International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3800

(10/2019)

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

Cloud Computing

Overview on networks supporting quantum key distribution

Recommendation ITU-T Y.3800

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.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.3800

Overview on networks supporting quantum key distribution

Summary

Recommendation ITU-T Y.3800 gives an overview on networks supporting quantum key distribution (QKD).

This Recommendation aims to provide support for the design, deployment, operation and maintenance for the implementation of QKD networks (QKDNs), in terms of standardized technologies.

The relevant network aspects of conceptual structure, layered model and basic functions are within the scope of the Recommendation to support its implementation.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3800	2019-10-25	13	11.1002/1000/13990

Keywords

Key management, key relay, key supply, QKD, QKD network, quantum key distribution.

* 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 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

Introduction

Quantum key distribution (QKD) technologies provide the means to distribute symmetric random bit strings as a secure key that can be proven to be secure even against an eavesdropper with an unbounded computational ability. As computing technologies, such as artificial intelligence (AI) and quantum computing, are advancing rapidly, QKD technologies are expected to be important to secure the transmission of critical data.

QKD is an add-on technology and service to communication networks. QKD network (QKDN) is a technology that extends the reachability and availability of QKD. The introduction of QKDN into current communication networks and cryptographic infrastructures brings new challenges to the design of the network architecture and security considerations, as QKD technologies have their unique features and restrictions. For example, QKD needs particular physical channels, i.e., quantum channels, and it is basically a point-to-point link technology. Keys generated by QKD should be properly managed and relayed in the network while taking into account various network security threats.

Therefore, there is a strong need to establish standards regarding the use of QKD technologies in networks. This Recommendation is an overview that provides basic QKDN conceptual structures with a clear security boundary. This is the first Recommendation of a series of QKDN Recommendations that cover various aspects such as network architectures and network security. Requirements will be for further study. As QKD and related technologies are in rapid progress, novel technologies and conceptual structures may emerge in the future. This Recommendation might be revised to take into account the future progress of technologies and standardization.

Recommendation ITU-T Y.3800

Overview on networks supporting quantum key distribution

1 Scope

This Recommendation gives an overview on networks supporting quantum key distribution (QKD) and addresses network aspects to implement QKD technologies.

In particular, this Recommendation addresses the following:

- an overview of QKD technologies;
- network capabilities to support QKD;
- conceptual structure and basic functions of QKD networks (QKDNs).

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 classical channel [b-ETSI GR QKD 007]: Communication channel that is used by two communicating parties for exchanging data encoded in a form that may be non-destructively read and fully reproduced.

3.1.2 quality of service (QoS) [b-ITU-T Q.1743]: The collective effect of service performances, which determine the degree of satisfaction of a user of a service. It is characterized by the combined aspects of performance factors applicable to all services, such as:

- service operability performance;
- service accessibility performance;
- service retainability performance;
- service integrity performance; and
- other factors specific to each service.

3.1.3 quantum channel [b-ETSI GR QKD 007]: Communication channel for transmitting quantum signals.

3.1.4 quantum key distribution (QKD) [b-ETSI GR QKD 007]: Procedure or method for generating and distributing symmetrical cryptographic keys with information theoretical security based on quantum information theory.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 application link: A communication link used to provide cryptographic applications in the user network.

3.2.2 information theoretically secure (IT-secure): Secure against any deciphering attack with unbounded computational resources.

3.2.3 key life cycle: 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.

3.2.4 key management: 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.

3.2.5 key manager (KM): A functional module located in a quantum key distribution (QKD) node to perform key management in the key management layer.

3.2.6 key manager link: A communication link connecting key managers (KMs) to perform key management.

3.2.7 key relay: A method to share keys between arbitrary quantum key distribution (QKD) nodes via intermediate QKD node(s).

3.2.8 key supply: A function providing keys to cryptographic applications.

3.2.9 quantum key distribution module: 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).

3.2.10 quantum key distribution link: 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.

3.2.11 quantum key distribution network (QKDN): 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.

3.2.12 quantum key distribution network controller: A functional module, which is located in a quantum key distribution (QKD) network control layer to control a QKD network.

3.2.13 quantum key distribution network manager: A functional module, which is located in a quantum key distribution (QKD) network management layer to monitor and manage a QKD network.

3.2.14 quantum key distribution node: 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).

3.2.15 security demarcation boundary: A security boundary to demarcate quantum key distribution network's responsibility on keys to be supplied from the user network's responsibility on keys for use.

