INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2022-2024

SG13-TD47-R1/WP3

STUDY GROUP 13

Original: English

Question(s): 16/13 Geneva, 4 -15 July 2022

TD

Source: Editors

Title: Draft new Recommendation ITU-T Y.QKDNf _fr "Framework of Quantum Key Distribution Network Federation"

Contact: Dong-Hi SIM
SK Telecom
Korea, Republic of
E-mail: donghee.shim@sk.com

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

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: Zhangchao Ma
CAS Quantum Network Co., Ltd.
China
Tel: +86-10-83057625
Email:mazhangchao@casquantumnet.com

Abstract: This TD is to propose a new work item for the framework of QKDN federation.

Proposal

A new work item proposal with A.1 justification and the very first draft with the skeleton is attached in Annex I and II respectively. This TD is the output based on the discussion of C178(Rev3).

Attachments:

Annex I: A.1 justification for proposed draft new recommendation

Annex II: A new work item proposal Y.QKDNf_fr "Framework of Quantum Key Distribution Network Federation"

Annex I :

A.1 Justification for proposed draft new recommendation

Question:	16/13	**Proposed new ITU-T Recommendation**	Switzerland [Geneva], 4-15 July 2022	
Reference and title:	ITU-T Y.QKDNf_fr "Framework of Quantum Key Distribution Network Federation"			
Base text:	Annex II of this TD		**Timing:**	2023-12
Editor(s):	Dong-Hi SIM, SK Telecom; Yuhang Liu, BUPT; Xiaosong Yu, BUPT; Yongli Zhao, BUPT, Zhangchao Ma, CAS Quantum Network.		**Approval process:**	AAP

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

This draft new Recommendation specifies the framework of Quantum Key Distribution Network federation.

In particular, the Recommendation covers:

- Overview and scenarios of QKDN federation (QKDNf)
- Reference architecture for enabling QKDNf
- Functional requirements for QKDNf
- Functional entities for QKDNf
- Reference points for QKDNf
- Overall operational procedures for QKDNf
- Security considerations

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

Despite the fact that the interworking aspects between different QKD providers and possibly between two different QKDN operators, this is very start of the large scale of QKDN networks to provide the end to end QKD service to cover the large areas to the end users and to provide the QKD service when the end user is not in the area of home network etc. Therefore, the federation of QKDNs to share the resources and capabilities of many QKDN providers shall be considered to create the industry ecosystem including operators, vendors, OEMS and service providers which could lead to eventually a platform to develop additional services in the future. Federation refers to the interaction and coordination between QKDN providers and QKDNs, supporting multi-operator, -network, - vendor environment to provide the seamless QKDN service to the end users. If the end user wishes to have the same level of security which QKDN provides when the end user moves to the region of other QKDN provider, then the end user needs to find the service capability in that region. The relevant QKDN service discovery, network capability discovery, resource allocation and negotiation and the subsequent service provisioning need to be performed. As QKD technology is being deployed around the world, however, still limited coverage exists from QKDN perspective as only some operators deploy them in part of their networks. Therefore, it is good to have the mechanisms to have the same level of security service in the different regions where possible and to combine resources among multiple operators. Furthermore, the QKDN sharing could be also considered where one operator does not have QKDN coverage in certain regions in a certain country.

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

ITU-T Y.3802, Y.QKDN_iwfr and related deliverables as the main reference recommendations for architecture, entities, and interfaces of QKDN

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 SG11, SG15 and SG17, ETSI ISG-QKD

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

SK Telecom; Beijing University of Posts and Telecommunications, CAS Quantum Network, ETRI, Telecom Italia S.p.A

Annex II:

Draft Recommendation ITU-T Y.QKDNf_fr

Framework of Quantum Key Distribution Network Federation

Summary

This draft Recommendation specifies the framework of Quantum Key Distribution Network Federation (QKDNf) including the overview of QKDNf, reference architecture for enabling QKDNf, functional entities of QKDNf, reference points for the QKDNf, functional requirements of the QKDNf, overall operational procedures of QKDNf and security considerations.

