International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3804

(09/2020)

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 – Control and management

Recommendation ITU-T Y.3804

International Telecommunication Union

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
Network control architectures and protocols	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.3804

Quantum key distribution networks – Control and management

Summary

To realize secure, stable, efficient, and robust operations of and services by a quantum key distribution (QKD) network as well as to manage a QKD network (QKDN) as a whole and support user network management, Recommendation ITU-T Y.3804 specifies functions and procedures for QKDN control and management based on the requirements specified in Recommendation ITU-T Y.3801.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3804	2020-09-29	13	11.1002/1000/14409

Keywords

Control and management, quantum key distribution, QKD, QKD network, QKDN.

* 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, 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 TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.3804

Quantum key distribution networks – Control and management

1 Scope

This Recommendation specifies control and management functions and procedures for quantum key distribution (QKD) networks. This Recommendation covers:

– Functional elements of QKD network (QKDN) control, management, and orchestration;

– Functions of QKDN control, management, and orchestration;

– Procedures of QKDN control, management, and orchestration.

Traditional fault, configuration, accounting, performance, and security (FCAPS) functionality which is not specific to QKDN is outside the scope of this Recommendation.

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.3111] Recommendation ITU-T Y.3111 (2017), *IMT-2020 network management and orchestration framework*.

[ITU-T Y.3800] Recommendation ITU-T Y.3800 (2019), *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 M.3400] Recommendation ITU-T M.3400 (2000), *TMN management functions*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 key data [ITU-T Y.3803]: Random bit strings, which are used as a cryptographic key.

3.1.2 key life cycle [ITU-T Y.3800]: A sequence of steps that a key undergoes from its reception by a key manager (KM) through its use in a cryptographic application and until deletion or preservation depending on the key management policy.

3.1.3 key management [ITU-T Y.3800]: All activities performed on keys during their life cycle starting from their reception from the quantum layer, storage, formatting, relay, synchronization, authentication, to supply to a cryptographic application and deletion or preservation depending on the key management policy.

3.1.4 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 KMA links.

3.1.5 key management agent-key (KMA-key) [ITU-T Y.3803]: Key data stored and processed in a key management agent (KMA) and securely shared between a KMA and a matching KMA.

3.1.6 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.

3.1.7 key manager link [ITU-T Y.3800]: A communication link connecting key managers (KMs) to perform key management.

3.1.8 key relay [ITU-T Y.3800]: A method to share keys between arbitrary quantum key distribution (QKD) nodes via intermediate QKD node(s).

3.1.9 key supply [ITU-T Y.3800]: A function providing keys to cryptographic applications.

3.1.10 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.

3.1.11 key supply agent-key (KSA-key) [ITU-T Y.3803]: Key data stored and processed in a key supply agent (KSA), and securely shared between a KSA and a matching KSA.

3.1.12 quantum key distribution module (QKD 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).

3.1.13 quantum key distribution link (QKD link) [ITU-T Y.3800]: A communication link between two quantum key distribution (QKD) modules to operate the QKD.

NOTE – A QKD link consists of a quantum channel for the transmission of quantum signals, and a classical channel used to exchange information for synchronization and key distillation.

3.1.14 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.

3.1.15 quantum key distribution network controller (QKDN 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.

3.1.16 quantum key distribution network manager (QKDN 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.

3.1.17 quantum key distribution node (QKD node) [ITU-T Y.3800]: A node that contains one or more quantum key distribution (QKD) modules protected against intrusion and attacks by unauthorized parties.

NOTE – A QKD node can contain a key manager (KM).

3.1.18 user network [ITU-T Y.3800]: A network in which cryptographic applications consume keys supplied by a quantum key distribution (QKD) network.

NOTE – In this Recommendation, "key" means "symmetric random bit strings" produced by QKDN.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

BSS Business Support System

CDR Charging Data Record

FCAPS Fault, Configuration, Accounting, Performance and Security

ID Identifier

IMT International Mobile Telecommunications

IP Internet Protocol

KM Key Manager

KMA Key Management Agent

KMLM Key Management Layer Management

KSA Key Supply Agent

OSS Operation Support System

QBER Quantum Bit Error Rate

QCLM QKDN Control Layer Management

QKD Quantum Key Distribution

QKDN Quantum Key Distribution Network

QLM Quantum Layer Management

QoS Quality of Service

TMN Telecommunications Management Network

VPN Virtual Private Network

XLMO Cross Layer Management and Orchestration

5 Conventions

None.

6 Overview

This Recommendation specifies functional elements and associated functions, reference points, and procedures for the QKDN control and management. Basic control and management functions and layered structures of QKDN are defined in [ITU-T Y.3800]. More specific functions are:

– control and management specific functions (e.g., path computation for routing control, session control including access traffic steering/switching/splitting for session control, quality of service (QoS) and charging policy control, FCAPS management for each layer);

– control and management reference points among/between control and management functional components and those of other layers;

– control and management orchestration functions of multi-layers. QKDN management layer includes multiple functional components responsible for multi-layers (quantum, key management, and QKDN control layers) and cross-layer management orchestration;

– interworking functions with external management systems especially user network management system, management capability exposure function, etc.

7 Functional architecture of the control, management, and orchestration of QKDN

This clause specifies functional components of QKDN control and management. Figure 1 highlights functional components and reference points relevant to QKDN control and management in a QKDN. Each layer has a layer specific control and management function associated with a corresponding management function in the QKDN management layer. Each layer specific control and management function provides a management agent capability between each layer management function of the QKDN manager and its respective layer functions. Cross-layer management orchestration function provides orchestration capability among multiple layer management functions. Reference points Cx, Ck, Cq, Cops and Cqrp are defined as standard interfaces between the QKDN controller(s) and the functional components under control for the purpose of QKDN control.

Reference points Mq, Mqrp, Mops, Mk, Mc, and Mu are defined as standard interfaces between the QKDN manager and the functional components under management for the purpose of QKDN management.