3.2.16 user network: 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.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AES	Advanced Encryption Standard

API	Application Programming Interface
HMAC	Hash-based message authentication code
ICT	Information and Communication Technology
ID	Identifier
IT-secure	Information-Theoretically secure
KM	Key Manager
MDI-QKD	Measurement Device Independent QKD
OTP	One-Time Pad
P-to-P	Point-to-Point
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
QKDN	QKD Network
QoS	Quality of Service
QKD-Rx	QKD Receiver
TF-QKD	Twin Field QKD
QKD-Tx	QKD Transmitter

5 Conventions

None.

6 Overview of QKD technologies

6.1 QKD technologies

A QKD protocol allows the distribution of symmetric random bit strings as a secure key that can be proven to be secure, even against an eavesdropper with unbounded computational resources under some assumptions supporting the security proof model. This kind of security is referred to as information theoretic security. Since a QKD protocol is based on the laws of quantum mechanics, implementation security should be taken into account [b-ETSI White Paper 8], [b-IEEE Trans. Inf. Theory 39]. Keys generated by QKD modules implementing the QKD protocol can be consumed by any cryptographic applications using symmetric keys such as one time pad (OTP) [b-cryptomuseum] encryption, advanced encryption standard (AES) [b-ISO/IEC 18033-3], [b-FIPS PUB 197] and hash based message authentication code (HMAC) [b-FIPS PUB 198] authentication, among others.

The basic elements of a QKD are a transmitter (QKD-Tx) and a receiver (QKD-Rx), each of which is referred to as a QKD module. A QKD link connects the QKD modules, potentially with the help of a quantum relay point (See clause 6.2). The keys are shared via the QKD link. The QKD link usually consists of a quantum channel and a classical channel. The quantum channel is reserved for quantum signals, such as a single-photon-level coherent state of light, to transmit random bit strings. The classical channel is reserved for synchronization and data exchange between the QKD modules. Figure 1 illustrates an example of applying QKD to secure a point-to-point (P-to-P) application link. QKD modules generate keys and supply them to the applications. The application link where encrypted data is transmitted can be any communication link in a conventional or a future network. Therefore, QKD is an add-on technology (and service) to existing or future networks. This situation does not change even if QKD is networked as described below. The key can be proven to be information theoretically secure (IT-secure) of the QKD protocol but further assumptions are needed for implementations of QKD modules. Information theoretical security of QKD is guaranteed by the laws of quantum mechanics and quantum information theory. The details of the security aspects, however, are outside the scope of this Recommendation.

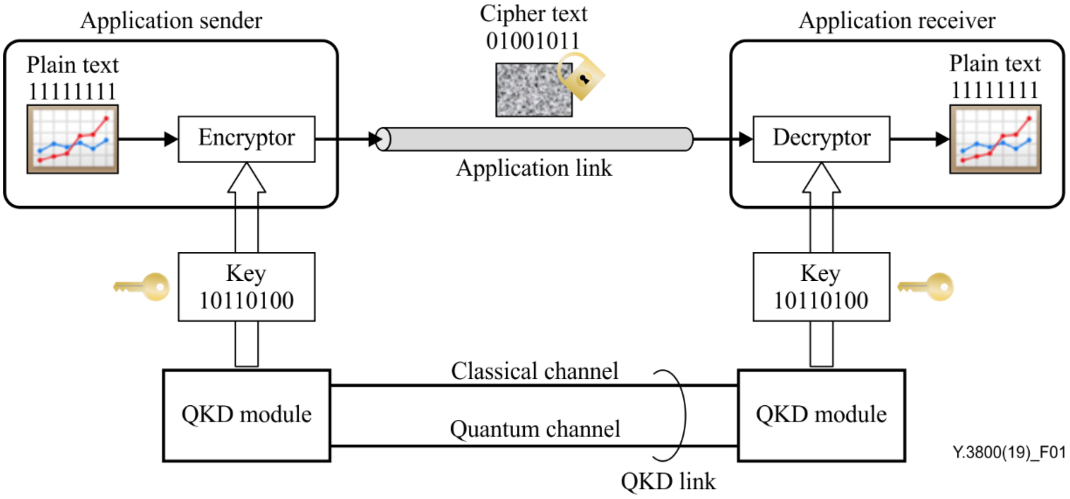

Figure 1 – Configuration example of QKD use for securing a P-to-P application link

6.2 QKDN and its relation to user networks

Although a pair of QKD modules can share keys between two parties connected by a P-to-P QKD link, it is desirable that any two or more designated parties in a user network can share the keys for various cryptographic applications. Furthermore, it is preferable to extend P-to-P QKD links to multi-point QKDN. There are possible several means as follows:

