International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1715

(07/2022)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Quantum communication – Security design for QKDN

Security requirements and measures for integration of quantum key distribution network and secure storage network

Recommendation ITU-T X.1715

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security (1)	X.1140–X.1149
Application Security (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1350–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1399
Distributed ledger technology (DLT) security	X.1400–X.1429
Application Security (2)	X.1450–X.1459
Web security (2)	X.1470–X.1489
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
Cyber Defence	X.1590–X.1599
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	**X.1712–X.1719**
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
Data protection	X.1770–X.1789
IMT-2020 SECURITY	X.1800–X.1819

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

Recommendation ITU-T X.1715

Security requirements and measures for integration of quantum key distribution network and secure storage network

Summary

Recommendation ITU-T X.1715 specifies security requirements and measures for integrating a quantum key distribution network (QKDN) with a secure storage network (SSN) in the service layer (Recommendation ITU-T Y.3800) and public key infrastructure (PKI) (Recommendation ITU-T X.509).

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T X.1715	2022-07-14	17	11.1002/1000/14995

Keywords

QKD, QKDN, security measures, security requirements, 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 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

Page

Recommendation ITU-T X.1715

Security requirements and measures for integration of quantum key distribution network and secure storage network

1 Scope

This Recommendation specifies a framework for integrating a quantum key distribution network (QKDN) with a secure storage network (SSN) and public key infrastructure (PKI).

This Recommendation includes for an SSN:

- analysis of security threats;
- identification of security requirements; and
- specification of measures to meet identified security requirements.

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 (2019) | ISO/IEC 9594-8:2020, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[ITU-T X.1710] Recommendation ITU-T X.1710 (2020), *Security framework for quantum key distribution networks*.

[ITU-T X.1712] Recommendation ITU-T X.1712 (2021), *Security requirements and measures for quantum key distribution networks – Key management*.

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

[ITU-T Y.3801] Recommendation ITU-T Y.3801 (2020), *Functional requirements for quantum key distribution networks*.

[ITU-T Y.3802] Recommendation ITU-T Y.3802 (2020), *Quantum key distribution networks – Functional architecture*.

[ITU-T Y.3803] Recommendation ITU-T Y.3803 (2020), *Quantum key distribution networks – Key management*.

[ITU-T Y.3804] Recommendation ITU-T Y.3804 (2020), *Quantum key distribution networks – Control and management*.

[ITU-T Y.3808] Recommendation ITU-T Y.3808 (2022), *Framework for integration of quantum key distribution network and secure storage network*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 certification authority (CA) [ITU-T X.509]: An authority trusted by one or more entities to create and digital sign public-key certificates. Optionally the certification authority may create the subjects' keys.

3.1.2 key data [ITU-T Y.3803]: Random bit strings that are used as a cryptographic key.

3.1.3 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.

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

3.1.5 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.

3.1.6 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).

3.1.7 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.

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

3.1.9 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.

3.1.10 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.

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:

CA	Certification Authority
DoS	Denial of Service
FCAPS	Fault, Configuration, Accounting, Performance and 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, these conventions are applied to exclusively security requirements which are specified in clause 9.

The phrase "is required to" indicates a requirement that must be strictly followed and from which no deviation is permitted if conformity to this Recommendation is to be claimed.

The phrase "is recommended" indicates a requirement that is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformity.

6 Introduction

A QKDN supplies highly secure keys to cryptographic applications for protecting long-term confidentiality of data. Basic functions and layered structures of QKDN are defined in [ITU-T Y.3800]. Functional requirements and architectures are specified in [ITU-T Y.3801] and [ITU-T Y.3802], respectively. Key management as well as control and management of QKDN are specified in [ITU-T Y.3803] and [ITU-T Y.3804], respectively. A security framework for a QKDN is specified in [ITU-T X.1710] by addressing security threats to it and deriving general security requirements and security measures for it. Security requirements and measures for key management of QKDN are specified in [ITU-T X.1712].

