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 model for enabling 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 of QKDNf
- Reference model for enabling 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.

3.2.1 QKDN federation: QKDN service continuity in multi-QKDN provider operation scenarios through cooperation among QKDNs.

Editor's Note: Update on the definition on QKDN federation requested. Input contributions were kindly requested to revise the definition of QKDN federation.~~Editor's Note: More definitions will be added as work progresses~~

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 of QKDNf

While the interworking aspects between different QKDN providers are being taken into account, it is important to note that large-scale QKDN networks are still in their initial stages of development, aiming to provide end-to-end QKDN services covering extensive areas for end users. Consequently, it is highly recommended for QKDN providers to address service continuity in scenarios involving multi-provider operations. This can be achieved through cooperation among various QKDN networks, which is commonly referred to as QKDN federation.

Considering the user services involving multiple QKDN providers, this Recommendation specifies the framework of QKDNf, enabling QKDN providers to share resources and capabilities for user service covering a large network area.

6.1 Introduction of QKDNf

QKDNf refers to the interaction and coordination among QKDN providers, 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 recommended 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.

The QKDN federation is a QKDN network model in which QKDN with different providers share resources via a management framework that enforces consistent configuration and polices. Figure 1 shows a conceptual model of QKDN federation, where each federation involves QKDNs with authorized network resources or capabilities.

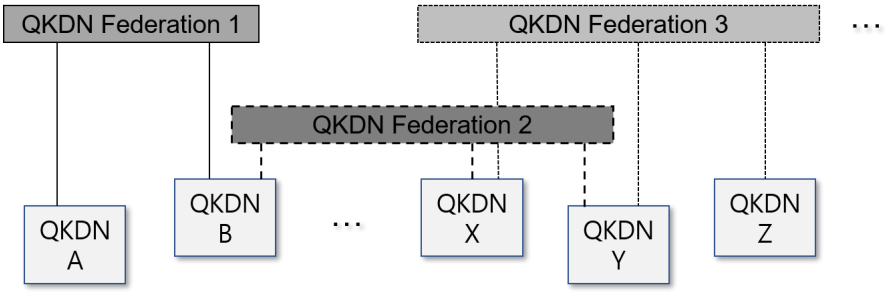

Figure 1 – Conceptual model of QKDNf

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

  If a user of a QKDN B provider is located where QKDN B does not cover the geographical region but but there is QKDN coverage of a provider of QKDN X in the case of 'QKDN federation 2' in Figure 1, QKDN B provider can collaborate with QKDN X provider to provide QKDN service to its user in QKDN X through QKDN sharing.

- Coordination of capabilities to ensure the mobility of the end users among QKDN providers

  If the user wishes to have the same level of security when the user moves to QKDN B from QKDN A in the case of 'QKDN federation 1' in Figure 1, QKDN providers for QKDN A and QKDN B collaborates to make sure the service continuity.

To realize these use cases, QKDN service discovery, resource allocation and relevant service provisioning should be done via cooperation between QKDN service providers.

6.2 Coordination among QKDN providers enabling QKDNf.

The primary advantage of QKDNf is to enable global access to QKDN services across different geographical regions. QKDNf allows QKDN providers to offer their services to end users, even when these users move across various QKDN networks. It is recommended that the QKDN service seamlessly continues as the end user connects to different visited networks.

To establish QKDNf, effective communication and coordination among QKDN providers are essential. This involves exchanging information related to QKDNf discovery, resource negotiation and allocation, service provisioning, security aspects (such as authentication and authorization), charging, identity management, and monitoring.

Federation agreements can be established directly between QKDN operators. However, QKDN providers may choose to utilize a federation broker if they intend to establish federation agreements with as many other providers as possible. The federation broker can have a pre-established list of agreements with a large number of QKDN providers, facilitating QKDNf operations.

6.3 Federation scenario among multiple QKDN operators

This scenario illustrates a use case similar to national roaming, where the end users of QKDN provider A can access the QKDN service provided by QKDN provider B through a mutual agreement between the two providers. In this scenario, the end user is a customer of QKDN provider A, but the optimal location for receiving QKDN service falls within the network coverage of QKDN provider B.