- Optical switching or splitting: Optical switches or splitters can switch or split QKD link traffic between pairs of QKD modules in the multi-point network, in order to form keys between different users on demand.
- Trusted relaying: In this scheme, keys are stored in QKD nodes (trusted nodes) and relayed to other distant QKD nodes via highly secure encryption, with OTP recommended. Currently, this is the only known solution widely adopted for long-range QKD fibre networks. The QKD node (trusted node) is assumed to be secure against intrusion and attacks by any unauthorized parties.
- Measurement-assisted relaying: Measurement device independent QKD (MDI-QKD) and twin field QKD (TF-QKD) are techniques for extending the range of QKD links, thereby allowing keys to be generated over longer distances or over channels with higher loss. MDI-QKD and TF-QKD utilize an intermediate measurement station in the link, which need not be located in a guarded location or their operation trusted (in contrast to the situation for the trusted relaying).
- Fully quantum networking: In the fully quantum network, information is retained in quantum form at the intermediate nodes, ensuring its protection at the node as well as in transit in the quantum channels between nodes. A quantum repeater works by distributing entanglement between a series of intermediate stations placed along the link. Theoretically, such an approach represents the ideal solution to distribute keys over long distances, as the intermediate stations do not need to be trusted.

NOTE 1 – Quantum repeater technology requires quantum memory or quantum error correction technologies that are not available for practical implementation with current technologies.

Figure 2 illustrates a QKDN incorporating these means, and its logical relation to a user network to which the key is supplied.

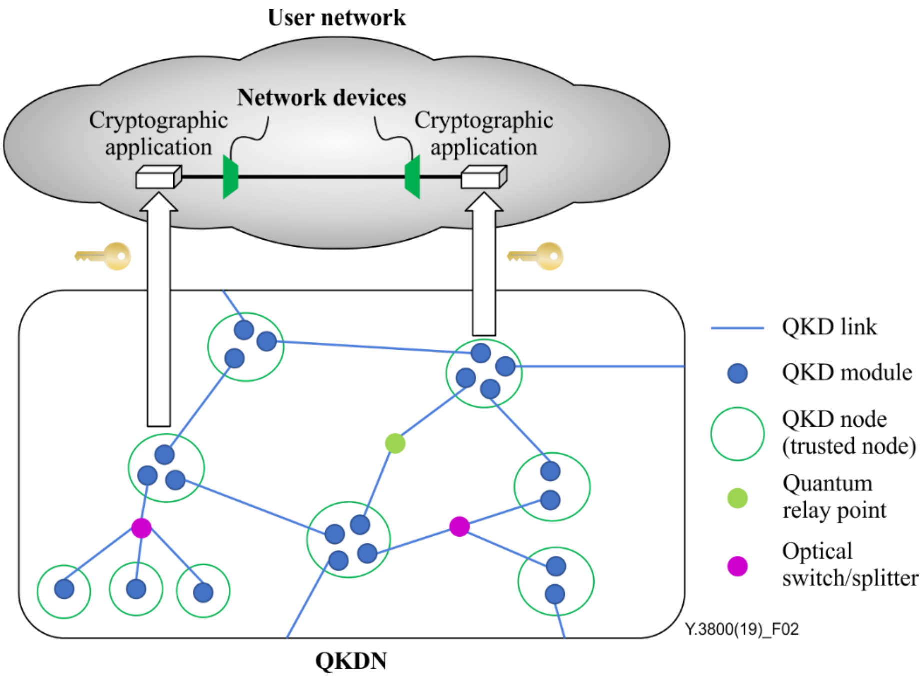

Figure 2 – Illustration of QKDN concepts and their relation to a user network

The keys are shared among the QKD nodes, that is, the QKD node acts as a node to share keys and/or the key relay point to extend the range of QKD. In contrast, the relay point for the optical switch, and the MDI-QKD, TF-QKD or the quantum repeater is referred to as the quantum relay point, which is the relay point of quantum signals and not necessarily trusted.

Thanks to these trusted or untrusted relay points, keys can be shared between arbitrary QKD nodes in the same QKDN. No keys are generated or shared in the quantum relay point. Therefore, the quantum relay point is included in the QKD link and thus provides longer distance or flexible topology for the QKDN. Technical description of these means is outside the scope of this Recommendation.

Due to the observation provided in the previous paragraph, this Recommendation focuses on QKDNs based on trusted nodes.

NOTE 2 – QKDN types and ways of cooperation with the user network varies. Such variations can be described with respect to several degrees of freedom. See Appendix I for examples of such variations.

NOTE 3 – Physical and software implementations of QKDNs and user networks are carried out in various ways, that is, either in a separated or integrated manner. However, such details are outside the scope of this Recommendation.

NOTE 4 – As mentioned in clause 6.2, the user network, i.e., the network where the keys are supplied and cryptographic applications run, can be any conventional or future communication network.

6.3 QKDN design considerations

A QKDN entails the following design considerations.

