International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3805

(12/2021)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Quantum key distribution networks

Quantum key distribution networks – Software-defined networking control

Recommendation ITU-T Y.3805

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Computing power networks	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3599
BIG DATA	Y.3600–Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	**Y.3800–Y.3999**
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.3805

Quantum key distribution networks – Software-defined networking control

Summary

Recommendation ITU-T Y.3805 specifies the requirements, functional architecture, reference points, hierarchical SDN controller and overall operational procedures of SDN control.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3805	2021-12-06	13	11.1002/1000/14770

Keywords

Functional architecture, hierarchical, operational procedure, QKDN (Quantum Key Distribution Network), reference point, SDN (Software-defined networking), SDN controller.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.3805

Quantum key distribution networks – Software-defined networking control

1 Scope

This Recommendation specifies the requirements, functional architecture, reference points, hierarchical software-defined networking (SDN) controller and overall operational procedures of SDN control in quantum key distribution networks (QKDNs). The scope of this Recommendation covers:

– Requirements for SDN control in QKDNs;

– Functional architecture of SDN control in QKDNs;

– Reference points of SDN control in QKDNs;

– Hierarchical SDN controllers in QKDNs;

– Overall operational procedures of SDN control in QKDNs;

– Appendix I: use cases of SDN control in QKDNs;

– Appendix II: comparison of control methods between traditional QKDNs and SDN-based QKDNs;

– Appendix III: controllable elements for SDN in QKDNs.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.3300] Recommendation ITU-T Y.3300 (2014), *Framework of software-defined networking.*

[ITU-T Y.3800] Recommendation ITU-T Y.3800 (2019), plus Corrigendum 1 (2020), *Overview on networks supporting 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), *Quantum key distribution networks – Functional architecture.*

[ITU-T Y.3803] Recommendation ITU-T Y.3803 (2020), *Quantum key distribution networks – Key management*.

[ITU-T Y.3804] Recommendation ITU-T Y.3804 (2020), *Quantum key distribution networks – Control and management*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 key manager (KM) [ITU-T Y.3800]: A functional module located in a quantum key distribution (QKD) node to perform key management in the key management layer.

3.1.2 key management agent (KMA) [ITU-T Y.3802]: A functional element to manage keys generated by one or multiple quantum key distribution (QKD) modules in a QKD node (trusted node).

NOTE – KMA acquires keys from one or multiple QKD modules, synchronizes, resizes, formats, and stores them. It also relays keys through key management agent (KMA) links.

3.1.3 key supply agent (KSA) [ITU-T Y.3802]: A functional element to supply keys to a cryptographic application, being located between a key management agent (KMA) and the cryptographic application.

NOTE – Application interfaces for cryptographic applications are installed into the key supply agent (KSA). The KSA synchronizes keys, and verifies their integrity via a KSA link before supplying them to the cryptographic application.

3.1.4 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.

3.1.5 quantum key distribution module [ITU-T Y.3800]: A set of hardware and software components that implements cryptographic functions and quantum optical processes, including quantum key distribution (QKD) protocols, synchronization, distillation for key generation, and is contained within a defined cryptographic boundary.

NOTE – A QKD module is connected to a QKD link, acting as an endpoint module in which a key is generated. These are two types of QKD modules, namely, the transmitters (QKD-Tx) and the receivers (QKD-Rx).

3.1.6 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.

NOTE – A QKDN allows sharing keys between the QKD nodes by key relay when they are not directly connected by a QKD link.

3.1.7 quantum key distribution network controller [ITU-T Y.3800]: A functional module, which is located in a quantum key distribution (QKD) network control layer to control a QKD network.

3.1.8 quantum key distribution network manager [ITU-T Y.3800]: A functional module, which is located in a quantum key distribution (QKD) network management layer to monitor and manage a QKD network.

3.1.9 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.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

KM Key Manager

KMA Key Management Agent

KML Key Management Layer

KSA Key Supply Agent

QKD Quantum Key Distribution

QKDN Quantum Key Distribution Network

QL Quantum Layer

SDN Software-Defined Networking

5 Conventions

In this Recommendation:

The phrase "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 phrase "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

Quantum key distribution (QKD) technology has been ready for practical use in existing and future communications and security infrastructures. [ITU-T Y.3800] gives an overview on networks supporting QKD; [ITU-T Y.3801] specifies functional requirements for the quantum layer, key management layer, QKDN control layer and QKDN management layer; [ITU-T Y.3802] specifies the functional architecture of QKDNs); [ITU-T Y.3803] specifies the key management of QKDNs. In QKDNs, network control is one of the most important fundamental functions, and [ITU-T Y.3804] specifies the control and management functions for QKDNs.

As one of the most promising control technologies, software defined networking (SDN) ([ITU-T Y.3300]) has several advantages in traditional communication networks. On the one hand, SDN controller supports centralized, programmable and hierarchical control; on the other hand, it can provide fast services for applications by opening northbound interfaces between the control layer and service layer. The change of control method by SDN in QKDN provides an alternative method to realize control functionalities by introducing logically centralized and programmable control of network resources through standardized interfaces and protocols. [b-ETSI GS QKD 015] provides an alternative solution to realize SDN control in QKDNs. The abstraction models and workflows between an SDN-enabled QKD node and the SDN controller are specified, including resource discovery, capabilities dissemination and system configuration operations. In addition, the YANG-structured information is defined as a base or core model for the integration of QKD technologies in operator's management architectures.

The considerations of introducing SDN into QKDNs are as follows:

– The SDN-based centralized control helps to collect the overall information of a QKDN independent of whether it is distributed or not. It is helpful to improve the performance monitoring and routing decision.

– The tunable components of QKDN (e.g., tunable laser and tunable optical switch) can be programmed and controlled dynamically by an SDN controller with southbound interfaces.

For example, a tunable optical switch can be controlled dynamically by an SDN controller to construct different quantum channels between different nodes.

– SDN supports hierarchical control in a large scale QKDN consisting of multiple, logical sub-QKDNs. Under such scenarios, the implementation of the controller for each sub-QKDN is independent of others, which makes QKDN control much easier. One upper layer controller is in charge of several lower layer controllers.

– By opening the northbound interface, which is defined as the application-control interface ([ITU-T Y.3300]) used for interactions between the service layer and the SDN control layer in QKDN, SDN can provide fast service provisioning for the customers. The overall operational procedures and its advantages are described in the clause 11 of this Recommendation.

– SDN supports QKDN virtualization that combines physical QKDN resources and QKDN functionality into a single software-based administrative entity, a virtual QKDN, according to different demands of specific customers or applications. With the programmability and controllability of southbound interfaces, it enables the creation of logically isolated network partitions over shared physical QKDNs and realizes QKDs in the network partitions by sharing the same resources in an efficient way.

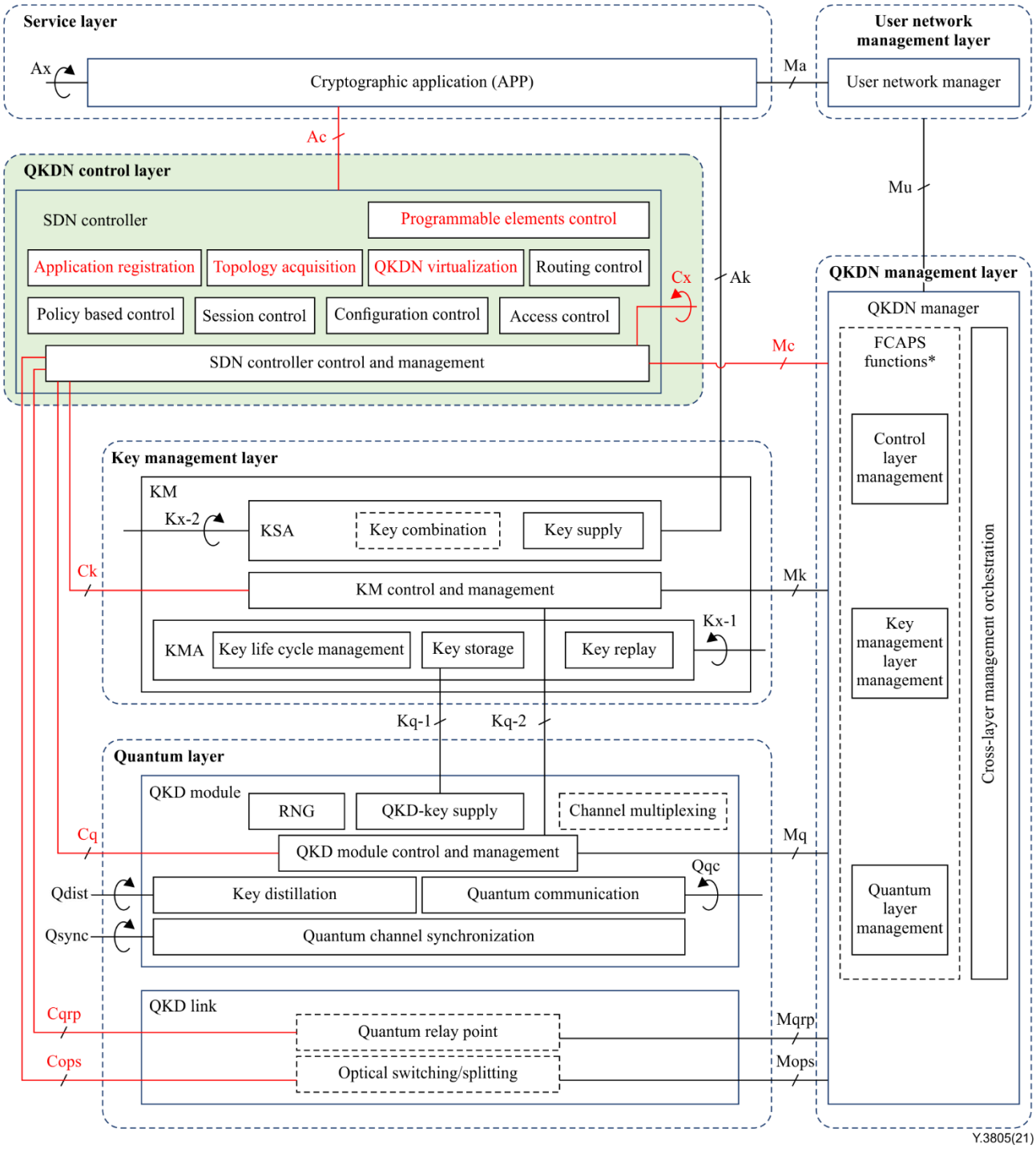
NOTE – The QKDN resources that can be virtualized include QKDN topology (nodes and links) and QKD-key resources.