To support the security measures for QKDN specified in [ITU-T X.1710] and [ITU-T X.1712], various kinds of security techniques and cryptographic methods need to be used in appropriate combinations. These techniques and methods include not only one-time pad (OTP) encryption for the key relay, but also a public key cryptography and a symmetric cipher for integrity and authenticity protection and encryption of control and management information. Public key cryptography and symmetric cipher are supported by cipher suites in IPsec [b-IETF RFC 4301] and transport layer security (TLS) [b-IETF RFC 8446] based on public key infrastructure (PKI) [ITU-T X.509]. Specifications for the integration of QKD technologies and existing secure network infrastructures such as PKI need to be studied further.

Keys supplied by QKDN are used to encrypt sensitive and high-value data in transmission in the service layer of the user network [ITU-T Y.3800]. As explained in [ITU-T Y.3800] and [ITU-T Y.3802], the user network represents existing secure network infrastructures in which various cryptographic applications exist. To exploit the advantages owing to highly secure symmetric keys supplied by QKDN, security aspects of integration of QKDN and secure network infrastructures need to be studied further. It is critical to know how to combine cryptographic technologies based on QKD and modern cryptography. While modern cryptography is based on the computational complexity of mathematical problems, QKD is based on the laws of quantum mechanics and information theory. Both these mechanisms and security levels are different.

Today, various kinds of digital data are accumulated in data centres and will be stored for a long period. These data are targeted by malicious attacks now for potential usage later when advanced computing technologies are available as they will be able to decrypt the data back to its original form. The stored data are also threatened by incidents like natural disasters. These threats give a strong impetus to introducing cryptographic technologies that aim to ensure long-term security as well as data availability. An SSN consisting of multiple data servers supported by a secret sharing scheme [b-Shamir] [b-Fujiwara] integrated with a QKDN provides a promising solution, as both secret sharing and QKD are based on information theoretically secure (IT-secure) protocols, and hence can support long-term secure data transmission and storage.

NOTE – The (*k*, *n*) threshold scheme in [b-Shamir] uses *n* shareholders and restores the original data by collecting at least *k* (≤*n*) of (data) shares (see also clause 7.2). With *k*–1 or fewer shares, the original data can never be reconstructed, even with unlimited computing power.

More precisely, combination of QKDN and secret sharing realizes confidentiality and availability of data. However, this combination itself cannot ensure integrity of the preserved data. It is necessary to introduce security technologies for integrity protection, such as digital signatures issued by the PKI. It should be noted that security requirements for protection of confidentiality and integrity generally differ and can also depend upon each other at some level. Therefore, the integration of secret sharing, QKD and PKI addresses the critical issues.

This Recommendation provides security requirements for integration of QKDN with secure network infrastructures. A concept of integration of QKDN with PKI and SSN is described in [ITU-T Y.3808], as shown in Figure 1.

