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].

- 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.

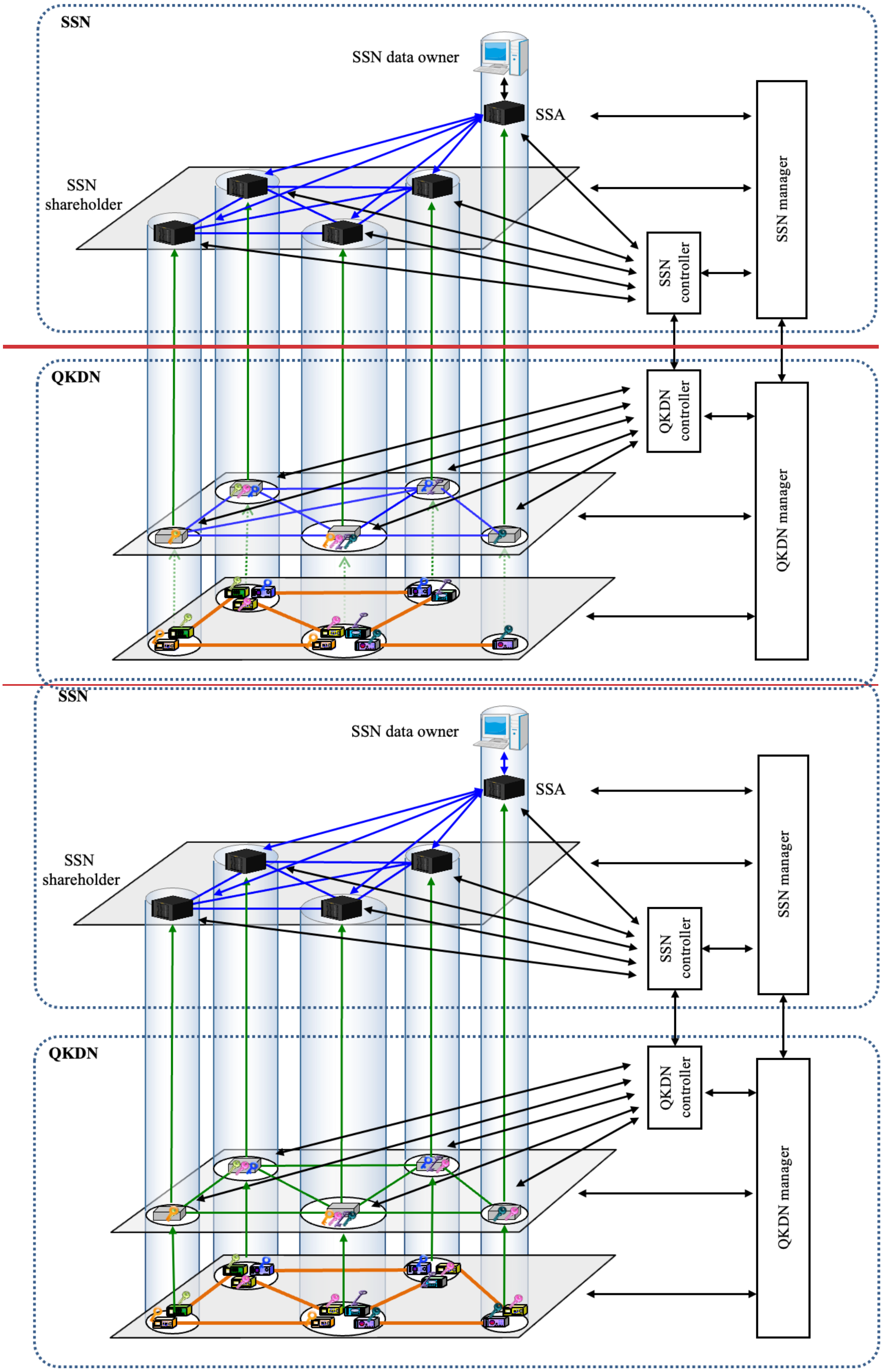


Figure 1 – A typical configuration of QKDN and SSN

NOTE – QKD links are shown in orange, key supply links and KM links are shown in green, control and management links are shown in black, SSN shareholder links and SSA links are shown in blue in Figure 1.

