INTERNATIONAL TELECOMMUNICATION UNION
TELECOMMUNICATION STANDARDIZATION SECTOR
STUDY PERIOD 2022-2024

SG13-TD239/WP3
STUDY GROUP 13
Original: English

Question(s): 16/13 Geneva, 13 - 24 March 2023

TD

Source: Editor

Title: Draft new Recommendation ITU-T Y.QKDN_SSNarch: “Functional architecture for integration of quantum key distribution network and secure storage network”

Contact: Kaoru Kenyoshi
NICT
Japan
Tel:
Fax:
E-mail: kaoru.kenyoshi@nict.go.jp

Abstract: This document includes the revised draft Recommendation ITU-T Y.QKDN_SSNarch “Functional architecture for integration of quantum key distribution network and secure storage network” (output of Q16/13 meeting, 13 - 24 March 2023)

Summary

This output document is the updated based on the discussion results of the following contribution in the Q16/13 meeting (Geneva, 13 - 24 March 2023).

Number	Title	Source
C395	Proposed update of the draft Recommendation ITU-T Y.QKDN_SSNarch “Functional architecture for integration of quantum key distribution network and secure storage network”	National Institute of Information and Communications Technology (NICT) (Japan) , NEC Corporation (Japan) , Toshiba Corporation (Japan)

Attachments:

Annex A is updated draft Recommendation ITU-T Y.QKDN_SSNarch: Functional architecture for integration of quantum key distribution network and secure storage network.

Revisions indicate modifications based on SG13-TD163/WP3.

Annex

Draft new Recommendation ITU-T Y.QKDN_SSNarch

Functional architecture for integration of quantum key distribution network and secure storage network

Table of Contents

Draft new Recommendation ITU-T Y.QKDN_SSNarch

Functional architecture for integration of quantum key distribution network and secure storage network

Scope

This draft Recommendation will study on functional architecture for integration of quantum key distribution network and secure storage network. It includes detailed description of the followings.

- functional architecture model
- functional elements and reference points
- operational procedures

1 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

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

2 Definitions

2.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

2.1.1 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.

2.1.2 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.

2.1.3 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.

2.1.4 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).

2.1.5 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.

2.1.6 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.

2.1.7 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.

2.1.8 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).

2.2 Terms defined in this Recommendation

None.

3 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

4 Conventions

None.

5 Introduction

Overview, functional requirements, functional architecture model, reference points and operational procedures for an integrating QKDN and SSN are specified in [ITU-T 3808]. This Recommendation specifies the following additional specifications to [ITU-T Y.3808].

Formatted: Font:

Formatted: Normal, No bullets or numbering, Tab stops: Not at 0.5"

- Detailed functional architectures including sub-functions of SSN
- …to be added.

Contributor's note – the following items are issues for further considerations. Contributions are invited on them.

- Advanced functional cooperation between QKDN and SSN
- Dynamic flow among functional elements
- Physical configurations to cover various implementations.
- Centralized and distributed controller
- Network topologies of SSN share holders
- Backup and resiliency of storage
- Metadata management of data and shares
- Additional operational procedures

Figure 1 illustrates a typical configuration of QKDN and SSN.

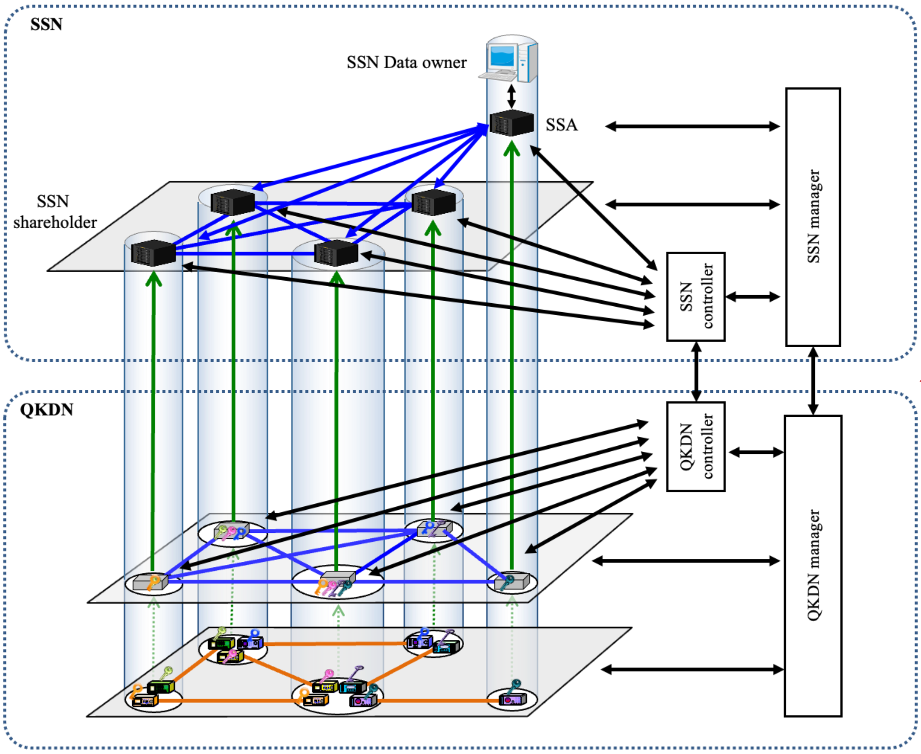

Figure 1 – A typical configuration of QKDN and SSN

In this configuration, functional elements in SSN such as a SSA, SSN shareholders are accommodated in the QKD nodes which include KMs and QKD modules. The KM supplies keys to the SSA and the SSN shareholder in the same QKD node. Shares which are transmitted through SSN shareholder links and SSN control links are encrypted with OTP encryption with keys which are supplied by QKDN.

