Annex I:

Draft new Recommendation ITU-T Y.QKDNi-SDNC

Quantum Key Distribution Network Interworking - Software Defined Networking Control

Formatted: English (United States)

Summary

This draft Recommendation specifies the ~~Software-~~software-d~~D~~efined ~~Network-~~networking (SDN) based QKDN control ~~for the~~in facilitating interworking between QKDN providers. It provides ~~including the~~an overview of the role of SDN control for the interworking between QKDN providers, the functional requirements for SDN controller for the interworking, the functional entities of SDN controlller for the interworking, the interfaces of SDN controlller for the interworking, the operational procedures of SDN controller for the interworking, ~~the functional requirements of SDN control for the interworking,~~ and the security considerations.

Keywords

Quantum key distribution (QKD); QKD network (QKDN); QKDN ~~Interworking~~ interworking (QKDNi); ~~Software-~~software-~~Defined-~~defined ~~Network-~~networking (SDN)~~Control (SDNC); interworking~~

Table of Contents

1. Scope 3
2. References 3
3. Terms and definitions 4
3.1. Terms defined elsewhere 4
3.2 Terms defined in this Recommendation 4
4 Abbreviations and acronyms 4
5 Conventions 4
6 Overview of the role of SDN control for the interworking between QKDN providers 5
7 Functional requirements ~~in~~ for SDN controller for QKDNi 6
8 Functional entities of SDN controller for QKDNi 6
9 Interfaces of SDN controller for QKDNi 11
10 Overall operational procedures of ~~SDN control for QKDNi~~SDN controller for QKDNi 12
11 Security considerations 17
Bibliography 17

Draft new Recommendation ITU-T Y.QKDNi-SDNC

Quantum Key Distribution Network Interworking - Software Defined Networking Control

1. Scope

Editor's note: The use of the term "SDN based QKDN control" should be clarified to ensure consistency and clear understanding by readers.

This draft Recommendation specifies the ~~Software~~ software-d~~D~~efined ~~Network~~ networking (SDN) based QKDN ~~Control~~ control ~~for the~~in facilitating interworking ~~scenarios~~ between QKDN providers.

In particular, the ~~recommendation~~ Recommendation covers:

- Overview of the role of SDN control for the interworking between QKDN providers
- Functional requirements ~~in~~ for SDN controller for QKDNi
- Functional entities ~~in~~ of SDN controller for QKDNi
- Interfaces ~~in~~ of SDN controller for QKDNi
- Overall operational procedures of SDN controller for QKDNi
- 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.3810~~QKDN_iwfr~~] ~~draft~~ Recommendation ITU-T Y.~~QKDN_iwfr~~3810 (2022), *Quantum ~~Key~~ key ~~Distribution~~ distribution ~~Networks~~ network – interworking – framework*

[ITU-T Y.~~QKDN_iwrq~~3813] ~~draft~~ Recommendation ITU-T Y.~~QKDN_iwrq~~3813 (2022), *Quantum ~~Key~~ key ~~Distribution~~ distribution ~~Networks~~ network – interworking – functional requirements*

[ITU-T Y.3818] Recommendation ITU-T Y.3818 (2023), *Quantum key distribution networks interworking – architecture*

~~< 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~~ **software-defined networking (SDN)** [ITU-T Y.3300]: A set of techniques that enables to directly program, orchestrate, control and manage network resources, which facilitates the design, delivery and operation of network services in a dynamic and scalable manner.

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

3.1.3

3.2 Terms defined in this Recommendation

~~This chapter defines all the terms used in this recommendation.~~

~~TBD~~None.

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
QKDNi	Quantum Key Distribution Network ~~interworking~~Interworking
QoS	Quality of Service
SDN	Software-Defined Networking
SDNC	Software-Defined Networking Controller
GWF	Gateway Function
IWF	Interworking Function
GWN	Gateway Node
IWN	Interworking Node

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.~~

Formatted: Font: Italic

Formatted: List Paragraph, Outline numbered + Level: 3 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 1 cm + Indent at: 2.27 cm

Formatted: English (United States)

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 the role of SDN control for QKDNi

~~The initial deployment of QKD networks was that of infrastructures for symmetric key delivery decoupled from the telecommunication network. A major objective is to enable QKD networks without building parallel physical infrastructures by finding ways to integrate QKD in communication networks, increasing their security as long as trust on the intermediary nodes is assumed.~~

The ~~software~~ SDN~~defined networking (SDN)~~ paradigm has emerged to intrinsically increase the flexibility of communication networks. The SDN approach introduces a centralized network controller, which creates on demand a dedicated virtual infrastructure out of general purpose but programmable resources. Using standard interfaces, any networking functionality is realized on a flexible, programmable environment, allowing a quick adaptation to new requirements. SDN is now a major trend in telecommunication, deployed by many operators. The adoption of SDN methods also is in practical QKD networking [b-ETSI GS QKD 015][b-ETSI GS QKD 018][ITU-T Y.3805].