7 Requirements for the SDN controller in the QKDN control layer

The requirements for the QKDN control layer are defined in [ITU-T Y.3801], and this Recommendation specifies the requirements for the SDN controller in the QKDN control layer.

1. The SDN controller is required to support the ability of application registration in QKDNs, which enables the fast provisioning of cryptographic applications in the service layer. The SDN controller makes decisions on whether to provide keys for cryptographic applications.
2. The SDN controller is required to support the ability of acquiring and updating network topology information from quantum layer or SDN child controllers (in a hierarchical SDN control architecture).
3. The SDN controller is recommended to support the ability of QKDN programmable element control when the QKDN consists of programmable elements in the quantum layer.
4. The SDN controller is recommended to support the ability of QKDN virtualization, which enables the creation of logically isolated network partitions over physical QKDNs.
5. The SDN controller is recommended to support the ability of communication among multiple SDN controllers which enable hierarchical SDN control.

8 Functional architecture for SDN control in QKDN



Note: * FCAPS represents fault, configuration, accounting, performance and security management

Figure 1 – Functional architecture for SDN control in QKDN

Based on the conceptual structure and functional architecture model for QKDNs defined in [ITU-T Y.3800] and [ITU-T Y.3802], respectively, the functional architecture for SDN control in QKDN is specified in Figure 1. The detailed description of functional elements as well as the reference points are given in [ITU-T Y.3800] and [ITU-T Y.3802], and this Recommendation specifies SDN related functional elements in QKDNs.

– Quantum layer: the functional elements in the quantum layer including the QKD link and QKD module are enabled to communicate with the SDN controller conveniently. The parameters of the QKD link and QKD module such as key generation rate, transition power and receive power could be adjusted by the SDN controller in the QKDN control layer.

– Key management layer: the functional elements in the key management layer the including key management agent (KMA) and key supply agent (KSA) exchange control and management messages with the SDN controller.

NOTE – With SDN technology, the QKD key can be virtualized and stored in the virtual QKD key storage entities to enhance the key management.

– QKDN control layer: the functional element in the QKDN control layer is the SDN controller. It controls the variable resources to ensure the secure, stable, efficient and robust operation of the QKDN. The functions of the SDN controller include application registration, topology acquisition, QKDN virtualization, programmable element control, routing control, policy-based control, session control, configuration control and access control. In addition, unlike traditional QKDN controllers, SDN controllers have northbound interfaces between the service layer and the QKDN control layer. The SDN controller opens northbound interfaces to cryptographic applications in the service layer, which enables fast service provisioning for applications in QKDN.

– Service layer: the cryptographic applications in the service layer are to utilize the key pairs provided by the QKDN and perform encrypted communication between remote parties. The cryptographic applications could be initialized and provided by the SDN controller with its northbound interface. Three typical cryptographic applications in the service layer are point-to-point applications, point-to-multipoint applications and multipoint-to-multipoint applications.

– QKDN management layer: the elements in the QKDN management layer communicate with the SDN controller to obtain configuration and management information.

– User network management layer: the user network management layer function is the same as that described in [ITU-T Y.3802].

9 Reference points

Most of the reference points in Figure 1 have been defined in [ITU-T Y.3802], and this Recommendation defines the newly added one and presents the existing ones related to SDN.

NOTE – When the SDN controller is involved in interaction with other QKDN elements, the existing reference points in [ITU-T Y.3802] are used. The new, extended functions of SDN control are implemented by extending the interaction information of reference points.

The newly added reference point is:

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

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

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

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

– **Cops**: a reference point connecting the SDN controller control and management function in the SDN controller with an optical switching/splitting function in a QKD link. It is responsible for the SDN controller to communicate control information on optical switching/splitting with the QKD link.

– **Cqrp**: a reference point connecting the SDN controller control and management function in the SDN controller with a quantum relay point function in a QKD link. It is responsible for the SDN controller to communicate control information on quantum relay point with the QKD link.

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

– **Cx**: reference point connecting two SDN controller control and management functions. It is responsible for the communication of control information between the two SDN controllers.

10 Hierarchical SDN controller in QKDNs

Clause 8 describes the basic functional architecture for SDN control in QKDNs. However, in certain scenarios, only a single SDN controller is unsuitable for overall control in QKDNs, and a hierarchical SDN controller could be adopted. Figure 2 illustrates a hierarchical SDN controller in a QKDN. Under such a scenario, SDN controllers are organized in a hierarchical way, and the functions and implementations of each SDN controller are independent of each other. The hierarchical controller is responsible for service provisioning within its control range. SDN controller of each layer has its northbound interface to communicate with the service layer, and the first layer has a southbound interface for controlling the controllable elements and collecting information from the key management layer and quantum layer. Most of the reference points in Figure 2 have been defined in clause 9, and this Recommendation only describes the newly added and updated ones.

– **Ac-x**: reference point between cryptographic application and the x_{th} layer SDN controller under hierarchical SDN control scenarios. It is responsible for service provisioning of network applications using the x_{th} layer SDN controller.

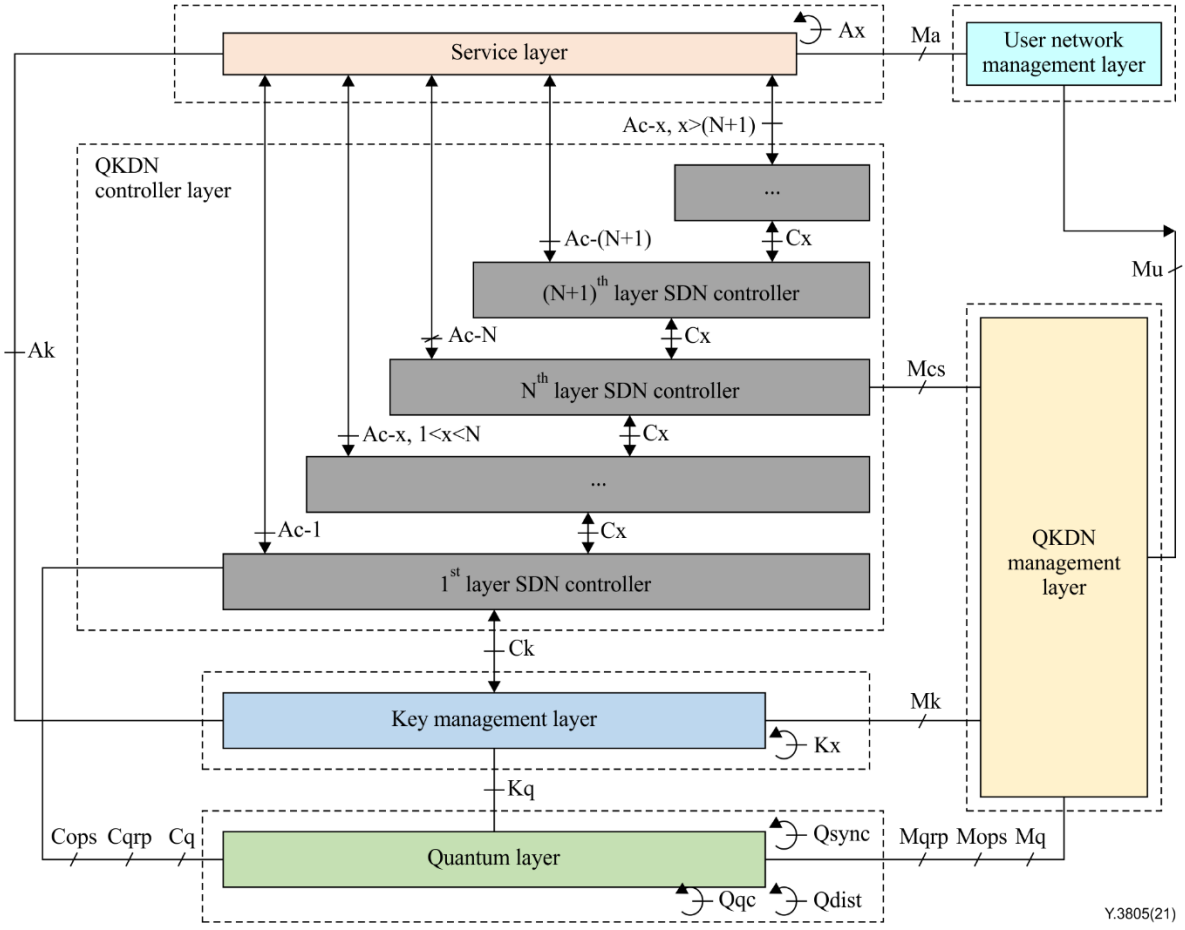


Figure 2 – A hierarchical SDN controller in a QKDN

For example, in a large scale QKDN as illustrated in Figure 3, each sub-QKDN could develop their 1st layer SDN controller that is able to control elements in the sub-QKDN through southbound interfaces. The 2nd layer SDN controller could be developed to take charge of the 1st layer SDN controllers and the 3rd layer SDN controller could be developed to take charge of the 2nd layer SDN controllers. Here, we consider three kind of services: 1) for provisioning the **service within sub-QKDN A**, it only needs to operate the 1st layer SDN controller C_A; 2) for provisioning the **service across sub-QKDN A and B**, it needs to operate the 2nd layer SDN controller C_{AB} which controls the 1st layer SDN controller C_A and C_B; 3) for provisioning the **service across sub-QKDN A and D**, it needs to operate the 3rd layer SDN controller which controls the 2nd layer SDN controller C_{AB} and C_{CD}.

NOTE – Different sub-QKDNs in a large scale QKDN can be implemented by multiple vendors but are provided by the same administrative authority. The first layer SDN controllers control different sub-QKDNs, and the higher layer SDN controller is responsible for the inter sub-QKDN cooperation and SDN controller orchestration.

