



**Question(s):** 16/13

Geneva, 13-24 March 2023

**TD**

**Source:** Editors

**Title:** Draft new Recommendation ITU-T Y.QKDNi\_SDNC: “Quantum Key Distribution Network Interworking – Software Defined Networking Control”

**Contact:** Dong-Hi SIM  
 SK Telecom E-mail: [donghee.shim@sk.com](mailto:donghee.shim@sk.com)  
 Korea, Republic of

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

**Contact:** Yongli Zhao Tel: +86-10-61198108  
 Beijing University of Posts and E-mail: [yonglizhao@bupt.edu.cn](mailto:yonglizhao@bupt.edu.cn)  
 Telecommunications.  
 China

**Contact:** Xiaosong Yu Tel: +86-10-61198108  
 Beijing University of Posts and E-mail: [xiaosongyu@bupt.edu.cn](mailto:xiaosongyu@bupt.edu.cn)  
 Telecommunications.  
 China

**Contact:** Zhangchao Ma Tel: +86-10-83057625  
 CAS Quantum Network Co., Ltd. E-mail: [mazhangchao@casquantumnet.com](mailto:mazhangchao@casquantumnet.com)  
 China

**Abstract:** This document includes the output of Recommendation ITU-T Y.QKDNi\_SDNC “Quantum Key Distribution Network Interworking – Software Defined Networking Control”.

**Summary**

This TD is the output document for draft Recommendation ITU-T Y.QKDNi\_SDNC “Quantum Key Distribution Network Interworking – Software Defined Networking Control” based on the following input contributions and discussion during the Q16/13 meeting, 13 - 24 March 2023.

C-440	BUPT	Proposal of adding the operational procedures of SDN control for QKDNi on Draft Recommendation Y.QKDNi-SDNC	Q16/13
-------	------	---	--------

- Proposal of contribution

- This contribution proposes to supplement a clause about the operational procedures of SDN control for QKDNi on Draft Recommendation QKDNi-SDNC to make the recommendation more complete.
- Meeting result
- The cryptographic application should be completed in the diagram. Other descriptions are accepted.

**Attachments:**

**Annex I:** Draft Recommendation ITU-T Y.QKDNi\_SDNC “Quantum Key Distribution Network Interworking – Software Defined Networking Control” (output of Q16/13, 13 - 24 March 2023)

**Annex A:**

**Draft new Recommendation ITU-T Y.QKDNi-SDNC**

**Quantum Key Distribution Network Interworking - Software Defined Network Control**

**Summary**

This draft Recommendation specifies the Software Defined Network control for the interworking including the overview of the role of SDN control for the interworking between QKDN providers, the functional entities of SDN control for the interworking, the interfaces of SDN control 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 (QKDNi); Software Defined Network Control (SDNC); interworking

## Table of Contents

1.	Scope.....	5
2.	References.....	5
3.	Terms and definitions .....	5
3.1.	Terms defined elsewhere .....	5
3.2	Terms defined in this Recommendation.....	6
4	Abbreviations and acronyms .....	6
5	Conventions .....	6
6	Overview of the role of SDN control for the interworking between QKDN providers .....	7
7	Functional requirements in SDN control for QKDNi.....	7
8	Functional entities of SDN control for QKDNi.....	8
9	Interfaces of SDN control for QKDNi.....	10
10	Overall operational procedures of SDN control for QKDNi.....	11
11	Security considerations .....	14
	Bibliography.....	14

## **Draft new Recommendation ITU-T Y.QKDNi-SDNC**

### **Quantum Key Distribution Network Interworking - Software Defined Network Control**

#### **1. Scope**

This draft Recommendation specifies the Software Defined Network Control for the interworking scenarios between QKDN providers.

In particular, the recommendation covers:

- Overview of the role of SDN control for the interworking between QKDN providers
- Functional requirements in SDN control for QKDNi
- Functional entities in SDN control for QKDNi
- Interfaces in SDN control for QKDNi
- Overall operational procedures of SDN control 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.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*

< 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*

### 3.2 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
QKDNi	Quantum Key Distribution Network interworking
QoS	Quality of Service
SDN	Software-Defined Networking
SDNC	Software-Defined Networking Controller
GWF	Gateway Function
IWF	Interworking Function

## 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 the role of SDN control for the interworking between QKDN providers

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 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). 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. 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.