Keywords

Quantum key distribution (QKD); QKD network (QKDN); Federation; QKDN federation (QKDNf)

Table of Contents

Draft Recommendation ITU-T Y.QKDNf_fr

Framework of Quantum Key Distribution Network Federation

1. Scope

This draft Recommendation specifies the framework of Quantum Key Distribution Network Federation (QKDNf).

In particular, the recommendation covers:

- Overview and scenarios of QKDNf
- Reference architecture for enabling QKDNf
- Functional requirements of QKDNf
- Functional entities of QKDNf
- Reference points for QKDNf
- Overall operational procedures of QKDNf
- Security considerations

2. References

[ITU-T X.1701] Recommendation ITU-T X.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.3805] Recommendation ITU-T Y.3805 (2022), *Quantum Key Distribution Networks - Software Defined Networking Control*

[ITU-T Y.QKDN_iwfr] draft Recommendation ITU-T Y.QKDN_iwfr, *Quantum Key Distribution Networks – interworking framework*

[ITU-T Y.QKDN_iwrq] draft Recommendation ITU-T Y.QKDN_iwrq, *Quantum Key Distribution Networks – interworking requirements*

[ETSI GS QKD 020] draft ETSI GS QKD 020, *Quantum Key Distribution (QKD); Protocol and data format of REST-based Interoperable Key Management System API*

< 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.

Editor's Note: More definitions will be added as work progresses

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.

API	Application Programming Interface
QKD	Quantum Key Distribution
QKDN	Quantum Key Distribution Network
QKDNf	Quantum Key Distribution Network federation
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" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

6 Overview and scenarios of the QKDNf

ITU-T SG13, SG17, ETSI and other SDOs have been standardizing many aspects of QKDN including QKDN architecture, key management, security requirements and security proofs and so on. However, the deliverables from these SDOs focused on the single provider of QKDNs, although, recently the interworking aspects have been considered in ETSI ISG-QKD [ETSI GS QKD 020] and ITU-T SG13 [ITU-T Y.QKDN_iwfr][ITU-T Y.QKDN_iwrq]. Y.QKDN_iwfr and Y.QKDN-iwrq are being studied for the interworking framework and requirements respectively in ITU-T SG13. Despite the fact that the interworking aspects between different QKD providers and possibly between two different QKDN operators, this is very start of the large scale of QKDN networks to provide the end to end QKD service to cover the large areas to the end users and to provide the QKD service when the end user is not in the area of home network etc. Therefore, the federation of QKDNs to share the resources and capabilities of many QKDN providers shall be considered to create the industry ecosystem including operators, vendors, OEMS and service providers which could lead to eventually a platform to develop additional services in the future.

Federation refers to the interaction and coordination between QKDN providers and QKDNs, supporting multi-operator, -network, - vendor environment to provide the seamless QKDN service to the end users If the end user wishes to have the same level of security which QKDN provides when the end user moves to the region of other QKDN provider, then the end user needs to find the service capability in that region. The relevant QKDN service discovery, network capability discovery, resource allocation and negotiation and the subsequent service provisioning need to be performed. As QKD technology is being deployed around the world, however, still limited coverage exists from QKDN perspective as only some operators deploy them in part of their networks. Therefore, it is good to have the mechanisms to have the same level of security service in the different regions where possible and to combine resources among multiple operators. Furthermore, the QKDN sharing could be also considered where one operator does not have QKDN coverage in certain regions in a certain country.

Several use cases of QKNDf can be summarized but not limited to:

- Use of cryptographic applications of the end user in the multiple QKDN providers
- QKDN sharing among QKDN providers
- Coordination of capabilities to ensure the mobility of the end users among QKDN providers

Editor's Note: Further descriptions will be added for the concept of QKDNf as work progresses

7 Reference architecture for enabling QKDNf

Editor's Note: Reference architecture for enabling QKDNf considering the mobility, charging, capability exposure and sharing etc will be described.

8 Functional requirements of QKDNf

Editor's Note: Functional requirements of QKDNf will be described to make sure use cases of federation.

9 Functional entities and reference points of QKDNf

Editor's Note: Functional entities and reference points of QKDNf considering the mobility, charging, capability exposure and sharing etc will be described.

10 Overall operational procedures of QKDNf

Editor's Note: Operational procedures to orchestrate the federation of the QKDNs for use cases will be described.

