ETSI GS QKD 018 V1.1.1 (2022-04)

Quantum Key Distribution (QKD); Orchestration Interface for Software Defined Networks

Disclaimer

The present document has been produced and approved by the Quantum Key Distribution (QKD) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGS/QKD-018OrchintSDN

Keywords
interface, management, orchestration, quantum cryptography, quantum key distribution, SDN, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Quantum Key Distribution (QKD).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The present document deals with the interface between an SDN orchestrator and an SDN controller of a QKD network. It describes the flow of information between both entities, the SDN controller performing as a server and the SDN orchestrator operating as a client. The information model is given in YANG and it is agnostic from the implementation by any vendors. This information model enables the SDN orchestrator to manage and configure the SDN controller of a QKD network, permitting it to orchestrate the QKD network and a classical optical transport network.

Introduction

Deploying an optical network where quantum channels and classical data channels can coexist is critical for adopting QKD networks in network 'operators' infrastructures. When network operators consider introducing QKD networks into their existing networks, there are a few implementation options to choose from, for example, the integration of quantum channels and classical data channels in a single optical fibre or separation of them in different optical fibres. There are two major technical issues with integrating quantum channels and classical data channels in a single optical fibre: differences between the transmitted optical powers and the achievable link distances of the channels. Network operators can optionally choose to separate such channels placing quantum channels in a QKD network and classical data channels in an Optical Transport Network (OTN). This can optimize performance of QKD networks in a fibre-rich environment. In this separated case, under the design principle of Software-Defined Network (SDN) architectures, the QKD network and OTN can be controlled by different SDN controllers.

However, if QKD-derived keys are to be supplied to secure application entities in an OTN for cryptographic use, network operators need to know which QKD nodes in the QKD network can supply QKD-derived keys to which secure application entities in an OTN. Each SDN controller has only resource information about the network it controls. Therefore, adopting an SDN orchestrator capable of controlling both the QKD and OTN networks is one option for achieving the end-to-end service provisioning of QKD-derived key generation in a QKD network and its use in secure application entities in an OTN. In this case, an SDN orchestrator plays the role of matching the addresses of QKD nodes in QKD network and ones of secure application entities in an OTN in order to supply secure application entities in OTN with QKD-derived keys generated in a QKD network.

In addition, with the introduction of an SDN orchestrator interface to the SDN controller of the QKD network, a network operator can operate and maintain a QKD network in terms of network topology, configuration, management policy and performance management.

So, adopting an SDN orchestrator for a QKD network can mitigate the burden of integrating the QKD network into network 'operators' communication networks where the network operators already have an SDN orchestrator for SDN controllers of their OTNs.

The information model for the interface between an SDN orchestrator and an SDN controller of QKD network is presented to simplify the management and configuration of QKD networks through the North Bound Interface (NBI) of the SDN controllers of the QKD networks.

1 Scope

The present document provides a definition of an orchestration interface between an SDN orchestrator and an SDN controller of a QKD network. This orchestration interface defines the abstract information models and workflows for QKD network resource management, configuration management, performance management, service provisioning, notifications and management of multi-domain QKD networks. Interfaces between an SDN orchestrator and SDN controllers of classical optical transport networks are out of scope.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents are necessary for the application of the present document.

[1] IETF RFC 6020 (October 2010): "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)".

[2] IETF RFC 7950 (August 2016): "The YANG 1.1 Data Modeling Language".

[3] IETF RFC 6241 (June 2011): "Network Configuration Protocol (NETCONF)".

[4] IETF RFC 8040 (January 2017): "RESTCONF Protocol".

[5] ETSI GS QKD 004 (V2.1.1): "Quantum Key Distribution (QKD); Application Interface".

[6] ETSI GS QKD 014 (V1.1.1): "Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API".