For the interworking scenarios of QKDNs, a multi-domain network orchestration is required as each domain can be provided by a different vendor where each domain can be independently controlled by means of their own customer SDN controller. This recommendation presents the framework of SDN orchestration and virtualization which allows a normalized control allowing the composition, at an abstracted level, of end-to-end provisioning services across multiple domains.

*Editor's Note: Further descriptions will be added for the concept of SDN control for the interworking of QKDNS between two QKDN providers as work progresses*

## 7 Functional requirements in SDN control for QKDNI

*Editor's Note:*

*Functional requirements for SDN control for the interworking will be added as work progress.*

*Descriptions should be further considered with more accurate terms and clarified intention. More interworking aspects should be highlighted.*

- Req\_1. The SDN controller is required to support the ability of normalized abstraction of shared resources from different QKDN providers to achieve more efficient resource configuration for QKDNI.

[Note: if possible, the commonly used QKDN parameters of different providers can be abstracted into a standardized format by SDNC for QKDNI.]

- Req\_2. The SDN controller can optionally support normalized control between different QKDN providers for interworking, and the upper layer controller can coordinate the operation of each domain's own SDN controller to complete the interworking functions.

[Note: In the QKDNi scenario with IWF, the SDNC in interworking node can be developed as an upper layer controller to coordinate the operations of controllers in both providers.]

- Req\_3. The SDN controller is required to support orchestration functions to realize the customized configuration of resources in both sides of QKDN providers.

## 8 Functional entities of SDN control for QKDNi

*Editor's Note: Two conceptual models for interworking of QKDNs in [ITU-T Y.QKDN\_iwfr] will be taken into account to consider the functional entities of SDN control. More details about SDNC functions for interworking should be clarified.*