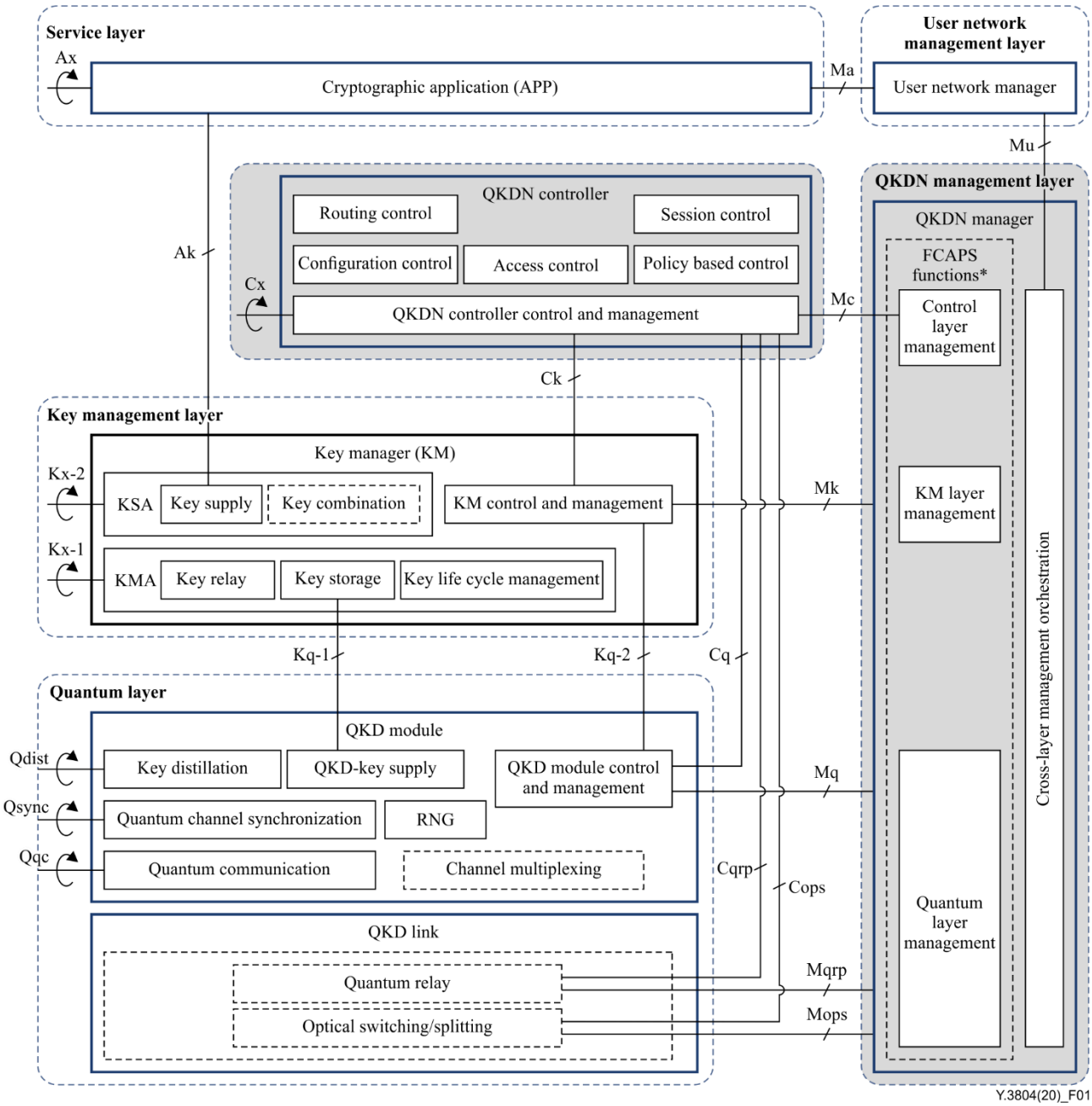

Figure 1 – Functional elements and reference points relevant to QKDN control and management

8 QKDN control layer

In order to realize secure, stable, efficient, and robust operations of and services by a QKDN, the QKDN controller(s) is/are introduced. The QKDN controller controls the quantum layer, the key management layer, and supports the functions of the QKDN management layer and the service layer.

The QKDN controller communicates control information with the KMs, the QKD modules, and the QKD link via the reference points Ck, Cq, Cqrp, and Cops, respectively. In the distributed architecture, the QKD controllers communicate with each other via the reference point Cx.

The QKDN controller communicates management information with the QKDN manager via the reference point Mc as recommended by Req_C 7 in [ITU-T Y.3801]. This function supports the FCAPS of QKDN.

The QKDN controller does not deal with keys themselves. Keys are supplied directly from a KM to a cryptographic application via the reference point Ak.

The QKDN controller performs the following functions:

– Routing control,
– Configuration control,
– Policy-based control,
– Access control,
– Session control.

8.1 Routing control function

As required by Req_C 1 in [ITU-T Y.3801], the routing control function provisions an appropriate key relay route between two end points of KMs in the key management layer.

Routing control function also performs the rerouting of key relay depending on the status of the key management layer and/or the quantum layer, ensuring the continued operation of the key supply/key relay.

For these purposes, the QKDN controller has the following functionalities:

– To manage a routing table which contains the necessary information on QKD node addresses and KM IDs;
– To acquire information on key consumption rate and the residual amount of keys from the KMs, QKD link parameters from the QKD modules, and QKDN topology information from QKDN manager;
– To be supported on optimization of key relay routes in the entire QKDN by the QKDN manager, which monitors the whole status of the quantum layer and the key management layer, and registers and updates them in a database.

The QKDN controller performs the provisioning and rerouting of key relay routes in the following ways:

1) Provisioning of key relay route

The two end-point KMs inform the QKDN controller of the required amount of keys from the two end-point cryptographic applications.

The QKDN controller analyses the status of the key management layer, especially on key consumption rate and the residual number of keys of the relevant KMs together with likely candidates of key relay routes.

The QKDN controller then finds and provisions an appropriate key relay route.

2) Rerouting of key relay

There are two typical cases where the rerouting is carried out.

Case 1: The key management layer attributed

– The residual amount of keys in the KM(s) in the relay node(s) runs short below a threshold.
– A fault is detected in the KM(s) in the relay node(s) and the KM link(s) connected to the relay node(s).

Case 2: The quantum layer attributed

– A quantum bit error rate (QBER) increases beyond a threshold in a certain QKD link connected to the relay node(s).
– A fault is detected in the QKD module(s) in the relay node(s).

In any case, faulty KMs, KM links, QKD modules, and QKD link are recommended to be de-activated, and the appropriate cause analysis and counter-measures should be applied by the QKDN manager.

Rerouting methods may include fixed rate rerouting, data-traffic adaptive rerouting, and scheduled rerouting as described in clause 8.2 of [ITU-T Y.3803] "Management of KMA-key and KSA-key in the key management layer".

8.2 Configuration control function

As recommended by Req_C 2 in [ITU-T Y.3801], the configuration control performs the following functions:

– To acquire control related configuration information on QKD modules and QKD links in the quantum layer and KMs and KM links in the key management layer;

– To control the state of these components (in service, out of service, standby, or reserved);

– To reconfigure QKD links and KM links if an alarm or failure diagnosis is notified.

In particular, alarms and failure diagnosis on QKD links include the increase of QBER implying that eavesdropping is launched against a quantum channel, or the loss of quantum channel is increased. The reconfiguration of a QKD link is made by controlling optical switch/splitter, modules in the quantum relay points, or by bringing a backup quantum channel into service.

The reconfiguration of KM links is mainly to replace faulty classical channels with new ones, and bring them into service, which actually is the same as that of a conventional telecommunications network.

8.3 Policy-based control function

Policy-based control function controls the QKDN based on QoS, key management and charging polices for cryptographic applications. Policy decision making is performed with the help of the QKDN manager.

8.4 Access control function

As recommended by Req_C 5 in [ITU-T Y.3801], the access control function provides capabilities to verify the claimed identity of functional components under the control and support of the QKDN controller and to restrict the functional components to pre-authorized activities or roles. Verified identities and their authorized rights/roles provide the basis of secure operations of and services by the QKDN.

The access control function has an access control repository of QKD nodes, QKD modules, KMs, and cryptographic applications. The access control repository also contains authorized roles, access rights of these functional components, and their priorities based on enforced policies. Based on this repository, the access control performs the following functions:

– To register and delete IDs of functional components;

– To issue certificates to the registered functional components;

– To perform authentication between the QKDN controller and a functional component, referring to their certificates;

– To support authentication between the functional components according to their certificates and the access control repository.

Detailed security mechanisms of access control function are outside the scope of this Recommendation.

8.5 Session control function

As recommended by Req_C 6 in [ITU-T Y.3801], the session control function supports the KMAs to establish the end-to-end key and/or the key supply agents (KSAs) to supply keys to cryptographic applications in the service layer of the user network which are specified in [[ITU-T Y.3802] and [ITU-T Y.3803]. The KMA controls the session based on key management policy and the KSA controls the session procedure of flows of key supply services for multiple cryptographic applications, based on charging policies enforced by the policy-based control function (see clause 8.3).

9 QKDN management layer

A QKDN management layer provides functions to manage a QKDN as a whole and support user network management. QKDN management functions are categorized into five functional areas, namely, FCAPS management just like those of other networks.

The generic functional aspects of FCAPS management have already been specified in detail, for example, by [ITU-T M.3400] for the telecommunications management network (TMN) and [ITU-T Y.3111] for the international mobile telecommunications (IMT)-2020. Some of those specifications can be directly imported into QKDN management function specifications, while some others have been already covered by functions of key management and QKDN control.

This recommendation focuses on the FCAPS management aspects for QKDN.

9.1 Common management functions

QKDN specific aspects of FCAPS arise especially from configurational restriction on the quantum layer due to point-to-point nature of QKD, and from security concerns due to natures of key establishment infrastructure. Thus, these aspects are related mostly to the quantum layer and the key management layer. Taking these aspects into account, the common FCAPS management functions across quantum, key management, and QKDN control layers of the QKDN are as follows:

As required by requirement Req_M 1 in [ITU-T Y.3801], the QKDN manager supports the following fault management functions:

– The QKDN manager monitors QKD link failures to support QKD modules for appropriate recovery actions including reconfiguration of QKD links and rerouting of key relay routes.