SDN is defined as a control framework that supports the programmability of network functions and protocols by decoupling the data plane and the control plane, which are currently integrated vertically in most network equipment. SDN proposes a logically centralized architecture where the control entity (SDN controller) is responsible for providing an abstraction of network resources through ~~Application Programming Interfaces (API)~~API. This abstraction enables SDN to perform network virtualization, that is, to slice the physical infrastructure and create multiple co-existing network slices (virtual networks) independent of the underlying wireless or optical technology and network protocols.

Constructing a large scale QKDN which covers wide area, it may consist of multiple QKDNs and they are interworking each other. An overview on QKDNi is addressed in [ITU-T Y.3810]. Moreover, QKDNi functional requirements are identified in [ITU-T Y.3813], QKDNi architectures are identified in [ITU-T Y.~~QKDN~~3818]. QKDNi is driven by the goal of enabling secure and efficient services across various QKDN providers, which transcends the boundaries of individual QKDNs. Interworking between QKDN providers introduces the capability to seamlessly exchange keys and extend the reach of secure communication. By establishing standardized interfaces and interoperable frameworks, QKDN providers can collectively reinforce the security and reliability of service, all while ensuring scalability and adaptability in the face of evolving networking demands.

Based on the advantages of SDN, it can serve as an enabler to facilitate this interworking. In the context of QKDNi, SDN is adopted to encompass multiple control domains, each comprising diverse network nodes from different vendors with various technologies, all controlled through standard interfaces. This Recommendation specifies the SDN-based QKDN control in facilitating interworking between QKDN providers.~~While SDN provides beneficial capabilities for network control, it should be noted that adopting SDN is only one optional approach for building the control plane of QKDN. The QKDN controller may also be implemented through other technical means beyond SDN. Therefore, SDN shall be considered as an enabler to achieve programmable control for QKDNi, but not the only approach that could be taken. Ideally, the SDN architecture is based on a~~

~~single control domain comprising multiple network nodes featuring diverse technologies provided by different vendors that are controlled through standard interfaces.~~

~~This recommendation presents the framework of SDN to achieve normalized control for QKDNi.~~

7 Functional requirements ~~in~~ for SDN controller for QKDNi

Editor's note: The SDN control information requires clarification. The revision should aim to provide a detailed explanation of the specific information encompassed by "SDN control information", and its role in the context of the document.

The requirements for SDN control for QKDN are defined in [ITU-T Y.3805], the requirements for QKDNi are defined in [ITU-T Y.3813], and this ~~recommendation~~ Recommendation specifies the requirements for SDN controller ~~for~~ to facilitate QKDNi.

- Req_1. For QKDNi, t~~T~~he SDN controller ~~for QKDNi~~ is required to support the ability of normalized abstraction of shared resources between QKDNs.

NOTE 1 – ~~the~~ The shared information between QKDNs can be abstracted into a standardized format by SDNC~~.~~, which refers to SDN control information for QKDNi.

~~Req_2. The SDN control for QKDNi is required to support the ability of acquiring and updating of network topology information in their own QKDN of the GWN and IWN from quantum layer.~~

- Req_2. For QKDNi, the SDN controller is required to support the interworking control function to support key relay and share SDN control information between QKDN providers.

~~- Req_3. The SDN control for QKDNi is recommended to support the ability of programmable elements controlling of GWN and IWN in their own QKDN, when the GWN /IWN consists of programmable elements in the quantum layer.~~

NOTE 2 – The "SDN control" refers to SDN-based QKDN control.~~When acquiring and updating network topology information with GWN /IWN, the SDN control for QKDNi shall ensure no private information is contained, so as to fulfill the security requirements of QKDNi.~~

~~- Req_4. The SDN control for QKDNi is recommended to support the ability of communication with SDNC orchestrator between QKDNs.~~

~~- Req_5. The SDN control for QKDNi is recommended to provide control information to a SDNC orchestrator between QKDNs.~~

~~NOTE 3 – the control information may include the network topology information, routing control information, virtualization information, etc., under the security restrictions.~~

Formatted: Font: Italic

Formatted: Font: Italic

Formatted: Font: Italic

Formatted: No bullets or numbering

Formatted: Font: (Asian) Chinese (Simplified, Mainland China), (Other) English (United States)