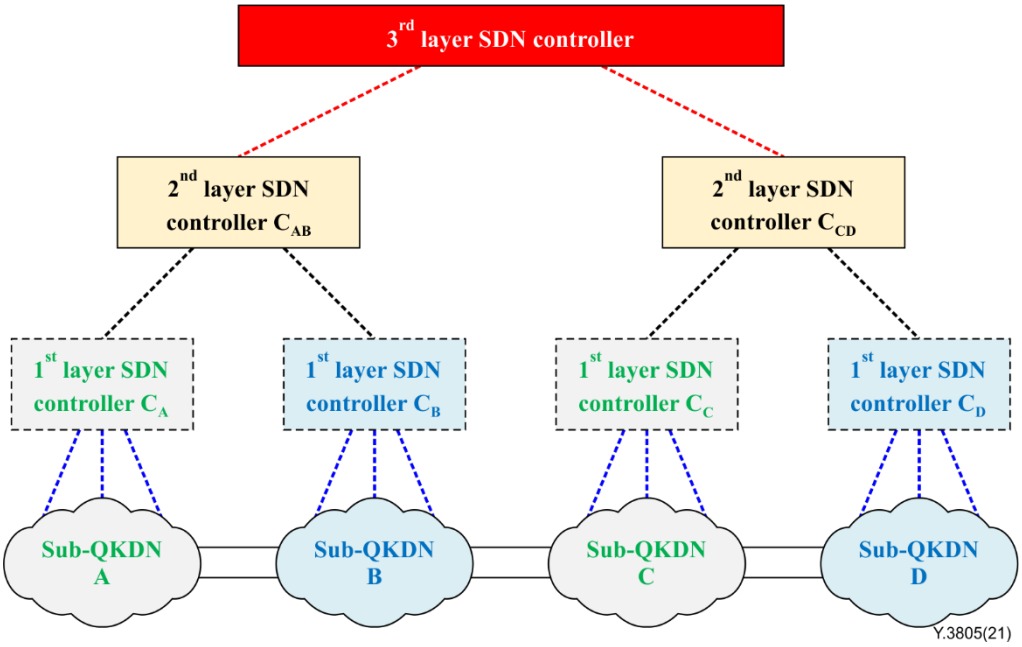


Figure 3 – Hierarchical SDN control in a large scale QKDN

11 Overall operational procedures of SDN control in QKDNs

Unlike other traditional operational procedures of QKD network functions without SDN control, the operational procedures of SDN control in QKDN reduce the time for provisioning different services using SDN control by skipping the QKDN manager. The SDN controller can also provide more efficient key resource utilization by deciding the end of key generation and controlling the management monitor in a global view. In addition, the SDN technology improves the flexibility of service provisioning and provides services for applications in a fast way by opening the northbound interface between the QKDN control layer and the service layer. Based on the functional architecture for SDN control defined in clause 8, this clause describes the overall operational procedures of SDN control in QKDN.

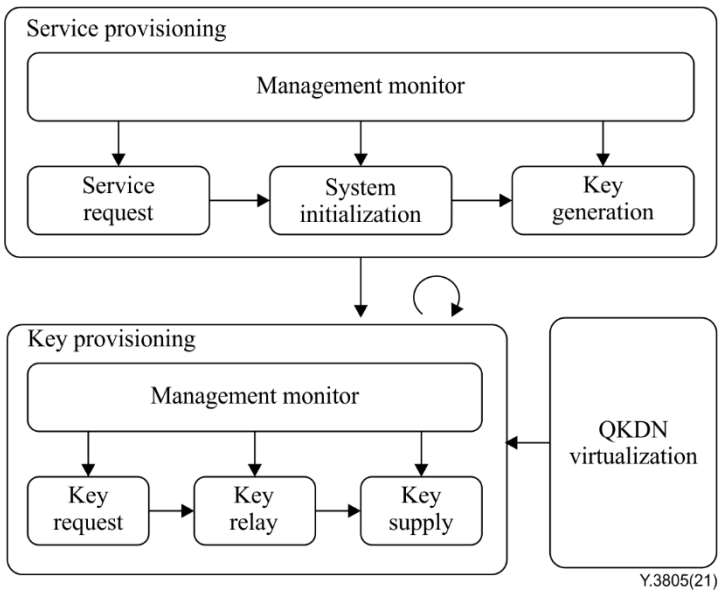


Figure 4 – The overall operational procedures of SDN control in a QKDN

The relationship of the overall operational procedures of SDN control in a QKDN is shown in Figure 4. There are two high-level modes in the overall operational procedures: service provisioning mode and key provisioning mode. When a service request arrives, the QKDN enters the service provisioning mode. The system is initialized, and quantum keys are generated under the control of the SDN controller. When a key request arrives, the QKDN enters the key provisioning mode, the key request, relay and supply phase decide the route information by using the SDN controller and the supplied keys are pushed up for the key request. At the same time, the real-time network monitoring operation is performed to collect and monitor all the QKD links in the service provisioning phase and analyse the status of keys in the key provisioning phase with the global view provided by the SDN controller. The QKDN virtualization is the function that can construct multiple logical QKDNs on a physical QKDN. The implementation of QKDN virtualization needs the support of "key provisioning", so that it remaps the virtual resources and physical QKDN resources to efficiently meet the demands of specific services or applications. Apart from these, a control action procedure is specified, which includes hierarchical SDN control associated with QKDN management. The overall typical operational procedures include those described below.

11.1 Normal operation mode: Service request and system initialization phase

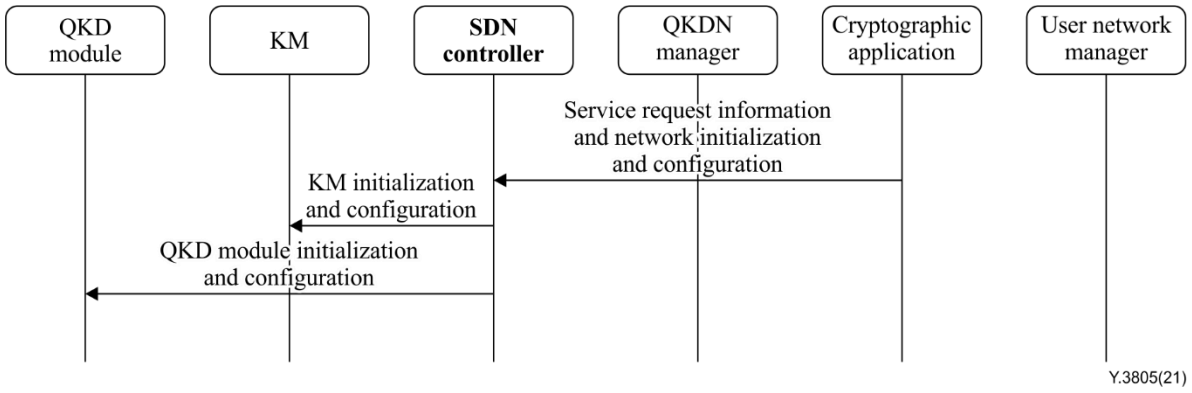


Figure 5 – An example of service provisioning and system initialization phase

Figure 5 illustrates procedures of SDN control for service request and system initialization with SDN technology. In this phase, the cryptographic application in the service layer directly provides service

request information and network initialization and configuration to the SDN controller, without providing information to the QKDN manager. Then the SDN controller initiates the QKDN controller, the KM and QKD module to configure the QKD network.

11.2 Normal operation mode: Key generation phase

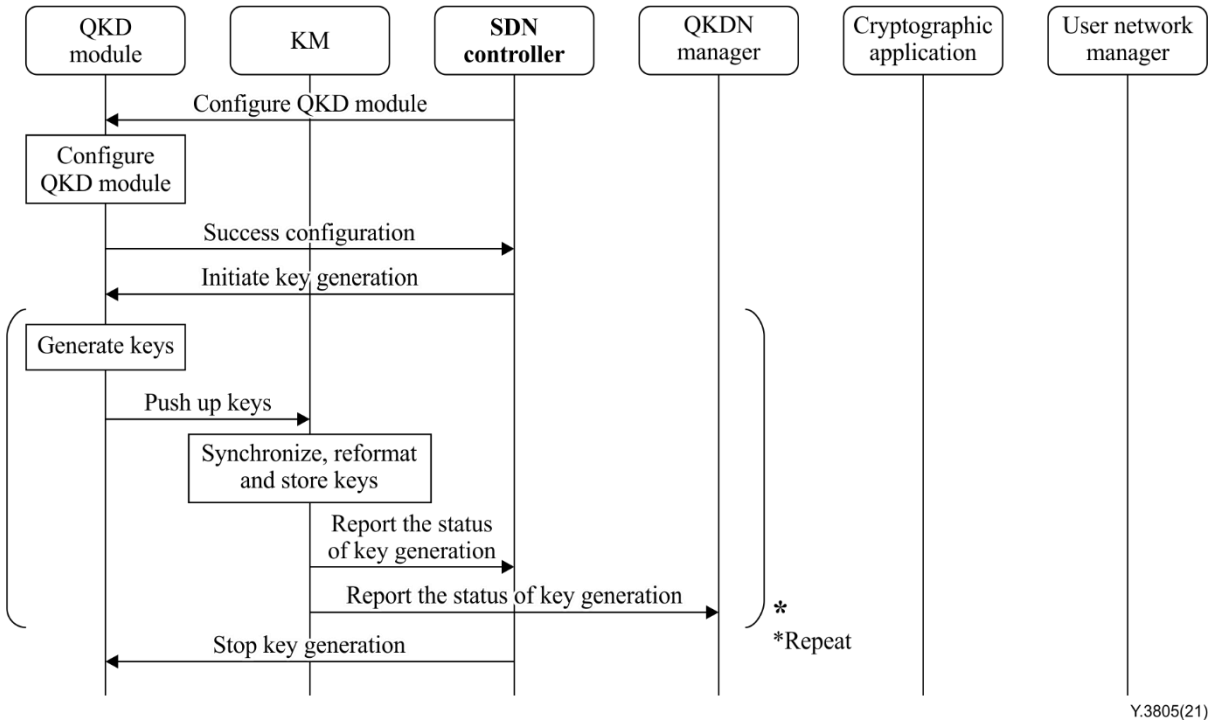


Figure 6 – An example of a key generation phase

Figure 6 illustrates the procedures of SDN control for key generation with SDN technology. In the phase, the SDN controller firstly sends the configuration of the QKD module to the QKD modules. After the QKD modules have been configured successfully, the SDN controller sends the initiation of the key generation to the QKD module directly. Then, the physical key generation procedures are repeated until the SDN controller sends the instruction to stop them. The status of key generation is reported to both the SDN controller and QKDN manager for future control and management requirements.