As recommended by requirement Req_M 2 in [ITU-T Y.3801], the QKDN manager supports the following fault management functions:

– The QKDN manager provides fault detection and root-cause analysis/diagnosis capability for quantum, key management, and QKDN control layers;

– The QKDN manager makes decisions and generation of failure resolving policies and interacts with each layer for healing actions;

– The QKDN manager discovers each layer managed resources and functions and bootstrap to make them ready for the operation based on the bootstrapping policies.

As required by requirement Req_M 3 in [ITU-T Y.3801], the QKDN manager supports the following configuration management functions:

– The QKDN manager provisions and configures the managed resources in each layer.

As recommended by requirement Req_M 4 in [ITU-T Y.3801], the QKDN manager supports the following configuration management functions:

– The QKDN manager manages the configuration status of each layer;

– The QKDN manager manages the network topology of each layer;

– The QKDN manager performs inventory management for all the QKDN resources in each layer;

– The QKDN manager manages the life cycle of the resource repositories (e.g., create, store, retrieve, modify, remove, etc.) in each layer.

As recommended by requirement Req_M 5 in [ITU-T Y.3801], the QKDN manager supports the following accounting management functions:

– The QKDN manager measures the resource usage data of each layer (e.g., usage for quantum keys in quantum layer) and generates accounting policies for charging.

As required by Req_M 6 in [ITU-T Y.3801], the QKDN manager supports the following performance management functions:

– The QKDN manager collects the performance data and status of each layer, registers them into a performance database, and updates them;

– The QKDN manager analyses the performance of collected data and generates performance reports.

As recommended by Req_M 7 in [ITU-T Y.3801], the QKDN manager supports the following performance management functions:

– The QKDN manager manages the key supply service policies.

As required by requirements Req_M 8 and M 9 in [ITU-T Y.3801], the QKDN manager supports the following security management functions:

– The QKDN manager collects management information including metadata, event logs, audit trail, and so on from each layer for detecting security anomalies;

– The QKDN manager supports key life cycle management by KMs, ensuring traceability of keys, by using the log database.

As recommended by requirement Req_M 10 in [ITU-T Y.3801], the QKDN manager supports the following security management functions:

– The QKDN manager has a root certification authority which issues root certificates to the QKDN controller. The QKDN manager supports the QKDN controller for the access control;

– The QKDN manager manages the key management policies and transmits them to the QKDN controller.

9.2 Layer specific management functions

A QKDN manager provides FCAPS management functions for each QKDN layer: the quantum layer, the key management layer, and the QKDN control layer. Thus, the QKDN manager contains the following three-layer specific functions:

– Quantum layer management (QLM) functions;

– Key management layer management (KMLM) functions;

– QKDN control layer management (QCLM) functions.

The above three functions perform FCAPS management. Also, for coordination, cross-layer, and external management issues, the management functions of the three layers can be orchestrated by:

– Cross-layer management orchestration (XLMO) functions,

which also support user network management.

9.2.1 QLM functions

The quantum layer specific FCAPS management functions are as follows:

– The QKDN manager detects eavesdropping attempts against a quantum channel;

– The QKDN manager performs collection and analysis of QKD specific performance information such as key generation rates;

– The QKDN manager manages availability and reliability of quantum key distribution based on redundancy of QKD links provided by the quantum layer;

NOTE – Redundancy of QKD links for their availability and reliability is assumed to be a well-accepted practice by QKDN operators. Thus, the associated requirement does not explicitly need to be defined.

– The QKDN manager supports meta data abstraction to map device dependent data into device independent data for the device interoperability in the quantum layer.

9.2.2 KMLM functions

The key management layer specific FCAPS management functions are as follows:

– The QKDN manager performs collection and analysis of available amounts of keys in KM for key relay, key supply services and the key life cycle management.

9.2.3 QCLM functions

The QKDN control layer specific FCAPS management functions are as follows:

– The QKDN manager supports the QKDN controller for routing and rerouting of key relay including instruction of policies and rules caused by the faults or performance degradation;

– The QKDN manager supports the QKDN controller for provisioning of routing and re-routing of key relay routes if QKDN supports key relay as the configuration management function.

9.3 XLMO functions

XLMO orchestrates the quantum layer, key management layer, and QKDN control layer management functions. It also orchestrates control and management functions. It exchanges management information with external management entities. The user network management layer is an external management entity from the QKDN management point of view. It can also interact and coordinate with any other management entities (e.g., operator's OSS, BSS, etc.) if necessary.

As recommended by Req_M 11 in [ITU-T Y.3801], the XLMO supports the management functions as outlined in clauses 9.3.1 and 9.3.2:

9.3.1 Orchestration for cross-layers management

– XLMO provides management coordination of the quantum layer, key management layer, and QKDN control layer;

– XLMO provides management orchestration of the QKDN control layer and QKDN management layer to support the QKDN controller to take necessary actions for anomalous situations (e.g., fault, performance degradation, security attacks, etc.);

– For entire QKDN provisioning, XLMO divides the provisioning information into three different types of initialization and configuration information for three layers (i.e., quantum layer, key management layer and QKDN control layer) and performs provisioning tasks per layer in sequence.

9.3.2 Orchestration for external management

– XLMO provides management orchestration with external management systems, especially with the user network management system;

– XLMO collects, stores and displays the topology of the QKDN;
– XLMO provides the QKDN resource usage status;
– XLMO supports the QKDN resource provisioning requested by the user network manager;
– XLMO provides friendly interaction with the user network manager on behalf of the users.

10 Procedures of control, management, and orchestration of QKDN

This clause includes typical examples of operational procedures of the control, management, and orchestration of QKDN. The details in each procedure are assumed to be arranged and/or varied depending on implementation and service use cases of the QKDN.

10.1 Fault management procedure

10.1.1 Fault management procedure: QKD link failure

An example of fault management procedures for QKD link failure is shown in Figure 2.

1) When a link failure occurs, QLM gets a QKD link level alert.
2) QLM decides the initiation of link diagnostic.
3) QLM optionally sends a QKD link diagnostics request to a QKD module if necessary, and the QKD module reports additional QKD link diagnostic information.
4) QLM analyses QKD link diagnostic information.
5) QLM reports the QKD link status to XLMO based on the QKD link diagnostic information.
6) XLMO sends QKD link diagnostic information to QCLM.
7) QCLM makes appropriate control decision(s) to deal with the alert.
8) QCLM sends it to the QKDN controller for the required actions.

