International Telecommunication Union

# ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

# Y.3802

**Corrigendum 1**

(04/2021)

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 – Functional architecture

## Corrigendum 1

Recommendation ITU-T Y.3802 (2020) – Corrigendum 1

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.3802

## Quantum key distribution networks – Functional architecture

## Corrigendum 1


**Summary**

Recommendation ITU-T Y.3802 defines a functional architecture model of quantum key distribution (QKD) networks. In order to realize this model, it specifies detailed functional elements and reference points, architectural configurations and basic operational procedures of QKD networks (QKDN).

Corrigendum 1 to Recommendation ITU-T Y.3802 (2020) removes "IT-secure" from the definition of key management agent (KMA) link.



**History**

| Edition | Recommendation | Approval | Study Group | Unique ID* |
|---|---|---|---|---|
| 1.0 | ITU-T Y.3802 | 2020-12-07 | 13 | 11.1002/1000/14407 |
| 1.1 | ITU-T Y.3802 (2020) Cor. 1 | 2021-04-13 | 13 | 11.1002/1000/14605 |

**Keywords**

Architectural configuration, functional architecture, operational procedures, QKD quantum key distribution network.


* 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.3802

## Quantum key distribution networks – Functional architecture

## Corrigendum 1

*Editorial note: This is a complete-text publication. Modifications introduced by this corrigendum are shown in revision marks relative to Recommendation ITU-T Y.3802 (2020).*

### 1 Scope

This Recommendation specifies the functional architecture of quantum key distribution (QKD) networks.

In particular, the scope of this Recommendation includes:

– Functional architecture model;

– Functional elements and reference points;

– Architectural configurations;

– Basic operational procedures.

NOTE – This Recommendation addresses a functional architecture of QKD networks (QKDNs) based on the conceptual structure illustrated in [ITU-T Y.3800] and the functional requirements in [ITU-T Y.3801].

### 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.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.*

### 3 Terms and 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 manager link (KM link)** [ITU-T Y.3800]: A communication link connecting key managers (KMs) to perform key management.

**3.1.3 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.

**3.1.4 quantum key distribution 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.

**3.1.5 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 the 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 quantum key distribution 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.

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

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

## 3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

**3.2.1 key management agent (KMA)**: 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.

**3.2.2 key management agent link**: A communication link connecting key management agents (KMAs) to perform ~~IT-secure~~ key relay and communications for key management.

**3.2.3 key supply agent (KSA)**: 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.

**3.2.4 key supply agent link**: A communication link connecting key supply agents (KSAs) to perform key synchronization and integrity verification.

**3.2.5 quantum key distribution key**: A pair of symmetric random bit strings generated by a pair of quantum key distribution (QKD) modules, particularly referring to random bit strings before being resized and formatted in a key manager.

## 4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

| | |
|---|---|
| AES | Advanced Encryption Standard |
| API | Application Programming Interface |
| FCAPS | Fault, Configuration, Accounting, Performance and Security |
| HMAC | Hash based message authentication code |
| ID | Identifier |
| IPsec | Internet Protocol Security |
| IT-secure | Information-Theoretically secure |
| KM | Key Manager |
| KMA | Key Management Agent |
| KSA | Key Supply Agent |
| MDI-QKD | Measurement Device Independent QKD |
| NTP | Network Time Protocol |
| OTP | One-Time Pad |
| PTP | Precision Time Protocol |
| QAN | QKD Access Network |
| QBER | Quantum Bit Error Rate |
| QBN | QKD Backbone Network |
| QKD | Quantum Key Distribution |
| QKDN | QKD Network |
| QoS | Quality of Service |
| QRNG | Quantum noise Random Number Generator |
| QKD-Rx | QKD Receiver |
| QKD-Tx | QKD Transmitter |
| QoS | Quality of Service |
| RNG | Random Number Generation |
| SPD | Single Photon Detector |
| TF-QKD | Twin Field QKD |
| TLS | Transport Layer Security |

## 5 Conventions

None.

## 6 Functional architecture model

An overview on networks to support quantum key distribution (QKD) including design considerations, network capabilities, conceptual structure and basic functions of a quantum key

distribution network (QKDN) is addressed in [ITU-T Y.3800]. Moreover, QKDN functional requirements are identified in [ITU-T Y.3801].

Based on the conceptual structure of QKDN illustrated in Figure 3 of [ITU-T Y.3800] and the functional requirements identified in [ITU-T Y.3801], a functional architecture model of QKDN is shown in Figure 1.

Figure 1 includes the following architectural essence:

– Layer structure defined in [ITU-T Y.3800]: a quantum layer, a key management layer, a QKDN control layer, a QKDN management layer, a service layer, and a user network management layer;

– Basic functions and links defined in [ITU-T Y.3800]: a QKD module, a key manager (KM), a QKDN controller, and a QKDN manager, a QKD link, and a KM link in the QKDN; a cryptographic application, a user network manager, and an application link in the user network;

– Functional elements defined in this Recommendation: Sub-functions contained in each basic function (e.g., a routing control function under the QKDN controller);

– Detailed reference points defined in this Recommendation.

Detailed descriptions of these functional elements and reference points are given in clause 7 and 8, respectively.

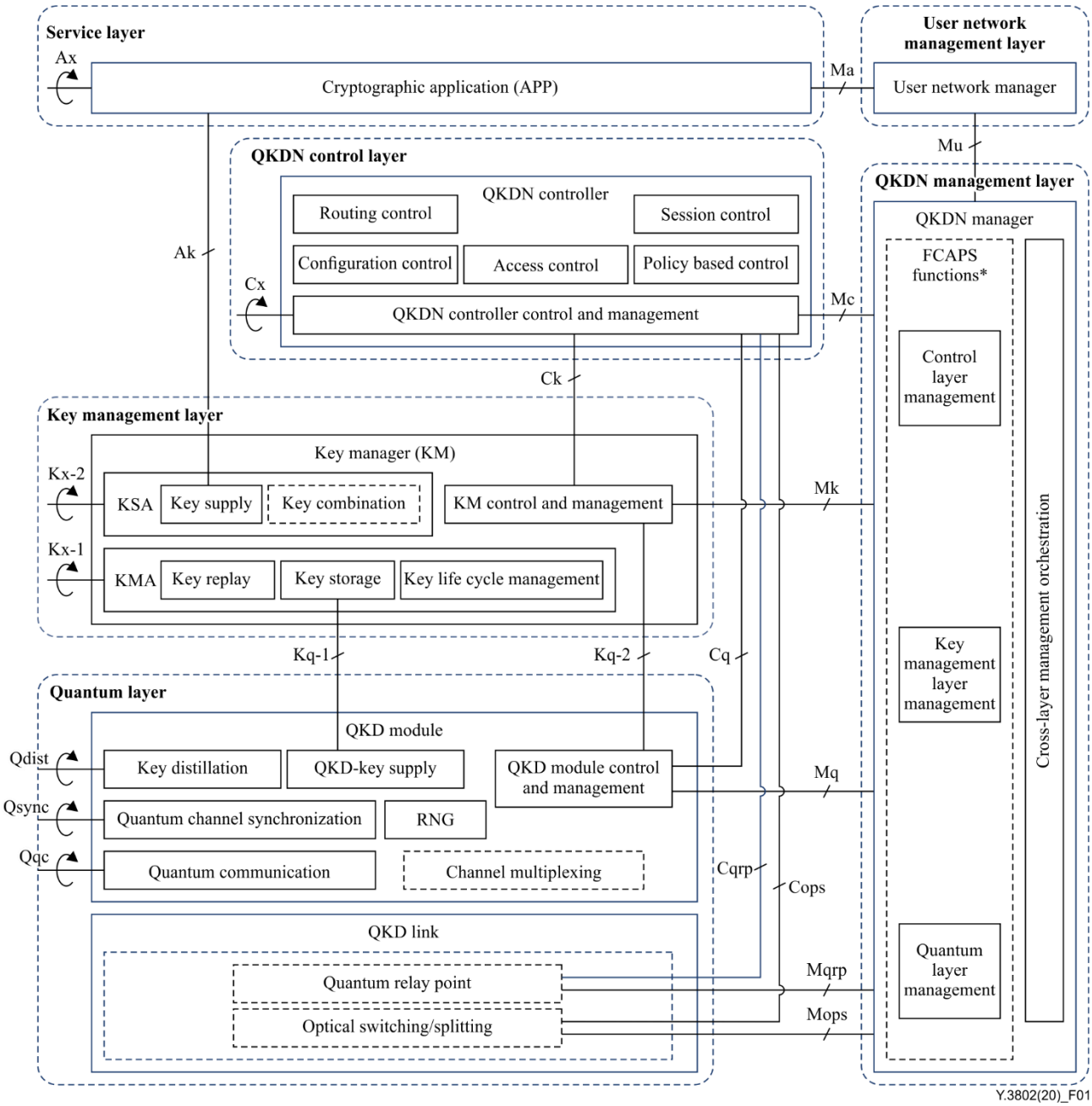


**Figure 1 – A functional architecture model of QKDN**

## 7 Functional elements

### 7.1 Functional elements in a quantum layer

In a quantum layer, a pair of QKD modules connected by a QKD link generates quantum key distribution keys (QKD-keys) by using QKD protocols.