11 Security considerations

Editor's Note: General security perspective are addressed here for QKDNf, however, the details of security are outside of scope of this recommendation

Appendix I

Editor's Note: This Appendix I is the placeholder for further discussion to develop the Recommendation from the contents of C178(Rev3) from Q16/13 July 2022 meeting.

Background

This draft Recommendation is to propose the framework of QKDN federation. Federation refers to the interaction and coordination between QKDN providers and QKDNs, supporting multi-operator, -network, - vendor environment to provide the seamless QKDN service to the end users. If the end user wishes to have the same level of security which QKDN provides when the end user moves to the region of other QKDN provider, then the end user needs to find the service capability in that region. The relevant QKDN service discovery, network capability discovery, resource allocation and negotiation and the subsequent service provisioning need to be performed. As QKD technology is being deployed around the world, however, still limited coverage exists from QKDN perspective as only some operators deploy them in part of their networks. Therefore, it is good to have the mechanisms to have the same level of security service in the different regions where possible and to combine resources among multiple operators. Furthermore, the QKDN sharing could be also considered where one operator does not have QKDN coverage in certain regions in a certain country. Please note that the key exchange is not necessary for the cases when in particular multiple operators are not geographically in the same region and the end user is in the region of other QKDN provider which means the QKDN interworking is not always initiated to exchange the keys for the federation.

Several use cases of QKND federation can be summarized but not limited to:

- Use of cryptographic applications of the end user in the multiple QKDN providers
- QKDN sharing among QKDN providers
- Coordination of capabilities to ensure the mobility of the end users among QKDN providers

Following is an example of possible framework diagram of QKDN federation with multiple QKDN providers.

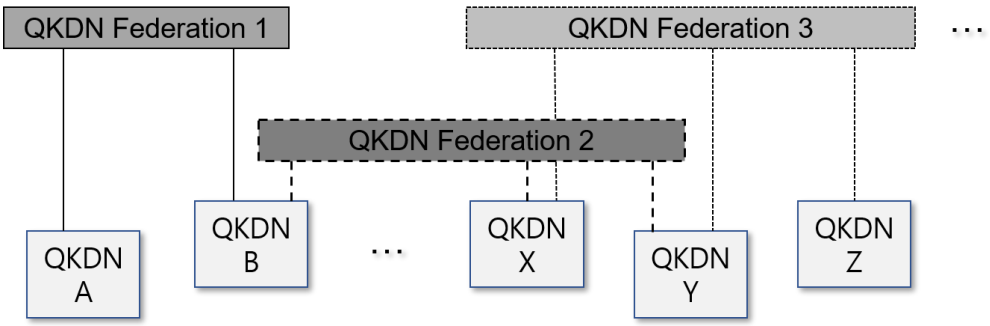

Fig. 1. Conceptual model of QKDN federation

Gap analysis

From standardization perspective, following functions, relevant reference points need to be standardized to realize the federation which is the interaction and coordination between QKDN providers and QKDNs, supporting multi-operator, -network, - vendor environment to provide the seamless QKDN service to the end users. To realize the federation, new functionality needs to be added on top of current architecture of QKDN as follows:

New Functions	Description	Remark
QKDN Service discovery for QKDN federation (QKDNf)	Discovery of cryptographic applications from other QKDN providers	Currently no standard to realize this function
Resource allocations and negotiations for QKDNf	When QKDN federation is allowed, the resource allocation and negotiation between providers are needed.	Same as above
Service provisioning for QKDNf	Relevant service provisioning is performed to the end user	Same as above
Service continuity for QKDNf	To continue the service offering by providing 'session continuity' which ensures the end user IP sessions established over any access networks will survive movements to and from other access networks	
Infrastructure sharing for QKDNf	Sharing of QKDN where one provider does not have the QKDN in certain regions but other providers might have the QKDN(s)	Same as above
Charging settlement based on charging policies between providers for QKDNf	When the federation is negotiated, the charging policy should be enforced and charging settlement is performed	Same as above

Bibliography

[b-ETSI GR QKD 007] ETSI GR QKD 007 (2018), *Quantum Key Distribution (QKD) – Vocabulary*

_____