[7] ETSI GS QKD 015 (V1.2.1): "Quantum Key Distribution (QKD); Control Interface for Software Defined Networks".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI GR QKD 007: "Quantum Key Distribution (QKD); Vocabulary Revision".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

NOTE: Where possible, the definitions from ETSI GR QKD 007 [i.1] are used.

entity: set of hardware, software or firmware components providing specific functionalities

Key Management Entity (KME): entity that manages keys in a network in cooperation with one or more other Key Management Entities

QKD application: entity consuming QKD-derived keys from the key management system

NOTE: They can be either external applications (similar to SAE, see below) or internal applications running in the QKD system.

QKD-derived key: secret key derived from QKD system(s) operating QKD protocol(s) over a QKD link

QKD interface: interface that is a high-level abstraction of a QKD system

NOTE: A QKD interface defines only attributes that are relevant from the point of view of the network. These attributes are revealed to a SDN controller to establish and manage QKD.

QKD link: set of active and/or passive components that connect a pair of QKD modules to enable them to perform QKD and where the security of symmetric keys established does not depend on the link components under any of the one or more QKD protocols executed

QKD module: set of hardware, software or firmware components that implements part of one or more QKD protocol(s) to be capable of securely agreeing symmetric keys with at least one other QKD module

QKD network: network comprised of two or more QKD nodes

QKD node: set of QKD modules installed in the same location within the same security perimeter

QKD protocol: defined set of procedures performed by QKD modules (and optionally link modules) to agree shared secret bit strings by QKD

QKD system: pair of QKD modules connected by a QKD link designed to provide Quantum Key Distribution functionality using QKD protocols

quantum channel: communication channel for transmitting quantum signals

Quantum Key Distribution (QKD): procedure involving the transport of quantum states to agree shared secret bit strings between remote parties using a protocol with security based on quantum entanglement or the impossibility of perfectly cloning or measuring the unknown transported quantum states

SD-QKD node: logical and abstracted representation of the QKD resources under the responsibility of a single SDN agent

Secure Application Entity (SAE): entity that requests one or more keys from a Key Management System for one or more applications running in cooperation with one or more other Secure Application Entities

service link: logical key association link between two QKD nodes connected by a set of one or more physical QKD links (single hop or multi-hop)

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

FCAPS	Fault-management, Configuration, Accounting, Performance, and Security
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
JSON	JavaScript Object Notation
KME	Key Management Entity
NBI	North Bound Interface
OTN	Optical Transport Network
QKD	Quantum Key Distribution
QoS	Quality of Service
RFC	Request For Comments
SAE	Secure Application Entity
SDN	Software-Defined Network
SDNO	Software-Defined Network Orchestrator
SD-QKD	Software-Defined Quantum Key Distribution
SDQNC	Software-Defined Quantum Network Controller
URI	Uniform Resource Identifier
XML	Extensible Markup Language
YANG	Yet Another Next Generation