A QKD module is comprised of the following functional elements.

– Quantum communication function: It prepares, transmits, and/or measures quantum signals.

NOTE 1 – In the case of QKD protocols called "prepare-and-measure" schemes, QKD modules can be either transmitters or receivers. In the case of QKD protocols based on measurement-assisted schemes such as measurement device independent QKD (MDI-QKD) and twin field QKD (TF-QKD) mentioned in [ITU-T Y.3800], QKD modules are transmitters, while a receiver is located at an intermediate point of a quantum channel. In the case of entanglement-based QKD protocols, QKD modules are receivers, while a transmitter of entangled quantum signals is located at an intermediate point of the quantum channel.

– Quantum channel synchronization function: It provides clock and timing synchronization for the quantum channel with adequate precision to support quantum signal transmission and measurement. This function may collaborate with the quantum communication function and/or the key distillation function mentioned below in order to provide clock and timing synchronization.

– Key distillation function: It typically performs the following classical data processing:

  a) A key sifting to match modulation and/or measurement bases between QKD modules;

  b) A parameter estimation to ensure security and to set parameters for the error correction and privacy amplification described below;

  c) An error correction and a privacy amplification to establish identical and secure keys between QKD modules.

NOTE 2 – The above classical data processing may be performed jointly.

– QKD-key supply function: It receives QKD-key requests from a key management agent (KMA) and supplies QKD-keys to the KMA securely.

– Random number generator (RNG) function: It generates random numbers and provides them to the quantum communication function and the key distillation function.

NOTE 3 – The RNG should be non-deterministic: This can be realized with conventional physical-noise-based schemes as specified in [b-ISO/IEC 18031], or with quantum principle-based schemes such as quantum noise random number generator (QRNG).

– QKD module control and management function: It is in charge of the overall control and management of functional elements in QKD modules, and communicates with functions in other layers, such as a KM, a QKDN controller, and a QKDN manager.

– Optional channel multiplexing function: It enables the wavelength division multiplexing of quantum and classical channels between QKD modules.

A QKD link optionally includes the following functional elements in addition to quantum signal transmission and classical communications for key distillation and synchronization.

– Optical switching/splitting function: It enables to switch or split quantum channel traffic, and/or quantum channel synchronization signal and distillation channel traffic between pairs of QKD modules in multi-point networks in order to establish the same keys between different users on demand.

– Quantum relay point function: It assists QKD by playing the role as an intermediate point in the QKD link or by relaying quantum and classical signals to extend QKD distance.

NOTE 4 – The optical switching/splitting function and the quantum relay point function may be included in QKD modules and may not have interfaces with the QKDN controller and the QKDN manager. It is dependent upon their implementation.

### 7.2 Functional elements in a key management layer

In a key management layer, a KM function is to receive and manage keys generated by QKD modules and QKD links, relay the keys, and supply the keys to cryptographic applications. The KM consists of a key management agent (KMA), a key supply agent (KSA), and a KM control and management function. In addition, a KM link defined in [ITU-T Y.3800] is divided into the KMA link (Kx-1) and the KSA link (Kx-2) corresponding to their independent roles. These are further comprised of the following functional elements:

1) KMA

– Key storage function: It receives keys from (a) QKD module(s), then synchronizes and authenticates, re-sizes (combines or splits), re-formats the keys with metadata such as key ID, key size, key type and generation time stamp, etc., and stores the processed keys and the metadata;

– Key relay function: It relays the keys from end to end in a QKDN through KMA links in a highly secure manner with an IT-secure encryption, i.e. one-time pad (OTP) [b-Shannon 1949] is recommended;

– Key life cycle management function: It manages the life cycle of the keys from reception by KM to consumption by cryptographic applications. In addition, it manages the deletion or preservation of the keys in the key storage function depending on the key management policies.

2) KSA

– Key supply function: It synchronizes and authenticates the keys shared between end-to-end KSAs through KSA links, and supplies the keys to the cryptographic applications on demand;

– Key combination function: It is an optional functional element. It combines the keys produced by QKD and other key exchange methods (e.g., post-quantum cryptography).

3) KM control and management function

– KM control and management function: It is in charge of the overall control and management of the functional elements in the KM, and communicates with functions in other layers, such as the QKD module, the QKDN controller, and the QKDN manager.

### 7.3 Functional elements in a QKDN control layer

In a QKDN control layer, a QKDN controller function is to control QKDN resources to ensure secure, stable, efficient, and robust operations of a QKDN. It is further comprised of the following functional elements:

– Session control function: It supports the KMAs, and controls the session procedures of key relay. It also supports KSAs to supply keys for multiple cryptographic applications;

– Routing control function: It provisions an appropriate key relay route between two end points of KMs, and also performs rerouting of key relay depending on fault, performance, and/or availability status of the quantum layer and/or the key management layer, for ensuring the continuation of key relay and key supply;

– Configuration control function: It performs the acquisition of configuration information on QKD modules, QKD links, KMs, and KM links, and the state of these components (e.g., in service, out of service, standby, or reserved). It conducts the reconfiguration of QKD links and KM links if an alarm including the result of failure diagnosis is notified;

– Policy based control function: It controls the QKDN resources based on the quality of service (QoS) and charging policies for cryptographic applications;

– Access control function: It provides capabilities to verify the claimed identity of functions and functional elements under control and support by the QKDN controller (i.e., authentication), and to restrict them to pre-authorized activities or roles by access rights based on enforced policies (i.e., authorization).

– QKDN controller control and management function: It is in charge of the overall control and management of the functional elements in the QKDN controller, and communicates with functions in other layers, such as the QKD module, the KM, and the QKDN manager.

### 7.4 Functional elements in a QKDN management layer

In a QKDN management layer, a QKDN manager function is to manage fault, configuration, accounting, performance and security (FCAPS) aspects of a QKDN as a whole, and support user network management. It contains the following functional elements:

– Fault management function: It performs to monitor, detect, diagnose including root causes and analysis, and remedy the faults of QKDN managed resources. It also supports the QKDN controller for the routing and rerouting control of key relay as needed in case of the faults.
– Configuration management function: It manages the provisioning of QKDN resources, collects and manages QKDN topology. Its management roles cover the provisioning, configuration, discovery of the QKDN resources. It also supports the QKDN controller for the provisioning of key relay routes if QKDN supports key relay.
– Accounting management function: It meters the usage of key supply services and support for charging/billing system to determine the costs of key usage by cryptographic applications;
– Performance management function: It monitors and analyses the performance status of the QKDN managed resources. It also supports quality of service (QoS) assurance, QoS policy management and visualizing the QKDN performance information;
– Security management function: It collects/receives security related management information from the QKDN, supports the key life cycle management, and manages the whole authentication and authorization in the QKDN.