Formatted: No bullets or numbering

Formatted: No bullets or numbering

Formatted: Highlight

8 Functional entities of SDN controller for QKDNi

8.1 Functional elements of SDN controller for QKDNi with GWNs

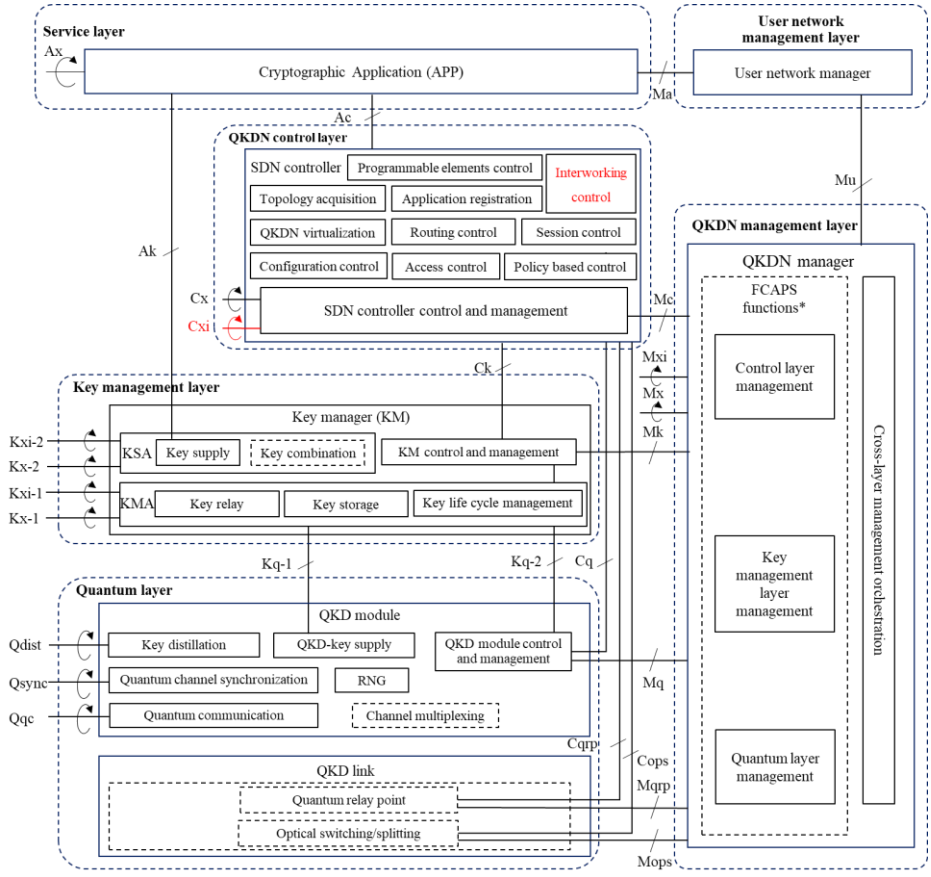


Figure 1 – Functional architecture of SDN control for QKDNi with GWNs

The functional architecture of SDN control for QKDNi with GWNs is specified in figure 1. Basically, ~~SDNC~~ SDN control functions as specified in [ITU-T Y.3805] can be supported ~~functions of QKDNs~~, and the corresponding interface Cxi is specified in [ITU-T Y.3810] and [ITU-T Y.~~QKDN~~ 3818].

~~NOTE 4 – The SDN-based QKDN controller is referred to as "SDN controller" across Clause 8, 9 and 10.~~

For QKDNi with GWNs, the functional entities of SDN controller ~~could~~ can support:

- Interworking control: to support key relay and share SDN control information between QKDNs through QKDN control layer, such as routing control, session control, authentication, ~~and~~ authorization control and QoS policy control, etc.
- QKDN virtualization: to normalize the information of shared resources for exchanging between different QKDN providers.

- Topology acquisition: to construct the ~~multi-domain~~network topology based on available information shared between SDN controllers for interworking.
- Application registration: to provide registration process for cryptographic application between different QKDN providers.

For the interworking, the functional elements of SDN controller includes:

- Quantum layer: the functional elements including the QKD link and QKD module are enabled to communicate with SDN controller for QKDNi between GWNs. The QKD parameters acquired from one of QKDNs can be normalized to construct a ~~single-domain~~ control topology between GWNs.
- Key management layer: the functional elements including the key management agent and key supply agent are enabled to communicate with SDN controller for information exchanging of keys between GWNs, such as key ID, etc. And keys can also be relayed between GWNs through key management layer.
- QKDN control layer: the functional element in QKDN control layer is SDN controller. It controls the variable resources to enable QKDNi with GWNs, and it supports interworking of key relay routing and rerouting between GWNs by enabling the SDN ~~-based QKDN~~ controller.
- QKDN management layer: the functional element in QKDN management layer is the QKDN manager, which can provide ~~the~~ SDN controller with available resource information between GWNs according to the policies of QKDN provider.

