International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3808

(02/2022)

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

Quantum key distribution networks

Framework for integration of quantum key distribution network and secure storage network

Recommendation ITU-T Y.3808

ITU-T Y-SERIES RECOMMENDATIONS

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

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

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

Recommendation ITU-T Y.3808

Framework for integration of quantum key distribution network and secure storage network

Summary

Recommendation ITU-T Y.3808 provides an overview of secure storage networks (SSNs) for quantum key distribution networks (QKDNs). It specifies the functional requirements, functional architecture model, reference points and operational procedures for SSNs.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3808	2022-02-13	13	11.1002/1000/14865

Keywords

Public key infrastructure (PKI), QKD network, QKD, quantum key distribution network (QKDN), secure storage network (SSN).

* 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.3808

Framework for integration of quantum key distribution network and secure storage network

1 Scope

This Recommendation describes a framework for a integrating quantum key distribution network (QKDN) and secure storage network (SSN). In particular, the scope of this Recommendation includes:

– overview of SSN;

– functional requirements for SSN;

– functional architecture model of SSN;

– reference points;

– operational procedures.

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 X.509] Recommendation ITU-T X.509 (2016), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[ITU-T Y.3802] Recommendation ITU-T Y.3802 (2020), *Functional architecture of the quantum key distribution network*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 key manager (KM) [b-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 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.

3.1.3 quantum key distribution link (QKD link) [b-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.

3.1.4 quantum key distribution module (QKD module) [b-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. There are two types of QKD modules, namely, the transmitters (QKD-Tx) and the receivers (QKD-Rx).

3.1.5 quantum key distribution network (QKDN) [b-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.

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

3.1.7 quantum key distribution network manager (QKDN manager) [b-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.

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

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

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AES	Advanced Encryption Standard
CA	Certification Authority
FCAPS	Fault, Configuration, Accounting, Performance and Security
IPsec	Internet Protocol Security
IT-secure	Information-Theoretically secure
KM	Key Manager
OTP	One-Time Pad
PKI	Public Key Infrastructure
QKD	Quantum Key Distribution
QKDN	Quantum Key Distribution Network
SSA	Secure Storage Agent
SSN	Secure Storage Network
TLS	Transport Layer Security

5 Conventions

In this Recommendation:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

6 Introduction

The purpose of introducing the quantum key distribution network (QKDN) into current communication networks and cryptographic infrastructures is to enhance their security level by supplying highly secure symmetric keys to cryptographic applications. Introducing the QKDN into these existing infrastructures can impose significant overhead costs/impacts on systems and elements. In the worst case, it may also introduce new vulnerabilities if the QKDN is not appropriately designed, operated, or interfaced with cryptographic applications.

In order to support the QKDN, various kinds of cryptographic methods need to be used in their appropriate combinations. To ensure the confidentiality of keys during the key relay process via trusted nodes, one-time pad (OTP) encryption, an information theoretically secure scheme, is recommended for use to ensure the long-term confidentiality of keys. Cryptographic methods such as public key cryptography and hash functions, which are computationally secure, can be employed to ensure the integrity of the keys, i.e., ensuring the keys remain unaltered. These methods also play important roles to realize authentication and access control of functional elements in the QKDN. Control and management information in the QKDN needs to be protected by the combination of public key cryptography (especially for authentication and key exchange) and symmetric cipher such as advanced encryption standard (AES), especially for data encryption. Cipher suites of these cryptographic technologies are implemented in Internet protocol security (IPsec) and transport layer security (TLS) based on public key infrastructure (PKI). Thus, building the QKDN means integration of quantum key distribution (QKD) technologies and existing secure network infrastructures.

Keys supplied by the QKDN can be used to encrypt sensitive and high-value data in transmission. Although the QKDN itself cannot protect the confidentiality of data storage, it can be used to enhance the security of storage networks. In fact, today, digital data are stored in data centres forever, and the data can easily be targeted by malicious attacks or even be threatened by non-malicious incidents such as natural disasters. Protection of critical data in storage networks for the long-term warrants the use of QKDN, and should be worth the overhead costs. A secure storage network (SSN) consists of multiple data servers and is supported by a secret sharing scheme. Some secret sharing schemes, such as the Shamir threshold scheme, ensure an information theoretic confidentiality of storage, provided that the number of corrupted servers is less than a certain threshold, and data shares are exchanged through highly private channels. These highly private channels can be realized by using OTP encryption with keys supplied by the QKDN. PKI plays an essential role again to realize authentication, access control, and integrity protection in the SSN.

A concept of integration of the QKDN with PKI and the SSN is depicted in Figure 1. This is a typical example of the integration of QKDN and secure network infrastructures.