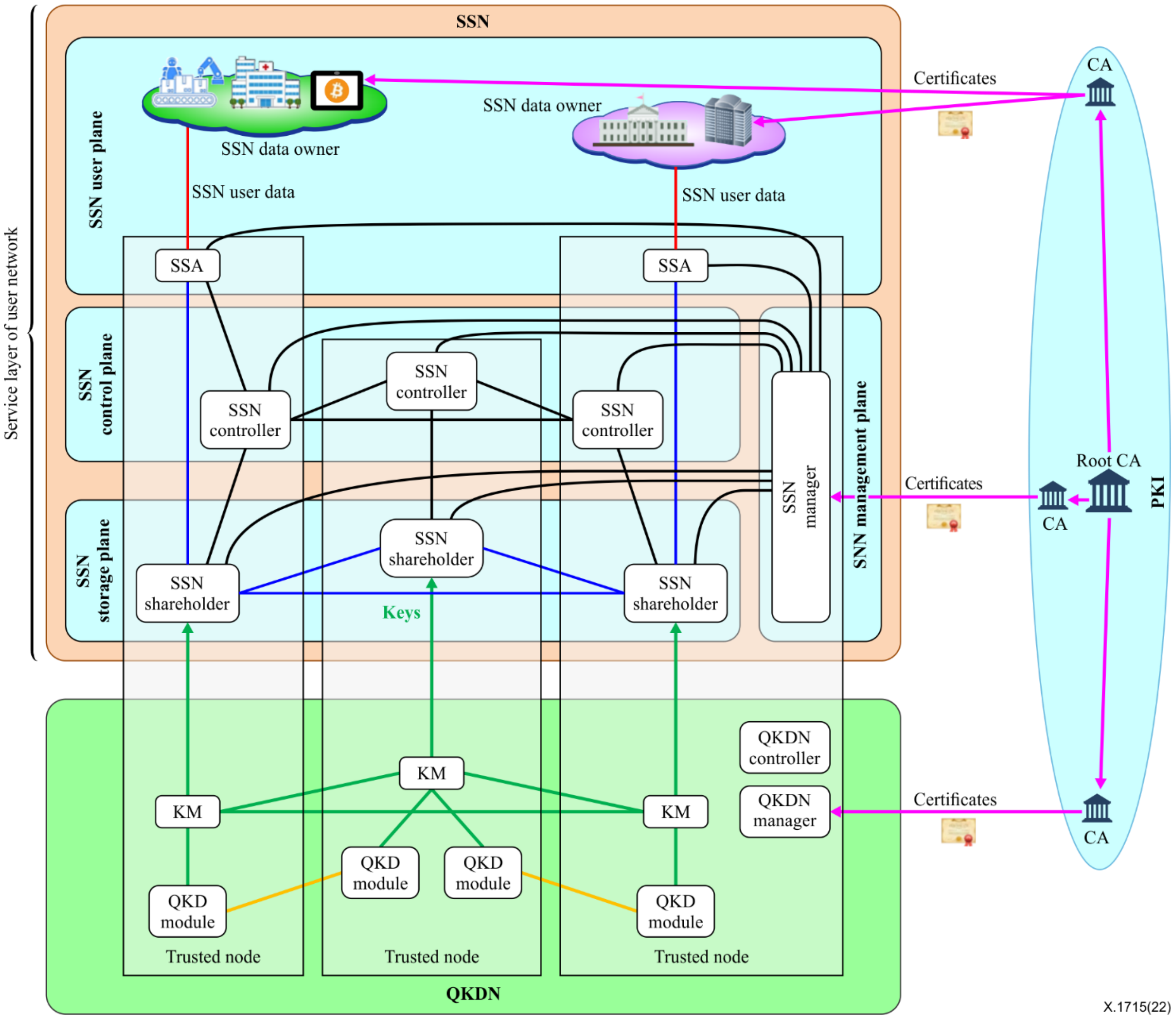

Figure 1 – Overview of integration of QKDN with PKI and SSN [ITU-T Y.3808]

7 Functional elements and information assets

7.1 Functional elements

7.1.1 QKDN functional elements

As specified in [ITU-T Y.3800] and [ITU-T X.1710], a QKDN contains the following functional elements and links: QKD module; key manager (KM); QKDN controller; QKDN manager; QKD link; KM link; control link; management link; QKD-KM link; KM-application link; and QKD network manager-network manager link.

7.1.2 PKI functional elements

The following functional element, as paraphrased from clause 7 of [ITU-T Y.3808], is included in a PKI:

– certification authority (CA): A functional element that issues a digital certificate. In a PKI, CAs form a tree structure to construct trust chains. A CA at the top of the tree is called a root CA.

7.1.3 SSN functional elements

For SSN application, the following functional elements are specified in clause 6 of [ITU-T Y.3808] in the user network.

– 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 them appropriately (e.g., transform them to shares by a secret sharing protocol), and control communication for the SSN shareholder.

– 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 the 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.

These are supplemented by:

– SSA link: a communication link between SSAs and the SSN data owners. SSA links are shown in red in Figure 1. These links transmit original data with highly secure encryption such as OTP.

– SSN management link: a communication between an SSN manager and other functional elements in SSN. SSN manager links are also shown in black in Figure 1. These links transmit management information between the SSN manager and other functional elements in the SSN.

7.2 Information assets in SSN

A SSN contains the following assets:

– key data, metadata: key data and metadata are delivered from a QKDN and used for encryption of data in SSN such as original data and shares;

  NOTE – Details of key data and metadata are specified in [ITU-T Y.3803] and [ITU-T X.1712].

– original data: data containing the information that needs to be protected with confidentiality and other security if required (such as integrity, availability and functionality);

– share: data generated from the original data by secret sharing;

– SSN control and management information: information related to the control and management of the SSN.