6.3.1 Security

- Provision of strict QKD protocol security proofs;
- provision of security certifications of QKD implementations;
- provision of effective countermeasures against known quantum layer threats;
- support for effective security enhancements for trusted nodes;
- support for IT-secure key establishment for any two remote parties connected to a QKDN.

6.3.2 Scalability

- Support for flexible and economic network expansion according to service growth;
- support for flexible network topology for wide-area coverage;
- support for efficient one-to-many QKD for an access network.

6.3.3 Stability

- Support for stable design, deployment and operation of a QKDN.

6.3.4 Efficiency

- Support for efficient key supply and key relay schemes;
- provision of high secure-key throughput and low latency to satisfy various security application requirements.

6.3.5 Application-oriented

- Support for diverse requirements of modules, users and applications;
- provision of developer-friendly application programming interfaces (APIs) for QKDN capabilities;
- facilitation of integration with various ICT protocols and applications.

6.3.6 Robustness

- Fast fault detection and recovery when some nodes or links fail to ensure service continuity.

6.3.7 Ability of integration

- Support of the ability of integration for various kinds of QKD technologies.

6.3.8 Interoperability

- Support for multi-vendor interoperability for both QKD and network modules.

6.3.9 Ability of migration

- Support of the ability of migration and crypto-agility for QKD technologies, modules and implementations.

6.3.10 Manageability

- Support for manageability for modules in a QKDN, network configuration, operation, monitoring, changes and upgrade of a QKDN.

7 Network capabilities to support QKD

7.1 QKDN capabilities

A QKDN has to support the following capabilities:

7.1.1 The QKDN has a capability to supply a requested IT-secure key within the security assumptions to a cryptographic application subject to agreed service availability and reliability specifications of the QKDN.

7.1.2 The QKDN has a capability to support security and protection, including consideration of confidentiality, integrity, authenticity, non-repudiation, availability and traceability.

7.1.3 The QKDN has a capability to co-operate with the user network either in an integrated or independent management manner.

7.1.4 The QKDN has key management capabilities.

7.1.5 The QKDN offering key relay function has to be capable of employing highly secure encryption, with OTP recommended for relaying keys.

7.1.6 The QKDN has a capability to be able to supply common keys for multiple terminal applications, in addition to P-to-P applications.

NOTE – Applications often require key sharing by multi-parties, e.g., in the case of secure smartphone communication between multiple terminals.

7.1.7 The QKDN has network control and management capabilities.

7.1.8 The QKDN has a capability to contain an interface between the user network and the QKDN to supply keys in an appropriate key format to various applications.

7.1.9 The QKDN has a capability to receive key requests from cryptographic applications in the user network and to apply the key management policy such as deleting or preserving the keys after the key supply has been executed.

7.1.10 The QKDN has a capability to supply a key in a format selected by the cryptographic application from various formats offered by the interface between the user network and the QKDN.

7.1.11 The QKDN has a capability to use optical fibre channels or direct free space optical channels for quantum channel networking.

7.1.12 The QKDN has a capability to use an authenticated channel for classical communication.

7.1.13 The QKDN has a capability to automatically authenticate and operate QKD nodes that are rebooted.

7.1.14 The QKDN has a capability to manage QoS taking into account the request from the user network.

7.2 User network capabilities to support QKD

A user network has to support the following capabilities:

7.2.1 The user network has a capability to enable key requests from cryptographic applications to the QKDN and keys to be received in response.

7.2.2 The user network has a capability to request keys with any necessary information.

NOTE – Examples of necessary information may include length of the key.

7.2.3 The user network has a capability to provide information necessary for management and control of the QKDN through the relevant interfaces.

7.2.4 The user network has a capability to request QoS requirements to the QKDN.

8 Conceptual structures and basic functions

This clause provides an overview and illustration of the conceptual structures of a QKDN and a user network. The details of these conceptual structures and relevant basic functions are then described.

8.1 Conceptual structures of QKDN and user network

The main goal of a QKDN is to increase the security of communication. One of the principal approaches to this end is to concatenate QKD links via QKD nodes in order to share IT-secure keys between designated QKD nodes even when they are not directly connected via a QKD link, and to supply the keys to cryptographic applications in a user network. In order to realize the goal of IT secure key-sharing, the key should be relayed from one node to another with the respective keys until it arrives at a destination node. The keys should then be stored in the QKD nodes, used for key relay when required, and supplied to cryptographic applications. The entire operation is referred to as key management. It is an essential assumption for the QKDN that the QKD node is a trusted node in the sense that it is secured against intrusion and attack by unauthorized parties.