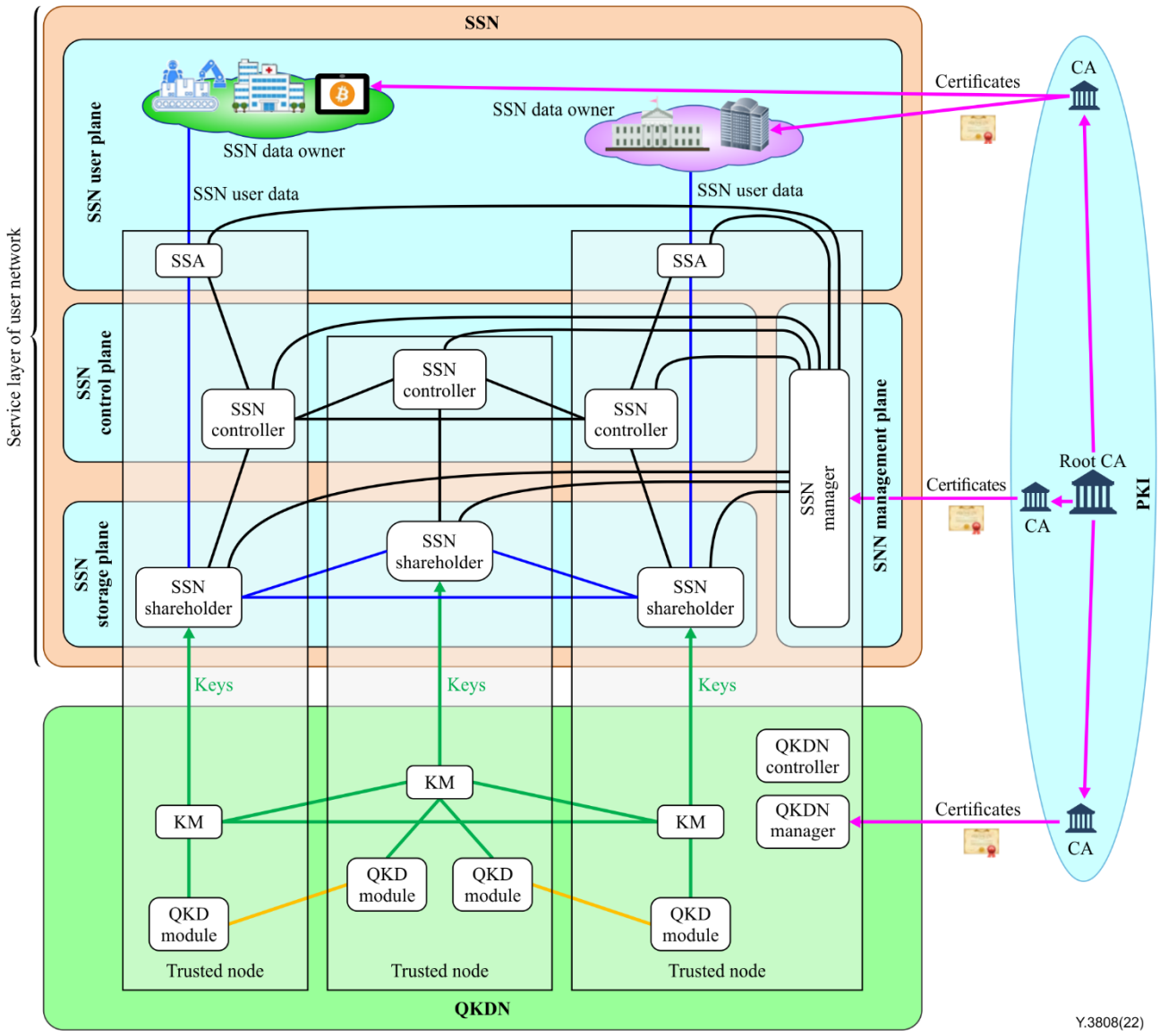

Figure 1 – A conceptual view of integration of the QKDN with PKI and the SSN

The following functional elements are contained in the SSN in Figure 1:

– Secure storage agent (SSA): a functional element which creates shares from the original data and reconstructs the original data from shares.

– SSN controller: a functional element which controls the secret sharing process, i.e., receive the original data, encrypt data appropriately (e.g., transform data into shares by a secret sharing protocol), and control communication for the SSN shareholder.

NOTE – SSN controller may communicate with QKDN controller, for example, when SDN controller controls both of networks.

– SSN manager: a functional element which manages the fault, configuration, accounting, performance and security (FCAPS) functions of the SSN.

– SSN shareholder: a functional element which processes, exchanges, renews and stores shares.

– SSN shareholder link: a communication link between SSAs and SSN shareholders and among SSN shareholders. SSN shareholder links are shown in blue in Figure 1. These links transmit shares with highly secure encryption such as OTP cryptography.