### 8.1 Functional elements of SDN control for QKDNi

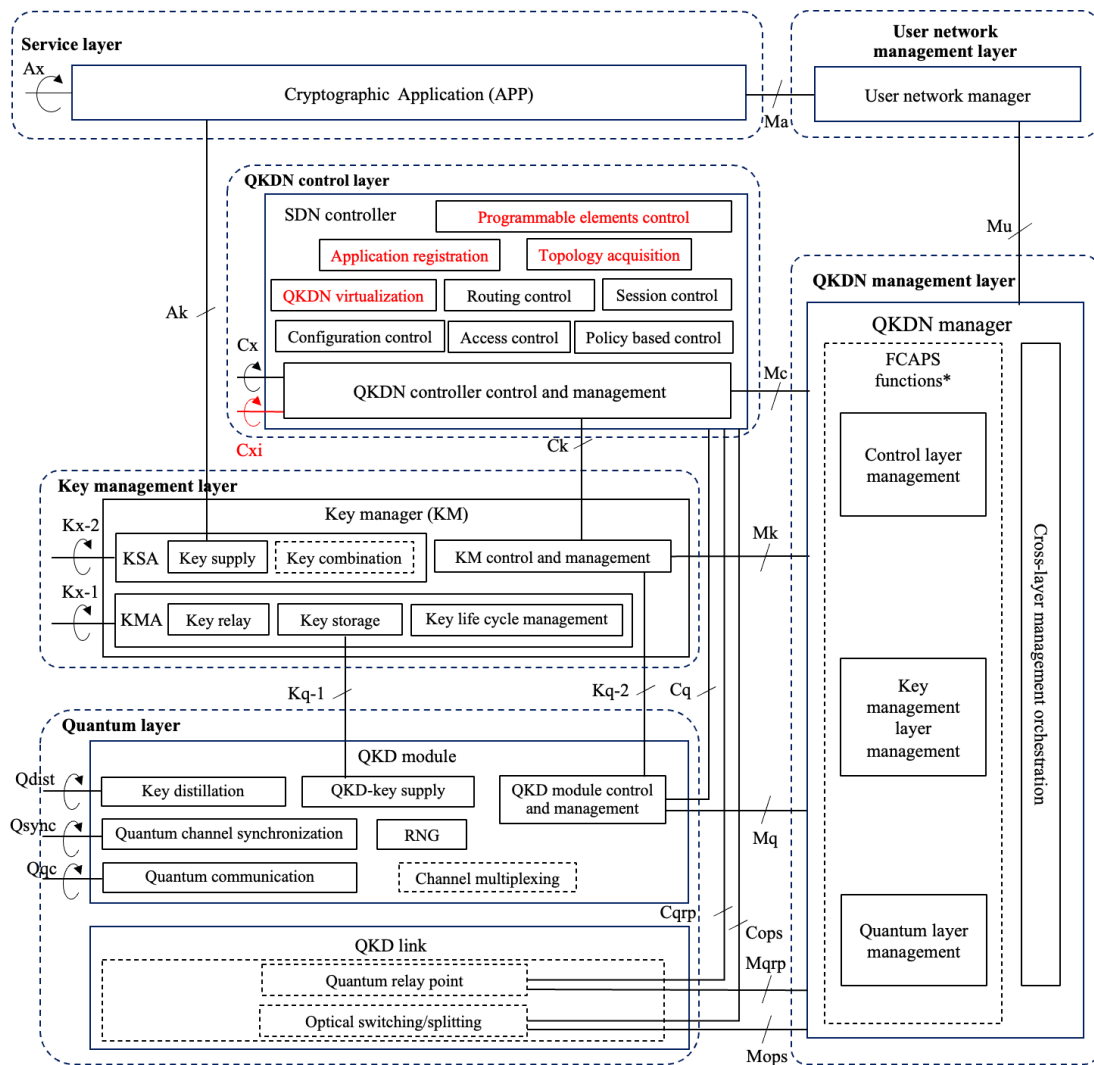


Figure 1 – Functional architecture of SDN control for QKDNi

The functional architecture of SDN control for QKDNi is specified in figure 1. Basically, SDNC functions as specified in [ITU-T Y.3805] can support functions of QKDNi, and the corresponding interface Cxi is specified in [ITU-T Y.3810]. This clause specifies the SDN related entities for interworking.

For QKDNi, the functional entities of SDN controller could support some more :

*[Editor's note: a preliminary version where the detailed descriptions of functions are still to be added and improved.]*



- QKDN virtualization: to normalize the information of shared resources for exchanging between different QKDN providers.
- Topology acquisition: to construct the multi-domain 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 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. The common QKD parameters acquired from QKD modules and links can be normalized to construct a single-domain control topology for interworking.
- 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, such as key ID, etc.
- QKDN control layer: the functional element in QKDN control layer is SDN controller. It controls the variable resources to enable QKDNi. The functions of SDN controller can be utilized with procedures supporting QKDNi.
- QKDN management layer: the functional element in QKDN management layer is QKDN manager, which can provide the SDN controller with available resource information for QKDNi according to the policies of QKDN provider.

