Annex A:

Draft new 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 new 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

Editor's Note:

Further descriptions will be added for the concept of QKDNf as work progresses.

More accurate and comprehensive description of QKDN federation should be provided.

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.

6.1 QKDNf technologies

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.

6.2 QKDNf scenario

Editor's note: Figure 2 needs to be corrected with some issues, such as the keys are not supposed to be provisioned to the QKDNf.

Parallel to distributed, centralized and other network models, the federated network is a decentralized network model in which QKDN with different providers share resources via a central management framework that enforces consistent configuration and polices. Figure 1 shows a conceptual model of QKDN federation, where each federation consists of separate QKDNs with different providers.

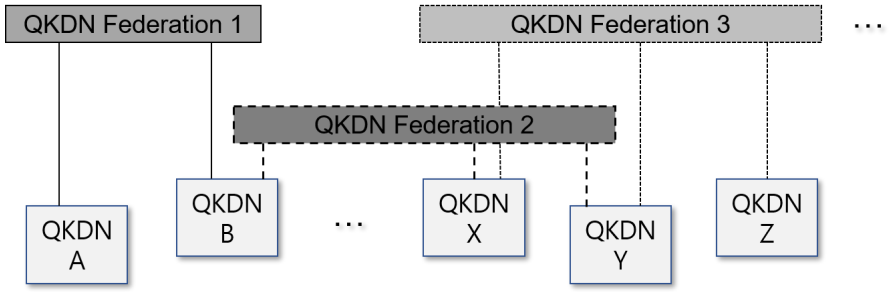

Figure 1 – Conceptual model of QKDN federation

In the scenario shown in Figure 2, a QKD user 1 moves from QKDN-A to QKDN-C, and requests the keys shared with user 2 in QKDN-D. Considering the user requirements, QKDN-C needs to provide the standardized policy as QKDN-A to provide QKD services to users, which requires QKDN-C to synchronize its control and management policies with QKDN-A. A QKDN federation is constructed covering QKDN providers A, B and C to share the necessary policies. There is a route configuration function in each federation, which can configure key transmission route crossing different QKDN providers. In this scenario, key resources belonging to QKDN-A will be distributed to QKDN-C through appropriate key relay methods in the federation 1, and then QKDN-C will provide keys to the mobile user 1 for use, so that QKDN-C can satisfy users' end-to-end key generation requirements. Specifically, the QKDN control and management functions and resource allocation could be performed in different locations.