– SSN control link: a communication link among SSN controllers and between an SSN controller and an SSN shareholder. SSN control links are shown in black in Figure 1. These links transmit control and management information between the SSN controller and the SSN shareholder.

7 PKI

The public-key infrastructure (PKI) is the infrastructure established to support the issuing, revocation and validation of digital certificates. The frameworks of the PKI are specified in [ITU-T X.509], which introduces the basic concept of asymmetric cryptographic techniques and data types of public-key certificates. In the PKI, a certification authority (CA) is a functional component that issues a certificate. CAs form a tree structure to construct trust chains. A CA at the top of the tree is called a root CA, and it may be a trust anchor. An SSN manager receives certificates from the PKI and the SSN manager can be a root CA in the SSN. The root CA in the SSN manager issues certificates for the next CAs which are located in functional components in the SSN, such as SSAs, SSN controllers and SSN shareholders. Functional components which receive certificates can use them for the validation of digital signatures in public-keys. Digital certificates which CAs provide can also be used for entity and message authentications in the SSN.

8 SSN

SSN is one of the representative use cases in the service layer. This clause reviews basic concepts and underlying technologies of the secure storage network, including secret sharing, private channels, PKI, etc. Particular attention is given to long-term security. Technical requirements and guidance for storage security are studied in [b-ISO/IEC 27040].

8.1 Secret sharing

Secret sharing satisfies confidentiality of storage, availability and functionality. In secret sharing, new multiple data shares are created from the original data by using a polynomial and storage in multiple data servers (shareholders). Shamir's (k, n) threshold scheme [b-Shamir] uses n shareholders and restores the original data by collecting at least k ($\leq n$) of shares. With k–1 or fewer shares, the original data can never be reconstructed even with unlimited computing power. Provided that the number of corrupted shareholders is less than k, and shares are exchanged through private channels, Shamir's (k, n) threshold scheme ensures information theoretic confidentiality of storage; that is, confidentiality is satisfied. Shares can be added and multiplied, meaning that full homomorphism – functionality – can be met. Even if shares up to n–k are lost, the original data can be reconstructed by using the k remaining shares, which provides availability.

XOR-based secret sharing schemes have been studied as another secret sharing scheme. Since the XOR-based secret sharing schemes perform distribution and reconstruction only by the exclusive OR (XOR) operation, high-speed processing for distribution and reconstruction are possible.

However, these schemes cannot protect integrity. Private channels should also be implemented somehow to protect the confidentiality of data transmission, which is another important confidentiality requirement.

8.2 Private channels supported by QKDN

The secret sharing method itself has a mathematical algorism and does not provide a solution to transmit a share securely to the remote storage (i.e., ensure the confidentiality of transmission). Combined with the QKDN, which realizes confidentiality of data transmission, a secret sharing method can be used for information theoretically SSN in a protocol level. An SSA creates shares from the original data and transmits them to SSN shareholders. SSN shareholders exchange shares

through SSN shareholder links. These links transmitting shares are private channels which are protected by encryption with keys provided by QKDN.

8.3 Secure operation supported by PKI

QKD and secret sharing can realize confidentiality and availability of data, but they cannot prevent corruption of data preservation for a long-term. Therefore, it is necessary to introduce security technologies such as digital signatures into the system. These functions are performed at the CA in the PKI in Figure 1. It should be noted that it is sufficient to ensure short-term security for a certain period for integrity protection. Timestamp chains are used to prolong the validity of digital signatures for the original data for any length of time. For example, a Pedersen commitment scheme is adopted, and commitments to the original data are timestamped and shared. While this scheme can protect the secrecy of the original data information theoretically, the correctness of the data must inevitably be computational. So, the commitments, as well as the timestamps, are renewed regularly. Thus, the integrity protection can be realized for a long-term.

9 Functional requirements for SSN

9.1 SSN user plane

An SSA should meet the following requirements:

Req_SSN_A 1. The SSA is required to receive the original data from data owners.

Req_SSN_A 2. The SSA is required to create shares of the original data.

Req_SSN_A 3. The SSA is required to send shares to SSN shareholders.

Req_SSN_A 4. When the data owners request restoring the original data, the SSA is required to reconstruct the original data from shares.

9.2 SSN control plane

An SSN controller should meet the following requirements:

Req_SSN_C 1. The SSN controller is required to control distribution of shares to SSN shareholders.

Req_SSN_C 2. The SSN controller is required to control collection of shares from SSN shareholders to reconstruct the original data.

Req_SSN_C 3. When failure occurs in an SSN shareholder, the SSN controller is required to control re-sharing of shares.

Req_SSN_C 4. The SSN controller is required to receive certificates from CAs and use them for security functions.