11.3 Normal operation mode: Key request, relay and supply phase

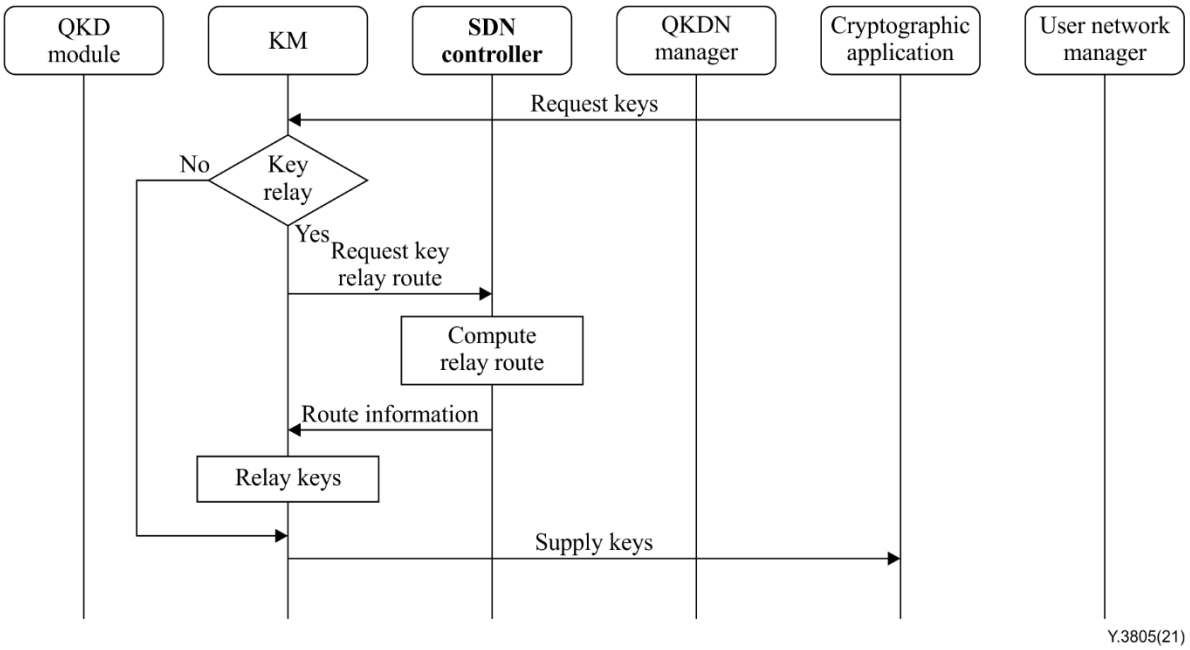


Figure 7 – An example of key request, relay and supply phase

Figure 7 illustrates procedures of SDN control for key request, relay and supply. A cryptographic application in the user network sends key request information to the KM in the QKD network. Then KM checks the need to relay keys to the SDN controller. If it needs to relay keys for service provisioning, the SDN controller will compute the relay route and decide the routing information. Based on the routing information, the KM initiates the key relay procedures between the originating QKD node and the destination QKD node and executes key relay according to the control by the SDN controller; if it does not need key relay, the KM supplies keys to the requesting cryptographic application directly. Finally, the KM pushes up keys to the requesting cryptographic application.

11.3.1 A key relay control procedure including hierarchical SDN control

A key relay control procedure including multiple sub-QKDN hierarchical SDN control is shown in Figure 8.

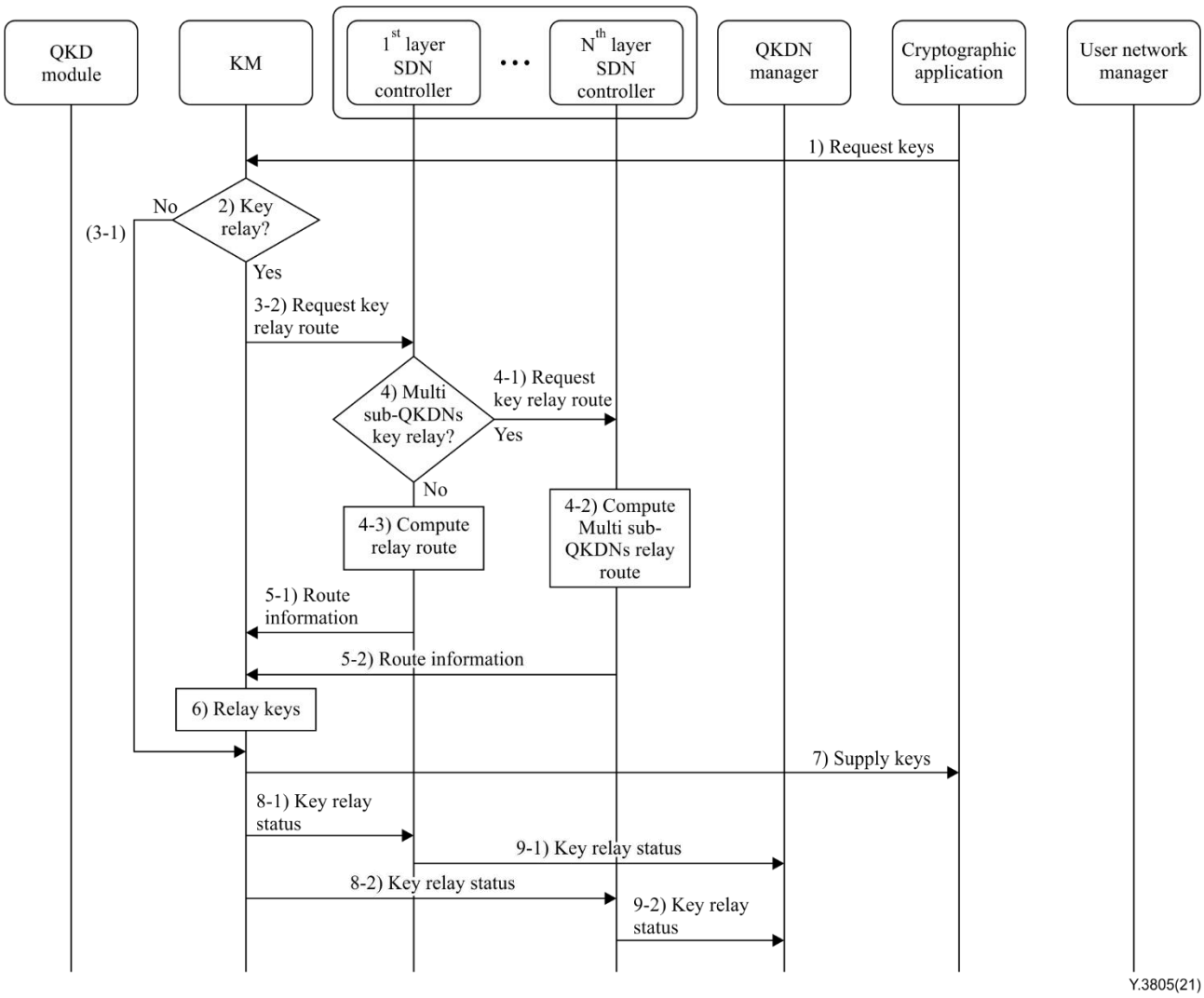


Figure 8 – An example of a key relay procedure including hierarchical SDN control

1) A cryptographic application makes a key request to the KM.

2) The KM checks if a key relay is needed.

3-1) If not, then a key is supplied via the KM to the application.

3-2) If yes, the KM then sends the key relay request to the SDN controller.

4) The SDN controller checks whether multiple sub-QKDN key relay is needed.

4-1) If not, it computes a relay route for a QKDN.

5-1) The computed relay route is sent to the KM.

4-2) If yes, the N^{th}-layer SDN controller computes multiple sub-QKDN key relay routes with support of underlying layer's SDN controllers.

5-2) The computed multiple sub-QKDN relay route is sent to the KM.

6) The KM then relays keys on the computed relay route.

7) The KM also supplies keys to the cryptographic application.

8-1) The status of the key relay is reported to the 1^{st}-layer SDN controller for logging purposes.

9-1) The status of the key relay is reported to the QKDN manager for logging purposes.

8-2) The status of the key relay is reported to the N^{th}-layer SDN controller for logging purposes.

9-2) The status of the key relay is reported to the QKDN manager for logging purposes.

11.3.2 A key relay rerouting procedure including hierarchical SDN control

A key relay rerouting procedure including multiple sub-QKDN hierarchical SDN control is shown in Figure 9.