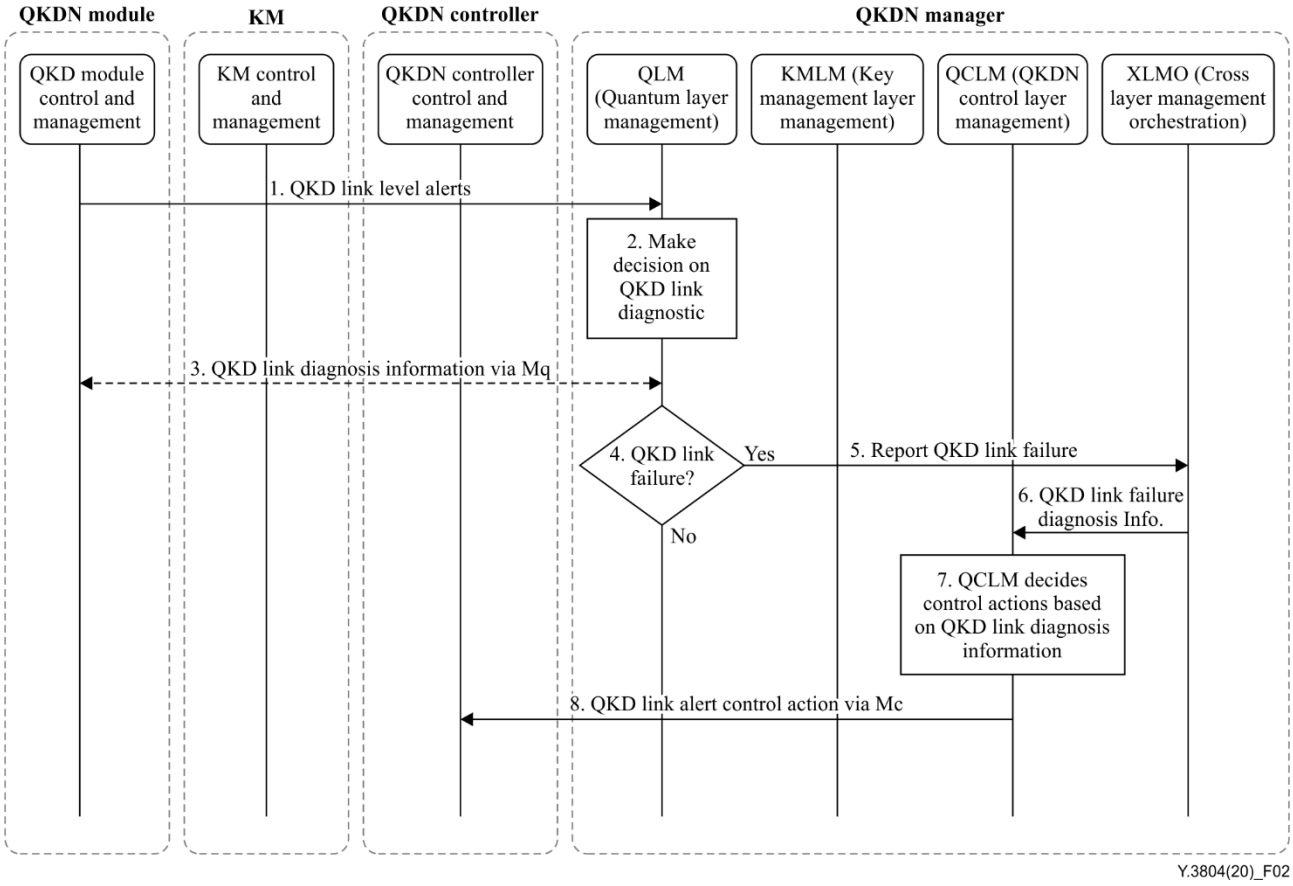

Figure 2 – An example of fault management procedures: QKD link failure

10.1.2 Fault management procedure: key relay failure in KM

An example of fault management procedures for key relay failure in KM is shown in Figure 3.

1) When the KM failure occurs, KMLM gets an alert such as KM relay alert.
2) KMLM decides initiation of KM relay diagnostic.
3) KMLM optionally sends KM relay diagnostics request to KM and receives a report of KM relay diagnostic information if necessary.
4) KMLM analyses KM relay diagnostic information and checks if the failure is related with key relay.
5) If yes, KMLM reports the key relay failure in KM to XLMO based on the KM relay diagnostic information.
6) XLMO sends it to QCLM.
7) QCLM makes appropriate control decision(s) to deal with the alert.
8) QCLM sends it to the QKDN controller for the required actions.

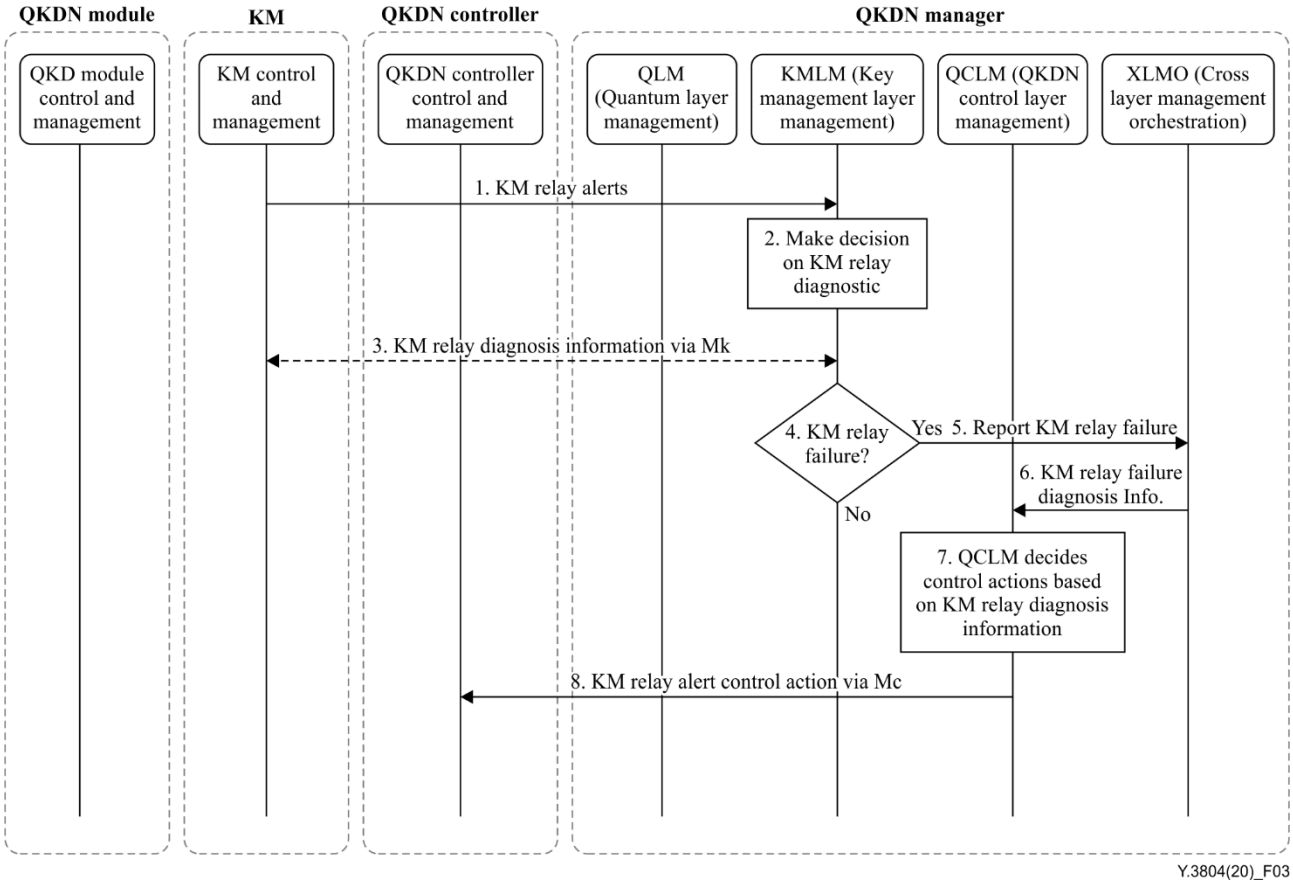

Figure 3 – An example of fault management procedures: Key relay failure in KM

10.2 Accounting management procedure

An example of accounting management procedures is shown in Figure 4.

1) KMLM meters accounting information from the KM via Mk.
2) KMLM processes the metered accounting information and generates a report.
3) KMLM sends the report to XLMO for further charging process.
4) XLMO, then, creates and stores charging data records (CDRs) based on the metered key management layer accounting reports and interacts with the billing system when it receives requests.