Formatted: Font:

Formatted: Centered

Formatted: Font: Not Italic, (Asian) Korean

6 functional architecture model

Figure 1 illustrates the functional architecture model of SSN. The functional architecture model of SSN is defined in [ITU-T 3808] and this figure indicates relations between sub-functions in SSN.

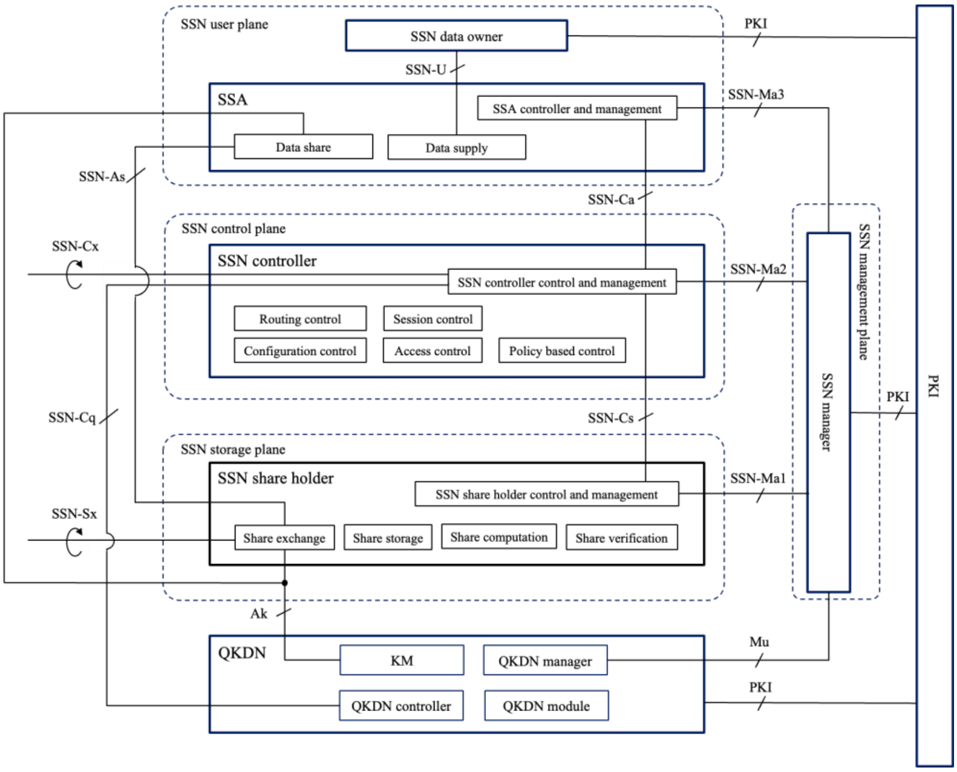

Figure 1 – Functional architecture model of SSN

7 functional elements

8 reference points

8.1 Reference points of SSN controller

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

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

9 share format and metadata

10 storage configuration

11 operational procedures

Appendix I
Further considerations on functional cooperation between QKDN and SSN

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

Formatted: Centered

There is a limit to the speed of key generation by QKD. For example, the key generation rate is about 300 kbps for 50 km. The key storage rate of each trusted node is about 100 kbps on average with normal operation of key relay. When encrypting with OTP, the amount of encrypted data is limited to the amount of storage of keys. For a transmitting data size of 100 Gbytes, 278h of storage is required. Therefore, there is a limit to support SSN only with OTP. Since the key consumption of SSN is high, advanced cooperation of key management between QKDN and SSN is important.

Formatted: No bullets or numbering, Tab stops: Not at 0.5"

There are multiple levels of data confidentiality. If the data is highly confidential, OTP is used to encrypt the share for limited size of data. If the data is moderately confidential, the AES-QKD hybrid can be used to encrypt shares. The QKD-AES hybrid expands the key size but compromises computational security. Security level is depending on the frequency of key updates. Policies and functions are necessary to classify the level of confidentiality of the data, and the encryption method should be chosen appropriately according to the level of confidentiality.

Periodic renewal of shares is necessary after distributing and storing shares. Threshold assumptions for share vulnerability are deteriorating over time. The renewal period must be determined according to the required security level. On the other hand, the renewal period depends on the amount of stored keys. For example, the maximum data size is 329GB (key generation rate:100kbps, interval of share renewal:10years, number of shareholders:4) .

Formatted: Centered