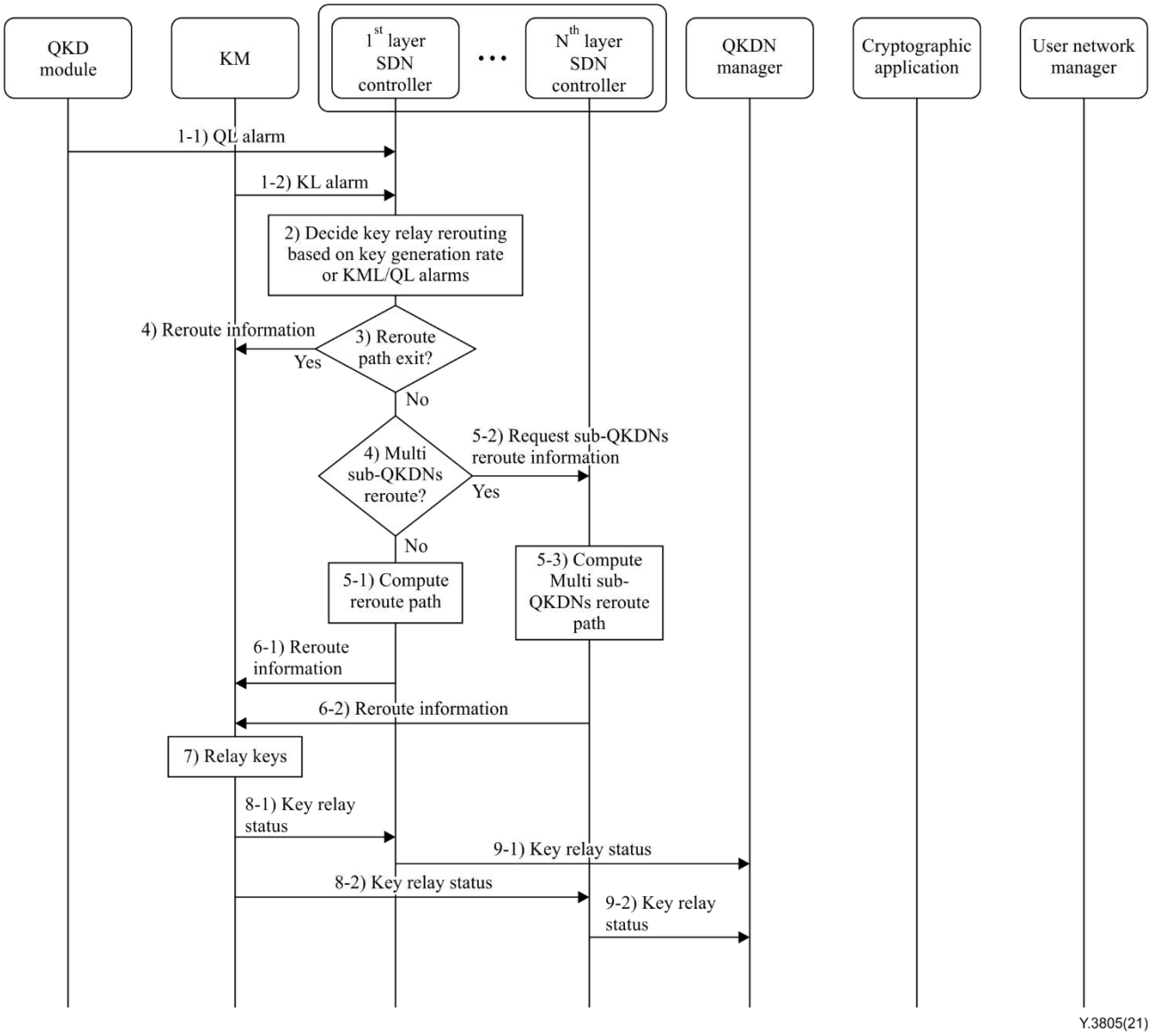


Figure 9 – An example of a key relay rerouting procedure including hierarchical SDN control

1-1) The SDN controller receives alarms from a quantum layer (QL) such as a quantum channel failure.

1-2) The SDN controller receives alarms, such as key generation rate falling below a defined threshold, from a key management layer (KML).

2) The SDN controller decides whether key relay rerouting is needed due to the alarms received.

3) If a reroute path for the failure exists, it returns the information to the KM for rerouting.

4) If not, it checks whether a reroute path involves multiple sub-QKDN route computation.

5-1) If not, it computes a QKDN reroute path.

6-1) Then it returns the computed reroute path to the KM.

5-2) If yes, it requests multiple sub-QKDN reroute path computation to the N^{th}-layer SDN controller.

5-3) The N^{th}-layer SDN controller computes the reroute path with the support of the underlying layer's SDN controllers.

6-2) Then it returns the computed reroute path to the KM.

7) The KM then relays keys on the computed relay route.

8-1) The status of the key relay is reported to the 1^{st}-layer SDN controller for logging purposes.

9-1) The status of the key relay is reported to the QKDN manager for logging purposes.

8-2) The status of the key relay is reported to the N^{th}-layer SDN controller for logging purposes.

9-2) The status of the key relay is reported to the QKDN manager for logging purposes.

11.4 Normal operation mode: Management monitor phase

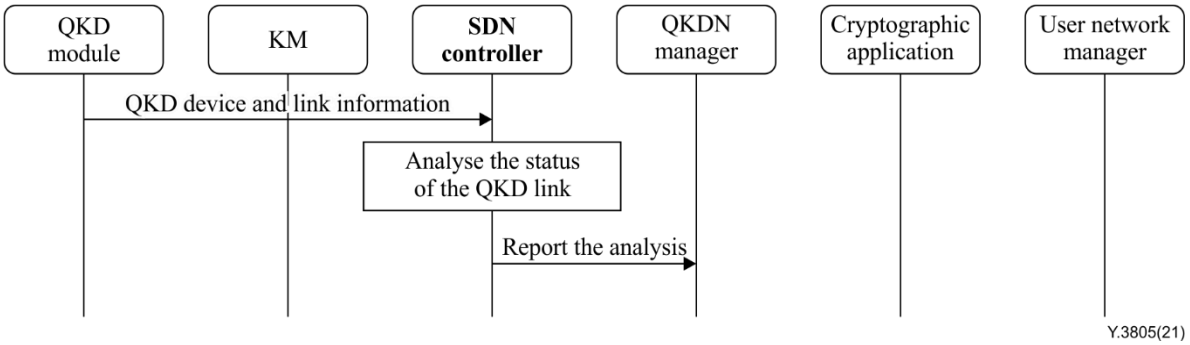


Figure 10 – An example of management monitor phase in the service provisioning mode

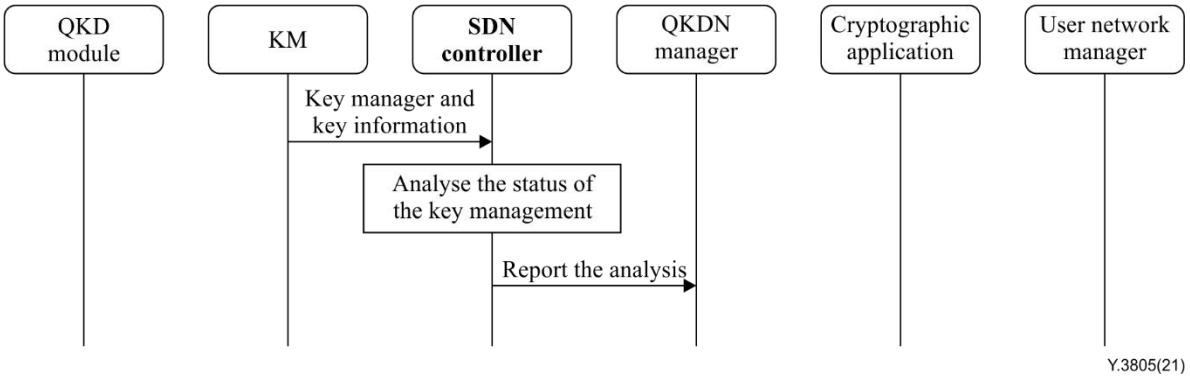


Figure 11 – An example of management monitor phase in the key provisioning mode

Figure 10 and Figure 11 illustrate the procedures for management monitor with the SDN controller. In the service provisioning mode, the QKD device and link information are sent to the SDN controller through its south interface. In the key provisioning mode, the SDN controller collects the key manager and key information from the KM. The status of the QKD link and key management are analysed by the SDN controller. Then the SDN controller reports the analysis to the QKDN manager.

11.5 Normal operation mode: QKDN virtualization phase

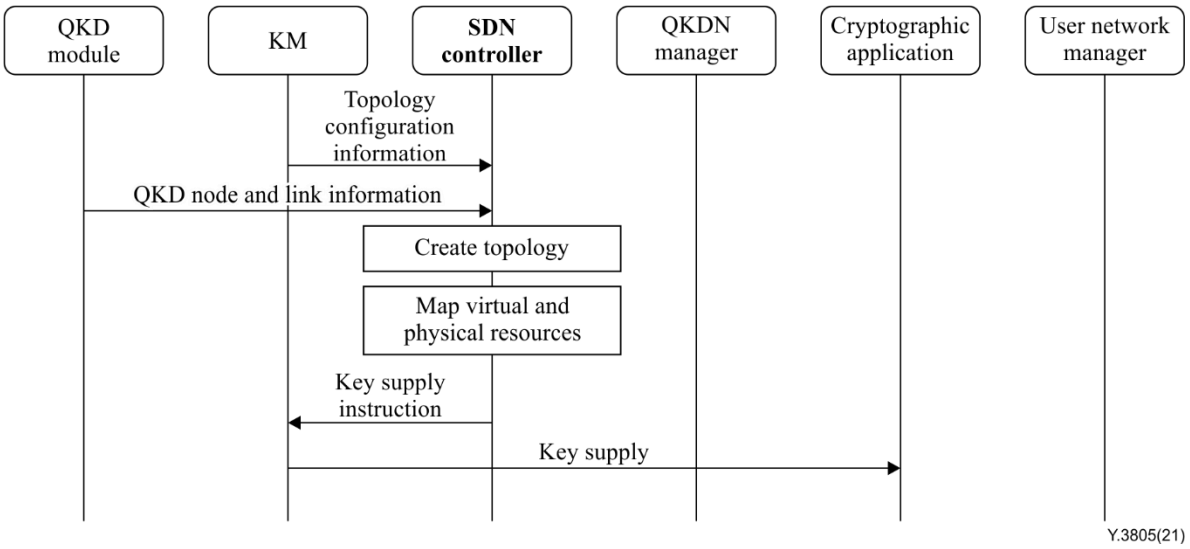


Figure 12 – An example of QKDN virtualization phase

Figure 12 illustrates the procedure of SDN control in the QKDN virtualization phase. First of all, the SDN controller uses the southbound interfaces to collect topology configuration information from the KM and the QKD node and link information from the QKD module. Then, the SDN controller creates the virtual topology based on the collected information. To meet the demand of specific services or applications, the SDN control maps the virtual and physical QKDN resources. Finally, the SDN controller sends the key supply instruction to the KM and the KM supplies keys to the cryptographic application.