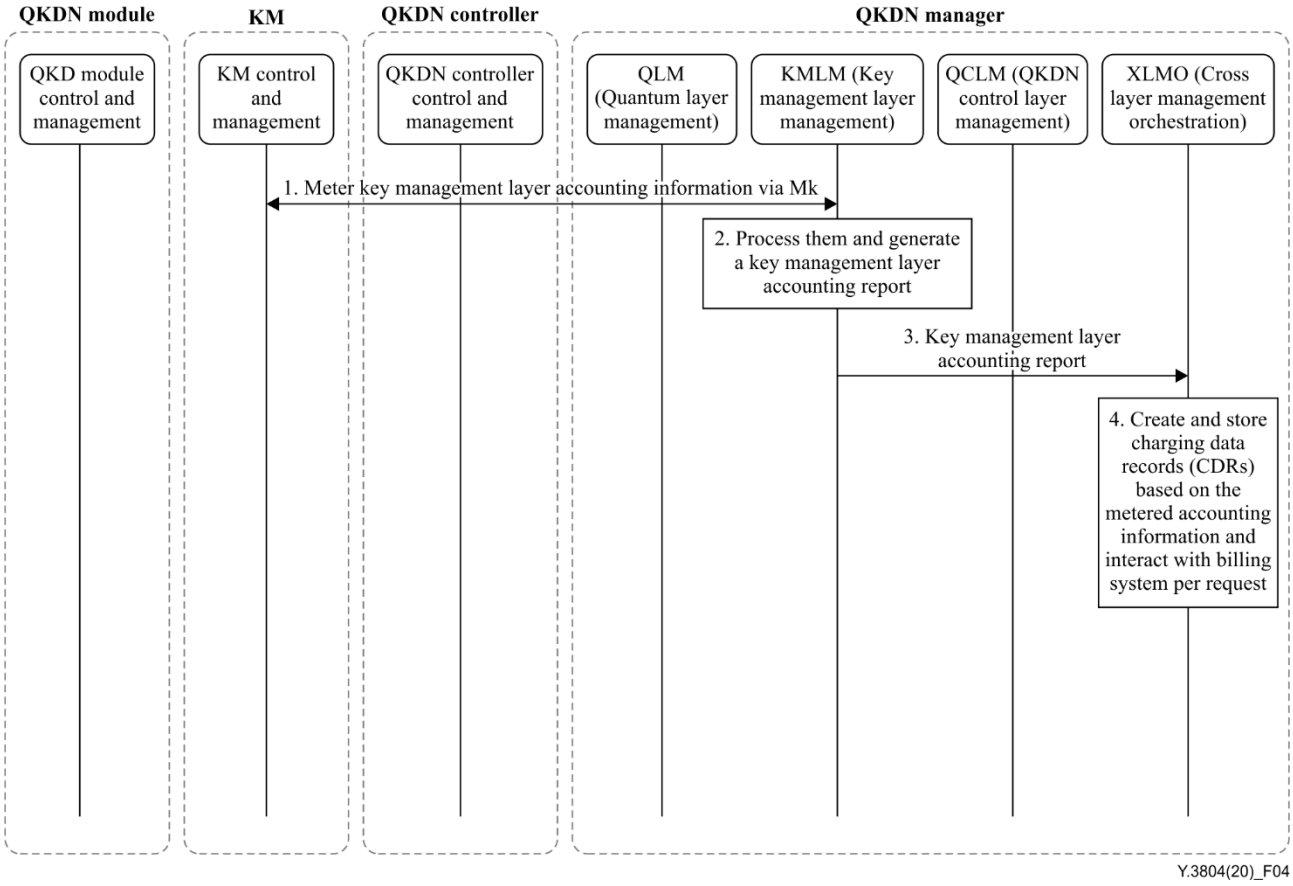

Figure 4 – An example of accounting management procedures

10.3 Configuration management procedure

An example of configuration management procedures is shown in Figure 5.

1) QLM discovers and collects quantum layer configuration information by the QKD module control and management function via the Mq reference point.
2) QLM generates quantum layer topology and creates quantum layer resource inventory.
3) QLM sends quantum layer configuration report to XLMO.
4) KMLM discovers and collects key management layer configuration information via Mk reference point.
5) KMLM generates key management layer topology and creates key management layer resource inventory.
6) KMLM sends key management layer configuration report to XLMO.
7) XLMO generates an entire QKDN topology by correlating quantum layer and key management layer topology information received and also checks any configuration errors.

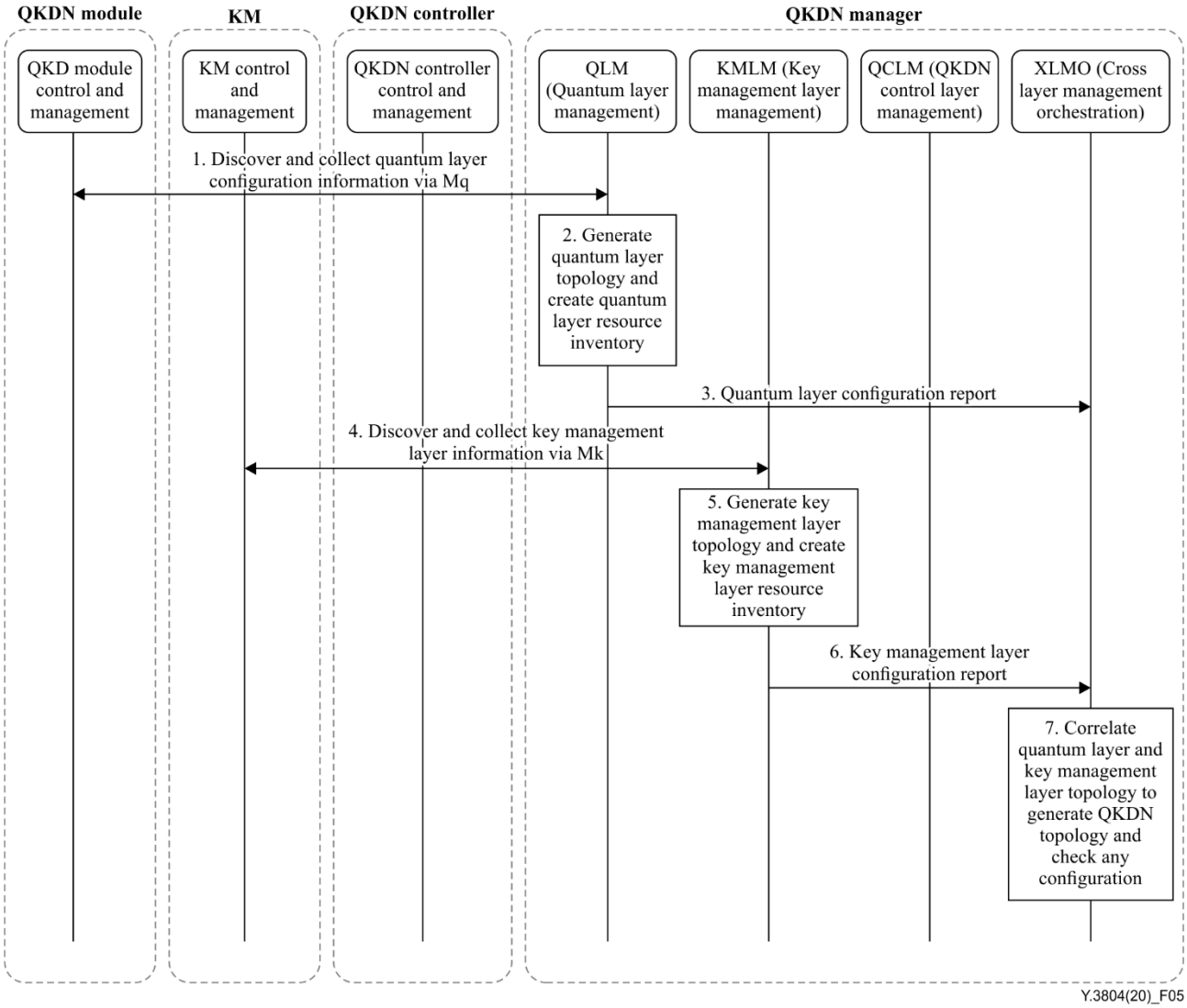

Figure 5 – An example of configuration management procedures

10.4 Performance management procedure

An example of performance management procedures is shown in Figure 6.

1) QLM collects quantum layer performance information by the QKD module control and management function via the Mq reference point.

2) QLM performs analysis of the collected performance information and generates and stores a report.

3) QLM then checks any performance degradation problems in the quantum layer. QLM then sends the performance report to XLMO.

KMLM also performs the same processes for key management layer performance management as in (1) ~ (3).

NOTE 1 – The order of collection process does not have any significance. Both can happen in parallel or in any order depending on the implementation.

4) XLMO correlates the performance information of the quantum layer and key management layer performance to identify cross-layer performance degradation problems. It then creates a remedial action policy for both the quantum layer and the key management layer.

5) XLMO then sends remedy actions to QCLM and QCLM sends it to the QKDN controller. XLMO also optionally sends control action if needed to remove the performance degradation problem.

6) The QKDN controller forwards remedial actions to the control and management functions in the QKD module and the KM.

NOTE 2 – Detailed suggestions for remedial decision making and associated actions are outside the scope of this Recommendation.