4 SDN orchestration of QKD Overview

4.1 Use case of SDN orchestration

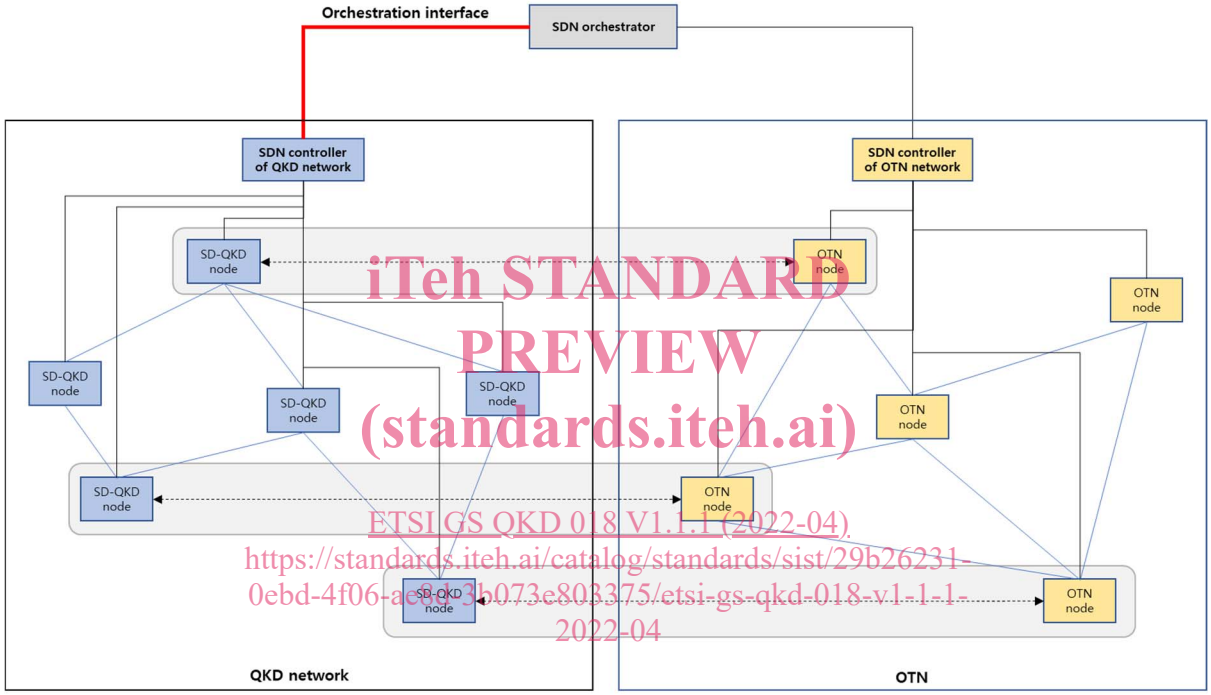
When network operators deploy a QKD network to secure data in a communication network, they need to consider how the QKD network will be incorporated into their classical communication network for QKD-derived 'keys' delivery to secure application entities in a classical communication network. Secure application entities can reside in various network domains within a classical communication network. While a QKD network domain and network domains containing secure application entities can be managed and configured independently via domain-specific SDN controllers, a network operator can introduce a multi-domain SDN orchestrator to orchestrate the whole network system.

For the use case of delivering QKD-derived keys to secure application entities in an Optical Transport Network (OTN), where the infrastructure is available to do so, network operators could choose to deploy a QKD network that is separate from a classical OTN and to operate and manage each network separately. Possible reasons for this include optimizing the performance of QKD links that depend upon fibre length and the presence of stray light, security isolation, or separation of responsibilities for management, etc. Both network domains need to be aware of nodes that belong to both network domains for QKD-derived keys to be delivered to secure application entities in the OTN. In particular, addresses for such nodes in the two network domains need to be matched. In this use case, the SDN orchestrator can perform this role with the information from the SDN controllers of the QKD network and the OTN.

In addition, a network operator can coordinate QKD networks and OTNs with an SDN orchestrator via each SDN controller to ensure end-to-end QKD service provisioning. The SDN orchestrator may be responsible for selecting network domains for a new service that is to be provisioned. Such domain selection is based on abstracted knowledge of intra- and inter-domain connectivity and topology. For the SDN orchestrator to coordinate between network domains, an interface between the SDN orchestrator and the QKD network SDN controller needs to be defined. This interface describes the flow of information between both entities, the SDN controller performing as a server and the SDN orchestrator operating as a client. The SDN orchestrator can orchestrate QKD networks through this interface in terms of network configuration and topology, management policy, performance management, and the address matching described above.

In this use case, a network operator starts to request end-to-end QKD service provisioning from the SDN orchestrator. Before the SDN orchestrator requests end-to-end QKD service provisioning from the SDN controller of the QKD network following a network operator's request, the SDN orchestrator should collect the topology and inventory information of the QKD network from the SDN controller of the QKD network as a previous step to check the status of QKD network. After collecting this information, the SDN orchestrator requests a service link and the candidate paths for the service link within a QKD network to transport QKD-derived keys for end-to-end QKD service provisioning from the SDN controller of the QKD network. After the SDN orchestrator receives the candidate paths from the SDN controller of the QKD network, the SDN orchestrator decides which candidate path in the QKD network it will use for end-to-end QKD service provisioning and requests to deploy a specific path from the SDN controller of the QKD network. In the YANG models included in the present document, the topology and inventory YANG models are separated from the connectivity YANG model to reflect this procedure.