11.6 A control action procedure including hierarchical SDN control associated with QKDN management

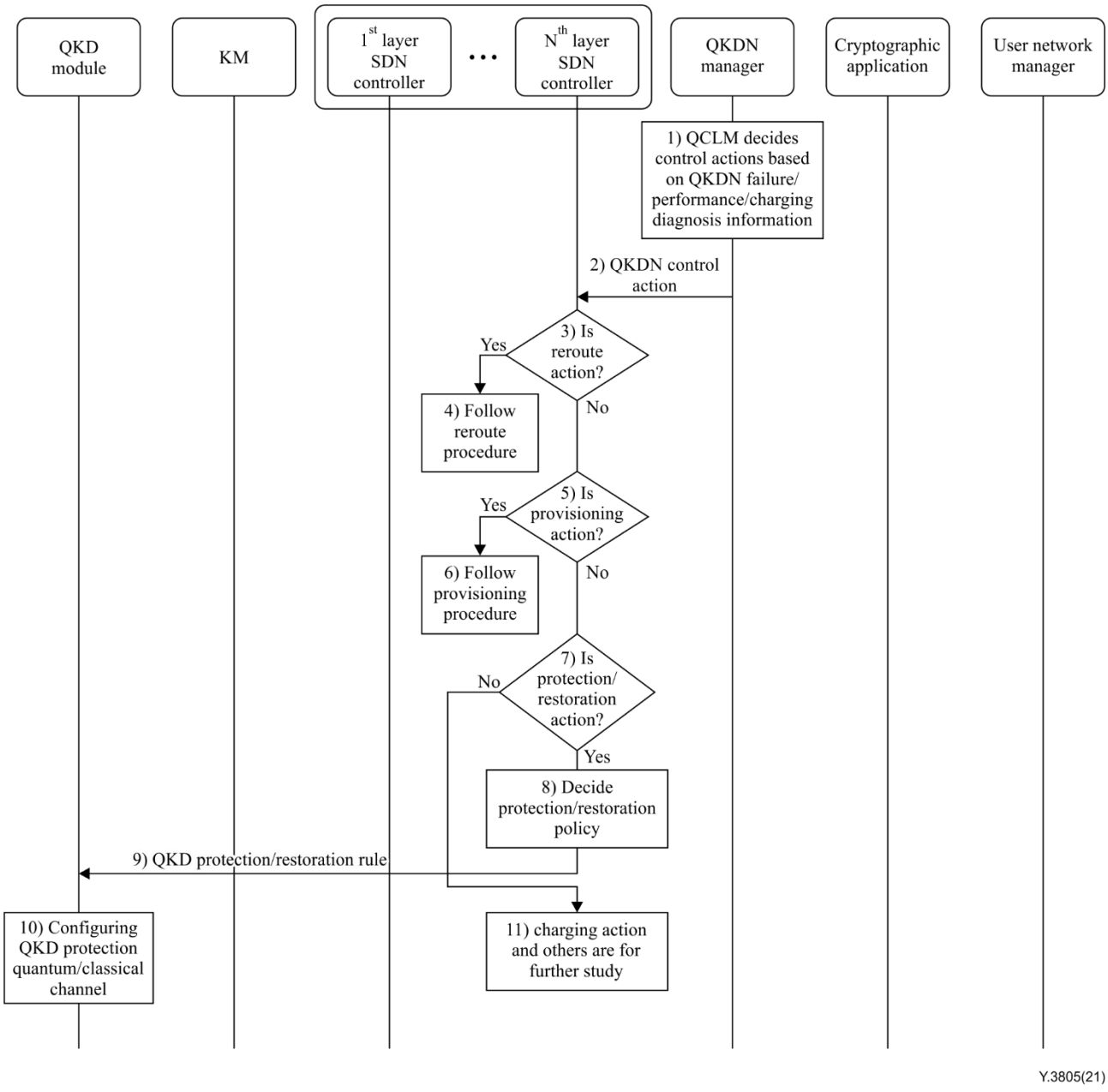


Figure 13 – An example of a QKDN control action procedure including hierarchical SDN control associated with QKDN management

A control action procedure including hierarchical SDN control associated with QKDN management is shown in Figure 13.

1) The QKDN manager decides QKDN control actions based on various factors: QKDN failure, performance degradation and charging policy.
2) The QKDN manager then sends the determined QKDN control action information.
3) The SDN controller checks if the action is a key relay reroute control action.
4) If yes, it invokes the reroute procedure.
5) The SDN controller further checks if the control action type is provisioning action.
6) If yes, the SDN controller invokes the provisioning procedure.

7) The SDN controller further checks if the control action type is protection/restoration action.

8) The SDN controller decides a protection and restoration policy based on the information received from the QKDN manager.

9) The SDN controller then sends the protection/restoration action rules to the QKD module. If the protection/restoration involves multiple sub-QKDNs, the SDN controller orchestrates protection/restoration.

10) The QKD module (or multiple QKD modules if multiple sub-QKDNs are involved) configures protection channels based on the received action rules.

11) If the control action types are others, including charging control action, the detailed control procedure needs to be further defined.

12 Security considerations

In SDN-control-based QKDNs, the security of the SDN controller is very important. On the one hand, the authority for the SDN controller should be well designed; on the other hand, the control channel of the SDN controller could be encrypted with QKD keys provided by the QKDN itself. Also note that the compatibility between the SDN controller and other controllers should be considered. Details are outside the scope of this Recommendation. Apart from that, security requirements described in [ITU-T X.1710], [ITU-T Y.3801] and [ITU-T Y.3802] and general network security requirements and mechanisms in IP-based networks described in [ITU-T Y.2701] and [ITU-T Y.3101] are recommended to be applied. Details are outside the scope of this Recommendation.

Appendix I

Use cases of SDN control in QKDNs

(This appendix does not form an integral part of this Recommendation.)

The following paragraphs describe several potential use cases for SDN control in QKDN.

– **Data centres**

With the rise of cloud services, data centres will become assets of enterprise competition, and their data security issues are receiving more and more attention. By combining SDN and QKDNs, the SDN-based centralized network control mode is adopted, and each data centre is provided with a QKD node, specifically including QKD devices and a KM. Routing relay between data centres, the configuration of key management services and QKD devices is the responsibility of the QKDN controller. The QKDN controller utilizes the advantages of centralized SDN control to efficiently manage the key resources of each data centre node and provide an open interface for third-party applications, which can greatly improve the security of data transmission and meet the requirements of service encryption between different data centres, as shown in Figure I.1.

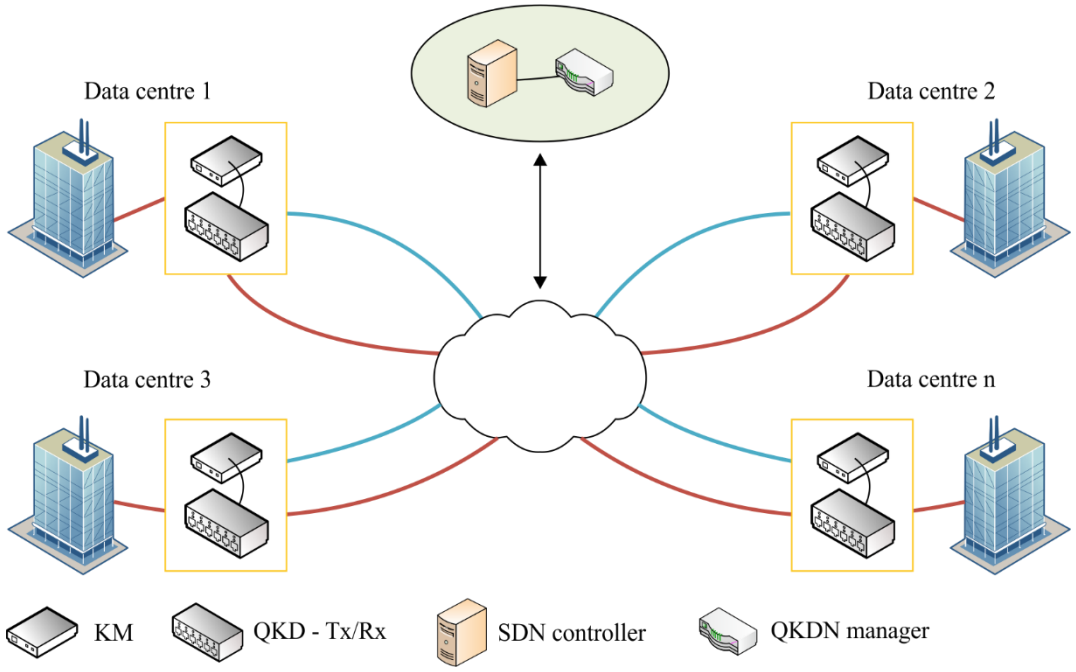


Figure I.1 – Data backup in data centres

– **Enterprise private networks**

Enterprises or government agencies usually require communication services to provide a high degree of confidentiality and authenticity, including the mandatory use of dedicated security systems. The QKDN controller can utilize the features of centralized SDN control to globally manage key information such as key resources, QKD devices and routing policies of different private networks. The SDN controller in QKDNs performs key resource allocation, rerouting and key generation among user nodes more quickly and efficiently. Thereby the secure key distribution of the enterprise private network is realized, as shown in Figure I.2.