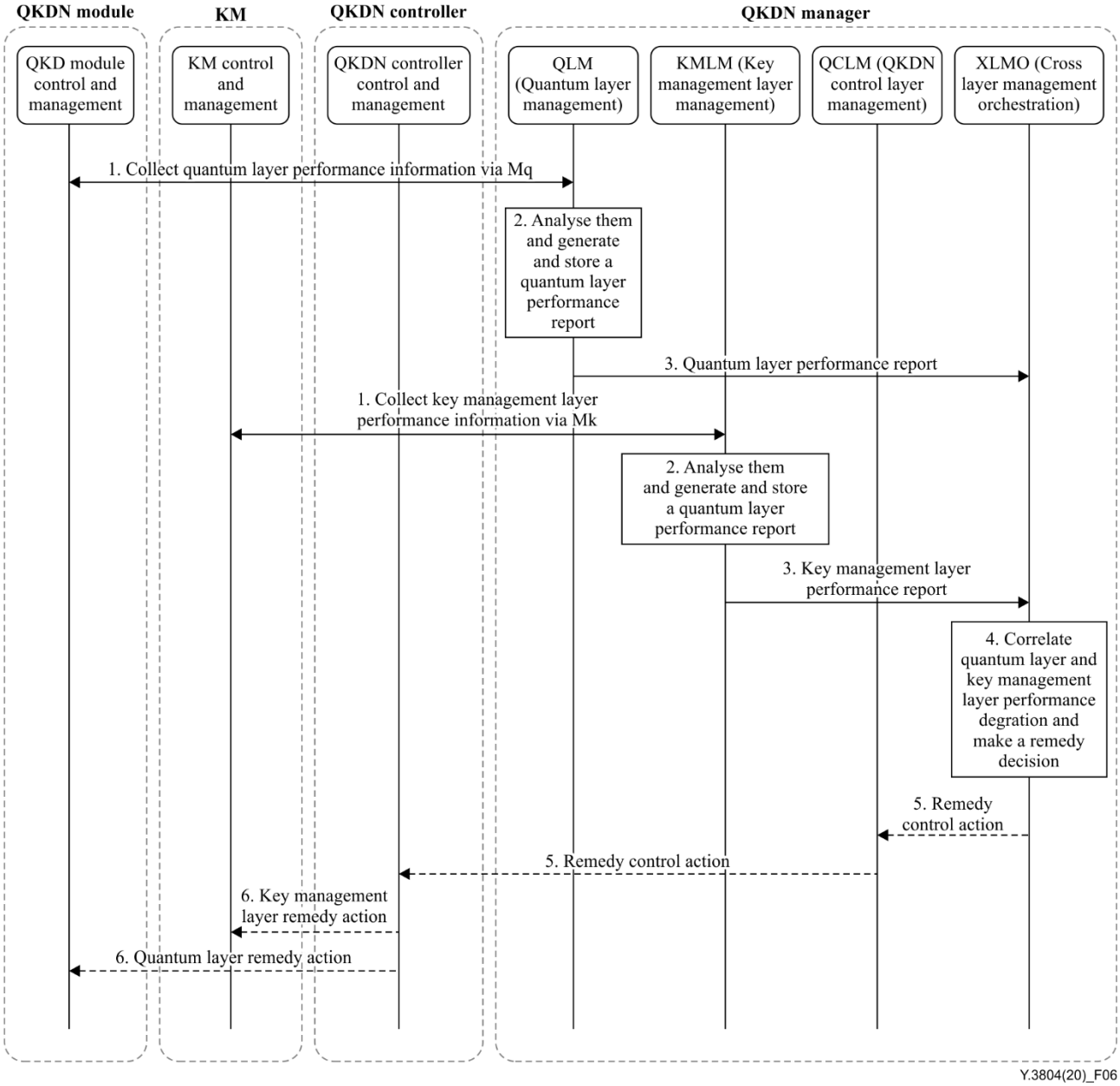

Figure 6 – An example of performance management procedures

10.5 Security management procedure

An example of security management procedures is shown in Figure 7.

1) QLM collects and/or receives the quantum layer security information by the QKD module control and management function via the Mq reference point.

2) QLM analyses the collected security information and generates and stores a report.

3) QLM then transfers quantum layer security information to XLMO.

The QKDN manager also collects security information from the key management layer and the QKDN control layer. The order of collection of security information in layers may vary by implementation of QKDN.

4) XLMO analyses the security anomaly based on the collected security information and makes a decision on solutions for security anomaly and control policy rules to remedy the anomaly.

5) XLMO reports the resulting security anomaly remedy policy rules to QCLM and QCLM sends it to the QKDN controller.

6) The QKDN controller forwards remedial actions to the control and management functions in the QKD module and the KM.

NOTE – Detailed suggestions for remedial decision making, and associated actions are outside the scope of this Recommendation.

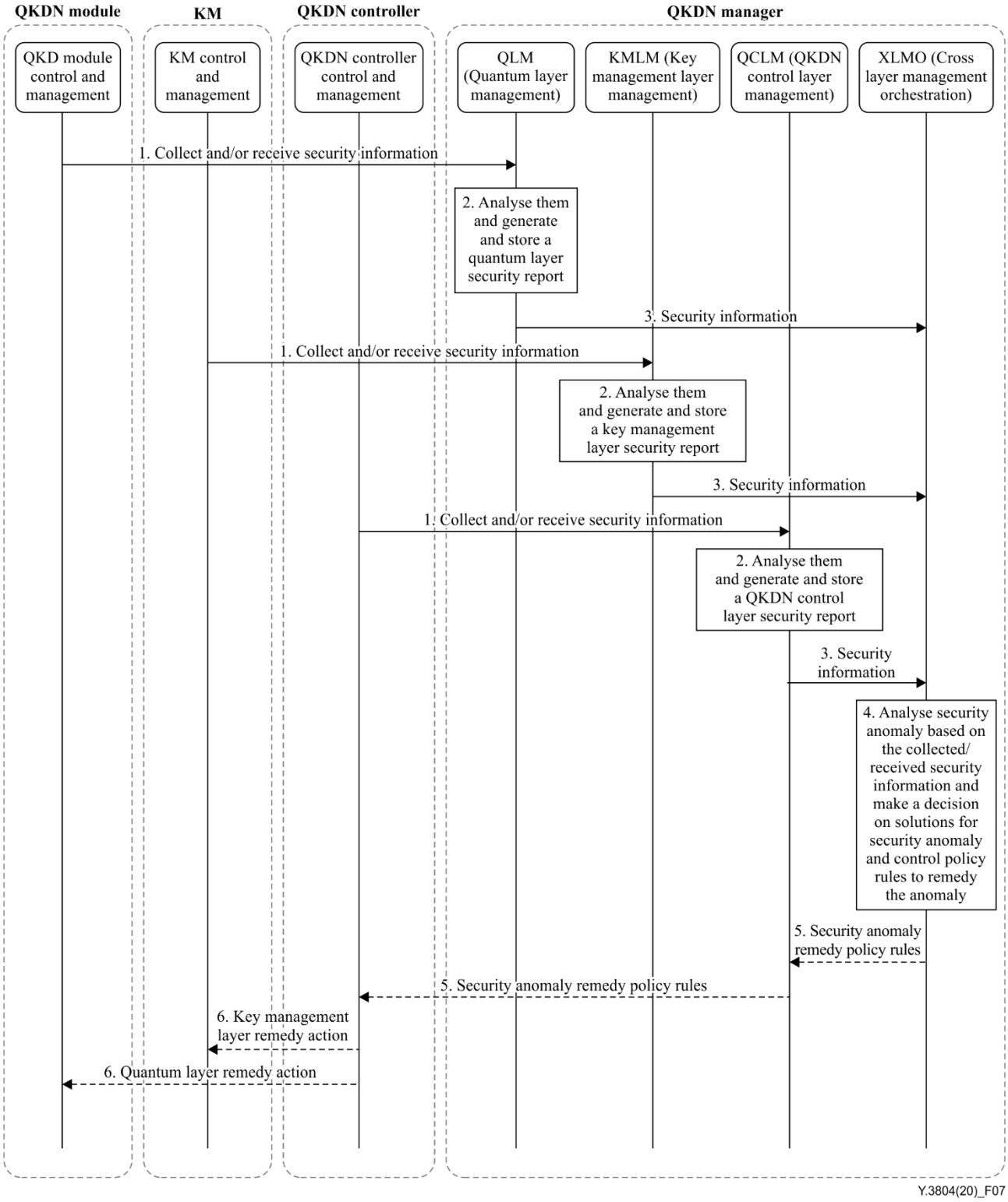

Figure 7 – An example of security management procedures

10.6 Key relay procedure

An example of key relay control procedures is shown in Figure 8.