8.2 Functional elements of SDN controller for QKDNi with IWN

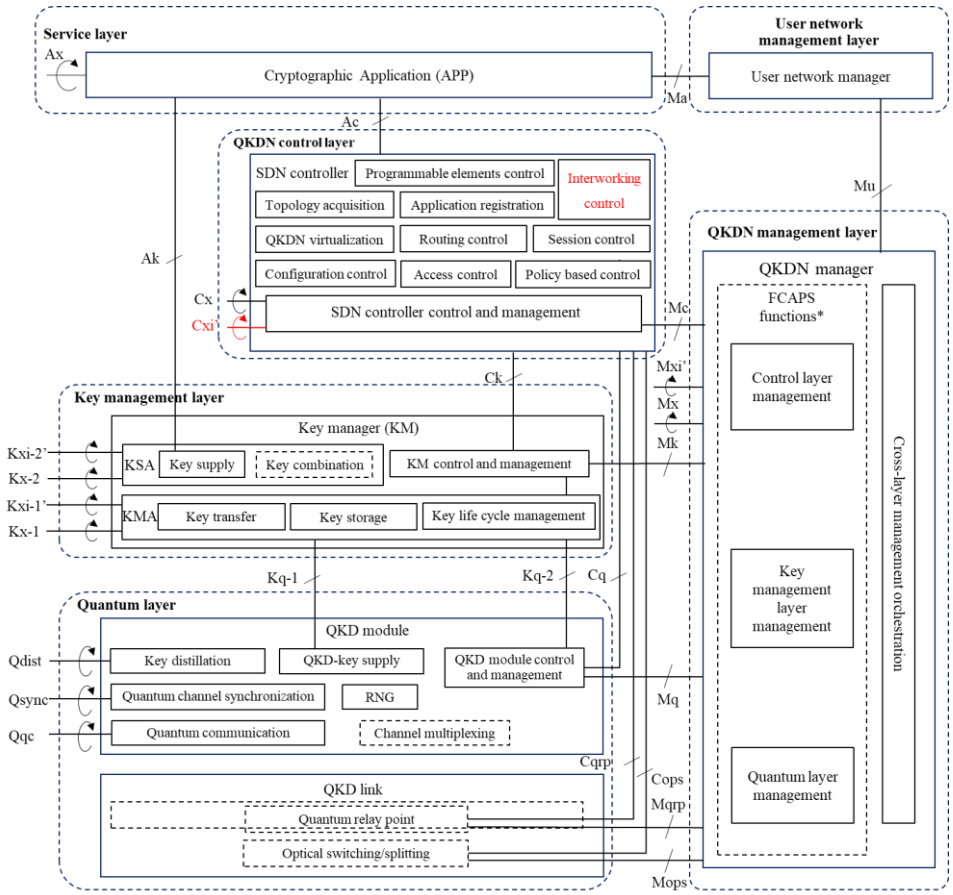


Figure 2 – Functional architecture of SDN control for QKDNi with IWN

For QKDNi with IWN, the functional entities of SDN controller ~~could~~ can support:

- Interworking control: to support key transfer and share SDN control information between QKDNs through QKDN control layer.

- For the interworking, the functional elements of SDN controller includes:

-

- Quantum layer: the functional elements in the quantum layer including the QKD link and the QKD module. The QKD module in IWN are enabled to communicate with SDN controller ~~between IWNs~~. The QKD parameters acquired from one of QKDNs can be normalized to construct ~~a single domain~~ control topology ~~between IWNs~~including IWN.
- Key management layer: the functional elements including the key management agent and key supply agent are enabled to communicate with SDN controller for information exchanging of keys ~~between IWNs~~in IWN, such as key ID, etc. And keys can also be transferred ~~between IWNs~~in IWN through key management layer.

Formatted: Font: (Asian) Japanese

Formatted: Normal

- QKDN control layer: the functional element in QKDN control layer is the SDN controller. It controls the variable resources to enable QKDNi with IWN, and it supports interworking of key transfer routing and rerouting ~~between IWNs~~ by enabling the SDN controller.
- QKDN management layer: the functional element in QKDN management layer is the QKDN manager, which can provide the SDN controller with available resource information ~~between IWNs~~of IWN according to the policies of QKDN provider.