With this configuration extended, an SDN orchestrator can orchestrate multi-QKD network domains from multi-vendors via each SDN controller of each QKD network as well as both QKD and classical network domains, as shown in Figure 1.



NOTE: The orchestration interface (solid red line) between the SDN orchestrator and SDN controller of the QKD network is shown. The key delivery API (dashed line) from ETSI GS QKD 014 [6] or remote function call from ETSI GS QKD 004 [5] can be used for Secure Application Entities (SAEs) in OTN nodes in the OTN network to retrieve keys from Key Management Entities (KMEs) in SD-QKD nodes in QKD network. SAEs in OTN nodes are located within the same security boundary as their connected KMEs in SD-QKD nodes.

Figure 1: Use case of SDN orchestrator for QKD network and OTN

4.2 Functions of SDN orchestrator

SDN orchestration can be defined as the continuing process of automatically coordinating the available resources according to optimization criteria to establish and release the end-to-end service provisioning through different network domains controlled by each SDN controller. SDN orchestration may be used to start the series of automated processes required to satisfy a customer service request generated via a customer website. An SDN orchestrator is a master entity that enables each SDN controller to establish and release multiple paths in its own network domain to meet end-to-end service provisioning requests from customers through different network domains.

To enable end-to-end service provisioning through different network domains, the SDN orchestrator has the following functions:

- Translation from the end-to-end QKD service provisioning requests from a customer to the configuration of the different network domains through each SDN controller and the allocation of secure application entities for this service provisioning.
- Establishment and release requests of the end-to-end QKD service provisioning with the inter-domain connections between secure application entities through orchestration interfaces.
- Identification of multi-domain path calculation across the different network domains, including inter-domain connections and endpoints for each request of the end-to-end service provisioning.
- Requests to change the established path calculation with constraints from a network operator.
- The QKD nodes and QKD links are discovered under each SDN controller in the QKD network and an abstracted view of the QKD network topology.
- Inventory monitoring of QKD-derived key resources available from the key management system in each QKD node and each QKD link.
- Monitoring of FCAPS management of the QKD network and notification of changes of FCAPS management in the QKD network.

The orchestration interface between the SDN orchestrator and the SDN controller of the QKD network needs to be defined to address the outlined functions of the SDN orchestrator. The SDN controller is a server through the orchestration interface, and the SDN orchestrator is a client in terms of communication between them.

5 SDN orchestration interface of QKD network

5.1 Discovery of QKD network topology

The information model includes the discovery of QKD nodes and each direct (physical) QKD link between QKD nodes under each SDN controller in the QKD network and an abstracted view of the QKD network topology.

An SDN orchestrator can compose the overall multi-domain network topology with the information from the underlying SDN controllers, one of which can expose its intra-domain QKD network topology. An SDN orchestrator does not need complete QKD physical network composition information but needs an abstracted view of the network domains and the inter-domain connectivity.

The discovery of QKD network topology can be done proactively or reactively. Proactively, the SDN orchestrator requests information about the QKD network topology from the SDN controller every time the SDN orchestrator needs to make a new path calculation request to the SDN controller. Reactively, the SDN orchestrator receives the information about the QKD network topology from the SDN controller whenever there is any change in the QKD network topology, for example, in case new QKD nodes are added, or the existing QKD nodes are removed from the QKD network.