When the end user initiates the QKDN service on their device, the QKDN network of QKDN provider A recognizes that the ideal location for service provision is within the network coverage of QKDN provider B, based on the established federation agreement. As a result, the QKDN service of QKDN provider A redirects the service request to the QKDN network of QKDN provider B, ensuring that the requested QKDN service is provided to the end user seamlessly.

6.4 Federation scenario for QKDN sharing

QKDNf can also be employed to facilitate the sharing of QKDN network capabilities between different providers, particularly in situations where one provider lacks QKDN capabilities in a specific geographical region. By enabling QKDN sharing, the federation function allows for QKDN service discovery and end user redirection through coordination among QKDN providers, all based on established federation agreements.

QKDN sharing presents an opportunity to minimize capital expenditure (CAPEX) for QKDN providers while promoting the sharing of QKDN resources. This approach allows providers to leverage existing infrastructure and resources of other providers, enabling efficient utilization and avoiding unnecessary duplication of QKDN deployments. By sharing QKDN resources, providers can optimize their operations and expand their service coverage without significant additional investments.

7 Reference model for enabling QKDNf

Editor's Note: ~~it is suggested to clarify whether QKDN federation focuses on network functions or user service requirements, in order to have a clear view on the service layer in the reference model for QKDNf~~It is suggested to focus on the framework and related network functions to realize QKDN federation descried in clause 6. Actual service requirements and related detailed architectures can be developed with separate deliverables.

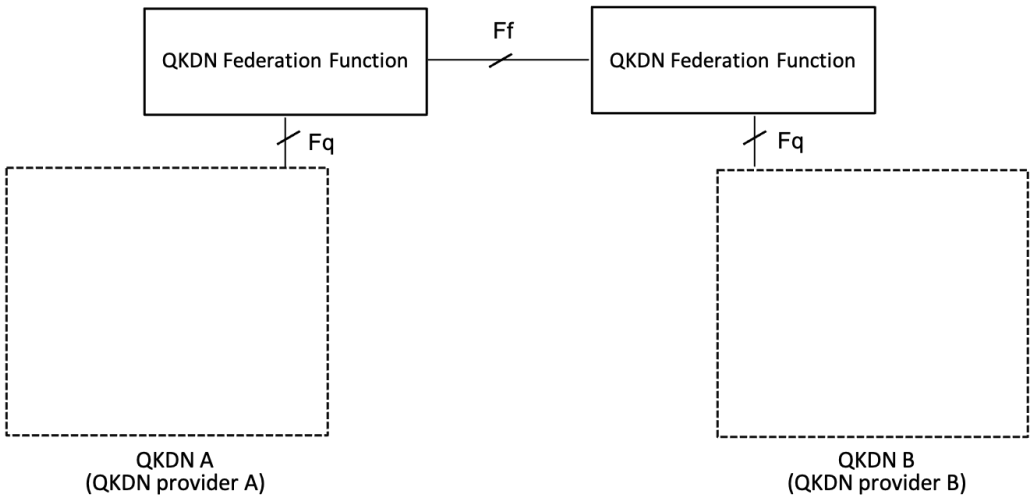

Figure 2 – Reference model for QKDNf with direct interface between QKDNf functions

Figure 2 presents a reference model that outlines the framework for enabling QKDNf, featuring a direct interface between QKDNf functions. The goal is to establish end-to-end QKDN services among different QKDN providers through the utilization of QKDNf.

In order to enable QKDNf, two reference points are identified within the reference model:

- Ff: This reference point serves as the interface between QKDNf functions, facilitating QKDNf-related procedures such as service discovery, resource negotiation and allocation, charging, security aspects (including authentication and authorization), and identity management. Ff ensures seamless coordination and communication between QKDNf functions across different providers.
- Fq: This reference point acts as the interface between QKDN and QKDNf functions. Fq supports QKDNf-related procedures including service discovery, resource negotiation and allocation, and service provisioning. It enables the exchange of information and capabilities between QKDNs and QKDNf functions, ensuring the effective integration and utilization of QKDN services within the QKDNf framework.