8 Security threats

The main purpose of the SSN described in clause 7 is to protect the confidentiality of the original data for a long time by integration of QKDN and secret sharing. General threats to QKDN are specified in [ITU-T X.1710]. This Recommendation focuses on security requirements specific to the SSN supported by QKDN and PKI. The following threats are considered in detail:

1) eavesdropping;

2) spoofing (masquerade);

3) deletion or corruption;

4) repudiation;

5) denial of service (DoS).

8.1 Eavesdropping

Capturing packets from networks is a kind of network layer attack. Though original data and shares are encrypted in the SSN, the emergence of a new harvest now, decrypt later" attack "is assumed.

A "harvest now, decrypt later attack" is the following deciphering attack. An attacker eavesdrops on the encrypted original data even if they do not have the computing ability to decrypt it at that time. In the future, when the attacker has gained advanced computing skills such as large-scale quantum computers, the original data can be decrypted. This type of attack causes negative effects on the confidentiality of data that keep the validity for the long term, such as genome information.

In the SSN, original data, (data) shares and key data are the information assets that are objects of this attack.

It is also a threat to eavesdrop on other information assets, such as SSN control and management information, where the attacker can understand sensitive network information or cause trouble on network operation. In this case, the attacker needs to decrypt the sensitive information in a relatively short period, during the time that networks are operated or immediately after. Thus, usually a "harvest now, decrypt later" attack is not effective.

8.2 Spoofing

Spoofing is an attack of pretending to be a different entity in order to gain an illegitimate advantage. To make this attack effective, the attacker needs to decipher security means against spoofing in a relatively short time, i.e., during the lifetime of communications. This threat is applied to all entities in the QKDN, the PKI and the user network.

8.3 Deletion or corruption

Deletion or corruption are attacks done to compromise the integrity of information assets transferred or stored by unauthorized deletion, insertion, modification, re-ordering, replay or delay. There are also deletions or corruptions due to unforeseen issues, such as disasters. These threats are applied to all information assets: original data, (data) shares, and key data.

8.4 Repudiation

Repudiation is denying the fact of executing some tasks. An administrator enforcing a malicious network policy (e.g., copying and forwarding specific traffic flows to malicious nodes), may claim that they did not create such a network policy enforcement.

8.5 Denial of service

DoS performs specific kinds of activities to disrupt the proper operations of the SSN. This may include denial of access to the SSN, denial of generation of shares and other communication by flooding the SSN.

Security threats identified in the integration of QKDN with PKI and SSN are depicted in Figure 2.