Figure 3 aims to illustrate the conceptual structures of a QKDN and a user network. In each QKD node are located, not only QKD module(s) but also a key manager (KM). A pair of QKD modules is connected by a QKD link, and the pairs and links are concatenated via QKD nodes. The KMs are connected by KM links. They provide key management functions including the key relay capability. QKD modules, QKD links, KMs and KM links are often controlled by the QKDN controller(s). Key relay routes can also be controlled by the QKDN controller(s). Keys are supplied from the KM to users, who are specifically called cryptographic applications in this Recommendation, and used for cryptographic applications in a user network. A key supply function is included in the KM as well. Details of the IT-secure key relay and its security aspects are outside the scope of this Recommendation. A QKDN manager usually monitors and manages the QKDN as a whole.

In a typical scenario, cryptographic applications in the user network request the needed keys to the KMs. According to this request, the corresponding KMs supply keys securely in the designated format. Data transmission in the application link is encrypted with the keys supplied by cryptographic applications. (Key can be also used for authentication or other purposes.) Once the keys are supplied to the cryptographic applications, applications use the keys under their own responsibility, while the QKDN should delete or preserve the keys according to the key management policy. Thus, the security demarcation boundary is set at the border of the user network and the QKDN. This boundary plays an important role in developing a common interface for requesting, supplying and receiving the key and network management functions, as well as in specifying security requirements and functions. More specifically, an application developer can simply create an interface for key reception without the need to know the details of the process within the QKDN. In the same way, a QKDN provider does not need to know how the cryptographic application uses the key but should have minimal information on required key size and application name or ID for authentication.

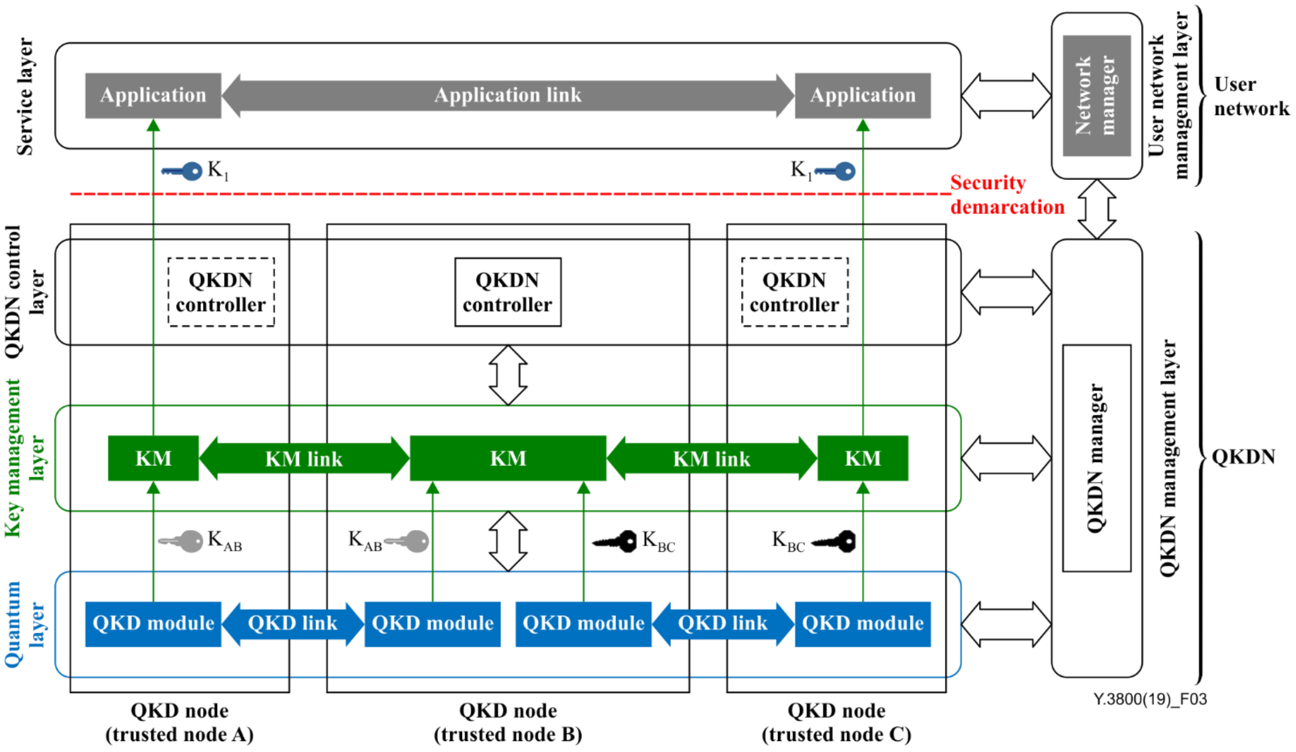

Figure 3 – Illustration of the conceptual structures of a QKDN and a user network

NOTE 1 – In Figure 3, rectangular boxes and arrows represent logical entities and logical links, respectively.