Req_SSN_C 5. The SSN controller is required to encrypt control and management information between SSN controllers.

Req_SSN_C 6. The SSN controller is required to manage configuration of SSN shareholders.

9.3 SSN storage plane

An SSN shareholder should meet the following requirements:

Req_SSN_S 1. The SSN shareholder is required to receive shares from SSAs.

Req_SSN_S 2. The SSN shareholder is required to have capabilities of processing shares.

Req_SSN_S 3. The SSN shareholder is required to transmit the shares to other SSN shareholders with IT-secure encryption such as OTP encryption and store them under the control of the SSN controller.

Req_SSN_S 4. The SSN shareholder is recommended to renew shares to secure the long-term integrity.

Req_SSN_S 5. The SSN shareholder is required to send shares to SSAs with IT-secure encryption such as OTP encryption when the original data are requested.

Req_SSN_S 6. When failure occurs in an SSN shareholder, the SSN controller is required to perform re-sharing of shares.

9.4 SSN management plane

An SSN manager should meet the following requirement:

Req_SSN_M 1. The SSN manager is required to provide FCAPS management of the SSN control plane and the SSN storage plane.

10 Functional architecture model of SSN

Figure 2 illustrates the functional architecture model of SSN.

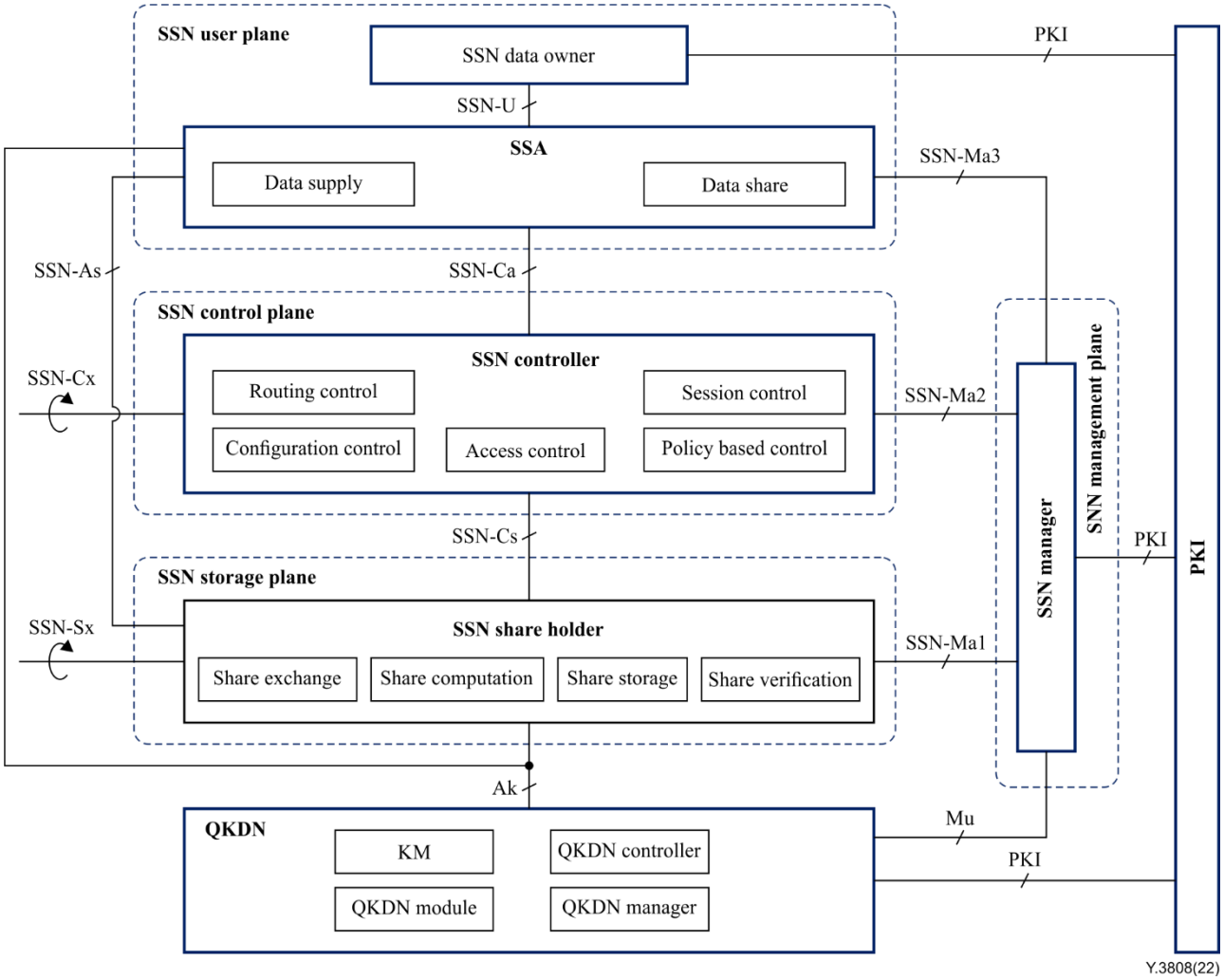

Figure 2 – Functional architecture model of SSN

10.1 Functions of SSA

In the SSN user plane, an SSA creates shares and reconstructs the original data. It also comprises the following functional elements:

– Data supply function: It receives original data from data owners and sends the original data to data owners with highly secure encryption (OTP encryption is recommended for use).