8.3 Functional model of SDN control for QKDNi with GWNs

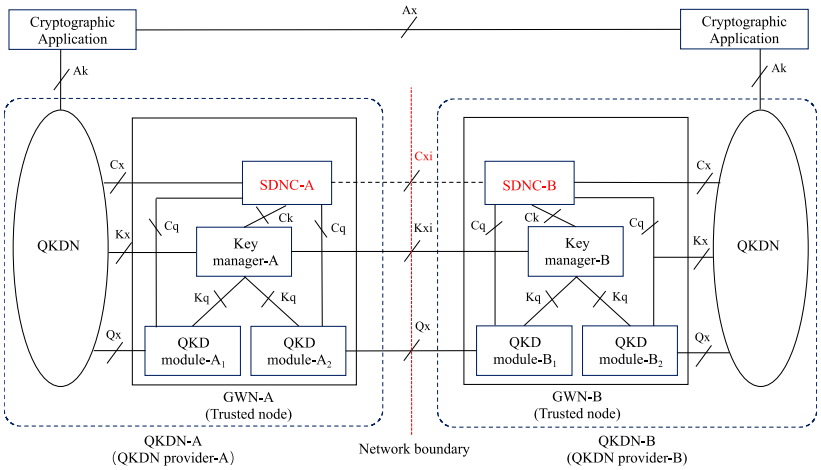


Figure ~~2~~ 3 – Functional model of SDN control for QKDNi with GWNs

Based on the functional model for QKDNi with GWNs specified in [ITU-T Y.3810], SDN controller can optionally be developed in GWNs of both QKDN providers for interworking and connecting optionally at Cxi.

Figure ~~2~~ 3 shows a functional model of SDN control~~C~~ for QKDNi with GWNs, where the SDN controller of each provider is developed in the GWN. The controllers coordinate with each other to complete the configuration of key manager and QKD module in GWNs. It can connect with the centralized upper layer SDN controller through the hierarchical structure to exchange the information on operations.

NOTE ~~1~~ 3 – The hierarchical structure of SDN controllers is specified in ITU-T Y.3805.

8.4 Functional model of SDN control for QKDNi with IWN

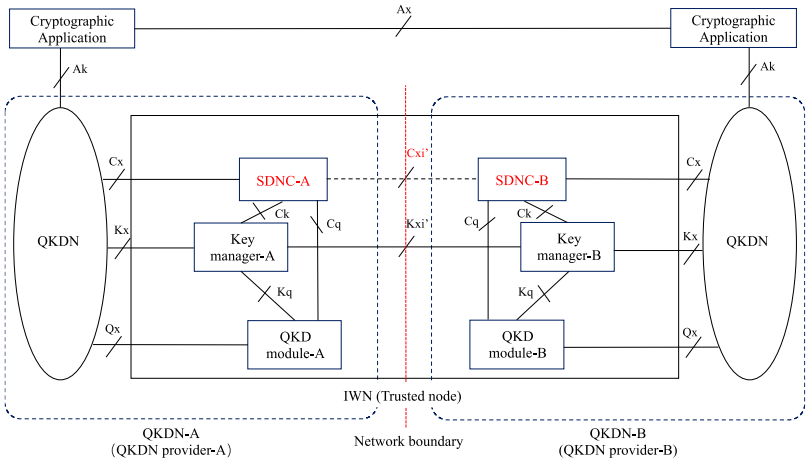


Figure ~~3~~ 4 – Functional model of ~~SDNC~~ SDN control for QKDNi with IWN

SDN controller can optionally be developed in IWN between QKDN providers for interworking and connecting optionally at Cxi'.

Figure ~~3~~ 4 shows a functional model of ~~SDNC~~ SDN control for QKDNi with IWN, where the SDN controllers of each provider is developed in the same QKD node. The controllers coordinate with each other to complete the configuration of key manager and QKD module on both sides in IWN.

9 Interfaces of SDN controller for QKDNi

Most of the reference points in Figure 1 have been defined in [ITU-T Y.3802], [ITU-T Y.3805] and [ITU-T Y.3810], and this ~~recommendation~~ Recommendation presents the existing ones related to SDN control for the interworking.

The existing reference point in [ITU-T Y.3810] related to SDN control for the interworking includes:

- **Cxi:** reference point between SDN controllers for interworking of QKDN control layers. It is responsible for the SDN controller to communicate interworking information with another SDN controller between QKDNs. QKDN control information can be shared between QKDNs through the SDN controller in QKDN control layers.

The existing reference points in [ITU-T Y.3802] related to SDN control for the interworking include:

- **Ck:** reference point between SDN controller and KM control and management. It is responsible for SDN controller to communicate interworking control information with the KM control and management.

- **Cq:** reference point between SDN controller and QKD module. It is responsible for the SDN controller to communicate interworking control information with QKD module.

- **Mc:** reference point between QKDN manager and SDN controller. It is responsible for the QKDN manager to communicate interworking management information with the SDN controller.

The existing reference point in [ITU-T Y.3805] related to SDN control for the interworking includes:

- **Ac:** reference point between cryptographic application and SDN controller in the QKDN control layer. It is responsible for interworking service provisioning of cryptographic applications.