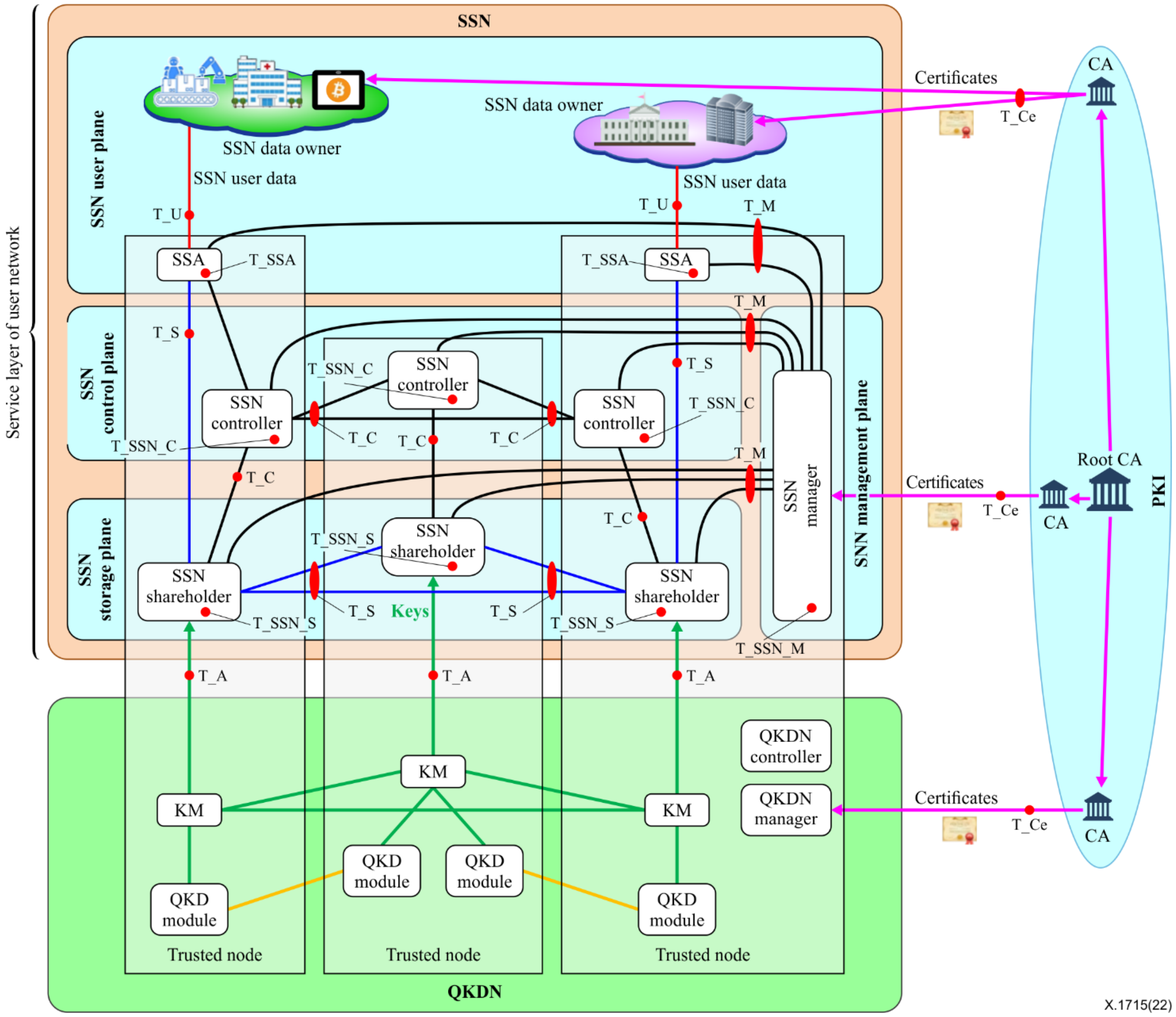

Figure 2 – Security threats identified in integration of QKDN with PKI and SSN

1) T_U: Security threat at the links between SSA and the SSN data owner:

– eavesdropping: intercepting and deciphering the SSN original data and related information from the SSN data owner;

– deletion or corruption: deleting or modifying the SSN original data and related information from the SSN data owner;

NOTE 1 – Information related to the SSN original data is, for example, control information to transmit the original data to the SSA.

– DoS: communication interruption or flooding data traffic such as shares and SSN control and management information.

2) T_S: Security threats at the SSN shareholder links:

– eavesdropping: intercepting and deciphering the shares;

– deletion or corruption: deleting or modifying the shares;

– DoS: communication interruption or flooding data traffic such as shares and SSN control and management information.

3) T_C: Security threats at the SSN control links:

– eavesdropping: intercepting and deciphering the SSN control information;

– deletion or corruption: deleting or modifying the SSN control information.

4) T_M: Security threats at the SSN management links:

– eavesdropping: intercepting and deciphering SSN management information;

– deletion or corruption: deleting or modifying the SSN management information;

– DoS: communication interruption or flooding data traffic such as shares and SSN control and management information.

5) T_Ce: Security threat at the CA link.

– eavesdropping: intercepting and deciphering the certification data;

– deletion or corruption: deleting or modifying the certification data;

NOTE 2 – The certification data is such data provided by PKI for certification in the SSN. The security requirements and measures of them lie outside the scope of this Recommendation.

– DoS: communication interruption or flooding data traffic such as shares and SSN control and management information.

6) T_A: Security threats at the links between the KM and the SSN shareholders:

– T_A is defined as a reference point Ak in [ITU-T Y.3802] and these threats are specified in [ITU-T Y.1710].

7) T_SSA: Security threat at SSAs in an SSN user plane:

– eavesdropping: stealing and deciphering shares and the original data;

– spoofing: an attacker masquerades as an SSA to breach information security – an attacker maliciously fabricates an information asset and claims that such an asset was received from another functional element or SSN data owner, or sent to another functional element or SSN data owner;

– repudiation: an attacker maliciously performs key management functions and subsequently denies that fact;

– DoS: denial of access or flooding data traffic.