In this configuration, functional elements in SSN such as an 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.

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.

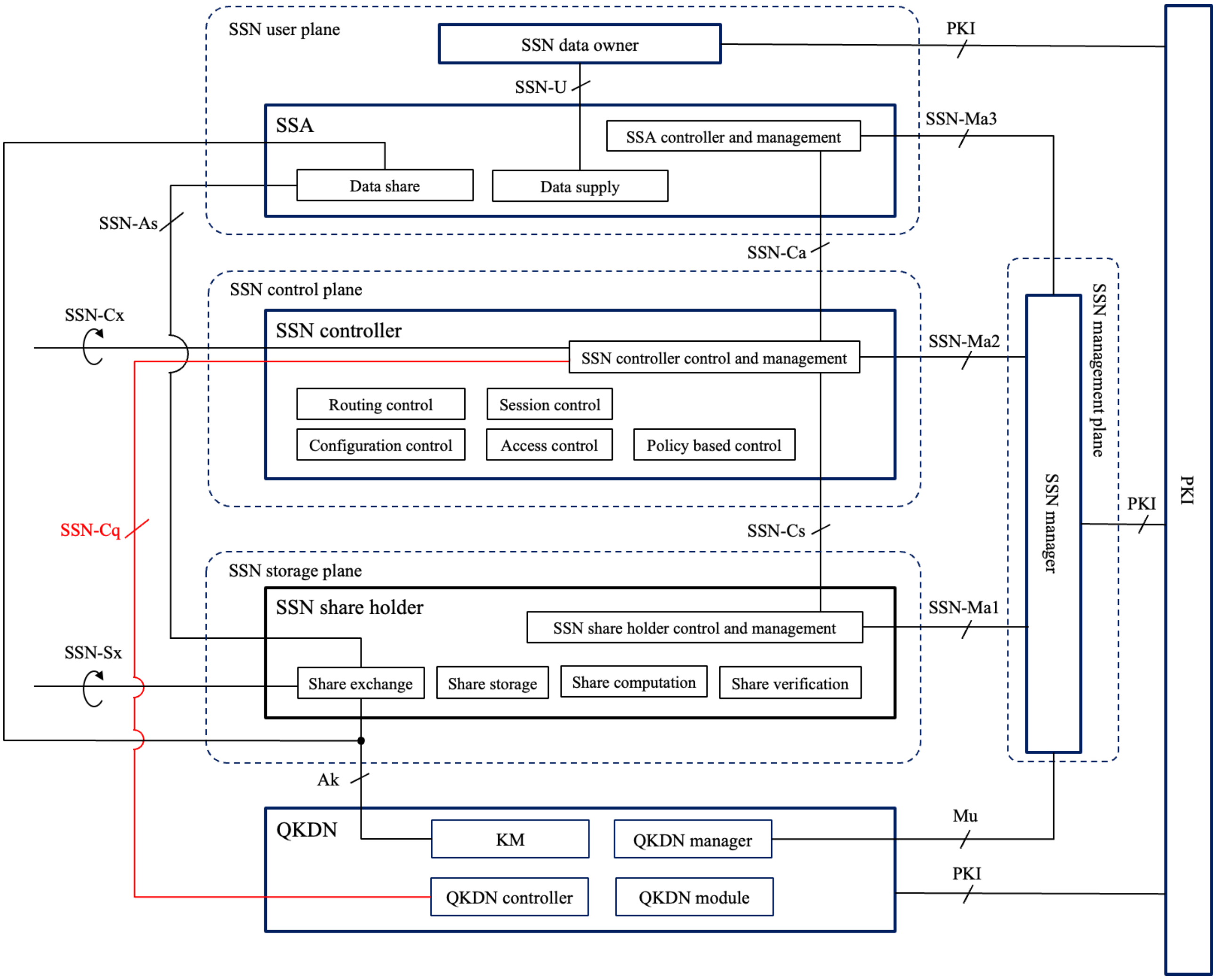


Figure 1 – Functional architecture model of SSN

7 Functional elements

8 Reference points

The reference points shown in black in Figure 1 are defined in [ITU-T Y.3808]. This clause specifies additional reference points to [ITU-T Y.3808]. They are shown in red in Figure 1.