For FCAPS management in the QKDN control, the key management, and the quantum layers, the following management functional elements exist:

– QKDN control layer management function: It provides FCAPS management functionality for functional elements in the QKDN control layer. Especially, this functional element supports the QKDN controller to control the routing and rerouting and provisioning of key relay paths in the case of faults and/or performance problems;
– Key management layer management function: It provides FCAPS management functionality for functional elements in the key management layer. In addition, this functional element also supports key life cycle management;
– Quantum layer management function: It provides FCAPS management functionality for functional elements in the quantum layer;
– Cross-layer management function: It orchestrates management decisions and actions among management functions and functional elements in the QKDN control layer, key management layer, and quantum layer. It also exchanges management information with external management elements, especially with a user network management element to indirectly support QKDN users.

### 7.5 Functional elements in a service layer

In a service layer, the following functional element exists:

– Cryptographic application function: It consumes the shared key-pairs provided by a QKDN and performs secure communication between remote parties.

### 7.6 Functional elements in a user network management layer

In a user network management layer, the following functional element exists:

User network manager function: It performs FCAPS management features of a user network.

## 8 Reference points

This clause addresses details of each reference point identified in Figure 1.

The common functionalities of the QKDN reference points including session processing and information exchange are given in Appendix I.

## 8.1 Reference points on a QKD module

The following reference points are relevant to connections between QKD modules in a QKD link:

– **Qqc**: a reference point connecting two quantum communication functions through a quantum channel in the QKD link. It is responsible for exchanging quantum state signals via optical fibre or free space required for quantum communication.

– **Qsync**: a reference point connecting two quantum channel synchronization functions through a classical channel in the QKD link. It is responsible for exchanging information required for quantum channel synchronization.

– **Qdist**: a reference point connecting two key distillation functions through a classical channel in the QKD link. It is responsible for exchanging information on sifting, parameter estimation, error correction and privacy amplification in QKD protocols required for key distillation.

NOTE 1 – A primitive connection in QKD layer is a set of QKD module A, QKD link and QKD module B. Interface specifications at both ends of the QKD link are assumed to be the same; therefore, one single Qqc, Qsync and Qdist in the primitive set are sufficient reference points.

NOTE 2 – Qsync and Qdist are indicated as a single link Qx for simplicity in the figures on QKDN configurations in clause 9.

## 8.2 Reference points on a KM

The following reference points are relevant to connections with KM(s) in a KM link:

– **Kq-1**: a reference point connecting a key storage function in a KMA with a QKD-key supply function in a QKD module. It is responsible for transferring QKD-keys generated by a QKD module to the KM.

– **Kq-2**: a reference point connecting a KM control and management function in the KM with a QKD module control and management function in the QKD module. It is responsible for allowing the QKD module to transmit QKD link parameters to the KM and responsible for allowing the KM to control the operation of the QKD module.

– **Kx-1**: a reference point connecting two KMAs in each QKD node via a KMA link. It is responsible for exchanging information and operations required for key relay, key synchronization and authentication between KMAs.

– **Kx-2**: a reference point connecting two KSAs in each QKD node via a KSA link. It is responsible for exchanging information and operations required for synchronization and authentication of the keys shared between KSAs.

– **Kx'**: a reference point connecting a local KM in each QKD node and a centralized KM via a KM link. It is responsible for exchanging information and operations required for performing centralized key relay. (See Figure 5 in clause 9)

NOTE – Kx-1 and Kx-2 are indicated as a single link Kx for simplicity in figures on QKDN configurations in clause 9.

## 8.3 Reference points on a QKDN controller

The following reference points are relevant to communications for QKDN controller(s).

– **Ck**: a reference point connecting the QKDN controller control and management function in a QKDN controller and a KM control and management function in a KM. It is responsible for the QKDN controller to communicate control information with a KMA and a KSA.

– **Cq**: a reference point connecting the QKDN controller control and management function in the QKDN controller with a QKD module control and management function in a QKD module. It is responsible for the QKDN controller to communicate control information with the QKD module.

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

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

– **Cx**: a reference point connecting two QKDN controller control and management functions in each QKD node. It is responsible for the two QKDN controllers to communicate control information with each other.

### 8.4 Reference points on a QKDN manager

The following reference points are relevant to communications for a QKDN manager.

– **Mq**: a reference point connecting the QKDN manager with a QKD module control and management function in a QKD module. It is responsible for the QKDN manager to communicate management information with the QKD module.

– **Mops**: a reference point connecting the QKDN manager and an optical switching/splitting function in a QKD link. It is responsible for the QKDN manager to communicate management information with the QKD link.

– **Mqrp**: a reference point connecting the QKDN manager and a quantum relay point function in a QKD link. It is responsible for the QKDN manager to communicate management information on the quantum relay point with the QKD link.

– **Mk**: a reference point connecting the QKDN manager and a KM control and management function in a KM. It is responsible for the QKDN manager to communicate management information with a KMA and a KSA.

– **Mc**: a reference point connecting the QKDN manager and a QKDN controller control and management function in a QKDN controller. It is responsible for the QKDN manager to communicate management information with the QKDN controller.

– **Mu**: a reference point connecting a user network manager in a user network and the QKDN manger in the QKDN. It is responsible for the QKDN manager to communicate management information with the user network manager.

### 8.5 Reference point on a user network manager

– **Ma**: a reference point connecting a cryptographic application and a user network manager in a user network. It is responsible for management of the cryptographic application.

### 8.6 Reference points on cryptographic applications

The following reference points are relevant to communications of cryptographic applications in user networks:

– **Ak**: a reference point connecting a cryptographic application and a key supply function in a KSA. It is responsible for sending key requests from the cryptographic application to the KSA, performing authentication between the cryptographic application and the KSA, and supplying keys from the KSA to the cryptographic application.

– **Ax**: a reference point connecting two cryptographic applications in a user network. It is responsible for the two cryptographic applications to exchange information based on communication protocols.

NOTE – The communication protocols used for Ax may include Internet protocol security (IPsec) [b-RFC 4301], Transport Layer Security (TLS) [b-RFC 8446], or other dedicated cryptographic protocols.

## 9 Architectural configurations

There are multiple possible network configurations of inter-connecting various entities supported within the QKDN architecture.

Under the functional architecture model defined in clause 6, a QKDN consists of different types of nodes that contain various functions in different configurations as illustrated in this clause.

NOTE – Nodes defined in this clause are logical entities that are individually identifiable in the QKDN. As logical objects, such nodes may or may not be mapped to physical objects.

### 9.1 Configuration 1: Distributed QKDN

A configuration of a distributed QKDN is illustrated in Figure 2 as configuration 1.

In configuration 1, the QKDN consists of type 1 QKD nodes.

Each type 1 QKD node can perform QKDN functions in a distributed manner, without relying on a centralized network controller.

The type 1 QKD node contains the functions of QKD module(s), a KM and a QKDN controller.