These reference points play a crucial role in enabling the necessary communication and interaction between QKDNf functions, as well as between QKDNs and QKDNf functions, to establish a seamless QKDNf ecosystem.

Figure 3 shows a reference model for enabling QKDNf with QKNDf broker. Same reference points are identified as shown in Figure 2.

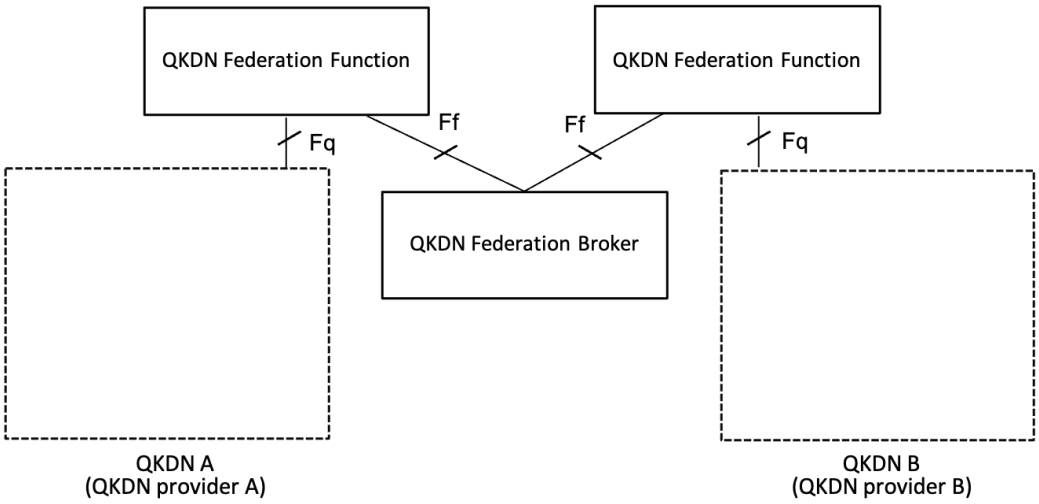

Figure 3 – Reference model for QKDNf with direct interface between QKDNf functions

8 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.

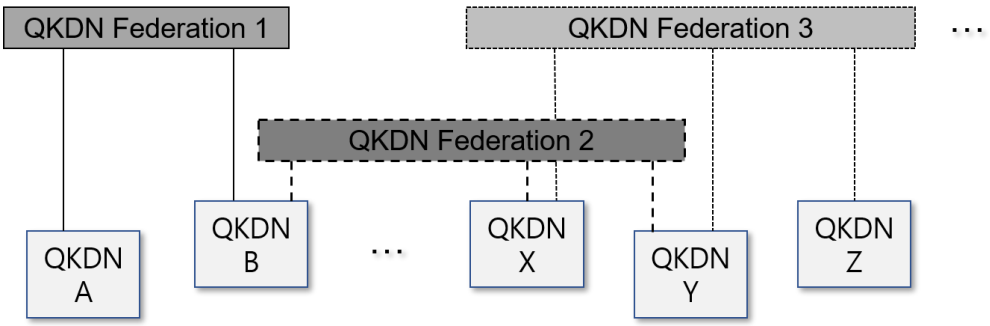

Fig. 1. Conceptual model of QKDN federation

Use cases

- Cryptographic applications for user network in multiple QKDNs

For cryptographic applications provisioning, multiple QKDNs can share management information to support the combination of cryptographic applications for user network. If the user wishes to have the same level of security which the QKDN-B provides when the end user moves to QKDN-X and QKDN-Y, QKDN-B can acquire and update the service capability with QKDNf.