– Data share function: It supports creating shares of the original data and reconstructing the original data from shares.

10.2 Functions of SSN controller

In the SSN control plane, an SSN controller controls functions in SSN storage plane. It also comprises the following functional elements.

– Session control function: It supports the control of the session procedures among SSN shareholders, between the SSN controller and the shareholders and between the SSA and the SSN shareholders.

– Routing control function: It provisions an appropriate distribution route among SSN shareholders and performs routing of re-sharing shares depending on fault, performance, and/or availability status of the SSN shareholder links to ensure the continuation of secret sharing.

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

– Policy based control function: It controls the SSN resources based on the quality of service (QoS) and charging policies for SSN data owners.

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

10.3 Functions of SSN shareholder

In the SSN storage plane, an SSN shareholder exchanges shares with other shareholders and stores them. It further comprises the following functional elements:

– Share exchange function: It receives shares from SSAs and exchanges shares with other SSN shareholders with highly secure encryption (OTP encryption is recommended for use.). It exchanges shares for renewal in an appropriate, timely manner.

– Share computation function: It performs the computation of shares with random numbers and secret sharing schemes.

– Share storage function: It stores shares securely.

– Share verification function: It verifies the integrity of shares with certificates for the following cases, including share renewal and reconstructing the original data from shares.

10.4 Functions of SSN manager

In the SSN management plane, an SSN manager supports FCAPS functions of SSAs, SSN controllers and SSN shareholders.

11 Reference points

11.1 Reference points of SSA

The following reference points are relevant to connections with an SSA:

– SSN-U: a reference point connecting an SSN data owner and an SSA. It is responsible for sending the SSN user data.

– SSN-As: a reference point connecting an SSA and an SSN shareholder. It is responsible for sending shares from the SSA to the SSN shareholder and supplying the shares from the SSN shareholder to the SSA.

11.2 Reference points of SSN controller

The following reference points are relevant to connections with an SSN controller:

– SSN-Ca: a reference point connecting an SSA and an SSN controller. It is responsible for the SSN controller to communicate control information with the SSA.

– SSN-Cs: a reference point connecting an SSN controller and an SSN shareholder. It is responsible for the SSN controller to communicate control information with the SSN shareholder.

– SSN-Cx: a reference point connecting two SSN controllers. It is responsible for the two SSN controllers to communicate control information each other.

11.3 Reference points of SSN shareholder

The following reference point is relevant to connections with an SSN shareholder:

– SSN-Sx: a reference point connecting an SSN shareholder and other SSN shareholders. It is responsible for exchange of shares with other SSN shareholders.

11.4 Reference points of SSN manager

The following reference points are relevant to connections with an SSN manager:

– SSN- Ma1: a reference point connecting an SSN manger with an SSN shareholder. It is responsible for the SSN manager to communicate management information with the SSN shareholder.

– SSN- Ma2: a reference point connecting an SSN manager with an SSN controller. It is responsible for the SSN manager to communicate management information with the SSN controller.

– SSN- Ma3: a reference point connecting an SSN manager with an SSA. It is responsible for the SSN manager to communicate management information with the SSA.

11.5 Reference points of QKDN

Ak and Mu reference points are defined in [ITU-T Y.3802].

11.6 Reference points of PKI

Reference points of PKI are connecting PKI and an SSN data owner, an SSN manager and a QKDN. It is responsible for the PKI to provide digital certificates to the SSN and the QKDN. Data types of public-key certificates are specified in [ITU-T X.509].

12 Operational procedures

This clause comprises basic operational procedures of the SSN. The details in each procedure are assumed to be arranged and/or varied depending on the implementation of the SSN.