1) A KM requests a key relay route to the session control function in the QKDN controller.

2) The session control function checks whether there is any session between a source QKD node and a destination QKD node or not.

3) If there is no session, the session control function asks the routing control function for the key relay route.

4) The routing control function asks for the configuration control function configuration information.

5) The configuration control function replies with the configuration information.

6) The routing control function evaluates an optimal route based on the answered configuration information.

7) The routing control function replies with the route information to the session control function.

8) The session control function replies with the route information to the KM.

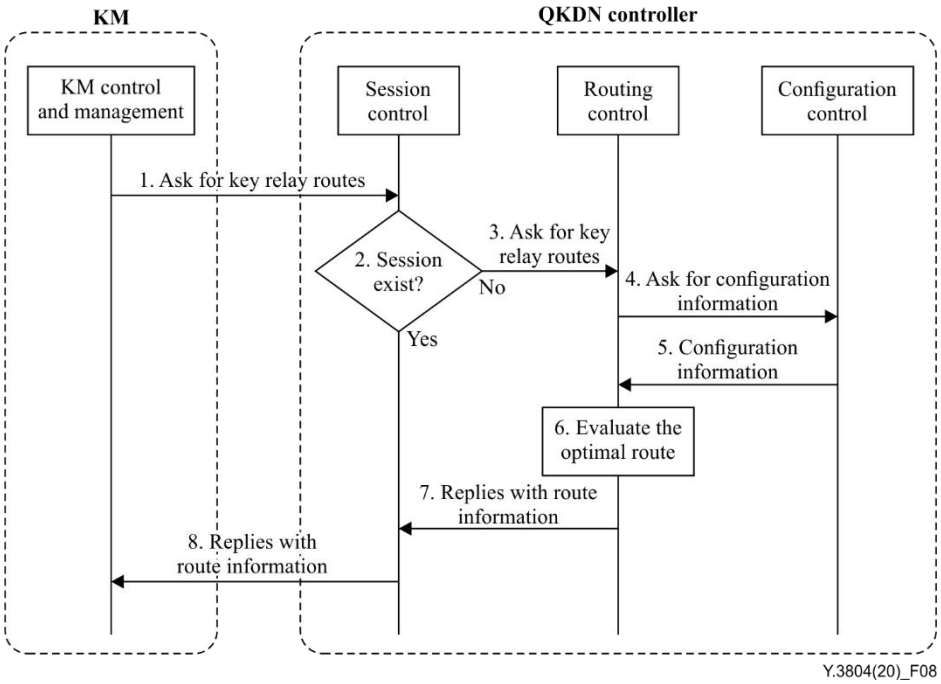

Figure 8 – An example of key relay procedures

10.7 Key relay rerouting procedure

An example of key relay rerouting procedures is shown in Figure 9.

1) QCLM receives a key relay routing and re-routing support information requested by the QKDN controller control and management function.

2) QCLM requests network topology information from XLMO, and XLMO reports it to QCLM.

3) QCLM analyses and selects matching key relay topology information and other supporting information.

4) QCLM reports the resulting supporting information to the QKDN controller for controlling key relay routing and re-routing actions.

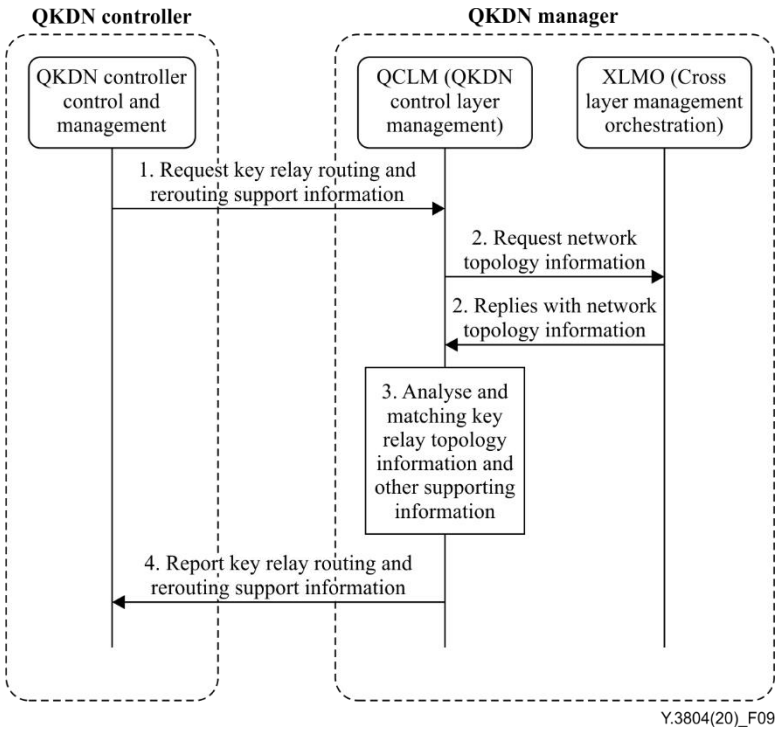

Figure 9 – An example of key relay rerouting procedures

11 Security considerations

In order to mitigate security threats and potential attacks, issues of confidentiality, integrity, authenticity, non-repudiation, availability, and traceability need to be addressed, and the appropriate security and privacy protection schemes should be considered in QKDN, the user network, and interfaces between the two networks. Details are outside the scope of this Recommendation.

Appendix I

Functions and information components for reference points

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

I.1 Reference points of the control, management and orchestration of QKDN

I.1.1 Session processing functions

To assure the reliability and performance of QKDN management session operations across a management reference point, the following capabilities are provided:

Overload control: The reference point provides the function to support overload control for preventing the overflow of information messages exchanged.

Synchronization and audit: The reference point is required to provide the function to support synchronization and audit of the QKDN management session status in support of recovery and operational information statistics and auditing.

Session state maintenance: The reference point is required to be able to maintain the session state using either soft-state or hard-state approaches.

I.1.2 Information exchange functions

This clause provides a brief description of the information exchange functions for the reference point.

Request-response transactions: The reference point allows a QKDN requesting management function to request a transaction to be performed by a responding QKDN management function and get a response (that can be correlated with the request) in return and also vice versa.

Notifications: The reference point supports the notification of asynchronous events between management functions in two layers.

Reliable delivery: The reference point provides reliable delivery of messages.

Capabilities: Each layer determines the capabilities of appropriate corresponding layer management functions.

Security: The reference point supports the authentication between two exchanging layers such that requests from unauthenticated sources will not be performed and such that each layer can verify the source of notifications sent.

One-to–many/many-to-one: Two modes are supported: 1) one-to-many mode: a QKDN management function communicates with multiple management functions in QKDN layers; 2) many-to-one mode: multiple QKDN management functions make requests to a given QKDN management function.

I.2 Reference point common information components

This clause provides common information components applicable to all management reference points as shown in Table I.1.

Table I.1 – Common information components

Information component	Description
User identifier	A unique identifier for the layer management functional components (QCLM, KMLM, & QLM) within the same administrative domain of a single requestor.
Management operation request session identifier	An identifier for the session for which the management operation requests are sent to the QKDN layers (QKDN control, key management layer, and quantum layer). The identifier has to be unique within the same control layer.
Globally unique IP address information (Optional)	A set of IP address information used for locating the network in which each layer control and management function is requesting the management operations.
Unique IP address	The IP address for identifying each layer control and management function.
Address realm	The addressing domain of the IP address (e.g., Subnet prefix or VPN ID)
Management operation requestor identifier	An identifier for the requestor of each layer management service. It is unique over the requestors sending requests for each layer management functional component (QCLM, KMLM, & QLM).
Management operation request priority (Optional)	The indication of the importance of a management operation request. It can be used for processing simultaneous requests by each layer management functional component (QCLM, KMLM, & QLM) based on the priority level.
Management operation request result	Indication of the result for a management operation request (includes both synchronous and scheduled request result).
EventNotify	Allows each layer to send notifications to the layer specific management support functional component in QKDN manager for an event that may need to take an appropriate action for requested management operations.