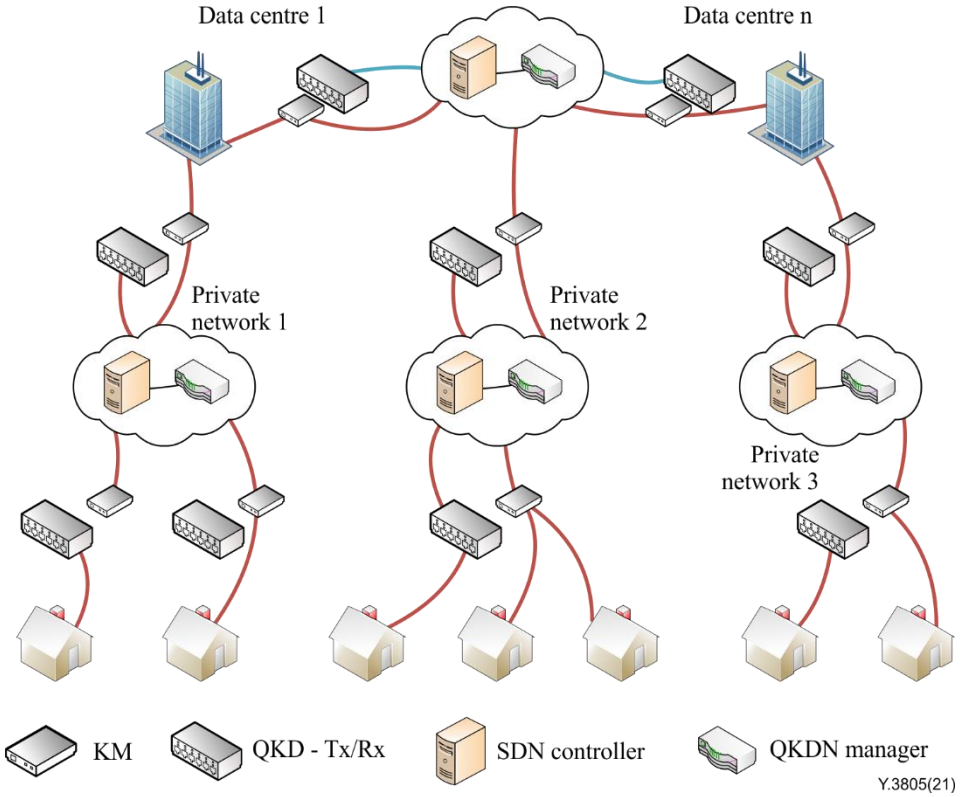


Figure I.2 – QKD private network

– **Backbone networks**

At present, the backbone network nodes communicate with each other through optical fibres, and the technology of quantum signal and classical optical signal co-fibre transmission is gradually maturing, which provides a good infrastructure for the layout of QKD systems. Each node of a backbone network is equipped with QKD nodes, including QKD modules and a KM. Using an SDN-based centralized network control mode, the SDN controller can control the key resources, topology, routing and other information of each node in the backbone network. When a link fault occurs, the key requirements between nodes can be guaranteed through rerouting, as shown in Figure I.3.

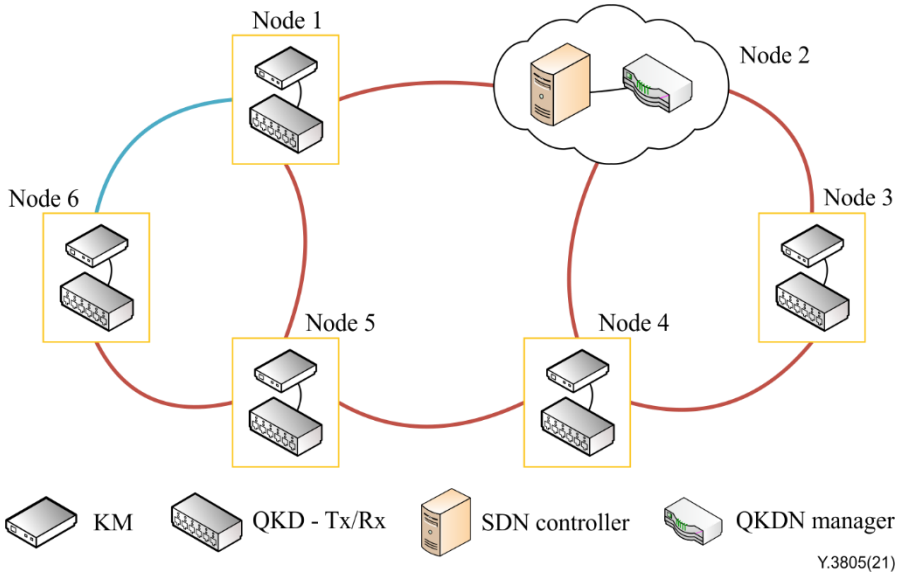


Figure I.3 – QKD backbone network

– **Access networks**

Each optical network unit (ONU) receives all downlink signals of the optical line terminal (OLT). Therefore, encryption measures must be used to prevent an ONU from eavesdropping on unsuitable content. By combining an SDN and a QKDN, each ONU is equipped with QKD nodes, including QKD devices and a KM, the OLT is equipped with an SDN controller and QKDN manager, using the centralized network control mode to achieve one-to-many QKD. Utilizing the centralized control features of SDN, QKDN can flexibly respond to user increases or decreases and meet user dynamic key requirements. Thus, the encrypted transmission of ONU user data is realized. Figure I.4 depicts the QKD access network.

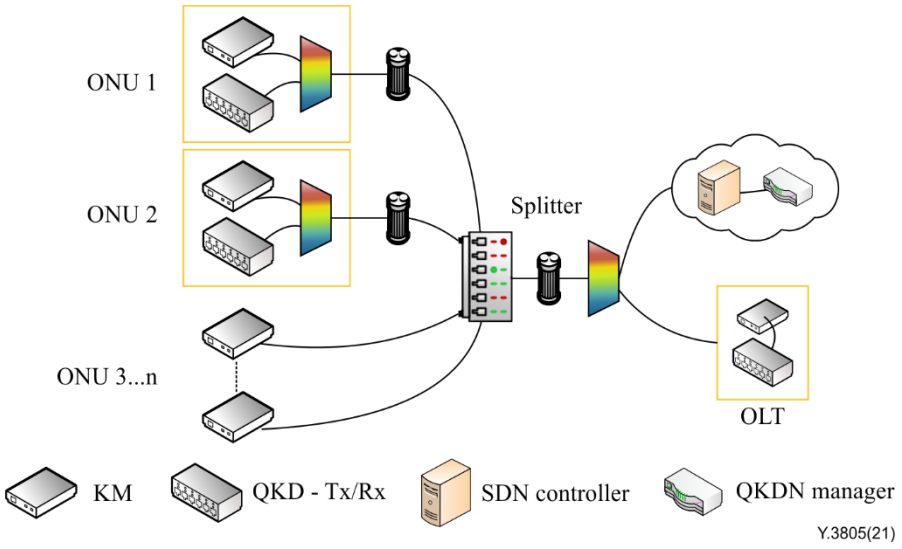


Figure I.4 – QKD access network

– **Mobile terminal communication**

As shown in Figure I.5, the QKDN based on SDN manages the resource allocation, path selection, and troubleshooting in the quantum key distribution process through the SDN controller when a secure communication service arrives. The SDN-based QKDN is combined with the key update terminal device close to the user. The aim is to charge the symmetric quantum key generated by the QKDN to the secure storage medium of the terminal for authentication and session encryption in the communication process. Thus, secure communication services between mobile terminals or between mobile terminals and servers are provided.

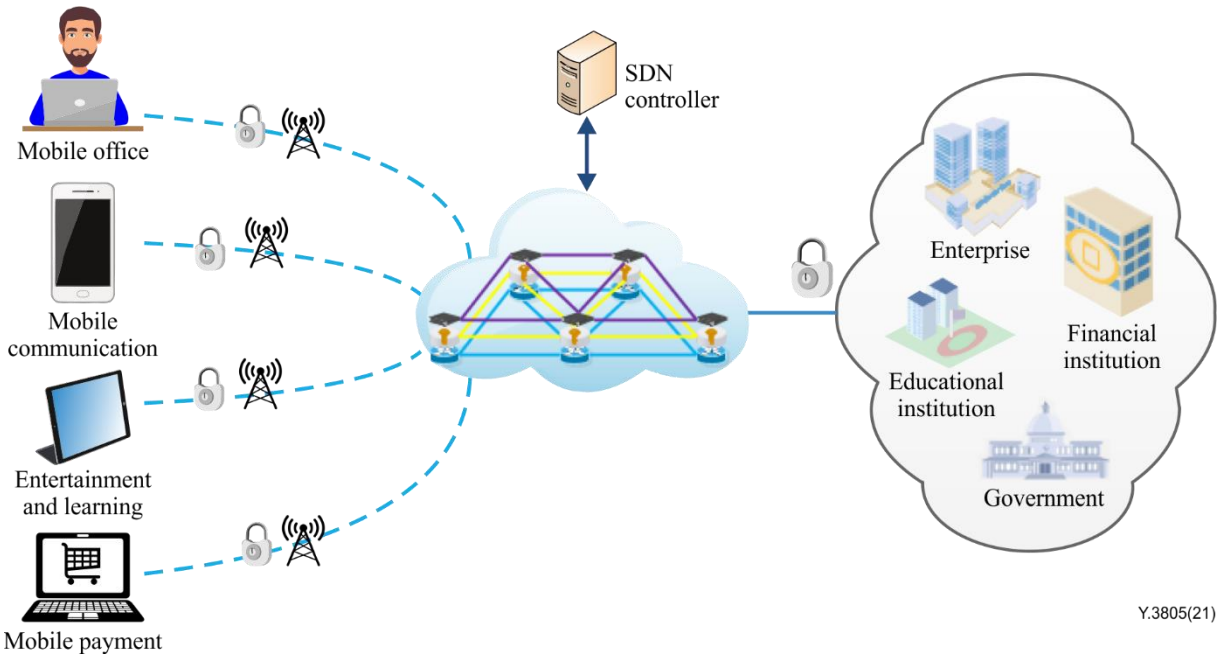


Figure I.5 – Mobile terminal communication

– **Others**

Other use cases can be applied such as secure finance, blockchain application, stable and reliable service environment for the purpose of key change and management, smart grid, intelligent transport system, mashup or convergence applications for control and management.

Appendix II

Comparison of control methods between traditional QKDNs and SDN-based QKDNs

(This appendix does not form an integral part of this Recommendation.)

To better understand SDN control in QKDNs, we compare the control method in QKDNs with that in SDN-based QKDNs by analysing examples. In Figures II.1 to II.3, the red arrows show control flows, and the green arrows show key flows. Note that interfaces are simplified in the figures, and the interfaces related to the control layer are highlighted. In the following three scenarios, there are the same key flows for key relay and key supply, but there are different control flows.

– **QKDN with distributed QKDN controllers**: As shown in Figure II.1, when terminals need keys to encrypt data, the terminal in source node requests and receives keys from the local KM. If the QKD needs key relay, the local KM will send a key relay request to the local QKDN controller to obtain calculated routing paths. Finally, the KM in destination node pushes keys to another terminal.