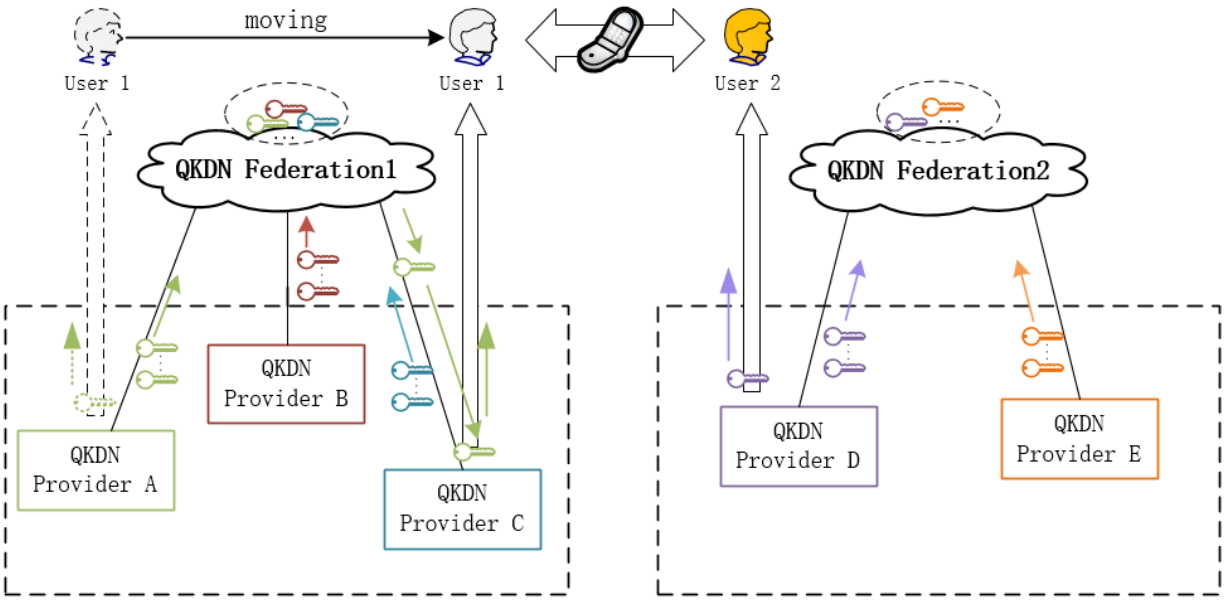

Figure 2 – Scenario of QKDN federation

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

7 Reference architecture for enabling QKDNf

Editor's Note: The mechanism or entity that operates or maintain the platform should be specified from the aspects that needed for multiple QKDNs to cooperate.

The large-scale QKDN need to meet the mobility needs of users. In order to realize cross-domain end-to-end QKD service, that is, users can have the unified QKD experience over multiple domains, QKDN must have the service capability in the scenario where the control and management functions and the underlying resource are separated. This usually requires information exchanging between QKDN domains. The interworking framework specified in [ITU-T Y.3810] provides the basic structure for information exchange between QKDN providers. Considering the larger-scale QKDN, where each point in the topology is regarded as a QKDN domain with its provider, end-to-end service among multiple domains needs to be split by upper layer entities, thus avoiding some overhead and service latency. In this regard, QKDN federation can provide effective end-to-end service establishment through standardized interfaces.

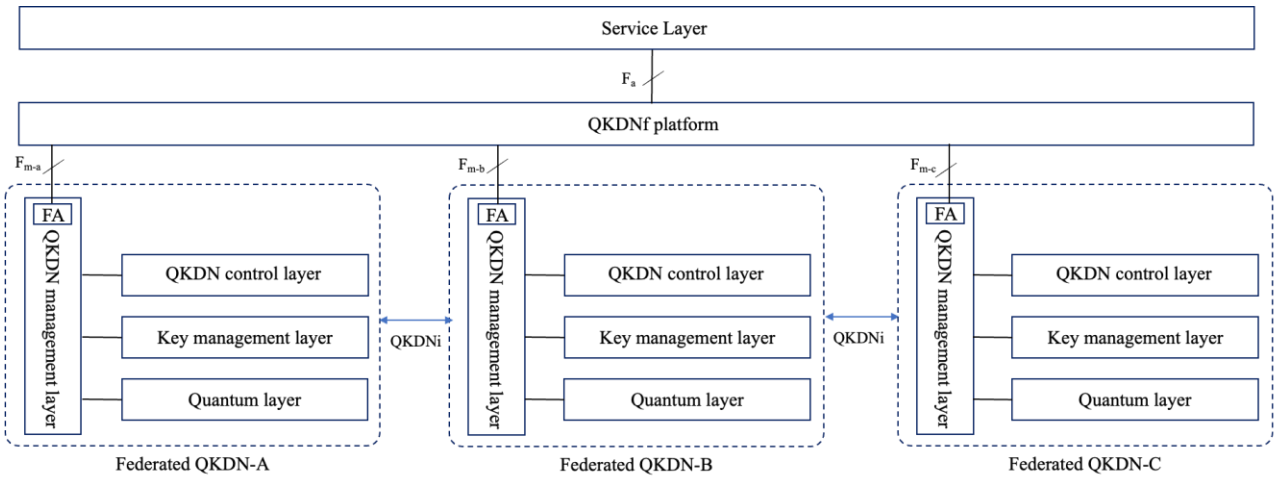

Figure 3 – Reference model for QKDNf

Figure 3 shows a reference model for enabling QKDNf. To establish the end-to-end service among multiple QKDN providers with QKDNf, QKDNs could be federated through a QKDNf platform. And federation agent (FA) is located at the QKDN management layer of each federated QKDN, which is a functional entity to support federation interfaces between each federated QKDN provider and QKDNf platform. The FA could discover resources that are allowed to be federated according to management policies of the provider and register these resources on the QKDNf platform through Fm. On the other hand, the QKDNf platform can distribute flow tables to FAs, splitting the end-to-end services into the specific operation of each federated QKDN.