I.3 Reference point Mc

The Mc reference point is required to support management request/response between the QCLM function of QKDN manager and the QKDN controller control and management function in QKDN control layer.

The Mc reference point operates as an intra-domain reference point.

I.3.1 Mc functions for QCLM

The Mc reference point provides the following functions for QCLM:

- Provisioning of QKDN control layer functions;
- Monitoring performance of QKDN control layer functions;
- Collecting alarm information of QKDN control layer functions;
- Requesting management decision for control actions (e.g., path configuration information, etc.);
- Requesting status of network operations (e.g., routing status, etc.);
- Performing control orchestration actions (e.g., path modification for load-balancing, etc.).

I.3.2 Information components

The information components exchanged across the Mc reference point are categorized in Table I.2.

Table I.2 – Information components for reference point Mc

Information Component	Description
Control orchestration action description	Describes information components related with control orchestration actions
Control orchestration action type	The indication of types of control orchestration action (e.g., path modification, path re-provisioning, etc.)
Control orchestration action priority	The indication of the priority of the action
Control orchestration action value	Specification of the control orchestration action per action type

I.4 Reference point Mk

The Mk reference point supports management request/response between the KMLM function of QKDN manager and the KM control and management function in the QKDN key management layer.

The Mk reference point operates as an intra-domain reference point.

I.4.1 Mk functions for KMLM

The Mk reference point provides the following functions for KMLM:

- Provisioning of key management layer functions;
- Monitoring performance of key management layer functions;
- Collecting alarm information of key management layer functions (e.g., key generation failure;
- Collecting key life cycle management information, QKD link parameter status, etc.

I.4.2 Information components

The information components exchanged across the Mk reference point are categorized in Table I.3.

Table I.3 – Information components for reference point Mk

Information component	Description
Key management layer resource description	Description of key management layer resource for management purpose
Key management layer managed resource ID	Identifier of key management layer managed resource of interests for management
Key management layer performance description	Description of performance information of the key management layer managed resource
Key management layer performance information type	Indication of type of performance information (e.g., key relaying delay, key data loss, etc.)
Key management layer performance information target managed object ID	Identifier of target managed object for collecting performance information
Key management layer performance information value	Value of the performance information collected
Key Management Layer Alarm Description	Description of alarm information of the key management layer managed resource

Table I.3 – Information components for reference point Mk

Information component	Description
Key management layer alarm type	Indication of type of key management layer alarm associated with fault or anomalous event
Key management layer alarm ID	Identifier of a key management layer alarm associated with fault or anomalous event
Key management layer alarm source ID	Identifier of a source of a key management layer alarm
Key management layer alarm value	Value of the key management layer alarm

I.5 Reference point Mq

The Mq reference point supports management request/response between the QLM function of QKDN manager and the QKD module control and management function in QKDN quantum layer.

The Mq reference point operates as an intra-domain reference point.

I.5.1 Mq functions for QLM

The Mq reference point provides the following functions for QLM:

- Provisioning of QKD module functions in the quantum layer;
- Monitoring performance of QKD module functions in the quantum layer;
- Collecting alarm information of QKD module functions in the quantum layer.

I.5.2 Information components

The information components exchanged across the Mq reference point are categorized in Table I.4.

Table I.4 – Information components for reference point Mq

Information component	Description
QKD module in quantum layer resource description	Description of QKD module in quantum layer resource for management purpose
QKD module in quantum layer managed resource ID	Identifier of QKD module in quantum layer managed resource of interests for management
QKD module in quantum layer performance description	Description of performance information of the QKD module in quantum layer managed resource
QKD module in quantum layer performance information type	Indication of type of performance information (e.g., key relaying delay, key data loss, etc.)
QKD module in quantum layer performance information target managed object ID	Identifier of target managed object for collecting performance information
QKD module in quantum layer performance information value	Value of the performance information collected
QKD module in quantum layer alarm description	Description of alarm information of the QKD module in quantum layer managed resource
QKD module in quantum layer alarm type	Indication of type of QKD module in quantum layer alarm associated with fault or anomalous event

Table I.4 – Information components for reference point Mq

Information component	Description
QKD module in quantum layer alarm ID	Identifier of a QKD module in quantum layer alarm associated with fault or anomalous event
QKD module in quantum layer alarm source ID	Identifier of a source of a QKD module in quantum layer alarm
QKD module in quantum layer alarm value	Value of the QKD module in quantum layer alarm

I.6 Reference point Mops

The Mops reference point supports management request/response between the QLM function of QKDN manager and the optical switching/splitting function in QKD link of the QKDN quantum layer.

The Mops reference point operates as an intra-domain reference point.

I.6.1 Mops functions for QLM

The Mops reference point provides the following functions for QLM:

- Provisioning of QKD-link functions in the quantum layer;
- Monitoring the performance of QKD-link functions in the quantum layer;
- Collecting alarm information of QKD-link functions in the quantum layer.

I.6.2 Information components

The information components exchanged across the Mops reference point are categorized in Table I.5.

Table I.5 – Information components for reference point Mops

Information component	Description
QKD link in quantum layer resource description	Description of QKD link in quantum layer resource for management purpose
QKD link in quantum layer managed resource ID	Identifier of QKD link in quantum layer managed resource of interests for management
QKD link in quantum layer performance description	Description of performance information of the QKD link in quantum layer managed resource
QKD link in quantum layer performance information type	Indication of type of performance information (e.g., key relaying delay, key data loss, etc.)
QKD link in quantum layer performance information target managed object ID	Identifier of target managed object for collecting performance information
QKD link in quantum layer performance information value	Value of the performance information collected
QKD link in quantum layer alarm description	Description of alarm information of the QKD link in quantum layer managed resource
QKD link in quantum layer alarm type	Indication of type of QKD link in quantum layer alarm associated with fault or anomalous event

Table I.5 – Information components for reference point Mops

Information component	Description
QKD link in quantum layer alarm ID	Identifier of a QKD link in quantum layer alarm associated with fault or anomalous event
QKD link in quantum layer alarm source ID	Identifier of a source of a QKD link in quantum layer alarm
QKD link in quantum layer alarm value	Value of the QKD link in quantum layer alarm

I.7 Reference point Mu

The Mu reference point supports management request/response between the cross-layer management orchestration (XLMO) function of QKDN manager and the user network manager in user network management layer.

The Mu reference point operates as an intra-domain reference point.

I.7.1 Functions for XLMO

The Mu reference point provides the following functions for XLMO:

- Requesting provisioning status of user network management layer functions;
- Requesting performance of user network management layer functions;
- Requesting alarm information of user network management layer functions (e.g., user network node/link failure;
- Responding and/or sending asynchronous notifications to QKDN management operation requests from user network manager(s);
- Requesting/responding to QKDN management operations to any other external management entities besides user network manager(s) if any.

I.7.2 Information components

The information components exchanged across the Mu reference point are categorized in Table I.6.

Table I.6 – Information components for reference point Mu

Information component	Description
User network management layer resource Description	Description of user network management layer resource for management purpose
User network management layer managed resource ID	Identifier of user network management layer managed resource of interests for management
User network management layer Performance Description	Description of performance information of the user network management layer managed resource
User network management layer performance information type	Indication of type of performance information (e.g., key relaying delay, key data loss, etc.)
User network management layer performance information target managed object ID	Identifier of target managed object for collecting performance information
User network management layer performance information value	Value of the performance information collected

Table I.6 – Information components for reference point Mu

Information component	Description
User network management layer Alarm Description	Description of alarm information of the user network management layer managed resource
User network management layer alarm type	Indication of type of user network management layer alarm associated with fault or anomalous event
User network management layer alarm ID	Identifier of a user network management layer alarm associated with fault or anomalous event
User network management layer alarm source ID	Identifier of a source of a user network management layer alarm
User network management layer alarm value	Value of the user network management layer alarm

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, 2021