## 8.2 Functional model of SDN control for QKDNi with GWF

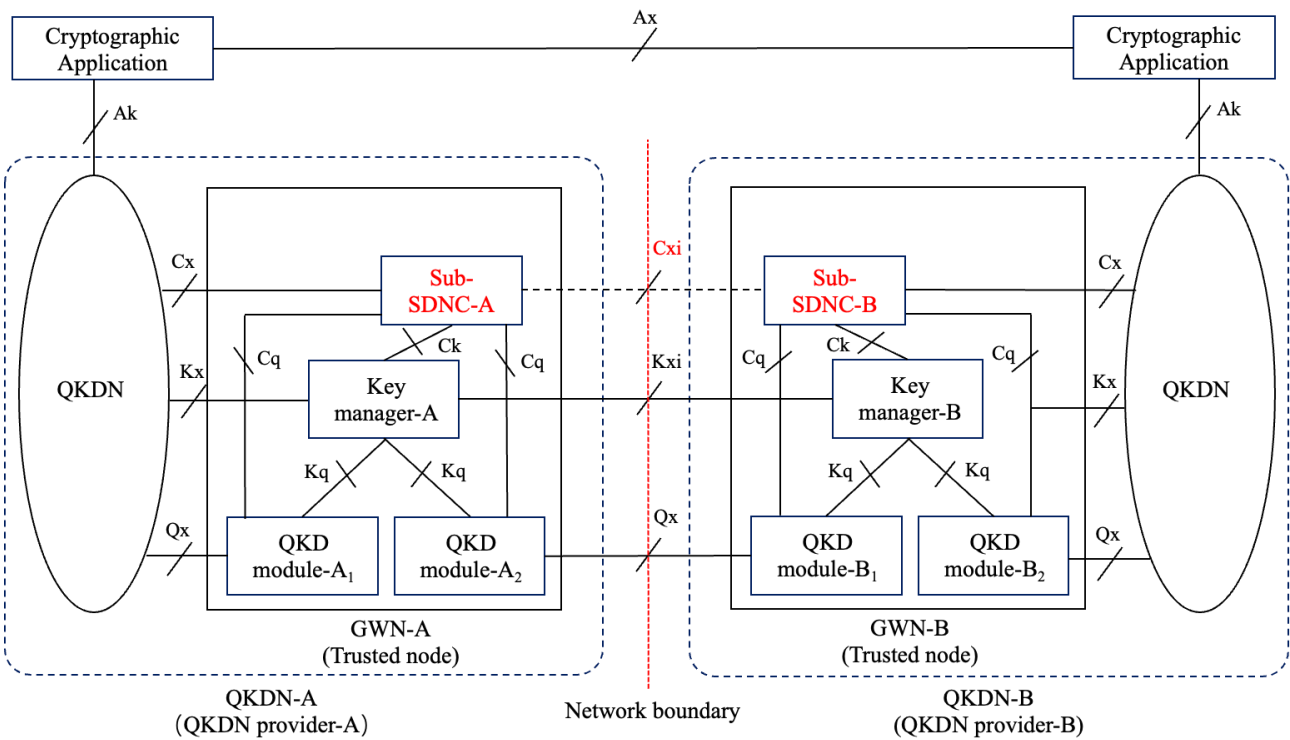


Figure 2 – Functional model of SDNC for QKDNi with GWNs

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 shows a functional model of SDNC for QKDNi with GWNs, where the sub-SDNC of each provider is developed in the GWN. The sub-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 – The hierarchical structure of SDN controllers is specified in ITU-T Y.3805.