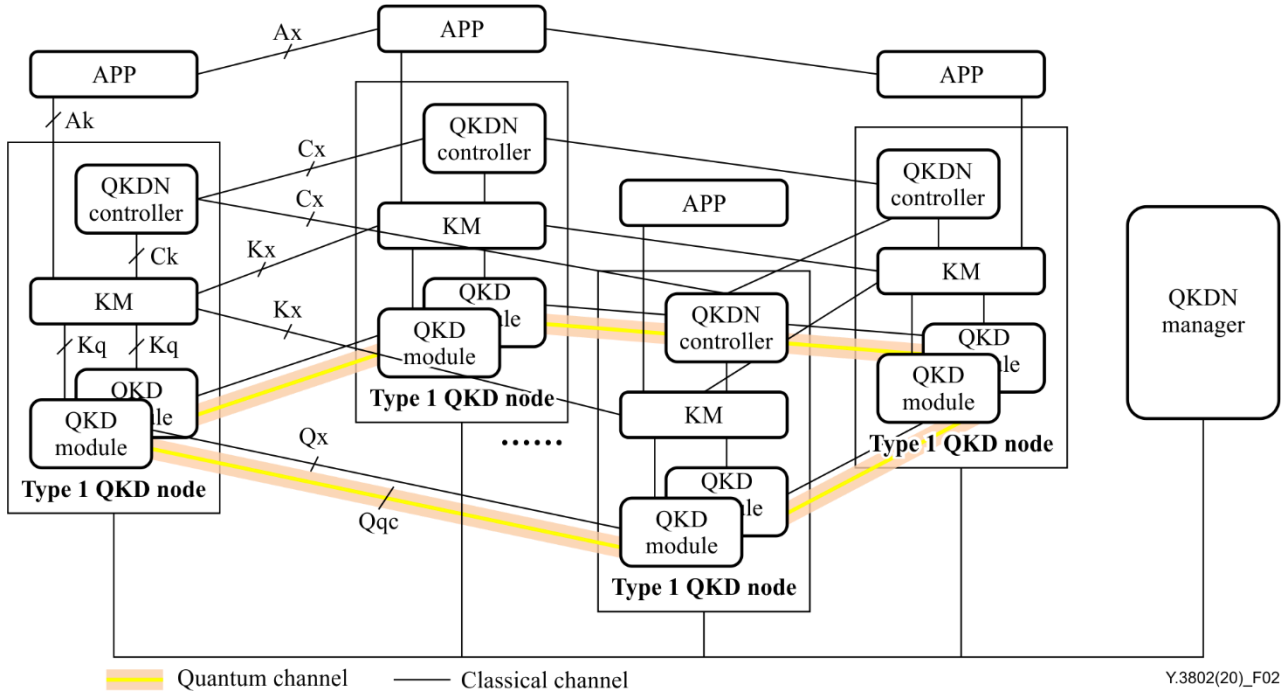


**Figure 2 – Configuration 1 of a distributed QKDN**

NOTE – An abbreviation "APP" appearing in the figures of clause 9 means cryptographic application.

### 9.2 Configuration 2: Centralized QKDN

To support efficient management of QKDN, it is a typical approach to centralize QKDN control functions in order to improve network control efficiency.

A configuration of centralized QKDN is illustrated in Figure 3 as configuration 2.

In configuration 2, the QKDN consists of type 2 QKD nodes and the centralized one or more QKDN controllers.

The type 2 QKD node contains the functions of QKD module(s) and a KM.

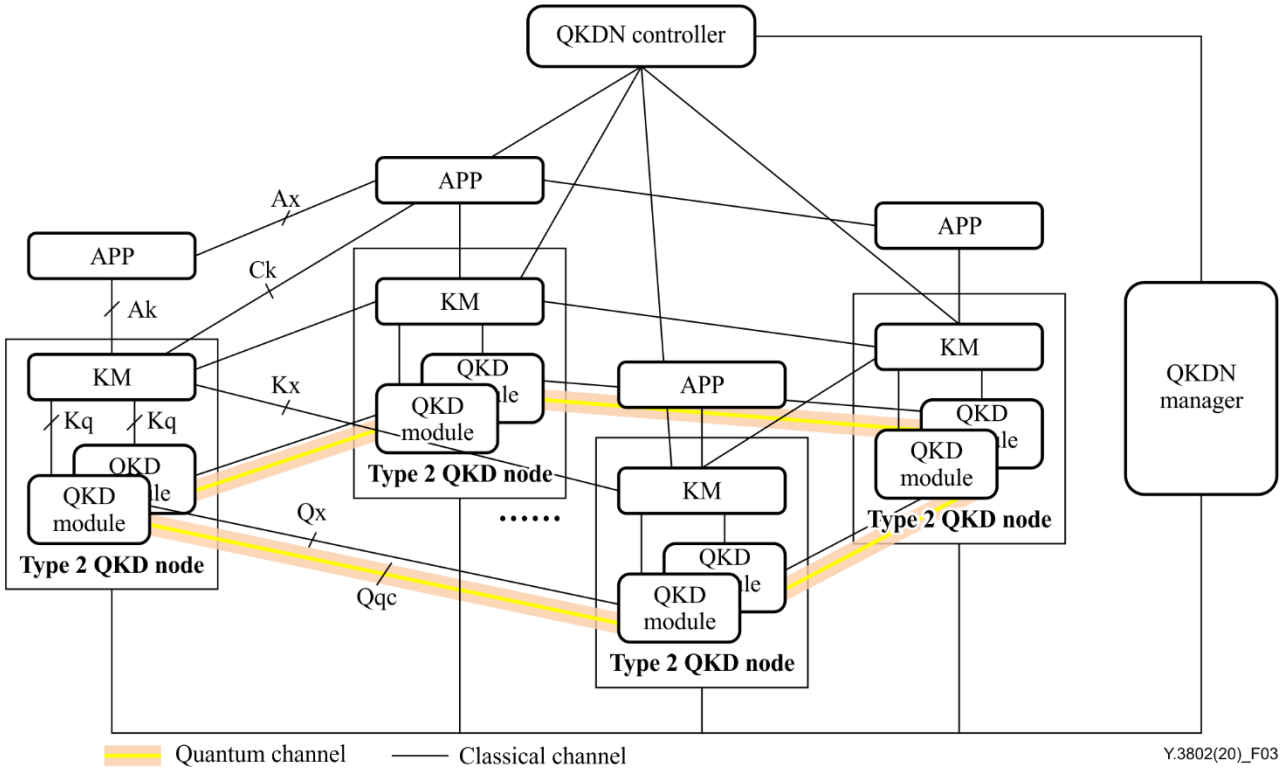


**Figure 3 – Configuration 2 of a centralized QKDN**

## 9.3 Configuration 3: Centralized QKDN with hierarchical QKD nodes

To support wide-area QKD network deployment and operation, the type 2 QKD nodes in clause 9.2 can be further classified into three kinds of nodes according to their roles: a QKDN user node, a QKDN access node and a QKDN relay node. A configuration of centralized QKDN with hierarchical QKD nodes is illustrated in Figure 4 as configuration 3.

1) QKDN user node

A QKDN user node is a trusted node which is located at QKD user side. It is in charge of obtaining keys from the QKDN, and providing the corresponding key for a specific cryptographic application for secure communication. The user node is comprised of a QKD module and a KM. It is conventional that the user node only contains one QKD-Tx to reduce user device cost. The KM of the user node performs key storage, key supply and key relay functions.

2) QKDN access node

A QKDN access node is a trusted node which is responsible for aggregating associated user nodes' key relaying service flows and forwarding them to remote QKD nodes according to key relay procedure. A user node can connect to the access node either directly or via an optical switch. The optical switch can be one optional component of the access node, which integrates multiple quantum channels in order to receive quantum signals from a plurality of user nodes simultaneously.

It is conventional that the access node contains a powerful QKD-Rx to handle the signals of associated user nodes. A multi-user scheduling function is integrated to allocate channel resources to the multiple associated user nodes respectively.

In addition, the access node can contain additional QKD modules to connect to remote QKD nodes (e.g., relay nodes) for key relay.

The KM of the access node is to perform key storage and key relay functions.

3) QKDN relay node

AQKDN relay node is a trusted node which is used to set up key relay routes in order to extend a QKD distance beyond the limitation of QKD quantum channels. The relay node usually contains at least one pair of a QKD-Tx and a QKD-Rx to connect at least two hops in QKD links. The KM of the relay node is to perform key storage and key relay functions.

Through the combination of user nodes, access nodes and relay nodes, this architectural configuration can support flexible QKDN topology. For example, multiple user nodes and their associated access nodes can form a QKD access network (QAN), which is suitable for metropolitan area coverage. And multiple relay nodes can form a QKD backbone network (QBN) to connect multiple QANs for wide area coverage.