NOTE 2 – QKD modules and QKD links that convey quantum signals are in the quantum layer. KMs, KM links and interfacing paths represented by vertical arrows connected to KM convey keys for which there are particular security concerns. Arrows between the layers indicate that functional entities in the relevant layers or the QKD nodes communicate classical information required for QKD operations, such as QKD link status and control signals.

NOTE 3 – The horizontal logical links between elements within the QKD nodes at the quantum layer and at the key management layer utilize the QKD links and KM links respectively, and should be further characterized for QKDN design and operation. For cost-efficiency, those logical links can be combined into a smaller number of physical links in their implementation. This explanation is provided in Appendix II.

NOTE 4 – The quantum channel in the QKD link is a physical link, in its implementation, to operate a QKD protocol based on the laws of quantum mechanics as described in clause 6.

NOTE 5 – The user network may have functions of the QKDN control layer and the key management layer. In this case, the security demarcation exists in the user network and not between the user network and the QKDN.

NOTE 6 – There may be direct interactions between the QKDN control layer and the quantum layer. See clause 8.2 for more details.

NOTE 7 – The configuration and the relationship between the QKDN and the user network may vary over time. Security demarcation need not be static. Detail of such variation of configurations with the user network is outside the scope of this Recommendation.

NOTE 8 – Figure 3 describes a QKDN in the simplest way with three nodes. In such a simplification, while key relay can be featured, rerouting cannot be well represented, but it is not excluded. Since Figure 3 represents logical concepts, there is a variety of physical and software implementations. Detailed architectural and practical implementation aspects are outside the scope of this Recommendation.

8.2 Layers of QKDN and user network

This clause provides a description of the layers shown in Figure 3. The QKDN consists of a quantum layer, a key management layer, a QKDN control layer and a QKDN management layer. The user network is described by a service layer and a user network management layer.

8.2.1 Quantum layer

In this layer, each pair of QKD modules connected by a QKD link generates symmetric random bit strings in its own way. Each QKD module pushes the random bit strings up to a KM that is located in the same QKD node. Each QKD module also sends QKD link parameters (e.g., quantum bit error rates (QBERs), etc.) to the QKDN manager. Pairs of QKD modules connected by a QKD link are concatenated via QKD nodes.

8.2.2 Key management layer

This layer includes KMs and KM links.

Each KM is located in a QKD node. The KM performs key management. The KMs are connected via KM links. The KM receives random bit strings from QKD module(s) located in the same QKD node. The KM synchronizes and re-formats these bit strings, and stores them as keys in the storage. Interfaces for various cryptographic applications are installed into the KM. The KM receives key requests from a cryptographic application, acquires the necessary amount of keys from the storage, synchronizes, authenticates the acquired keys via a KM link, and supplies them in an appropriate format to the cryptographic application.

If KMs do not have direct KM links between them, they should share the necessary number of keys by key relay. KMs then ask the QKDN controller(s) about an appropriate relay route. Upon control from the QKDN controller(s), each KM relays keys via a KM link, with the other key in another KM in highly secure encryption (e.g., OTP). Consequently, the keys are transferred and finally supplied to the cryptographic applications. Once the keys have been supplied to the cryptographic applications, the KMs should apply the key management policy, such as deleting or preserving the keys. Details of the IT-secure key relay and its security issues are outside the scope of this Recommendation.

NOTE – In Figure 3, key relay to share a key K_1 between the trusted nodes A and C via node B is exemplified. Key K_1 can, for example, be either a key K_{AB} generated between nodes A and B (case 1), or a random bit string, e.g., K_{RN}, generated locally at node A (case 2). In case 1, K_{AB} is relayed from node B to C by OTP encryption with key K_{BC}. In case 2, the key K_{RN} is first sent from node A to B by OTP encryption with key K_{AB}, decrypted in node B, OTP encrypted with key K_{BC}, then sent from node B to C, and finally decrypted in node C. Thus key K_1 (=K_{AB} or K_{RN}) can be shared between nodes A and C.

The KM may have access to QKD modules and QKD links for their activation, de-activation, parameter control and calibration.

The KM performs key lifecycle management.

8.2.3 QKDN control layer

QKDN control functions are provided by QKDN controller(s). These functions include routing control for key relay, control of QKD links and KM links, session control for QKD services, authentication and authorization control, as well as QoS and charging policy control.

NOTE – In a centralized architecture, a single QKDN controller executes QKDN control functions as illustrated in node B in Figure 3. In a distributed architecture, each QKD node should contain a QKDN controller to perform these functions as depicted by QKDN controllers enclosed by solid and dotted lines.