Specifically, two reference points are identified to enable QKDNf:

- Fm is a reference point between QKDNf platform and QKDN management layer of federated QKDN for enabling QKDNf, which supports the procedure of resource discovery and registration, service orchestration, etc.
- Fa is a reference point between service layer and QKDNf platform for enabling QKDNf, which supports the procedure of user registration, service orchestration and authorization, etc.

NOTE 1 – The resource discovery process for federation within each domain is determined by the specific policies set by the provider, i.e., which resources are available for QKDNf.

NOTE 2 - The QKDNf could be done “offline”, that is, before the service arrivals, the QKDNf platform could be built to register the resources in the federated QKDN.

NOTE 3 - For end-to-end cross-domain services, QKDNf can perform routing of the service at the domain level, that is, which domains are involved in the routing path to accomplish the key request. In each federated QKDN, the specific routing can be scheduled by its own provider.

NOTE 4 – QKDNi is introduced to handle the resources on both sides to establish connections for key relay between QKDN providers.

8 Functional requirements of QKDNf

Editor’s Note: Requirements should be updated and further identified as work progresses.

Editor’s Note: The following updated requirements of QKDNf should be clarified, since QKDNf itself is not an entity for actual requirements.

- Req_1.The QKDNf is recommended to authenticate QKDNf members and only allow them to use specific functions. All users should be identified and validated before using the QKDNf system. They are only allowed access to services within the bounds of their role.

- Req_2.The QKDNf is recommended to establish a service rating system in case a QKDN provider consistently fails to deliver as promised, in addition to traditional consumer/provider relationships.

- Req_3.The QKDNf is recommended to set up an administrator who can provide persistent states of QKDNf members and manage the services and resources available.The administrator also has authorization to grant or revoke QKDNf membership.

- Req_4.The QKDNf is recommended to allow a QKDNf service/resource owner to have the authorization to register services or resources, making them available within a federation. The QKDNf service/resource owners have the authority to define and update the discovery unilaterally and access policies for their resources based on the roles and authorization attributes know to the QKDNf.

8.1 High-level requirements for QKDNf

Editor's note: Specific details of federation should be clarified before formulating these requirements.

To provide the end users with the seamless QKDN service, QKDNf needs to realize the interaction and coordination between QKDN providers and QKDNs. Based on the requirements for different QKDN layers defined in [ITU-T Y.3801], the high-level requirements for QKDNf are defined as follows.

- *Req_1. It is required to support the discovery of cryptographic applications from other QKDN providers.*
- *Req_2. It is required to support the (re)configuration of QKDN federation groups according to the service requirements.*
- *Req_3. It is recommended to support the hierarchical control of QKDN federation groups.*
- *Req_4. It is required to support the infrastructure sharing of QKDNs with different providers.*
- *Req_5. It is required to support the continuous session control using QKDN controllers from different QKDN providers.*
- *Req_6. It is required to support the negotiation of routing control between different QKDN providers.*
- *Req_7. It is required to ensure end-to-end quality of service in real-time with different QKDN providers.*
- *Req_8. It is recommended to support charging settlement based on charging policies between different QKDN providers.*

9 Functional entities and reference points of QKDNf

Editor's Note: Possible functions and relevant components should be more considered, as well as the correlated mechanism for accomplishing the federation.

Figure 4 illustrates a functional model for QKDNf. QKDN-A, QKDN-B, and QKDN-C are federated to support end-to-end cross-domain services. The federated QKDN connects with QKDNf platform through Fm, and Fa is identified to support service orchestration for cryptographic applications.