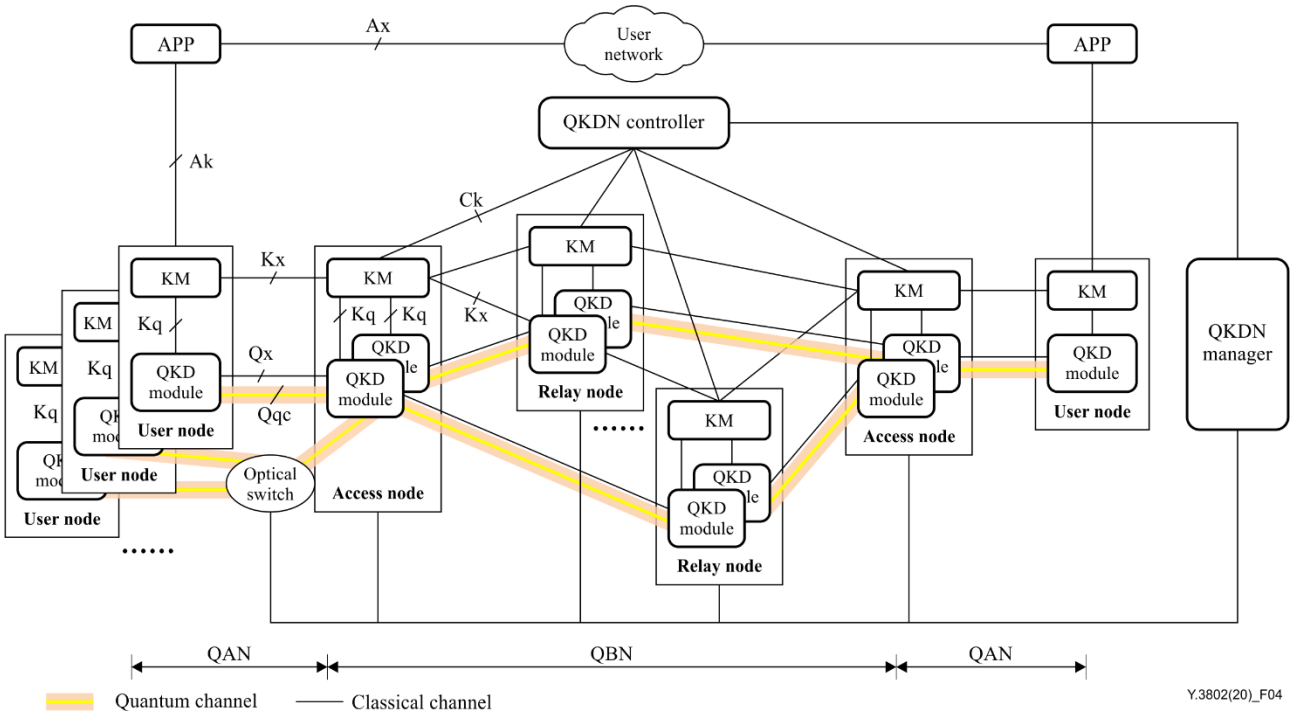


**Figure 4 – Configuration 3 of a centralized QKDN with hierarchical QKD nodes**

## 9.4 Configuration 4: Centralized QKDN with centralized key relay

There is another variation of the configurations of centralized QKDN as configuration 4. In configuration 4, key relay functions of KMs are centralized and can be co-located with a centralized QKDN controller as shown in Figure5.

In this way, the peer-to-peer mutual interaction interfaces between the QKD nodes in KM links can be removed, and thus, the complexity of QKD nodes can be further reduced, and the networking overhead is also reduced.

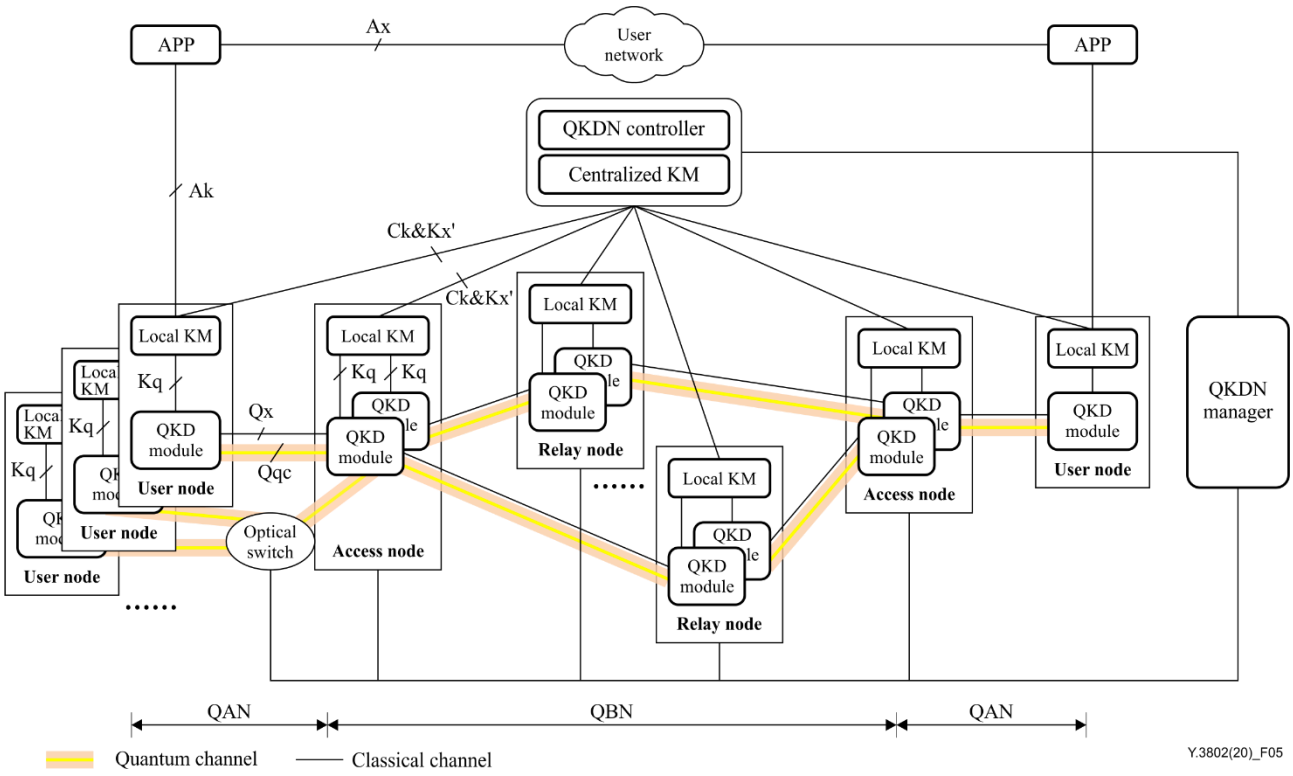


**Figure 5 – Configuration 4 of a centralized QKDN with centralized key relay**

## 10 Basic operational procedures of the QKD network functions

This clause describes basic operational procedures based on the functional architecture model defined in clause 6.

### 10.1 Service provisioning and system initialization procedure

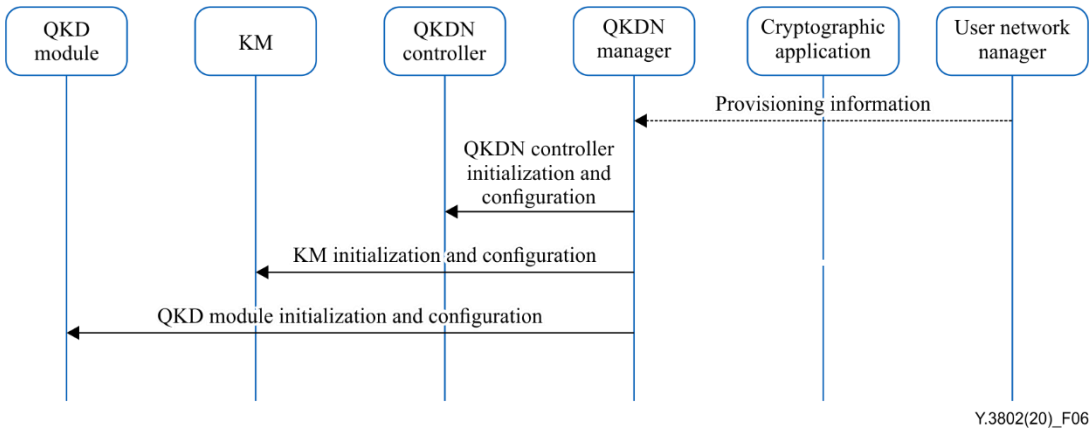


**Figure 6 – Service provisioning and system initialization procedure**

Figure 6 illustrates a procedure for service provisioning and system initialization. There are two alternatives for service provisioning.