8.1 Reference points of SSN controller

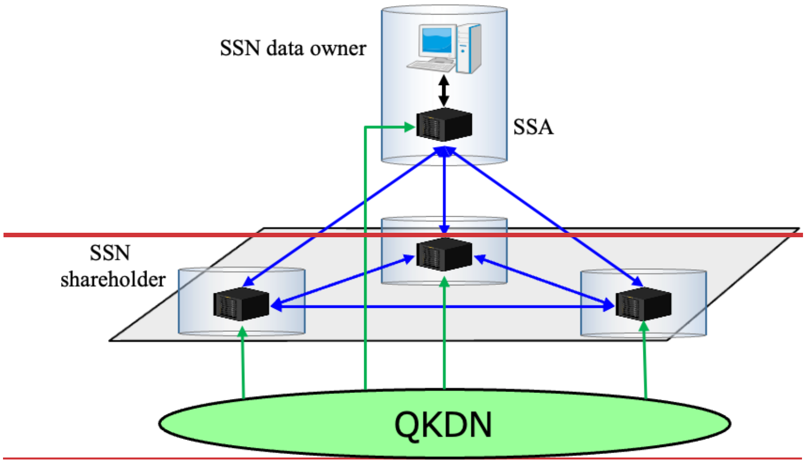
The following reference points are relevant to connections with an SSN controller:

- 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

Figure 2 shows a minimized configuration of the SSN where three shares are created from the original data. SSA transmits shares to three SSN shareholders through SSN shareholder links. These links are private channels. QKDN ~~delivers~~supplies keys for encryption in the private channels in SSN. SSN shareholder links are shown in blue in Figures in this clause.



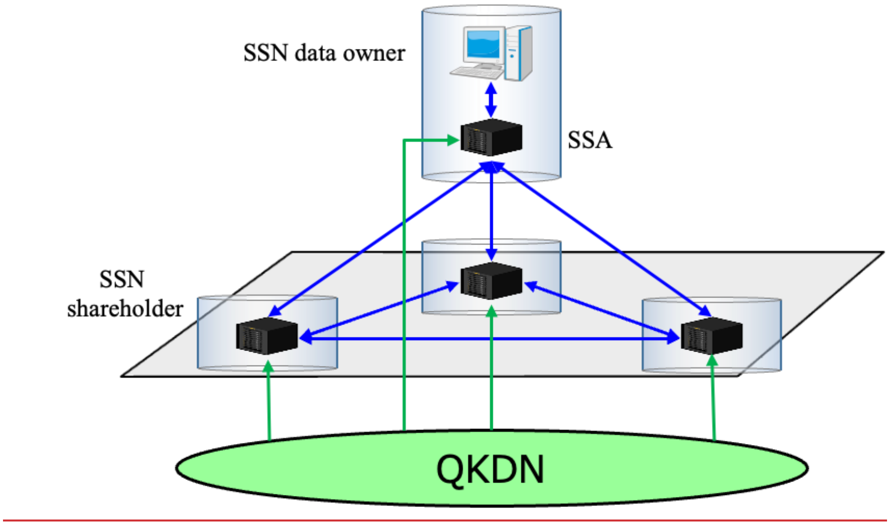
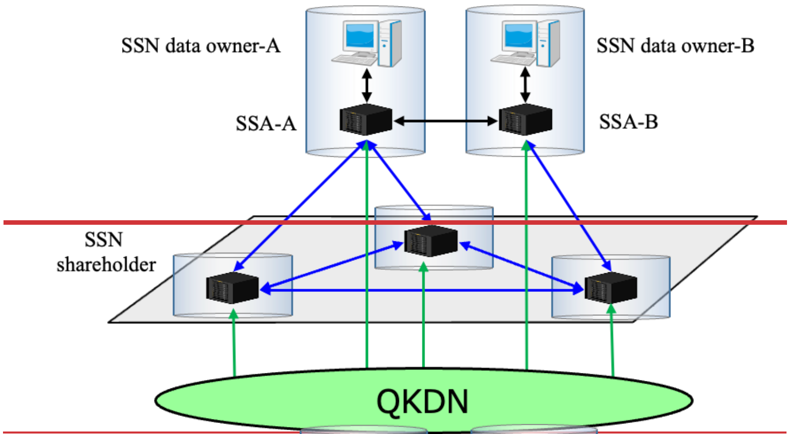