### 8.3 Functional model of SDN control for QKDNi with IWF

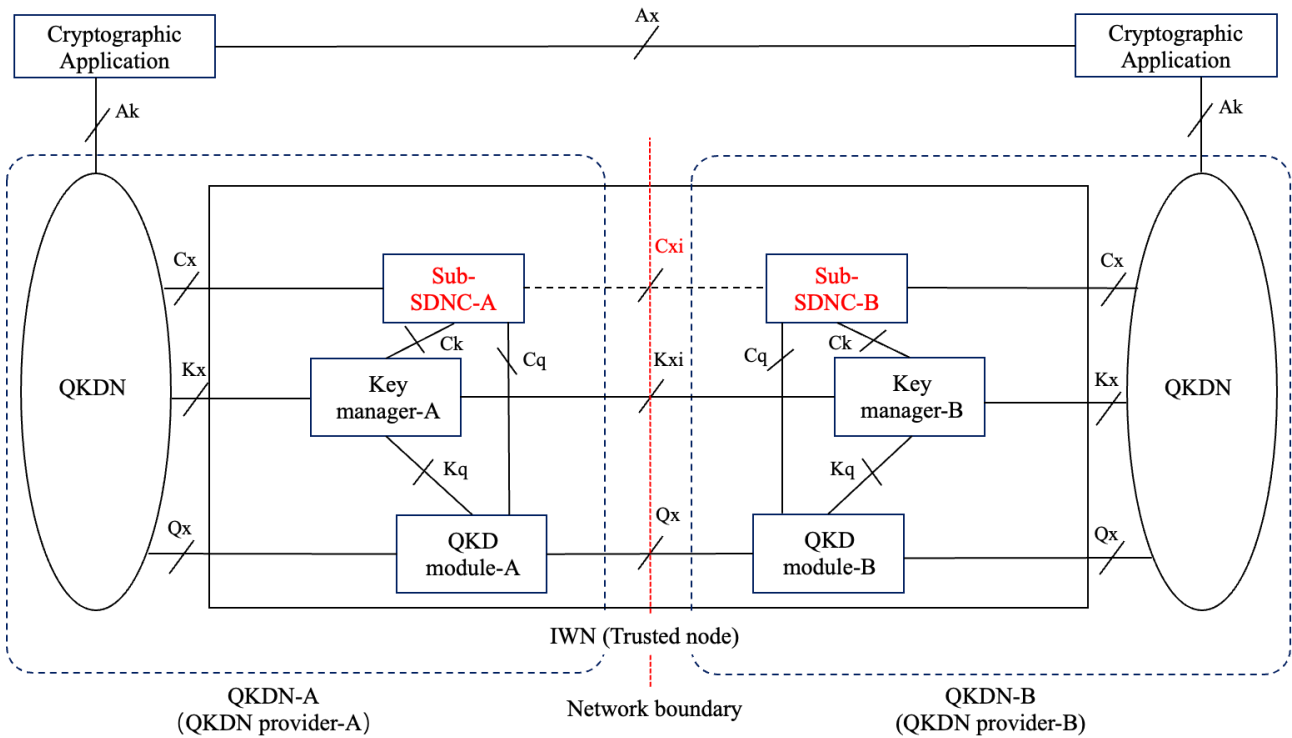


Figure 3 – Functional model of SDNC for QKDNi with IWN

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

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

### 8.4 Functional model of SDN control for QKDNi with orchestrator

To be added.

## 9 Interfaces of SDN control for QKDNi

*Editor's Note: Reference points for SDN control for the interworking will be studied*

## 10 Overall operational procedures of SDN control for QKDNi

*Editor's Note: Operational procedures to orchestrate the SDN control for the interworking between two QKDN providers will be described.*