10 Overall operational procedures of SDN controller for QKDNi

~~10.1 Operational procedures of SDN control for QKDNi with GWF~~

10.1~~.1~~ Service request and ~~system~~ initialization phase

~~*Editor's note: mechanism of interworking should be considered. There should be several distinguishing aspects to be reflected.*~~

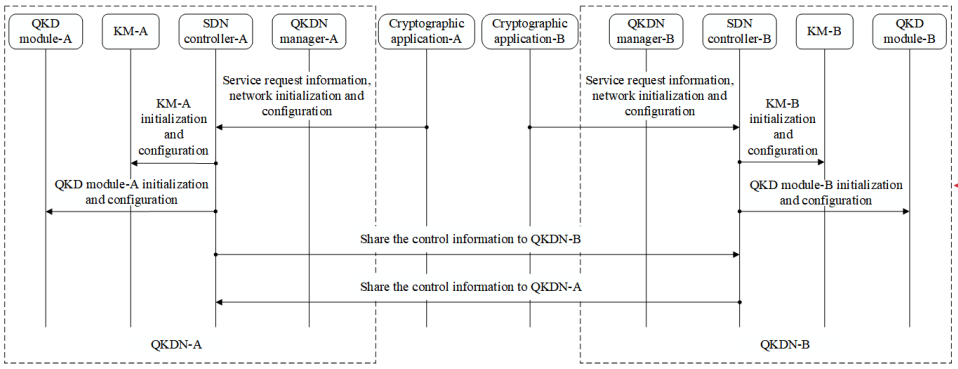
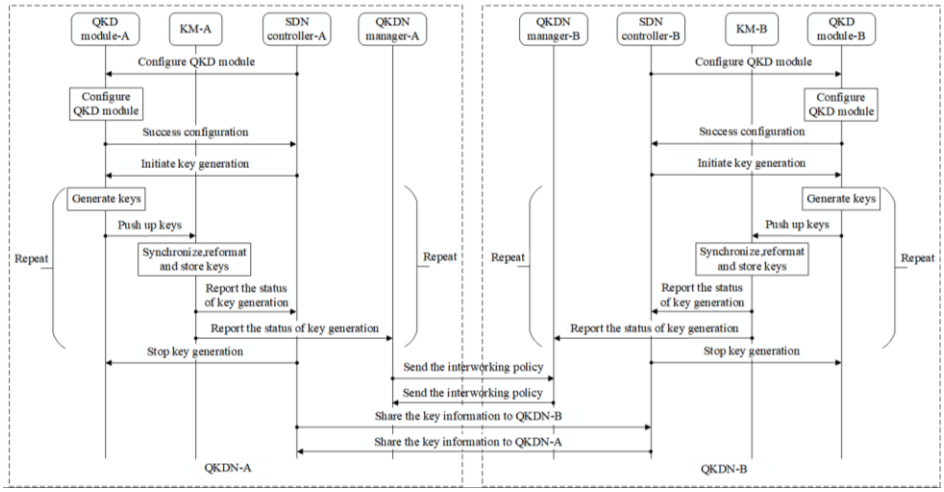


Figure ~~4-~~5 – An example of SDN control for service provisioning and ~~system~~ initialization ~~phase~~

Figure ~~4-~~5 illustrates procedures of SDN control for service request and ~~system~~ initialization ~~with SDN technology~~. In this phase, the cryptographic application-A/B in the service layer directly provides service request information and network initialization and configuration to the SDN controller-A/B, without providing information to the QKDN manager-A/B. Then the SDN controller-A/B initiates their respective QKDN controller~~,~~ for configuration of the KM-A/B and QKD module-A/B ~~to configure the two QKD networks from different QKDN providers~~. SDN controller-~~-~~A ~~connected~~ connects with SDN controller-B to share the QKDN control information which is defined in [ITU-T Y.~~QKDN_iwrq~~3813].

10.~~1~~2~~.2~~ Key generation ~~and transfer~~ phase

~~*[Editor's note: It is not clarified what is shared between controllers and managers for QKDNi.]*~~