12.1 Data storing procedures

Data storing procedures are shown in Figure 3 and are outlined as follows:

1) The SSN data owner sends a data storing request to the SSA.
2) The SSN data owner and the SSA request keys to the QKDN. The QKDN supplies keys to them.
3) The SSN data owner sends the original data to the SSA with OTP encryption using keys which the QKDN supplied.
4) The SSA creates shares from the original data.
5) The SSA sends share storing request to the SSN shareholder.
6) If the SSA and the SSN shareholder are not accommodated in the same trusted node, the SSA and the SSN shareholder request keys to the QKDN. The QKDN supplies keys to them.
7) The SSA transmits shares to the SSN shareholder with OTP encryption. If the SSA and the SSN shareholder are accommodated in the same trusted node, OTP encryption is not necessary to transmit shares.
8) When the SSA completes transmission of shares to the SSN shareholder, the SSA reports storing data to the SSN data owner.
9) When the SSN shareholder receives shares from the SSA, the SSA stores a part of shares and requests route information to the SSN controller to exchange the rest of the shares to other shareholders.
10) The SSN shareholder sends shares exchange request to the other SSN shareholders according to the route information which the SSN controller provided.
11) The SSN shareholder and the other SSN shareholders request keys to the QKDN. The QKDN supplies keys to them.
12) The SSN shareholder and the other SSN shareholders exchange the rest of the shares with OTP encryption.
13) The other SSN shareholders store the rest of the shares.

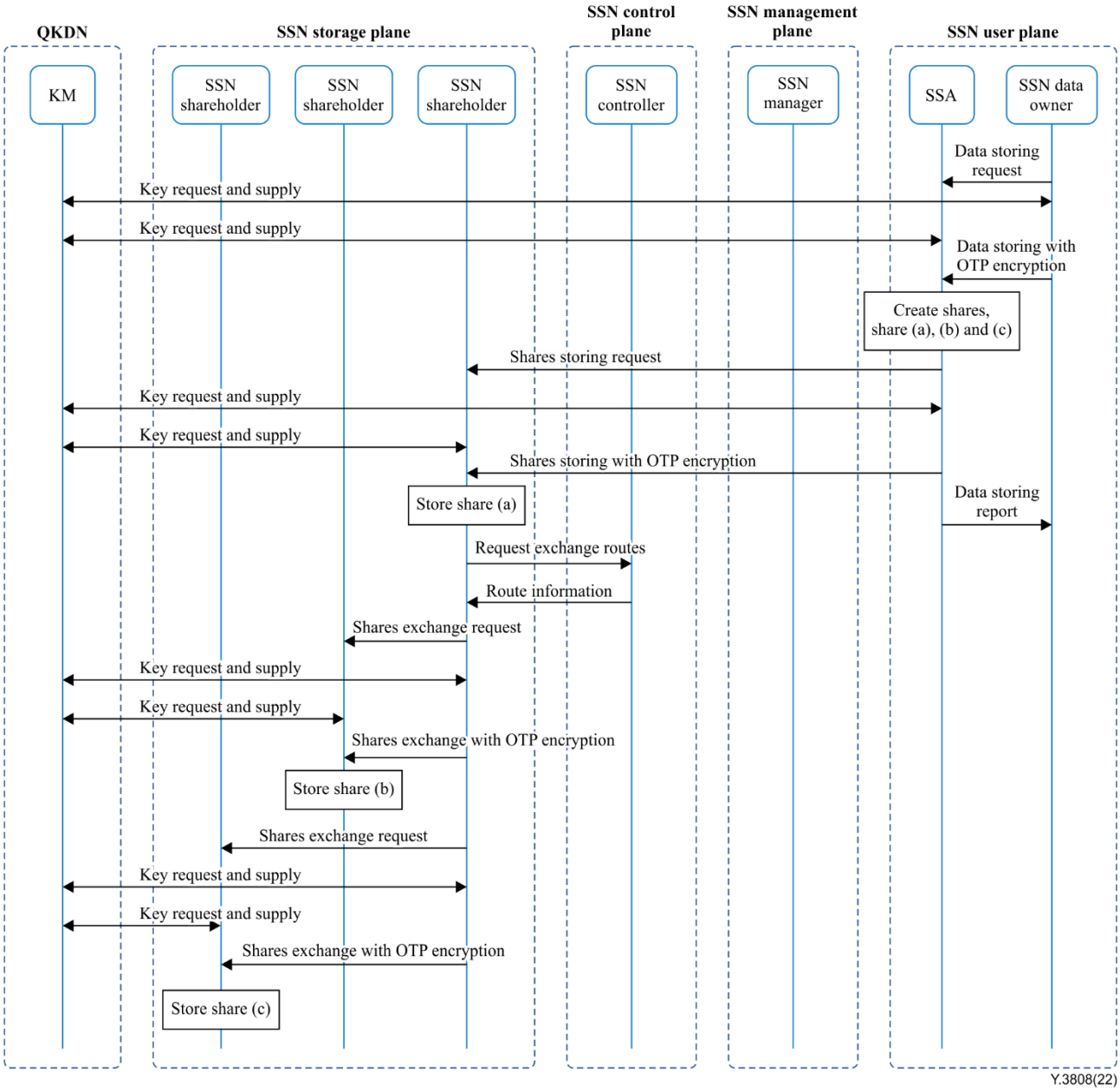

Figure 3 – Data storing procedures

12.2 Data retrieving procedures

Data retrieving procedures are shown in Figure 4 and are outlined as follows:

1) The SSN data owner sends a data retrieving request to the SSA.