### 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.*

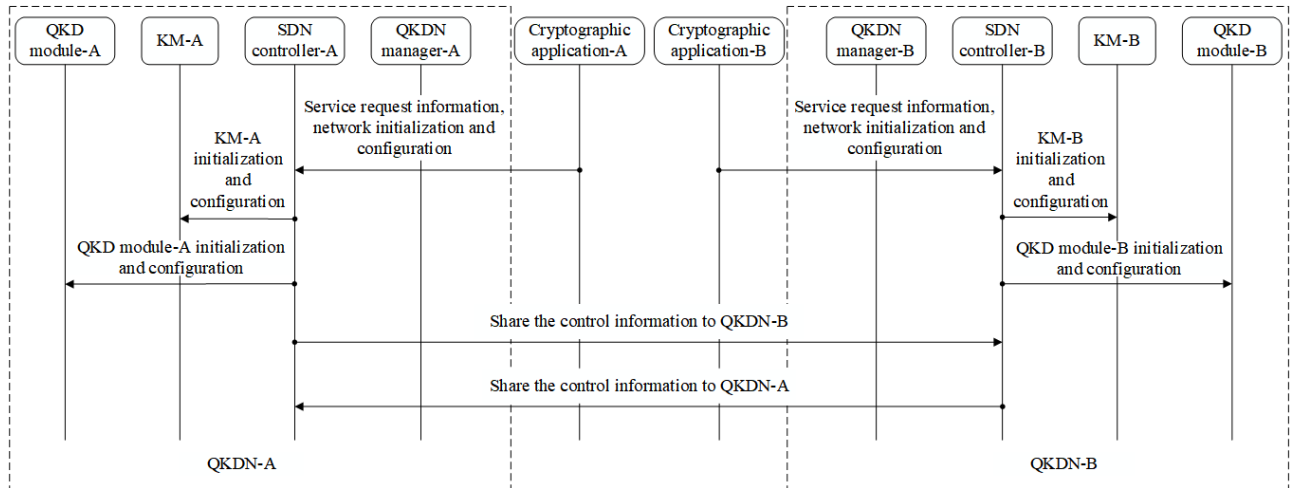


Figure 4 – An example of service provisioning and system initialization phase

Figure 4 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, the KM-A/B and QKD module-A/B to configure the two QKD networks from different QKDN providers. SDN controller-A connected with SDN controller-B to share the QKDN control information which is defined in [ITU-T Y.QKDN\_iwrq].

#### 10.1.2 Key generation and transfer phase

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

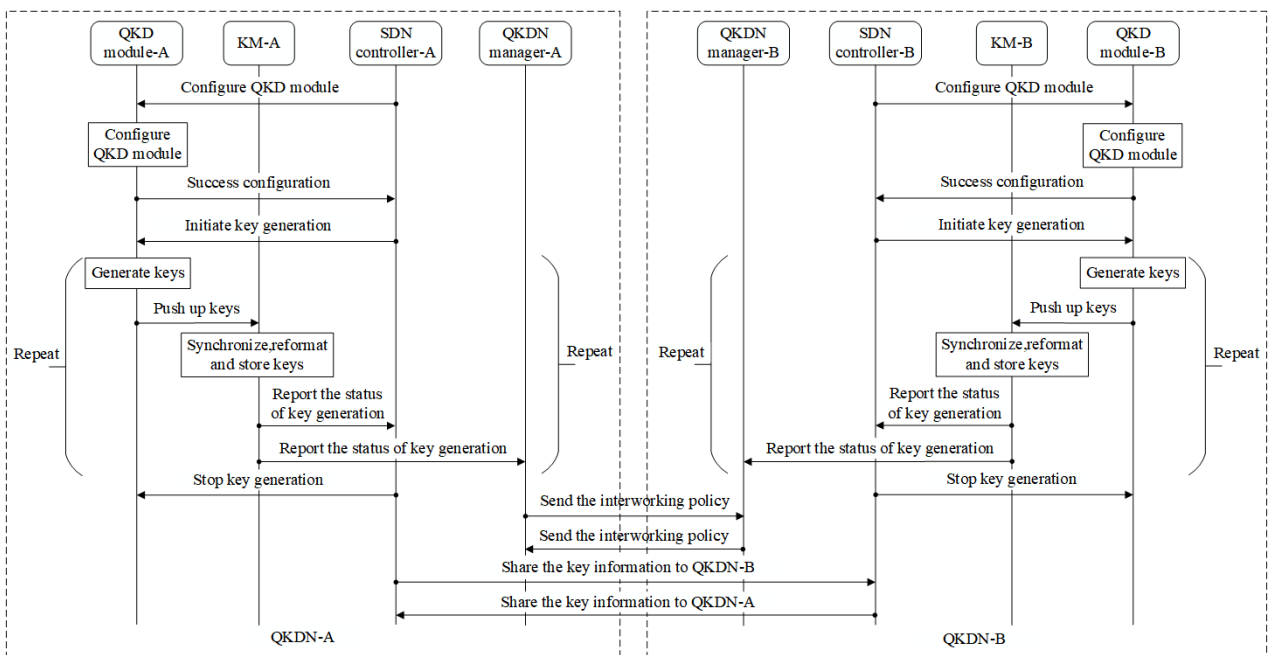


Figure 5 – An example of key generation and transfer phase

Figure 5 illustrates the procedures of SDN control for key generation with SDN technology. In the phase, the SDN-A/B controller firstly sends the configuration of the QKD module to the QKD module-A/B. After the QKD modules have been configured successfully, the SDN controllers send the initiation 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. The status of key generation is reported to both the SDN controllers and QKDN managers for future control and management requirements. After the keys are generated, QKD managers send the interworking policy to each other. SDN controller-A connected with SDN controller-B to share the key information which is defined in [ITU-T Y.QKDN\_iwrq].