- Resilience with shared QKDN resources in multiple QKDNs

For resilience, multiple QKDNs can share fault management information to support the failure resolving policies, and interactions with relevant functional components for healing actions. If there occurs failure in a key relay route of QKDN-B, the rerouting of key relay over QKDN-B, X, and Y can be enabled with QKDNf.

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

Requirements for QKDNf

High-level requirements for QKDNf

- Req_1. It is required that the QKDNs can access or withdraw from the QKDNf following its consistent configuration and policy.
- Req_2. It is required that the QKDNf can ensure the service continuity among multiple QKDN providers.
- Req_3. It is recommended that the QKDNs can exchange information of available cryptographic applications for QKDNf.
- Req_4. The QKDN is recommended to support the mechanism of infrastructure sharing for QKDNf.
- Req_5. The QKDN is recommended to support the identity authentication for QKDNf.
- To be added.

Functional requirements for QKDNf

- *Req_1. It is recommended to authenticate QKDNf members and configure specific functions for them.*

- *Req_2. It is recommended to establish a service rating system in case a QKDN provider consistently fails to deliver as promised.*
- *Req_3. It is recommended to set up an administrator who can provide persistent states of QKDNf members and manage the services and resources available.*
- *Req_4. It is recommended to allow a QKDNf service/resource owner to have the authorization to register services or resources, making them available within a federation.*

Functional entities and reference points of QKDNf

Figure 2 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.

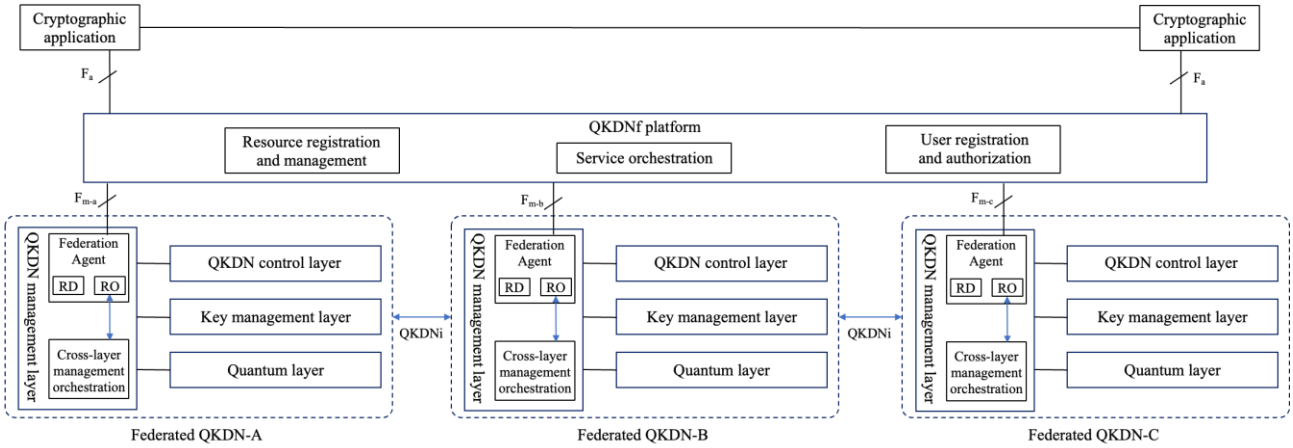

Figure 2 – Functional model for QKDNf

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.

Overall operational procedures of QKDNf

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

This clause describes overall operational procedures of QKDNf based on the reference architecture for enabling QKDNf defined in clause 7.

QKDN federation establishment procedure

1) Membership application

QKDN providers and other service/resource owners who want to join the federation can apply to the QKDNf .

2) Membership authentication and authorization

The federation administrator verifies the identity of the member, determines whether the member can join the federation, and only allows the member to access the services within the scope of the role. Members can join the federation by connecting to the QKDNf platform through the F_m.

3) Resource discovery and access

QKDN providers can discover resources that are allowed to be federated according to management policies through the FA of the QKDN management layer and register these resources on the QKDNf platform through F_m.

Bibliography

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

_____