8) T_SSN controller: Security threat at SSN controllers in an SSN control plane:

– eavesdropping: stealing and deciphering the SSN control information;

– spoofing: an attacker masquerades as an SSN controller to breach information security – an attacker maliciously fabricates SSN control and management information and claims that such information was received from another functional element or sent to another functional element;

– repudiation: an attacker maliciously performs SSN control functions and subsequently denies that fact;

– DoS: denial of access or flooding data traffic such as shares and SSN control and management information.

9) T_SSN shareholder: Security threat at shares stored in data servers in an SSN storage plane:

– eavesdropping: stealing and deciphering the shares;

– spoofing: an attacker masquerades as an SSN shareholder to breach information security – an attacker maliciously fabricates an information asset and claims that such an asset was received from another functional element or SSA, or sent to another functional element or SSA;

– repudiation: an attacker maliciously performs key management functions and subsequently denies that fact;

– DoS: denial of access or flooding data traffic such as shares and SSN control and management information.

10) T_SSN_manager: Security threat at SSN managers in an SSN management plane:

– spoofing: an attacker masquerades as a SSN manager to breach information security – an attacker maliciously fabricates SSN management information and claims that such information was received from another functional element or sent to another functional element;

– repudiation: an attacker maliciously performs SSN management functions and subsequently denies that fact;

– DoS: denial of access or flooding data traffic such as shares and SSN control and management information.

The relation between security threats and each element of the QKDN are summarized in Table 1 with three different priority levels.

Table 1 – Relation between security threats and secure storage functional elements, and their links, with three different priority levels

Element	**Threat**				
	Spoofing	**Eavesdropping**	**Deletion or corruption**	**Repudiation**	**DoS**
SSA link		3	3		1
SSN shareholder link		1	2		1
SSN control link		1	2		1
SSN management link		1	2		1
CA link		1	2		1
KM-SSN shareholder link		1	2		1
SSA	3			2	1
SSN shareholder	2			2	1
SSN controller	2			2	1
SSN manager	2				1

Numbers in Table 1 indicate the following levels of threat.

– 3: High level

This level is fatal if a threat occurs. Such a threat is expected to result in a break in confidentiality, integrity and availability of the original data.

– 2: Medium level

It is essential for this level of threat to be averted. These are threats against, for example, control and operational information in processes of secret sharing, SSN control and SSN management. If such threats occur, secure and reliable operations of an SSN cannot be achieved.

– 1: Low level

This level includes two kinds of threats. The first is the DoS attack which is recognizable and needs to be considered. If such a threat occurs, an SSN cannot operate normally. The second is eavesdropping on the SSN control and management information of the SSN, which can be done unrecognizably. This neither causes leakage of the original data nor disruption of the SSN operations, but may be beneficial to the adversary.

9 Security requirements and measures

The basic security requirements and security measures for QKDN are specified in [ITU-T X.1710]. This clause describes additional and specific security requirements and measures in an SSN.

Table 2 – Mapping of security dimensions and security threats

Dimensions		**Threat**				
		Spoofing	**Eavesdropping**	**Deletion or corruption**	**Repudiation**	**DoS**
Confidentiality		✓	✓			
Integrity		✓		✓		
Authentication and access control		✓		✓	✓	
Availability	Creating, exchanging, and storing shares			✓		✓
	Damage control and recovery			✓		✓
Accountability	Activity logging	✓		✓		✓
	Alarm reporting	✓		✓		✓
	Audit	✓			✓	✓

The basic concept on the nature of information assets is as follows:

– confidentiality of the original data: long-term security;

– the other dimensions/assets: short-term security.

Security requirements for the SSN in terms of eavesdropping, spoofing, and deletion or corruption are specified, and their security measures are specified in clauses 9.1 to 9.3.

9.1 Security requirements and measures on original data

Requirements and measures for security protection of the original data are summarized in Table 3.