### 10.1.3 Virtualization phase

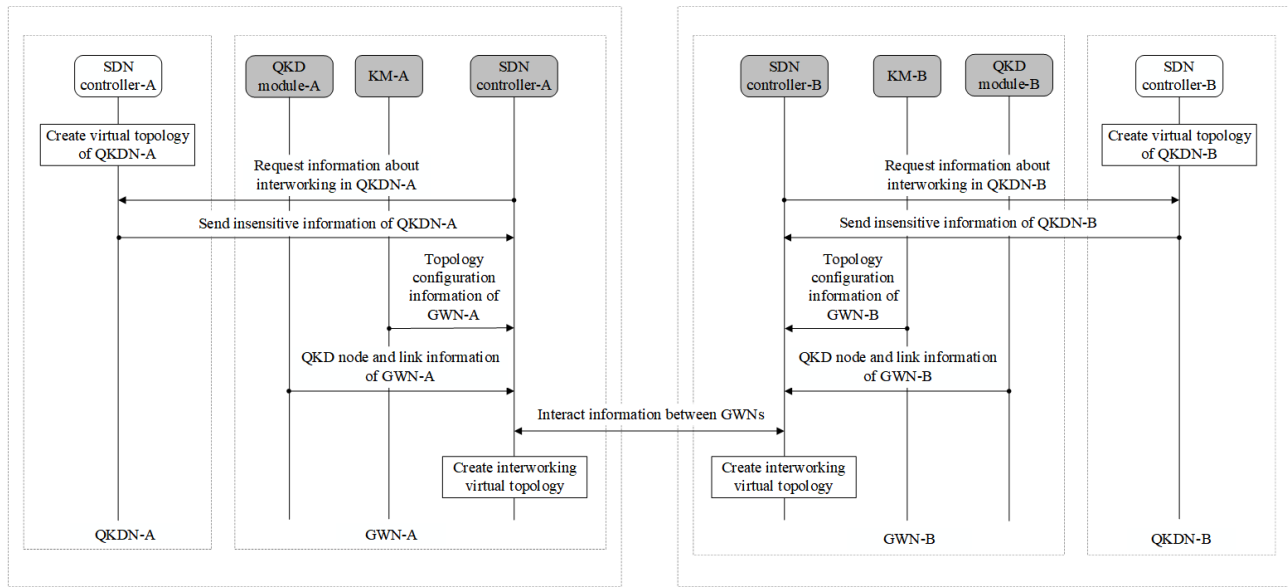


Fig. 1 An example of virtualization phase

Fig. 1 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. Next, The SDN 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, The SDN controller-A/B in GWNs create interworking virtual topology after interacting information between GWNs.

### 10.1.3.4 Key request, relay and supply phase

*Editor's note: The controlling aspects for key delivering of QKDNi should be further clarified.*