In case where a user network manager is in charge of service provisioning, the user network manager provides service provisioning information including profiles of cryptographic applications to a QKDN manager.

On the other hand, in case where the QKDN manager is in charge of service provisioning as standalone mode, the QKDN manager uses its own service provisioning information directly.

According to the provisioning information, the QKDN manager initiates the action of a QKDN controller, a KM and a QKD module to initialize and configure a QKDN. The sequence of the initialization and configuration of the QKDN controller, the KM and the QKD module can be in arbitrary order.

## 10.2 Key generation procedure

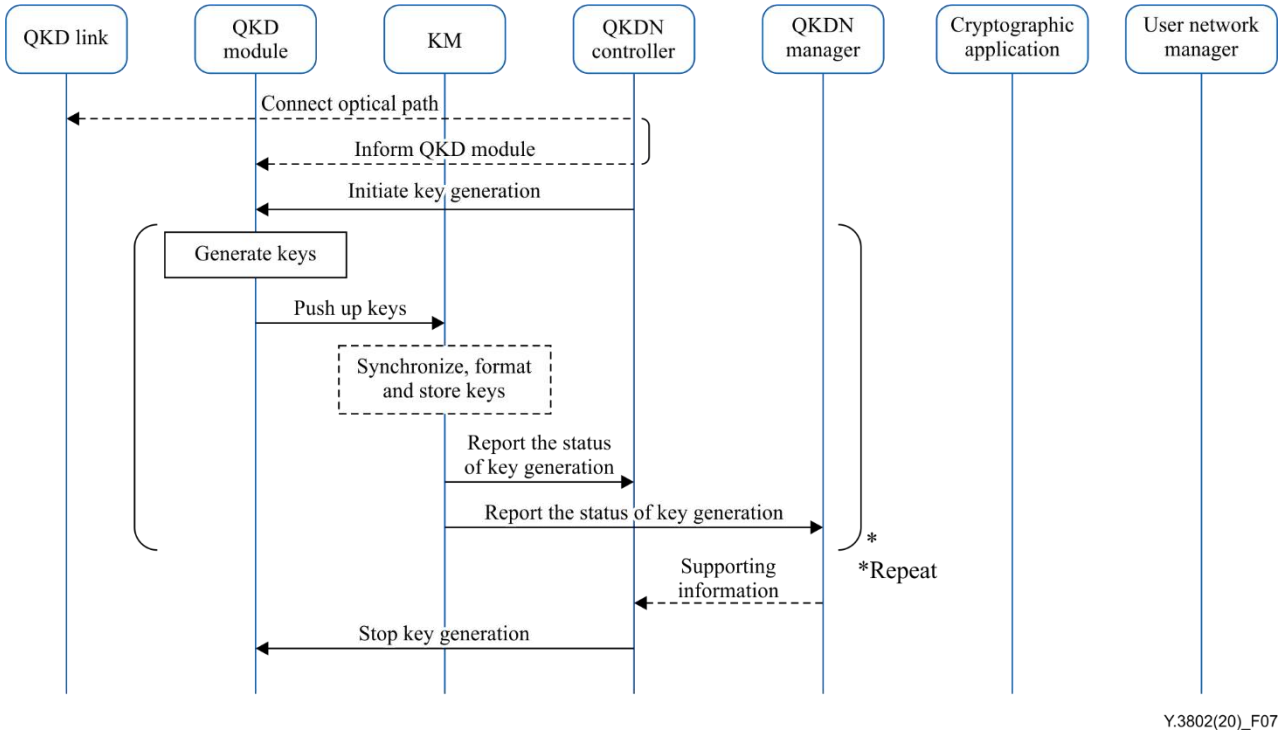


**Figure 7 – Key generation procedure**

Figure 7 illustrates a procedure for key generation containing the following steps:

1) A QKDN controller optionally instructs to initiate the connection of an optical path in a QKD link and informs QKD modules of the initiation result if necessary.
2) The QKDN controller requests QKDN modules to initiate key generation.
3) The QKD modules send and/or receive quantum signals and then perform synchronization of quantum signals and key distillation for key generation.
4) The QKD modules push up the generated keys to KMs.
5) The KMs optionally synchronize, format and store these keys if necessary.
6) The KMs report the status of key generation to the QKDN controller and the QKDN manager for control and management functions respectively.
7) The sequence from step 3 to step 6 can be repeated (and often executed in parallel) until a sufficient number of keys are generated.
8) The QKDN manager optionally sends supporting information to the QKDN controller if necessary.
9) The QKDN controller requests to stop key generation to the QKD modules due to the completion of key generation or other reasons.

## 10.3 Key request and supply procedure

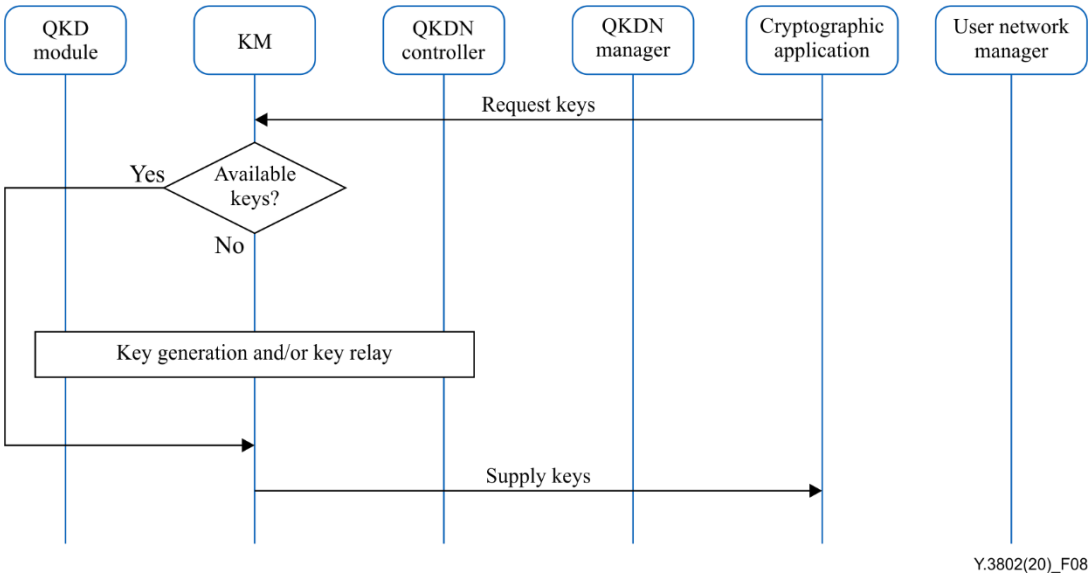


**Figure 8 – Key request and supply procedure**

Figure 8 illustrates a typical procedure for key request and supply containing the following steps:

1) A cryptographic application in a user network requests secure keys from a corresponding KM in a QKDN.

2) The KM checks the availability of keys, which are shared with a matching KM corresponding to a matching cryptographic application, to supply to the cryptographic application:

   a) If the KM has a sufficient amount of available keys, then go to step 3;

   b) If the KM does not have the available keys, the KM gets the available keys through key generation and/or key relay processes.

3) The KM supplies keys to the requesting cryptographic application.