2) When the SSN shareholder receives data retrieving request from the SSA, the SSA retrieves a part of shares and requests route information to the SSN controller to retrieve the rest of the shares to other shareholders.

3) The SSN shareholder sends a shares retrieving request to the other SSN shareholders according to the route information provided by the SSN controller.

4) The SSN shareholder and the other SSN shareholders request keys to the QKDN. The QKDN supplies keys to them.

5) The SSN shareholder and the other SSN shareholders retrieve the rest of the shares with OTP encryption.

6) If the SSN shareholder and the SSA are not accommodated in the same trusted node, the SSA and the SSN shareholder request keys to the QKDN. The QKDN supplies keys to them.

7) The SSN shareholder transmits shares to the SSA with OTP encryption. If the SSA and the SSN shareholder are accommodated in the same trusted node, OTP encryption is unnecessary to transmit shares.

8) When the SSA retrieves necessary shares from the shareholders, the SSA reconstructs the original data from shares.

9) The SSA and the SSN data owner request keys to the QKDN. The QKDN supplies keys to them.

10) The SSA transmits the original data to the SSN data owner with OTP encryption.

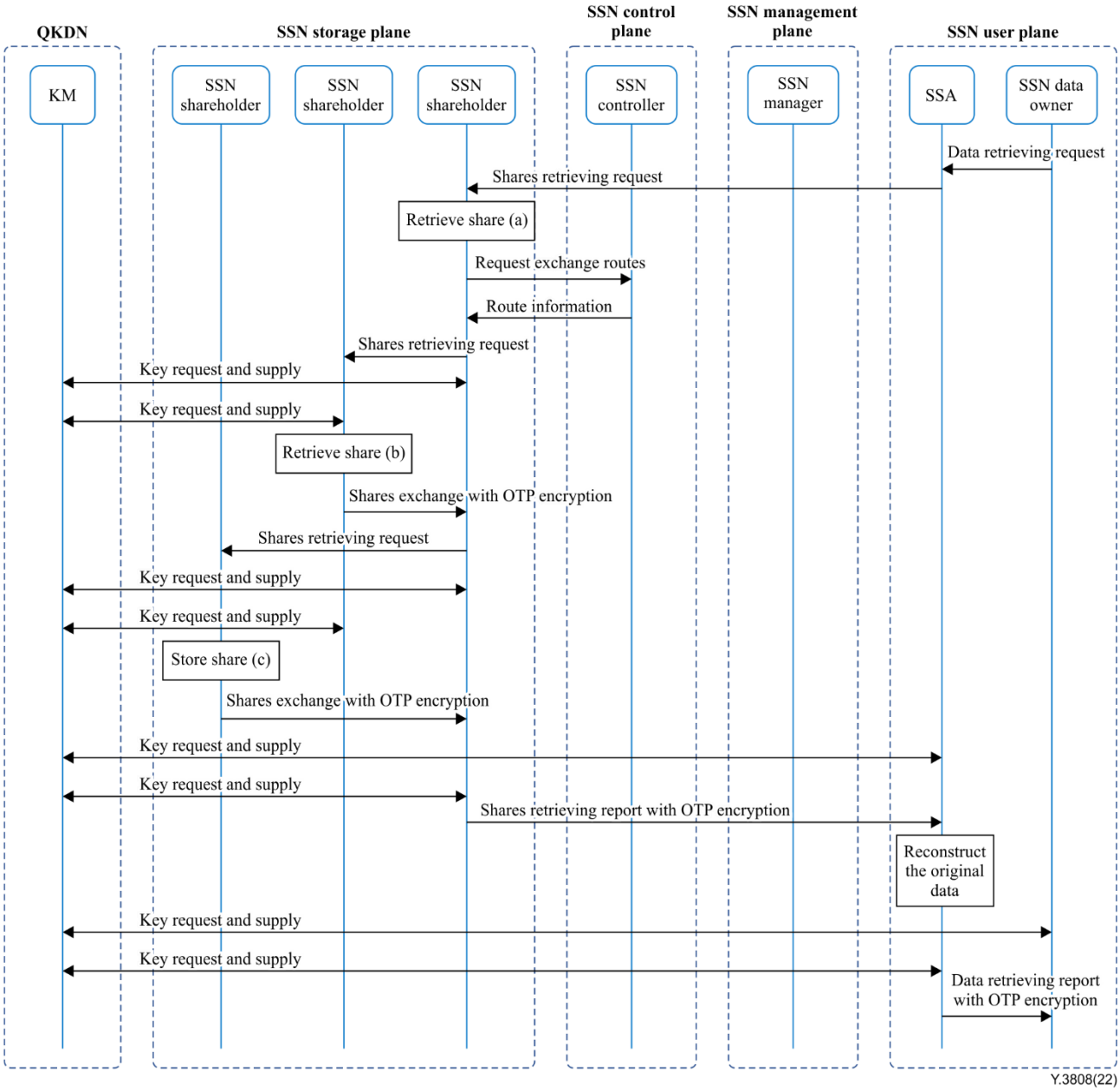

Figure 4 – Data retrieving procedures

12.3 Shares renewing procedures