8.2.4 QKDN management layer

A QKDN manager located in this layer monitors and manages the QKDN as a whole. Its tasks may include fault, configuration, accounting, performance and security management. The QKDN manager gathers information about the performance of QKD modules and QKD links (including quantum relay points) in the quantum layer and key management information in the key management layer, to monitor these two layers.

8.2.5 Service layer

Cryptographic applications are located in this layer, supplied with keys from the QKDN and conduct secure communications in application links.

8.2.6 User network management layer

The functions in the user network management layer perform management and orchestration of virtualized and non-virtualized resources in the user network.

8.3 Basic functions of QKDN

This clause describes basic functions of a QKDN.

8.3.1 Quantum key generation

Quantum key generation performs the following tasks:

- QKD module authentication via the classical channel;
- key generation by each QKD module;

NOTE – Different QKD links may use different QKD protocols.

- delivery of a key-pair to the corresponding pair of the KMs (e.g., pushing up the key from QKD modules to the KMs, or pulling the key by the KMs from QKD modules) as depicted in Figure 3.

8.3.2 Key management

Key management performs the following tasks:

- Key re-size, key re-format with meta data (necessary headers and footers such as key ID, generation date and, key length, etc., for key management), key storage;

- acquisition of QKD link parameters which may include QBER, key rate, link status, etc., a set of those depends on QKD protocol and its implementation;
- IT-secure key relay between KMs via KM links, e.g., by OTP encryption of a key with another key generated in a neighbouring QKD link or previously relayed;

NOTE – In case the necessary amount of keys for IT-secure key relay is not available, keys may be relayed by another appropriate method according to key management policy (such as by AES).

- key synchronization and authentication via KM links;
- key supply to cryptographic applications in the user network;
- key life cycle management (key ID, QKD module ID, key generation date, name of cryptographic application to which the key is supplied, key supply date, etc.).

8.3.3 QKDN control

QKDN control performs the following tasks:

- Control of key relay routes including rerouting between the two end points of cryptographic application which require the key;
- control of key relay based on request from the service layer, and status of the key management layer and quantum layer;
- control for the reconfiguration of the QKD link if failure or eavesdropping occurs;
- control of KMs and KM links;
- control of QKD modules and QKD links;
- authentication and authorization control;
- QoS and charging policy control.

8.3.4 QKDN management

QKDN management performs the following tasks:

- Support fault management, accounting management, configuration management, performance management and security management;
- monitors the status of the whole QKDN;
- support key life cycle management in KM;
- authentication and authorization management;

NOTE – For example, management of the identification and registration of modules in a QKDN, and their access rights.

- QoS and charging management.

9 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 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.

Appendix I

Variations for forming QKDN and user network

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

There are various ways of forming QKDNs and user networks with respect to several degrees of freedom, namely, the type of keys supplied from the QKDN, key consuming in the user network and the level of integration of these two. Examples of variations for forming the QKDNs and user networks are described in clauses I.1 to I.3 with an illustration of these variations given in Figure I.1 as it relates to QKD trusted nodes.

I.1 Type I variation

Relayed key K_1 is supplied from the QKDN to two end points A and D, which are not directly connected by a QKD link. Key relay is performed in the QKDN, from node A to D via nodes B and C. This key relay can be understood by a straightforward extension by adding one or more intermediate nodes to Figure 3.

I.2 Type II variation

The keys K_{AB}, K_{BC} and K_{CD} generated in three QKD links are independently supplied directly, without any key relay, to the application modules in the user network. In each application link, data is encrypted with the supplied key. In the application trusted node B, the received data is first decrypted by the key K_{AB}, then encrypted by the key K_{BC}, and then sent to node C. This is referred to as data relay as illustrated in Figure I.1. Similarly, data relay is performed in node C.

I.3 Type III variation

Type I and Type II variations can be combined in a network.

