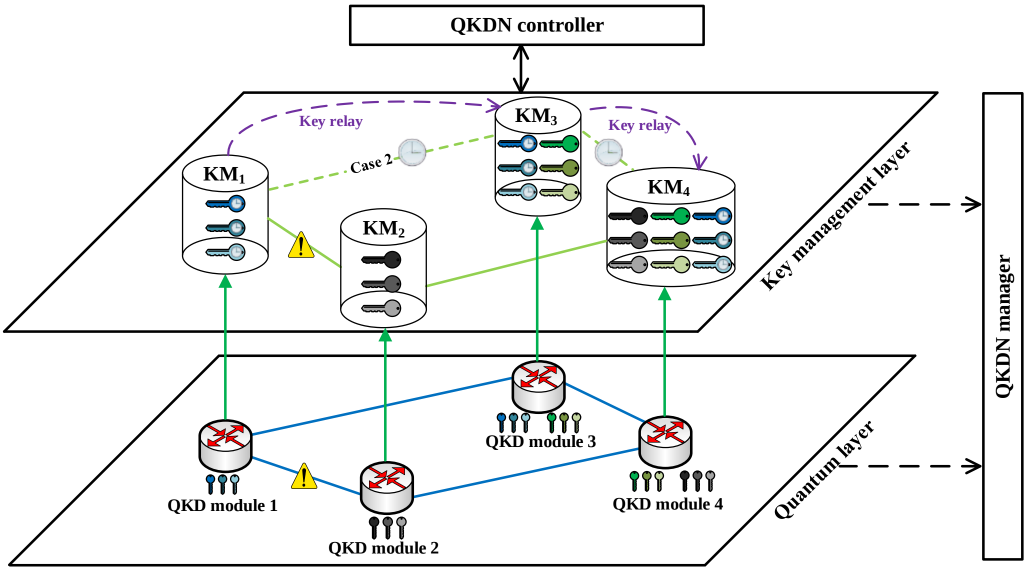

Figure 3 – Case 3 of resilience in QKDN with alternative schemes such as re-routing

Case 3) When QKDN failures happen such as interrupted key supply, a QKD routing path is constructed for re-routing of key relay to recover the impaired QKD-key services, while additional time overhead should be considered. This process is supported by QKDN multi-layer functions and architecture. There should be requirements for QKDN entities in multiple layers such as an acceptable time threshold for the re-routing of key relay as well as an acceptable wavelength consumption ratio.

Appendix I

Title of Appendix I

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

Bibliography