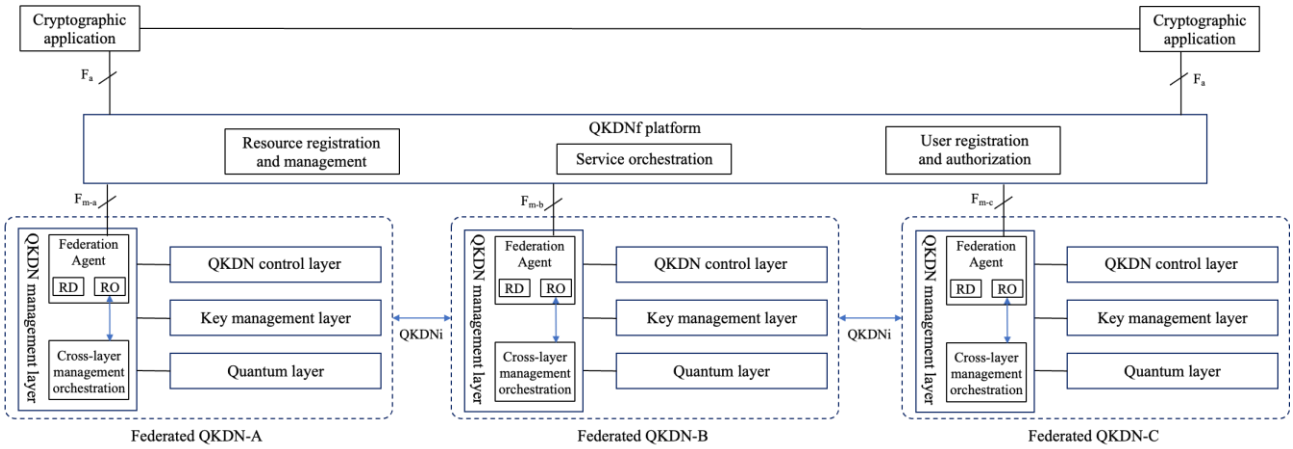

Figure 4 – Functional model for QKDNf

When the federation is established, the available resources in federated QKDNs are registered in QKDNf platform, the status of these resources could be updated as federated QKDNs progress. Users from the service layer could be registered and authorized on the QKDNf platform to obtain permission to establish end-to-end services with QKDNf. Based on the above "offline" preparations, "online" services are orchestrated in the QKDNf platform, which includes the cross-domain routing, splitting key requests for each federated QKDN, etc. The orchestrated key requests are distributed to the FA of each federated QKDN in parallel to further establish services within each federated QKDN.

In a federated QKDN, FA supports the functions of resource discovery (RD) and resource orchestration (RO) in federated QKDN. According to the provider's policy, available resources are collected during resource discovery for QKDNf. Dealing with the key request that orchestrated in QKDNf platform, the FA coordinates with the cross-layer management orchestrator in QKDN management layer to schedule the underlying resources.

NOTE – QKDNi is introduced to handle the resources on both sides to establish connections for key relay between QKDN providers.

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.

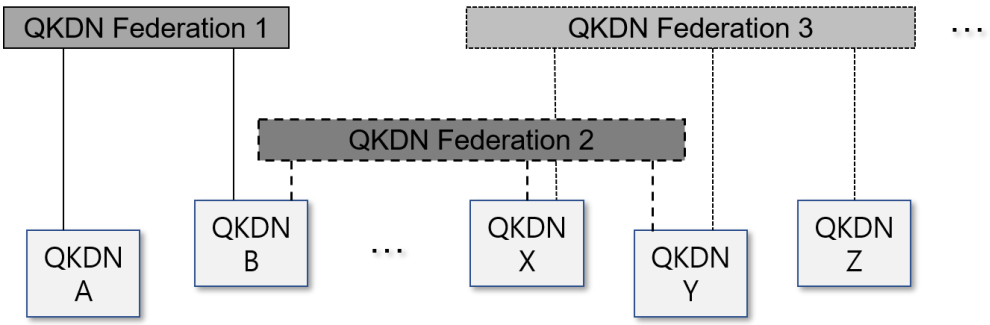

Fig. 1. Conceptual model of QKDN federation

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	Same as above

	between providers are needed.	
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*

_____