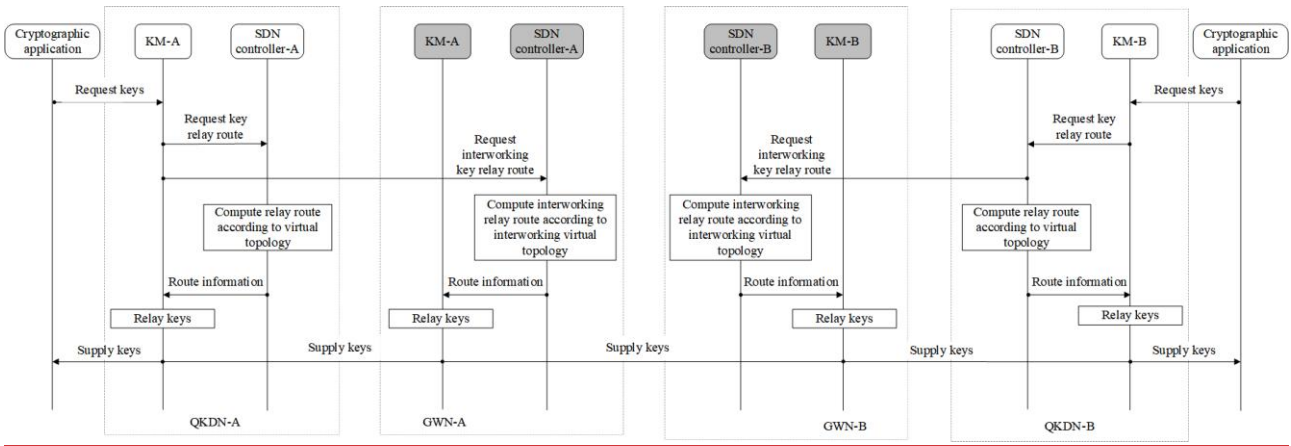


Fig. 2 An example of key request, relay and supply phase

Fig. 2 illustrates procedures of SDN control for key request, relay and supply between two QKDN providers with GWNs. A cryptographic application 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 will compute relay route and 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 keys to the requesting cryptographic application.

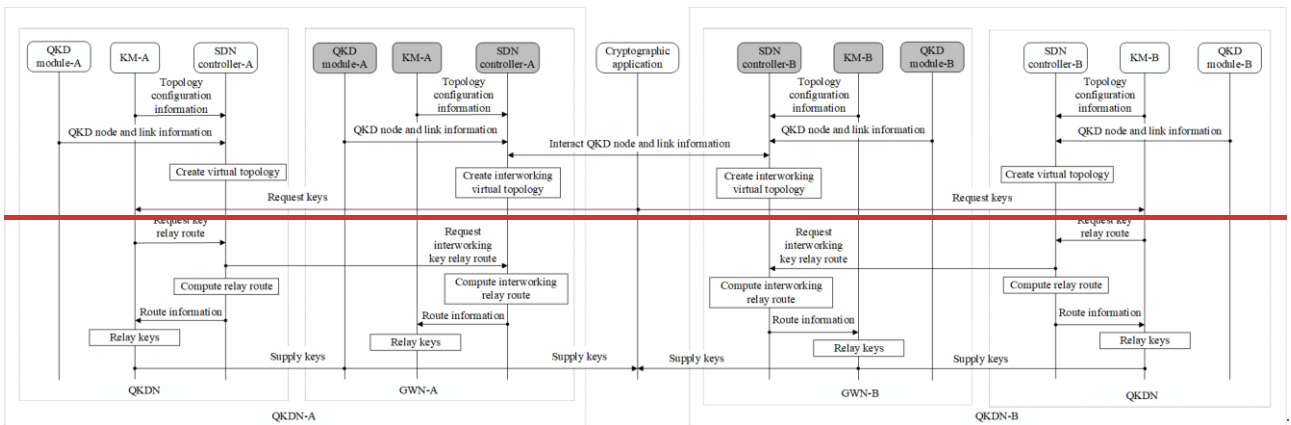


Figure 6—An example of key request, relay and supply phase

Figure 6 illustrates procedures of SDN control for key request, relay and supply between two QKDN providers with GWNs. Before the cryptographic application sends the key request, the SDN controller A/B creates virtual topology and interworking virtual topology. The SDN controller A/B collect topology configuration information from the KM A/B and the QKD node and link information from the QKD module A/B. Then, the SDN controller A/B in QKDN create the virtual topology based on the collected information. The SDN controller A/B in GWN create the interworking virtual topology after interact QKD node and link information with each other. A cryptographic application sends key request information to the KM A/B in QKDN. Then KM A/B request key relay route from SDN controller A/B in QKDN, and SDN controller A/B in QKDN request interworking key relay route from SDN controller A/B in GWN. Then the SDN controller A/B will compute relay route and 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 keys to the requesting cryptographic application.

## 11 Security considerations

*Editor's Note: General security perspective are addressed here for SDN control for the interworking, however, the details of security are outside of scope of this 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 V1.1.1 (2022-04), *Quantum Key Distribution (QKD); Orchestration Interface for Software Defined Networks.*
-