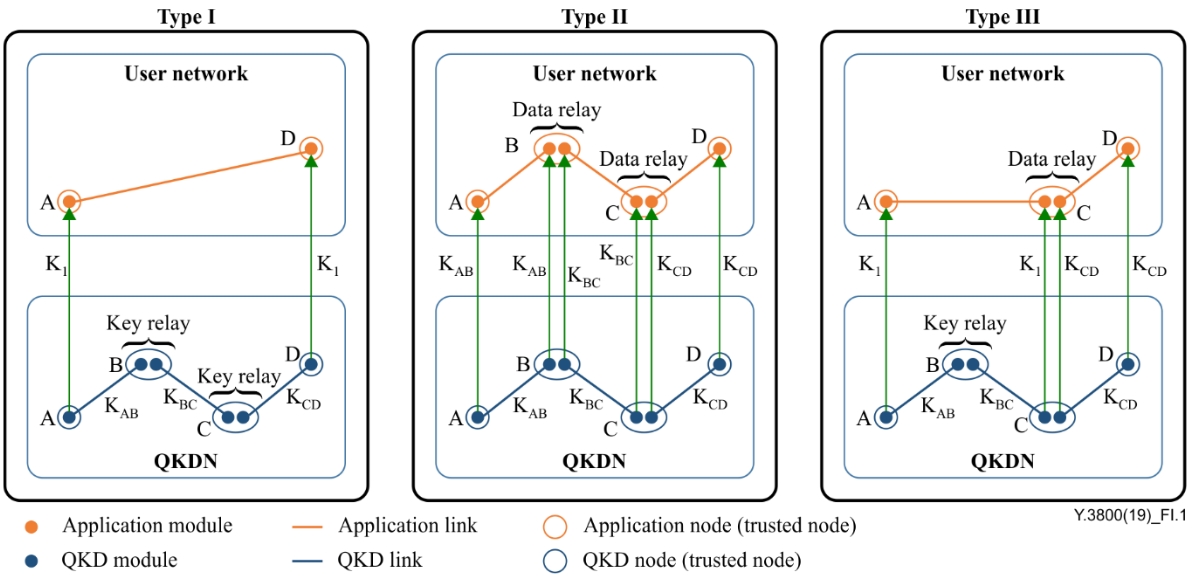

Figure I.1 – Examples of variations for forming QKDNs and user networks

It should be understood that the QKD node (trusted node) and the application node represent a logical node in the QKDN and the user network, respectively. In practice, it is mostly the case that these logical nodes are located in the same physical node.

Appendix II

Further clarification on horizontal links in QKDN

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

Figure 3 of this Recommendation describes the case of two horizontal links between QKD nodes, that is, the KM link and QKD link. Each link should be clearly identified in order to avoid difficulty and complexity to design, deploy, operate or manage the QKDN for real implementation.

This appendix illustrates that KM links and QKD links can be further classified into logical and physical links. KM links are logical and may exist between any pairs of QKD nodes. In Figure II.1, QKD links include two channels, that is, the quantum channel and the classical channel. The quantum channel is a physical optical link, whereas the classical channel is a logical link that can be implemented by two or more physical links for synchronization, distillation, etc.

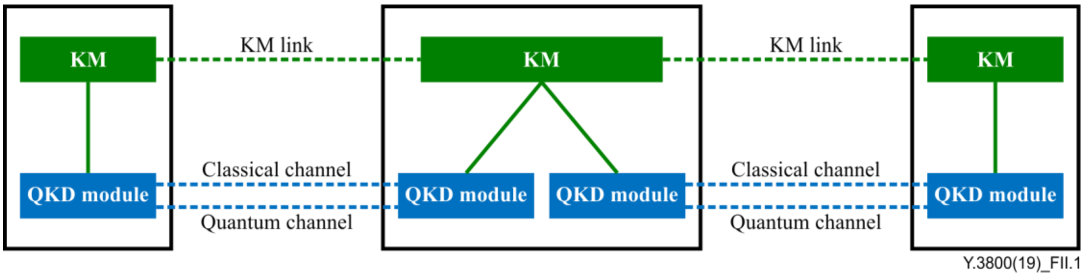

Figure II.1 – Three horizontal links in QKDN

For the purpose of efficient deployment and operation of the QKDN, those links can be realized in the combination of logical link(s) through multiplexing in QKD nodes as follows:

1) combination of KM link and classical channel in a single physical link, except quantum channel;

2) combination of KM link and two channels in a single physical link.

Bibliography

[b-ITU-T Q.1743]	Recommendation ITU-T Q.1743 (2016), *IMT-Advanced references to Release 11 of LTE-Advanced evolved packet core network.*
[b-cryptomuseum]	http://www.cryptomuseum.com/crypto/otp.htm
[b-ETSI GR QKD 007]	Group Specification ETSI GS QKD 007 (2018), *Quantum Key Distribution (QKD); Vocabulary*.
[b-FIPS PUB 197]	Federal Information Processing Standards Publication 197 (2001), Announcing the ADVANCED ENCRYPTION STANDARD (AES)
[b-FIPS PUB 198]	Federal Information Processing Standards Publication FIPS PUB 198-1 (2008), The Keyed-Hash Message Authentication Code (HMAC)
[b-ISO/IEC 18033-3]	ISO/IEC 10833-3:2010 (2010), *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers.*
[b-IEEE Trans. Inf. Theory 39]	*Network Information Theory* (1993), by El Gamal and Kim, Cambridge University Press. More precisely, U. Maurer, IEEE Trans. Inf. Theory 39, 733.
[b-ETSI White Paper 8]	ETSI White Paper No. 8, *Quantum Safe Cryptography and Security*.

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, 2019