Shares renewing procedures are shown in Figure 5 and are outlined as follows:

1) The SSA sends a shares renewing request to the SSN shareholder.

2) When the SSN shareholder receives a shares renewing request from the SSA, the SSN shareholder renews a part of shares and requests route information to the SSN controller to renew the rest of the shares to other shareholders.

3) The SSN shareholder sends the shares renewing request to the other SSN shareholders according to the route information provided by the SSN controller.

4) When the other SSN shareholders receive the shares renewing request from the SSN shareholder, the other SSN shareholders renew the rest of the shares.

5) The SSN shareholder sends a shares renewing report to the SSA.

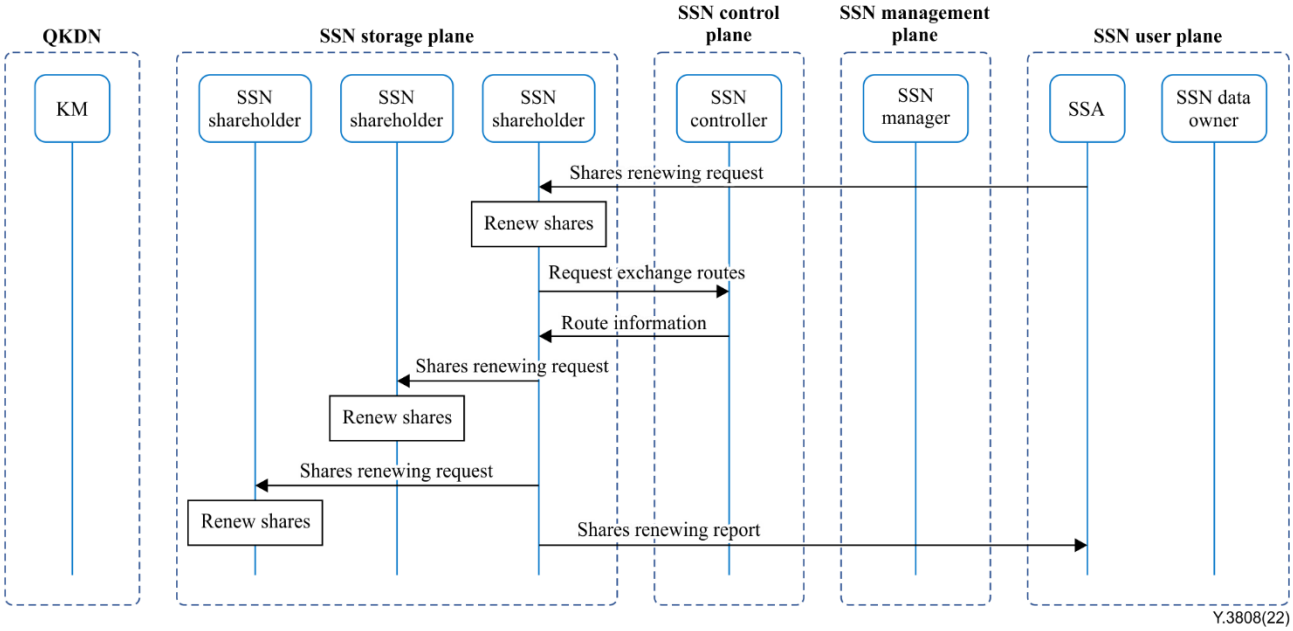

Figure 5 – Shares renewing procedures

Bibliography

[b-ITU-T Y.3800] Recommendation ITU-T Y.3800 (2019), *Overview on networks supporting quantum key distribution*.

[b-ISO/IEC 27040] ISO/IEC 27040:2015, *Information technology – Security techniques – Storage security.*

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

[b-Shamir] Adi Shamir, How to share a secret, *Communications of the ACM*, vol. 22, No. 11, pp. 612-613, 1979.

SERIES OF ITU-T RECOMMENDATIONS

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

Printed in Switzerland
Geneva, 2022