## 10.4 Key relay procedure

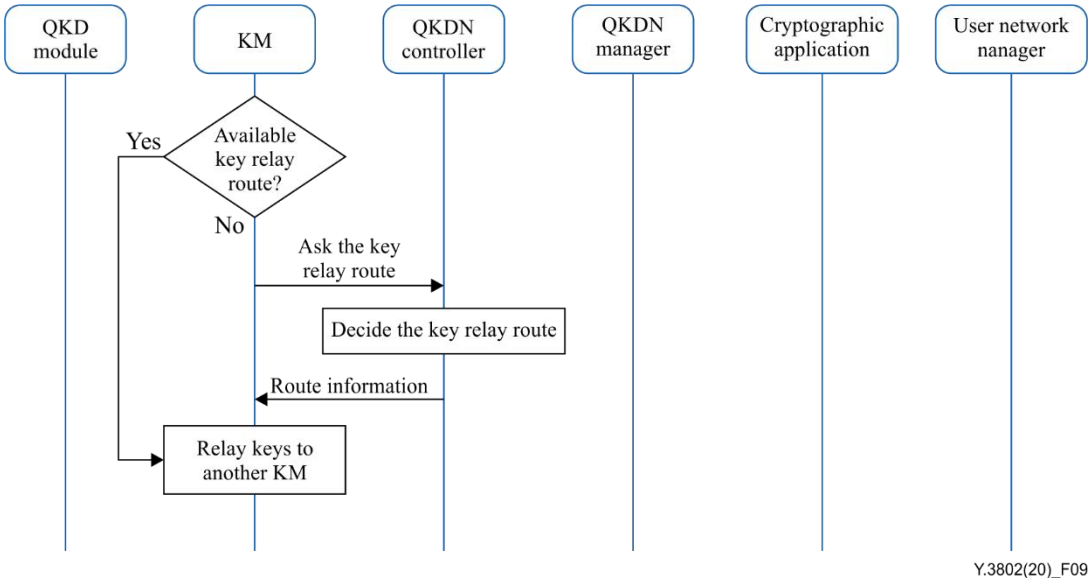


**Figure 9 – Key relay procedure**

Figure 9 illustrates a procedure for key relay containing the following steps:

1) When key relay is needed, a KM checks the availability of key relay routes:
   a) If the KM confirms an available key relay route for the KM to relay keys to another KM, then go to step 3;
   b) If the KM does not have the available key relay route to relay keys, the KM can request the key relay route to a QKDN controller.
2) The QKDN controller decides a key relay route and sends route information to the KM.
3) The KM executes key relay.

## 10.5 Key relay rerouting control procedure

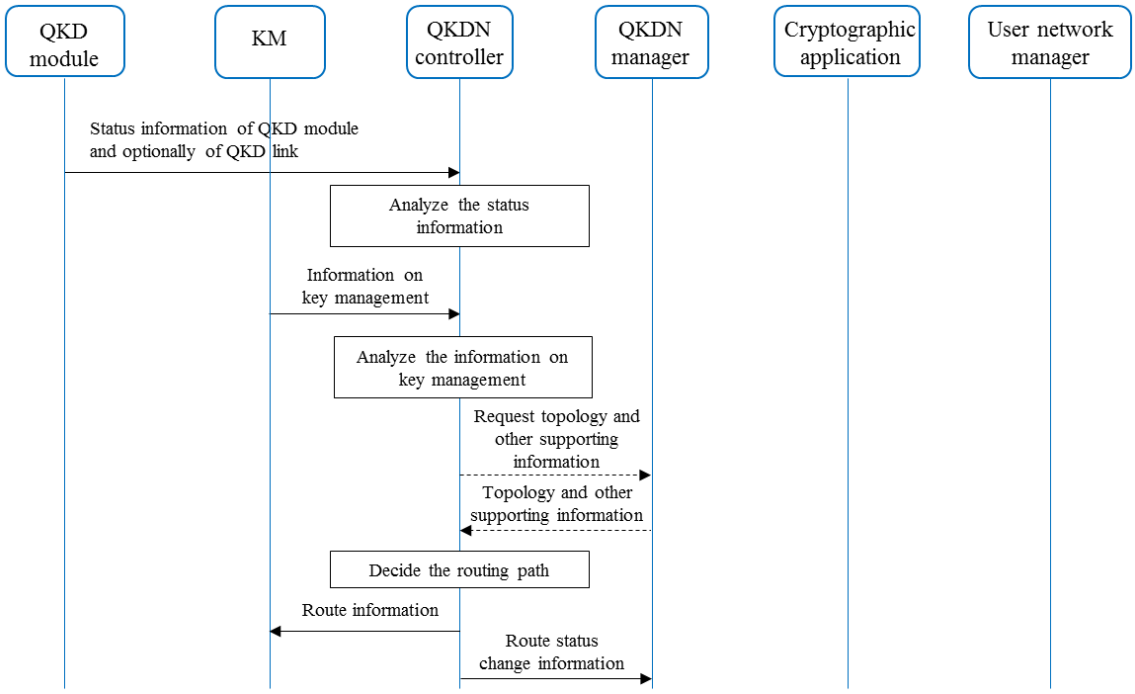


**Figure 10 – Key relay rerouting control procedure**

Figure 10 illustrates a procedure for key relay rerouting control by a QKDN controller containing the following steps:

1) A QKD module sends status information (e.g., fault, performance, availability) of the QKD module and optionally of a QKD link to a QKDN controller.
2) A KM sends information on key management to the QKDN controller.

The information in step 1 and step 2 are periodically updated by the QKD module and the KM so that the QKDN controller can successively monitor the status of QKD links, QKD modules, KM links and KMs.

3) The QKDN controller analyzes the provided information and decides whether the rerouting of key relay is necessary or not.
4) The QKDN controller sends updated route information to the KM and reports the route status change information to the QKDN manager.

# 11 QKDN synchronization function considerations

Similar to other existing types of communication networks, a QKDN also needs to support frequency and time synchronization.

A quantum channel synchronization function is required to implement synchronization of quantum-state optical signals between QKD modules. It needs an ultra-high precision requirement (at picoseconds level) and cannot be fulfilled by the recent existing standardized network-based synchronization technologies.

Except for the quantum channel synchronization, the synchronization for other QKDN functions can be supported by traditional network-based synchronization technologies.

NOTE 1 – Network time protocols (NTPv3 [b-RFC 1305] or NTPv4 [b-RFC 5905]) support synchronization with milliseconds precision. They can be used to satisfy classical channel synchronization requirements of QKDN.

NOTE 2 – The QKDN synchronization function requirements and supporting technologies are further analysed in Appendix II.

## 12 Security considerations

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

# Annex A

## Functional elements in the quantum layer

(This annex forms an integral part of this Recommendation.)

Figure A.1 illustrates the relationship among the functional elements in a quantum layer. In Figure A.1, a centralized QKDN controller model is employed as an example.

An optical switching/splitting and a quantum relay point in a QKD link are optional functional elements and do not need to be trusted. Depending on the implementation, these functional elements may be connected to a QKDN controller and a QKDN manager via specific reference points. Definitions of reference points, Qdist, Qsync, and Qqc, may vary depending on the implementation of the QKD link. Typical implementation examples are described below:

- **No intermediate functional elements in the QKD link**:

In this case, two QKD modules are directly connected. Qdist, Qsync and Qqc are simple reference points between the two QKD modules.

- **Optical switching/splitting in the QKD link**:

The optical switching/splitting functional element can typically switch/split a quantum channel and a classical channel for synchronization, and optionally switch/split the classical channel for key distillation when it is multiplexed with the quantum channel and the classical channel for synchronization in the same fiber.

In this case, Qdist, Qsync and Qqc are also treated as the reference points between two QKD modules while these channels are connected through the optical switching/splitting functional element.

- **Quantum relay point in the QKD link**:

A quantum relay point functional element is used for some QKD protocols or it acts as a quantum repeater for fully quantum networking as illustrated in clause 6.2 of [ITU-T Y.3800].

For twin-field QKD (TF-QKD) and measurement device independent QKD (MDI-QKD) protocols, the quantum relay point acts as an intermediate measurement station receiving quantum signals sent from the QKD modules. For entanglement-based QKD protocols, the quantum relay point is an entanglement source which distributes entangled pairs to the QKD modules. In these cases, Qqc and Qsync are reference points between the QKD module and the quantum relay point. For TF-QKD and MDI-QKD protocols, Qdist is split into two reference points where one is in between the QKD module and the quantum relay point, and the other is in between the two QKD modules. For entanglement-based QKD protocols, Qdist is a reference point between the QKD modules.