Formatted: Centered

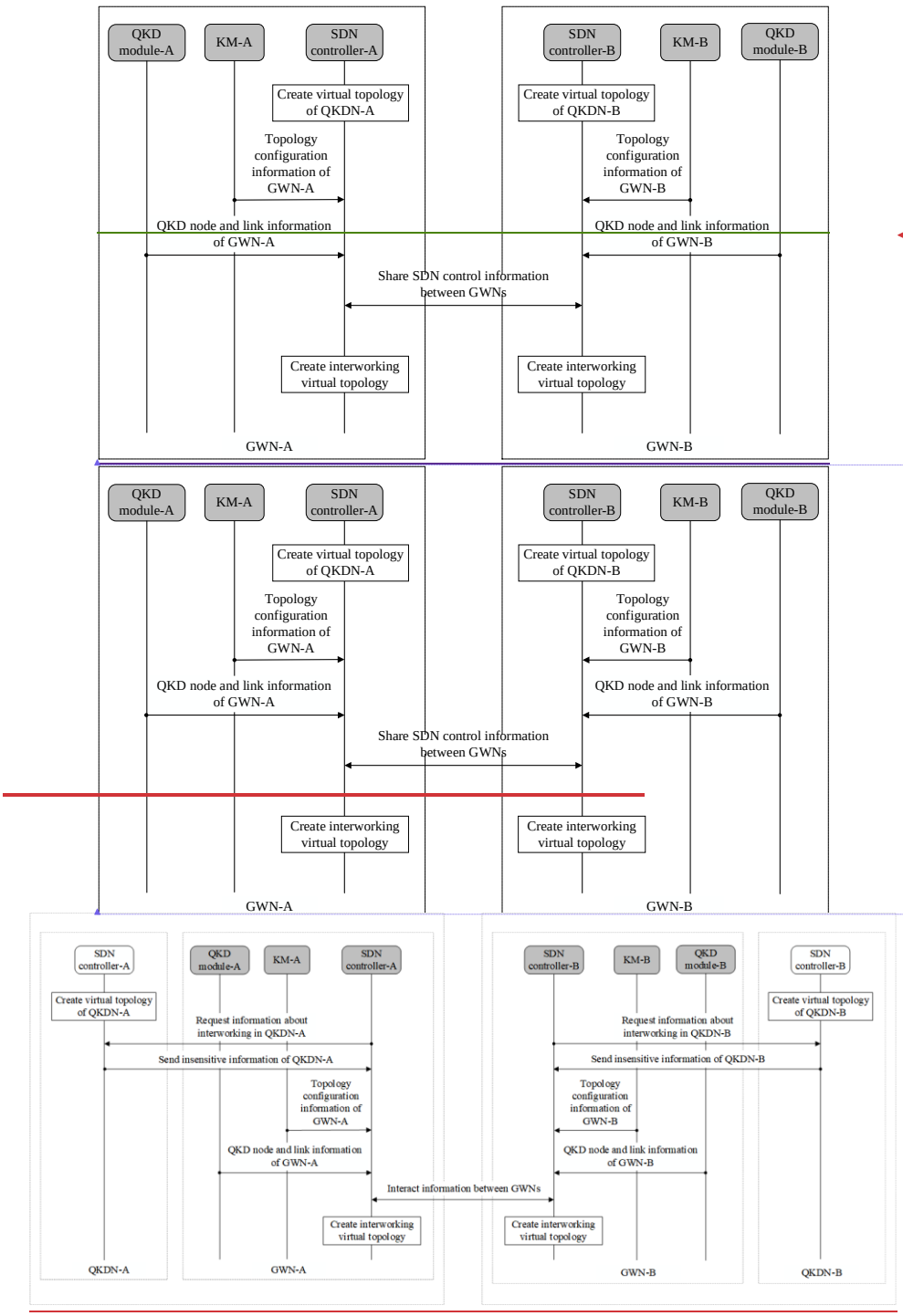
Figure ~~5~~ 6 – An example of SDN control for~~of~~ key generation ~~and transfer phase~~

Figure ~~5~~ 6 illustrates the procedures of SDN control for key generation ~~with SDN technology~~. In the initialization phase, the SDN controller-A/B ~~controller firstly sends the configuration of the QKD module to~~configures the QKD module-A/B respectively. After ~~the QKD modules have been configured successfully~~successful configuration, the SDN controllers ~~send the~~instruct the QKD modules to ~~initiation~~ initiate ~~of the~~ key generation ~~to the QKD modules directly~~. ~~Then, the physical key generation procedures are repeated until the SDN controllers send the instruction to stop them.~~

During the key generation, the QKD modules report ~~The~~ status ~~of key generation is reported to both the~~their respective SDN controllers and QKDN managers ~~for future control and management requirements~~. ~~After the keys are generated,~~ The QKDN managers ~~send the~~exchange interworking policy ~~to~~ with each other, specifying management information. ~~SDN controller-A connected with SDN controller-B to share the key information which is defined in [ITU-T Y.QKDN_iwrq].~~

After keys are generated, the SDN controllers share keys information with each other, including parameters such as key generation rate, etc., which allows coordinated control for key usage and relay routing over different QKDNs. For security consideration, the actual key values are not exchanged between SDN controllers.

10.~~1~~3 Virtualization phase



Formatted: Centered

Field Code Changed

Field Code Changed

Fig. ure 7 – An example of virtualization for interworking phase

Figure. 7 illustrates procedures of SDN control for virtualization between two QKDN providers with GWNs. First, the SDN controller-A/B in QKDNs create the in domain virtual topology of their respective QKDN with GWN., where the controllers collect topology configuration information from KM-A/B, as well as the QKD node and link information from the QKD module-A/B in GWNs. Next, The the SDN control information can be exchanged between SDN controllers of QKDN-A/BSDN controller-A/B in GWNs request information related to interworking to the SDN controller-A/B in QKDNs, and the SDN controller-A/B in QKDNs will send insensitive information to the SDN controller-A/B in GWNs. Then, the SDN controller-A/B in GWNs collect topology configuration information from the KM-A/B and the QKD node and link information from the QKD module-A/B. Finally, Tthe SDN controller-A/B in GWNs, enabling the creation ofe an interworking virtual topology after interacting information between GWNs..