In the discovery of the QKD network topology, the information about internal or external applications that consume QKD-derived keys for their own purpose is not incorporated. Therefore, QKD physical links that connect QKD nodes directly are displayed in the QKD network topology. After starting the operation of the QKD network and preparing end-to-end QKD service provisioning, the QKD network has set up QKD service links and information about the QKD service links is also given in terms of QKD service link connection.

The SDN controller of a QKD network shall provide the following parameters and values to the SDN orchestrator.

Table 1: SD-QKD node parameters for QKD network topology

Name	Type	Detail	Description
sdqkd_nodes	container	None	Container of SD-QKD nodes.
sdqkd_nodes/ qkdn	list	Key: "qkdn_id"	List of SD-QKD nodes.
qkdn/ qkdn_id	ietf-yang-types: uuid	None	Unique ID of the SD-QKD node.
qkdn/ qkd_interfaces	container	None	Container of the physical QKD modules of the SD-QKD node.
qkd_interfaces/ qkdi	list	Key: "qkdi_id"	List of the physical QKD modules of the SD-QKD node.
qkdi/ qkdi_id	uint32	None	Interface id. It is described as a locally unique number, which is globally unique when combined with the SD-QKD node ID.

Table 2: QKD link parameters for QKD network topology

Name	Type	Detail	Description
qkd_phys_links	container	None	Container of QKD physical links to directly connect SD-QKD nodes in the QKD network.
qkd_phys_links/ phys_link	list	Key: "phys_link_id"	List of QKD physical links to directly connect SD-QKD nodes in the network.
phys_link/ phys_link_id	ietf-yang-types: uuid	None	Universally Unique ID of the QKD physical link.
phys_link/ link_type	etsi-qkdn-types: QKD-LINK-TYPES	None	The QKD physical link type is included. The identity is PHYS according to ETSI GS QKD 015 [7].
phys_link/ local_qkdn_id	ietf-yang-types: uuid	None	Unique ID of the local SD-QKD node which is connected to the QKD physical link.
phys_link/ local_qkdi_id	uint32	None	Interface ID of the local SD-QKD node which is connected to the QKD physical link.
phys_link/ remote_qkdn_id	ietf-yang-types: uuid	None	Unique ID of the remote SD-QKD node which is connected to the QKD physical link.
phys_link/ remote_qkdi_id	uint32	None	Interface ID of the remote SD-QKD node which is connected to the QKD physical link.
qkd_svc_links	container	None	Container of QKD service links (end-to-end key association links) in the QKD network.
qkd_svc_links/ svc_link	list	Key: "svc_link_id"	List of QKD service links in the network.
svc_link/ svc_link_id	ietf-yang-types: uuid	None	Universally Unique ID of the QKD service link.
svc_link/ link_type	etsi-qkdn-types: QKD-LINK-TYPES	None	The QKD service link type is included. The identity is VIRT according to ETSI GS QKD 015 [7].
svc_link/ local_qkdn_id	ietf-yang-types: uuid	None	Unique ID of the local SD-QKD node which is connected to the QKD service link.
svc_link/ local_qkdi_id	uint32	None	Interface ID of the local SD-QKD node which is connected to the QKD service link.
svc_link/ remote_qkdn_id	ietf-yang-types: uuid	None	Unique ID of the remote SD-QKD node which is connected to the QKD service link.
svc_link/ remote_qkdi_id	uint32	None	Interface ID of the remote SD-QKD node which is connected to the QKD service link.

5.2 Monitoring of QKD network status and resource inventory

The information model includes monitoring QKD network status and QKD-derived key resources available from the key management system in each QKD node and each direct (physical) QKD link.

With the discovered QKD network topology based on QKD nodes and each direct (physical) QKD link between QKD nodes, the SDN orchestrator needs to monitor QKD network status and QKD-derived key resources for intra-domain QKD network operation and maintenance.

The information model of monitoring QKD network status includes QKD node status, QKD physical link status, and physical performance. The information model of monitoring resource inventory includes the QKD-derived key generation rate in each QKD physical link and the available QKD-derived key rate in each QKD physical link after internal consumption.