For fully quantum networking, the quantum relay point acts as the quantum repeater. The main role of the quantum repeater is to distill and distribute entanglement to the QKD modules. In this case, Qqc and Qsync are reference points between the QKD module and the quantum relay point. Qdist is split into two reference points: one is in between the QKD module and the quantum relay point, and the other is in between the two QKD modules. These two reference points are used as classical channels for entanglement distillation among the QKD modules and the quantum relay point, and, if necessary, also used for key distillation between the QKD modules. Details of these functions and exchanged information through the reference points may vary depending on protocols of the quantum repeater and their implementations.

NOTE – The entanglement distillation is a protocol to distil entanglement from distributed quantum signals via local quantum operations and classical communication. The classical communication may be done through the reference point Qdist. The local quantum operations do not require any reference point.

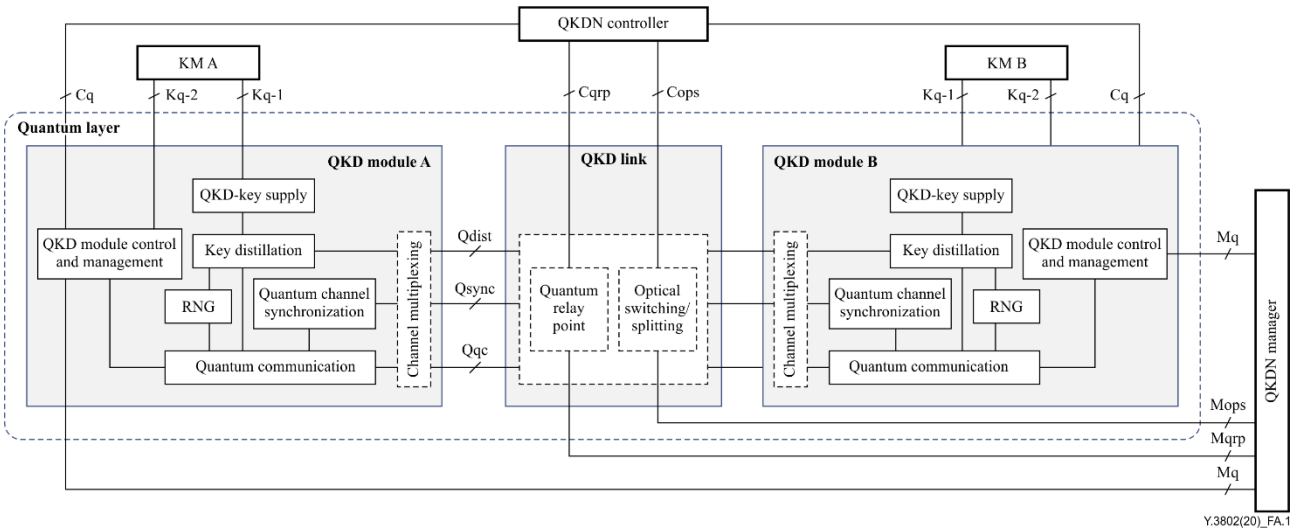


**Figure A.1 – Relationship among sub-functions in the quantum layer**

# Appendix I

## Common functionalities for reference points

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

At the reference points in clause 8, a QKDN may have the following common functionalities:

### I.1 Session processing functionalities

To assure the reliability and performance of session operations across a reference point, the following functionalities are expected to be provided by the QKDN:

**Overload control**: It supports overload control for preventing the overflow of information messages exchanged.

**Synchronization and audit**: It supports synchronization and audit of the session status in support of recovery and operational information statistics and auditing.

**Session state maintenance**: It enables the session state to be maintained using either soft-state or hard-state approaches.

### I.2 Information exchange functionalities

The following information exchange functionalities are provided for the reference points:

**Request-response transactions**: It allows a requesting function or functional elements to request a transaction to be performed by a responding function and get a correlated response in return.

**Notifications**: It supports the notification of asynchronous events between functions in two layers.

**Reliable delivery**: It provides reliable delivery of messages.

**Capability estimation**: It determines the capabilities of appropriate corresponding layer functions.

**Cross layer security**: It supports the authentication between two layers such that requests from unauthenticated sources cannot be performed and such that each layer can verify the source sending notifications.

# Appendix II

## Synchronization function and implementation in QKD network

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

Synchronization technology including frequency and time synchronization, is considered to play a fundamental supporting role in ICT networks, including a QKDN.

Considering the trade-off between implementation cost and technology maturity, the selection of synchronization technology is suggested to match synchronization requirements. For example, the synchronization requirements on configuration query/delivery, life cycle management, information update and fault diagnosis in the existing information communication networks are usually at the level of tens of millisecond accuracy. In most instances, the Network Time Protocol (NTP) technology can fulfill this synchronization requirement, NTP is commonly applied in IP networks.

In a typical prepare-and-measurement-based discrete variable QKD system, the transmitter for synchronization will send optical pulses synchronized to the quantum signal through a synchronization channel to the receiver. The detected synchronization signal with frequency-and-phase recovery is used as the trigger of a single photon detector (SPD) in the receiver. For typical continuous variable QKD, which is based on transmitter with gaussian modulation and a receiver with coherent detection, a physical layer synchronization channel is optional.

The typical pulse width of the quantum signal and effective SPD detection response time window are at about the hundreds picoseconds level, the jitter of these signals and responses are usually limited to hundreds of picoseconds, which means the precision requirement of frequency synchronization between transmitter and receiver need to achieve sub-microsecond level.

The current network-based frequency synchronization solutions cannot fulfill the precision requirement of the QKD link, and thus a point-to-point synchronization-channel-based frequency synchronization is the practical solution.

For key supply of the QKDN, the QKD-key generation time information needs to be attached to the corresponding key metadata with other necessary information such as device ID. The QKD-key generation rate of commercially available QKD systems is typically at several tens Kbit/s, which means QKD-key generation time information will be updated at the tens of milliseconds level and thus NTP-based network frequency synchronization could be adequate for that precision requirement.

If the QKD-key generation rate could be significantly enhanced in the future, the timing precision of these keys should be improved accordingly, other kinds of network time and synchronization solutions such as Precision Time Protocol (PTP) could be used. Furthermore, absolute time information provided by NTP can also be used by a QKDN control unit for alarm and performance monitoring.

In a key management layer, a KM stores point-to-point key pairs generated by QKD modules and provides end-to-end keys through a key relay function. In key storage and relay procedures, a key life cycle needs to be managed according to security requirements, such as key authentication, backup, destruction, and storage time management. NTP-based network time-and-frequency synchronization information with tens of millisecond precision timing reference can be attached to the QKD-key metadata to indicate timestamp information such as generation time, relay time, storage time, provisioning time, and destruction time. For monitoring and reporting of alarm and performance information of the KM, it is also necessary to support NTP-based time synchronization with millisecond precision in the main control unit of the KM, so that the QKDN can realize unified time domain management of the entire network.

In the QKDN control and management layer, a master clock can be co-located within a QKDN manager in the QKDN. It can provide the reference timing information to the other functions to

implement unified time domain management of the QKDN. On this basis, the QKDN manager and/or controller can monitor the alarm information and performance parameters of the QKD module and KM in the QKDN, as well as the diagnosis and identification of the network link status and faults, and further provide the necessary time reference information for the interaction between the QKDN and a user network.

# Bibliography


[b-ETSI GR QKD 007] ETSI Group Report GR QKD 007 (2018), *Quantum Key Distribution (QKD); Vocabulary*.

[b-ISO/IEC 18031] ISO/IEC 18031, *Information technology − Security techniques − Random bit generation*.

[b-RFC 1305] IETF RFC 1305 (1992), *Network Time Protocol (Version 3) Specification, Implementation and Analysis.*

[b-RFC 4301] IETF RFC 4301 (2005), *Security Architecture for the Internet Protocol.*

[b-RFC 5905] IETF RFC 5905 (2010), *Network Time Protocol Version 4: Protocol and Algorithms Specification.*

[b-RFC 8446] IETF RFC 8446 (2018), *The Transport Layer Security (TLS) Protocol Version 1.3.*

[b-Shannon 1949] Shannon, Claude, 1949, *Communication Theory of Secrecy Systems, Bell System Technical Journal,* vol. 28, pp. 666–682.

## 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