The interworking virtual topology incorporates essential routing information related to the interworking key relay routes, including the availability and status of GWNs. It ensures that the appropriate GWNs can be seamlessly selected for key relay, thus enhancing the overall efficiency and reliability of the interworking.

10.1.4 Key request, relay and supply phase

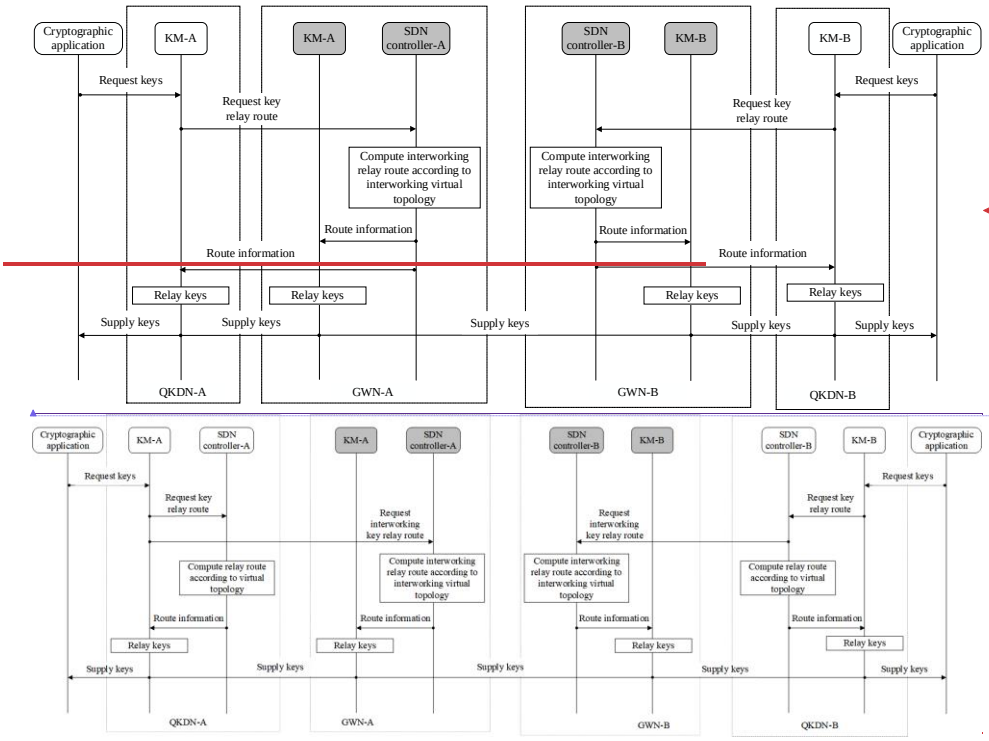


Figure. 8 – 2 An example of key request, relay and supply phase

Fig. ure 82 illustrates procedures of SDN control for key request, relay and supply between two QKDN providers with GWNs. A cryptographic application between QKDN-A and QKDN-B sends cross-domain key request information to the KM-A/B in QKDNs. Then KM-A/B request key relay route from SDN controller-A/B in QKDNs, and SDN controller-A/B in QKDNs request interworking key relay route from SDN controller-A/B in GWNs. Then the SDN controllers, which will compute

Formatted: Centered
Field Code Changed

~~relay route and~~the interworking relay route and decide the routing information. Based on the routing information, the KMs initiate the key relay and interworking key relay procedures~~ between the originating QKD node and the destination QKD node and execute key relay and interworking key relay according to the control by the SDN controllers~~. Finally, the KMs ~~push up~~supply keys to the requesting cryptographic application.

Formatted: English (United States)

11 Security considerations

In SDN control for QKDNi, the security considerations of SDN controller within their own QKDN have been mentioned in [ITU-T Y.3805]. Information within controllers and different QKDNs should be kept secret from external controllers, where privacy should be considered for QKDNi. Details are outside the scope of this ~~recommendation~~Recommendation.

Bibliography

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

[b-ETSI GS QKD 015] ETSI GS QKD 015 V2.1.1 (2022-04), *Quantum Key Distribution (QKD); Control Interface for Software Defined Networks*.

[b-ETSI GS QKD 018] ETSI GS QKD ~~015~~ 018 V1.1.1 (2022-04), *Quantum Key Distribution (QKD); Orchestration Interface for Software Defined Networks*.

Formatted: English (United States)