– **QKDN with a centralized QKDN controller**: As shown in Figure II.2, the control method is the same as that in a QKDN with distributed QKDN controllers, except that the centralized QKDN controller calculates routing paths for terminals.

– **SDN-based QKDN with an SDN controller**: As shown in Figure II.3, when terminals need keys to encrypt data, the key request information is sent to the KM and then the KM sends a key relay route request to an SDN controller to provision services. The SDN controller is the core brain in operational procedures of SDN-based QKDNs.

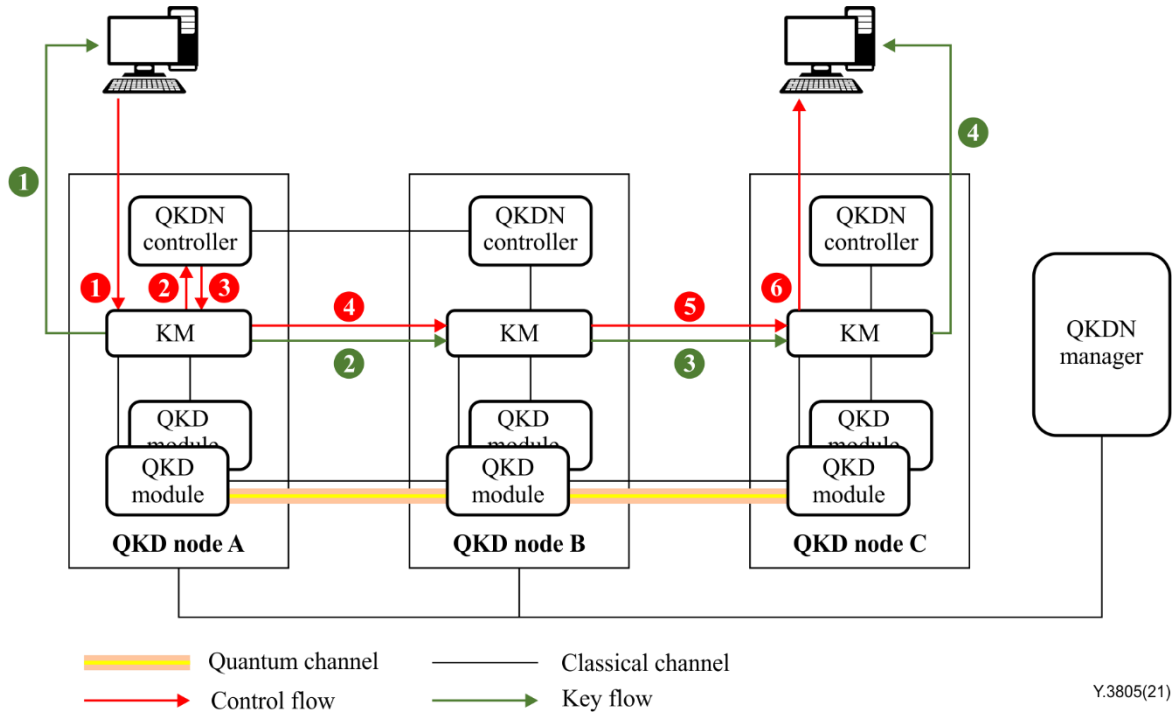


Figure II.1 – Diagram of control method in QKDNs with distributed QKDN controllers

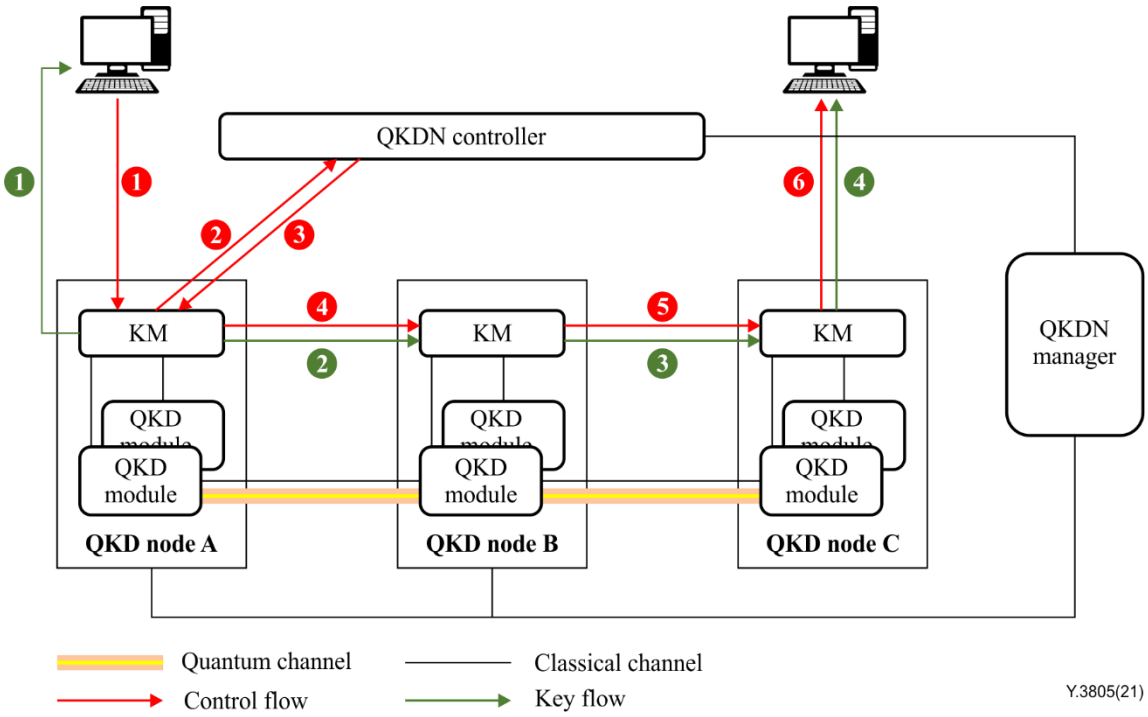


Figure II.2 – Diagram of control method in QKDN with a centralized QKDN controller

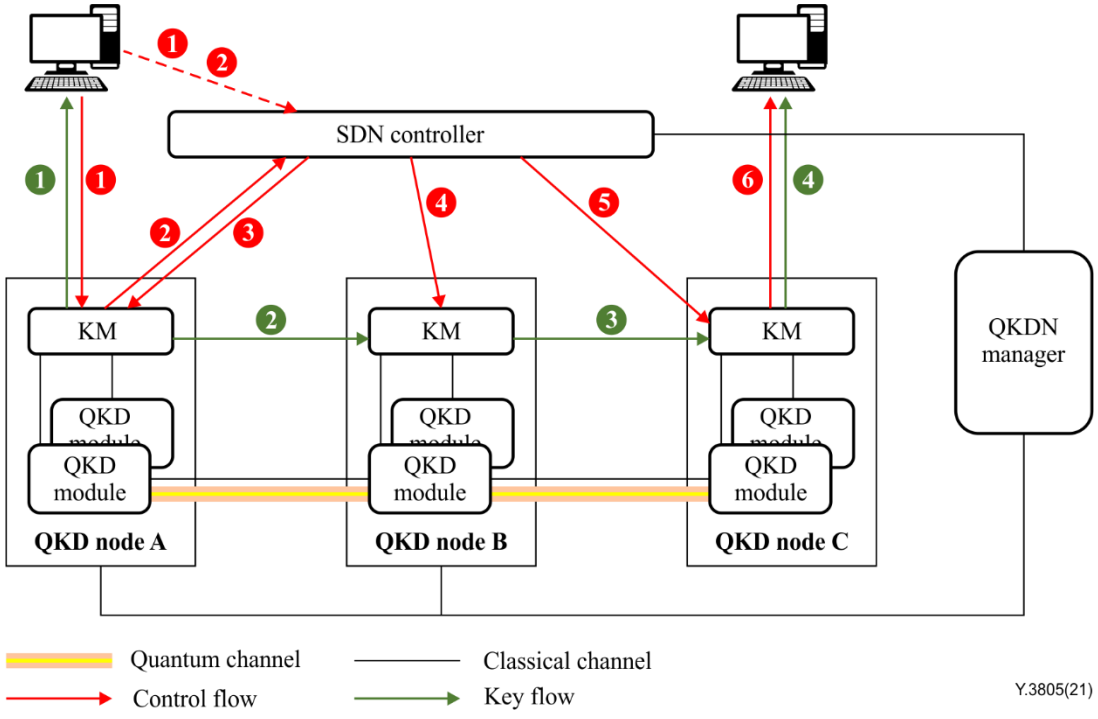


Figure II.3 – Diagram of control method in SDN-based QKDN with an SDN controller

Appendix III

Controllable elements for SDN in QKDNs

(This appendix does not form an integral part of this Recommendation.)

One of the most important advantages of introducing SDN technology into QKDNs is that SDN controllers include capabilities to support the programmable control of network elements. In a QKD network the SDN controller can control functions of programmable elements where required by the QKDN.

As the diversity and complexity of various services increase, the programmability of underlying elements becomes more important. When a service needs to change certain parameters of underlying programmable elements, the SDN controller can calculate and control their necessary parameters.

Many parameters of a QKDN, such as parameters of QKD modules, are critical for the secure operation of the QKDN. Making QKDN elements remotely programmable can introduce security concerns and additional requirements are likely to be necessary. Such security considerations are outside the scope of this document. Examples of functions of programmable elements in the quantum layer that might be considered for control by an SDN controller after consideration of related security issues include:

- Laser: launch power and wavelength according to different requirements.
- Intensity modulator: repetition rate of light pulses (limited by the bandwidth of the intensity modulator and any other restrictions), duration of light pulse, intensities of the signal state and decoy states.
- Phase modulator: repetition rate and phase shifts.
- Single photon detector: dead time, detection efficiency and repetition rate for gated detectors.
- Main control unit: switching QKD protocols by modifying the workflow/logic of modulators and single photon detectors.
- Post processing unit: monitoring parameters such as gain, error rate and error correction efficiency to ensure the system is carrying out "honest" privacy amplification according to the specified QKD security model.

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 V1.1.1 (2020-03), *Quantum Key Distribution (QKD); Control Interface for Software Defined Networks*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2022