Table 3 – Security requirements and measures on the original data

	Description	**Security requirements**	**Security measures**
(i) confidentiality	Any information on the original data is protected from being leaked to unauthorized elements and parties.	SReq.1 – An SSA is required to ensure confidentiality of the original data transmitted via an SSA link in collaboration with the SSN data owner. SReq.2 – The SSA is required to ensure confidentiality of the original data when processed by or stored in the SSA.	– Towards SReq.1, the SSA has capabilities to supply or receive the original data with encryption or decryption to protect the required confidentiality. – Towards SReq.2, the SSA is protected by appropriate means, which include physical protection measures or the use of cryptographic measures. (Note 1)

Table 3 – Security requirements and measures on the original data

	Description	Security requirements	Security measures
(ii) integrity	The original data remains unaltered.	SReq.3 – The SSA is required to ensure the integrity of the original data.	– Towards SReq.3, the SSA verifies the integrity of the original data received from the SSN data owner. – Towards SReq.3, the SSA is protected by appropriate means, which include physical protection measures or the use of cryptographic measures. (Note 2)
(iii) authentication and access control	An owner and sender of and access to the original data are restricted to authorized entities.	SReq.4 – The SSA is required to ensure that the original data received from an SSN data owner is not trusted unless the identity of the sending entity has been authenticated and it is authorized to supply the original data. SReq.5 – The SSA is required to ensure that it does not allow another entity access to the unencrypted original data without ensuring that the other entity is authorized to receive it.	– Towards SReq.4 and SReq.5, the SSA performs mutual authentication with other entities with which they communicate, or utilize other approaches. – Towards SReq.4 and SReq.5, the SSA has the capability to handle security-relevant attributes and to implement access control security policies.
(iv) availability	The original data is available whenever required.	SReq.6 – The SSA is required to supply the original data following a request from the SSN data owner. SReq.7 – When some shares are lost by malfunctions or disruptions of SSN shareholders, the SSN shareholder is required to reconstruct the original data from the remaining shares if their number is the same or more than the threshold.	– Towards SReq.6 and SReq.7, the SSA has capabilities to retrieve shares and reconstruct the original data from the partial shares.
(v) accountability	The original data is traceable.	SReq.8 – The SSA is recommended to inform an SSN controller or an SSN manager of incident-relevant parameters.	– Towards SReq.8, the SSA has capabilities to create incident-relevant parameters and send them to the SSN controller or the SSN manager. (Note 3)
NOTE 1– Tamper protection implemented by functional entities and security measures provided by a trusted node are examples of physical protection. NOTE 2 – Tamper protection implemented by functional entities and security measures provided by a trusted node are examples of physical protection. NOTE 3 – Actual actions on information to the QKDN controller or the QKDN manager depend on the implementation.			

9.2 Security requirements and measures on (data) share

Requirements and measures on security protection of the (data) share are summarized in Table 4.

Table 4 – Security requirements and measures on share

	Description	Security requirements	Security measures
(i) confidentiality	Any information on the share is protected from being leaked to unauthorized elements and parties.	SReq.9 – The SSA and the SSN shareholder are required to ensure confidentiality of the shares in the SSN shareholder links when they are transmitted through them. SReq.10 – The SSA and the SSN shareholder are recommended to use highly secure confidentiality measures to transmit shares via SSN shareholder links. SReq.11 –The SSA and the SSN shareholder are required to ensure confidentiality of the share when processed by or stored in the SSA or the SSN shareholder.	– Towards SReq.9, the confidentiality of the share is protected by appropriate means, which include physical protection of the SSN shareholder links or cryptographic methods provided by the SSA and the SSN shareholder. – Towards SReq.10, the SSA and the SSN shareholder encrypt the shares by IT-secureencryption/decryption such as OTP when it is transmitted to the other SSN shareholders. – Towards SReq.11, the SSA and the SSN shareholder are protected by appropriate means, which include physical protection measures or the use of cryptographic measures. (Note 1)
(ii) integrity	The share remains unaltered.	SReq.12 –The SSN shareholder is required to ensure the integrity of the shares that are processed and stored.	– Towards SReq.12, the following items i), ii) and iii) are performed. i) The SSN shareholder verifies the integrity of shares received from the SSA. ii) The SSN shareholder verifies the integrity of shares received from the other SSN shareholders. iii) The SSN shareholder has the capability to renew the shares regularly to ensure their long-term integrity of them. iv) The SSN shareholder is protected by appropriate means, which include physical protection measures or the use of cryptographic measures. (Note 2)
(iii) authentication and access control	Shares only trust content from and restrict unencrypted content access to authorized entities.	SReq.13 –The SSA and the SSN shareholder are required to ensure that the share received from the other entities are not trusted unless the identities of the sending entities have been authenticated and they are authorized to supply the share. SReq.14 The SSA and the SSN shareholder are required to ensure that they do not allow another entity access to the unencrypted shares without ensuring that the other entity is authorized to receive them.	– Towards SReq.13 and SReq.14, the SSA and the SSN shareholder perform mutual authentication with other entities with which they communicate, or utilize other approaches. – Towards SReq.13 and SReq.14, the SSA and the SSN shareholder have the capability to handle security-relevant attributes and to implement access control security policies.
(iv) availability	N/A	N/A	N/A