Figure 2 – A minimized configuration of the SSN with three SSN shareholders

If multiple SSN data owners are accommodated in different trusted nodes, an SSA may be included in each trusted node. Each SSA creates Shares from the original data of each SSN data owner. Metadata of shares can be mutually stored among multiple SSAs as a protection against SSA failure. Figure 3 shows a configuration in which two SSAs mutually have a backup function of metadata.



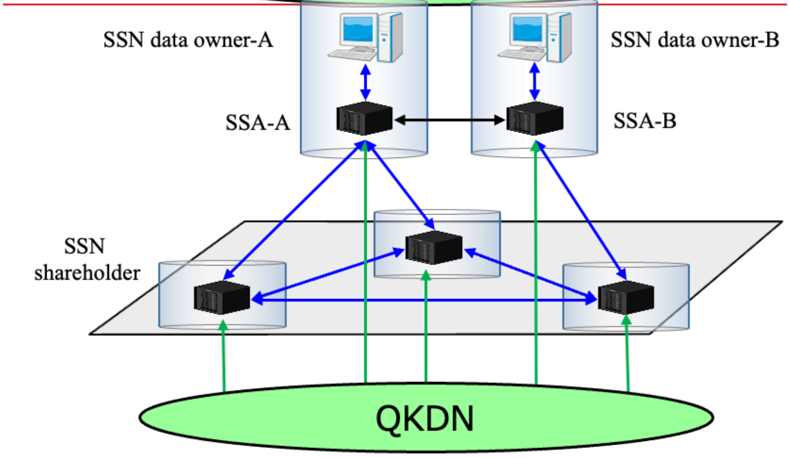


Figure 3- A SSN configuration with multiple SSAs

When the SSN becomes large scale and geographically distributed, the keys can be supplied~~delivered~~ by multiple QKDNs. The SSN shareholders are connected by private channels to store shares in a distributed manner. Each QKDN supplies~~delivers~~ keys to transmit shares with encryption in the SSNs.