Table 4 – Security requirements and measures on share

	Description	Security requirements	Security measures
(v) accountability	N/A	N/A	N/A
NOTE 1 – Tamper protection implemented by functional entities and security measures provided by a trusted node are examples of physical protection. NOTE 2 – Tamper protection implemented by functional entities and security measures provided by a trusted node are examples of physical protection.			

9.3 Security requirements and measures on SSN control and management information

Requirements and measures on security protection of SSN control and management information are summarized in Table 5.

Table 5 – Security requirements and measures on SSN control and management information

	Description	Security requirements	Security measures
(i) confidentiality	Any information on the SSN control and management information is protected from being leaked to unauthorized elements and parties.	SReq.15 –The SSA, SSN shareholder, SSN controller and the SSN manager are required to ensure confidentiality of the SSN control and management information in the SSN control and management links when they are transmitted through them.	– Towards SReq.15, the SSA, SSN shareholder, SSN controller and the SSN manager protect the SSN control and management information in the SSN control and management links by appropriate cryptographic methods.
(ii) integrity	The SSN control and management information remains unaltered.	SReq.16 –The SSA, SSN shareholder, SSN controller and SSN manager are required to ensure the integrity of the SSN control and management information that they manage.	– Towards SReq.16, the SSA, SSN shareholder, SSN controller and the SSN manager secure the integrity of the SSN control and management information when communicating with each other.

Table 5 – Security requirements and measures on SSN control and management information

	Description	Security requirements	Security measures
(iii) authentication and access control	The SSN control and management information are restricted to authorized entities.	SReq.17 – The SSA, SSN shareholder, SSN controller and the SSN manager are required to ensure that the SSN control and management information received from other entities are not trusted unless the identities of the sending entities have been authenticated and they are authorized to supply the SSN control and management information. SReq.18 – The SSA, SSN shareholder, SSN controller and SSN manager are required to ensure that they do not allow another entity access to the unencrypted SSN control and management information without ensuring that the other entity is authorized to receive it.	– Towards SReq.17 and SReq.18, the SSA, SSN shareholder, SSN controller and SSN manager perform mutual authentication with other entities with which they communicate, or utilize other approaches. – Towards SReq.17 and SReq.18, the SSA, SSN shareholder, SSN controller and SSN manager have the capability to handle security-relevant attributes and to implement access control security policies.
(iv) availability	N/A	N/A	N/A
(v) accountability	N/A	N/A	N/A

Bibliography

[b-ETSI GR QKD 007] Group Report ETSI GR QKD 007 V1.1.1 (2018), *Quantum key distribution (QKD); Vocabulary*.

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

[b-IETF RFC 8446] IETF RFC 8446 (2018), *The transport layer security (TLS) protocol Version 1.3*.

[b-Fujiwara] M. Fujiwara, M., Waseda, A., Nojima, R., Moriai, S., Ogata, W., Sasaki, M. (2016). Unbreakable distributed storage with quantum key distribution network and password authenticated secret sharing, *Sci. Rep*., **6**, pp. 28988(1)-28988(8). Available [viewed 2022-08-11] from: https://doi.org/10.1038/srep28988

[b-Shamir] Shamir, A. (1979). How to share a secret. *Commun. ACM*, **22**(11), pp. 612-613. Available [viewed 2022-08-11] from: https://doi.org/10.1145/359168.359176.

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