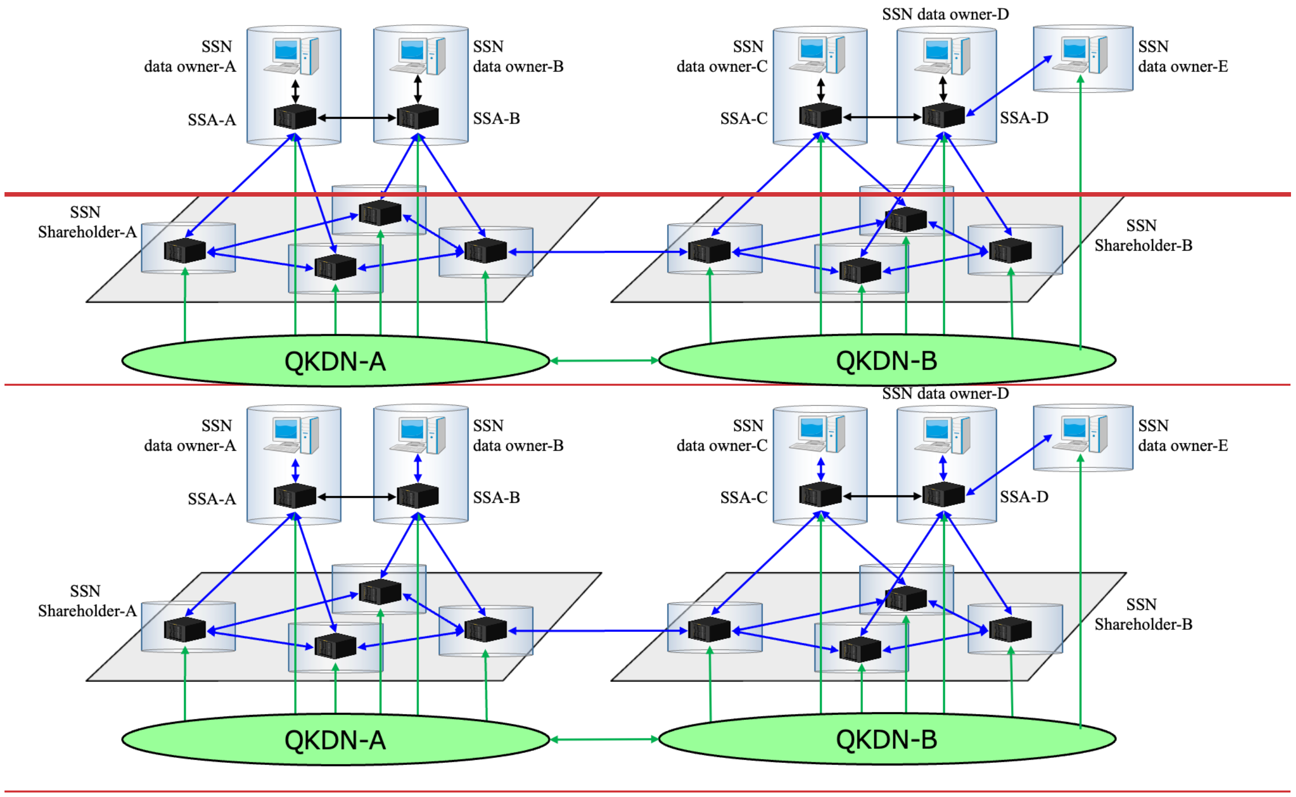


Figure 4 – A large scale SSN configuration supported by multiple QKDNs

11 Routing schemes of shares

The SSN controller decides the share distributing route and instructs it to SSN shareholders. Shares may be distributed directly from the SSA to each SSN shareholder in small-scale SSNs. The following routing schemes are used to distribute shares from SSA to SSN shareholders and among SSN shareholders.

a) Static routing: A share distributing route is set manually on SSAs and SSN shareholders.

b) Dynamic routing: The SSN controller decides share distributing routes based on the status information such as the amounts of keys which are stored in SSAs, SSN shareholders. The SSN controller may cooperate with the QKDN controller to collect information of QKDN such as amounts of keys which are stored in KMs.

c) Scheduled routing: Share renewing route is scheduled in advance for shares renewing procedures.

When the KM does not supply enough amounts of keys for OTP encryption on the request of keys to the KM based on an instruction from the QKDN controller, the SSN shareholder can take the following actions.

- The SSN controller determines a share re-routing route based on the amounts of keys stored in each SSN shareholder and instructs the SSN shareholders to re-route shares.
- The SSN controller collects the amounts of the KSA-keys storing in each KM from the QKDN controller and determines the re-routing route based on the information and instructs it to SSN shareholders.

As another option, the SSN shareholder may encrypt shares using other encryptions such as AES.

~~11~~12 Cooperated control between SSN and QKDN

In the data storing procedure, the SSN controller determines the distribution of the share, i.e., determines in which SSN shareholder each share is stored. As the shares are transferred from ~~a~~an SSN shareholder to another SSN shareholder over the SSN shareholder link with encryption using keys supplied from the QKDN, for ~~exmaple~~example OTP encryption, the performance of the data storing procedure could be affected by the state of QKDN, such as key amount and/or key supply rate available for the encrypted transfer of the shares. Then, the performance could be optimized or enhanced with the SSN controller receiving the information affecting the performance from the QKDN controller and determining the distribution manner using it.

The SSN controller may determine the optimal distribution route before the SSA distributes shares to the SSN shareholders in cooperation with the QKDN controller for data storing procedures. The SSN controller collects the amounts of KSA-keys of each KM from the QKDN controller in advance to distribution of shares. The SSN controller determines the share distribution route based on the collected information and instructs it the SSN shareholders. In this scheme, the QKDN controller can reserve the keys used by the SSN to each KM in advance.

It also applies to the data retrieving and re-sharing procedure.

~~*Contributor's note: texts and procedure diagram to be added for data storing / data retrieving with using information provided by the QKDN controller.*~~

Figure 5 illustrates an example of procedures for cooperated control between SSN and QKDN for routing of share distributing.

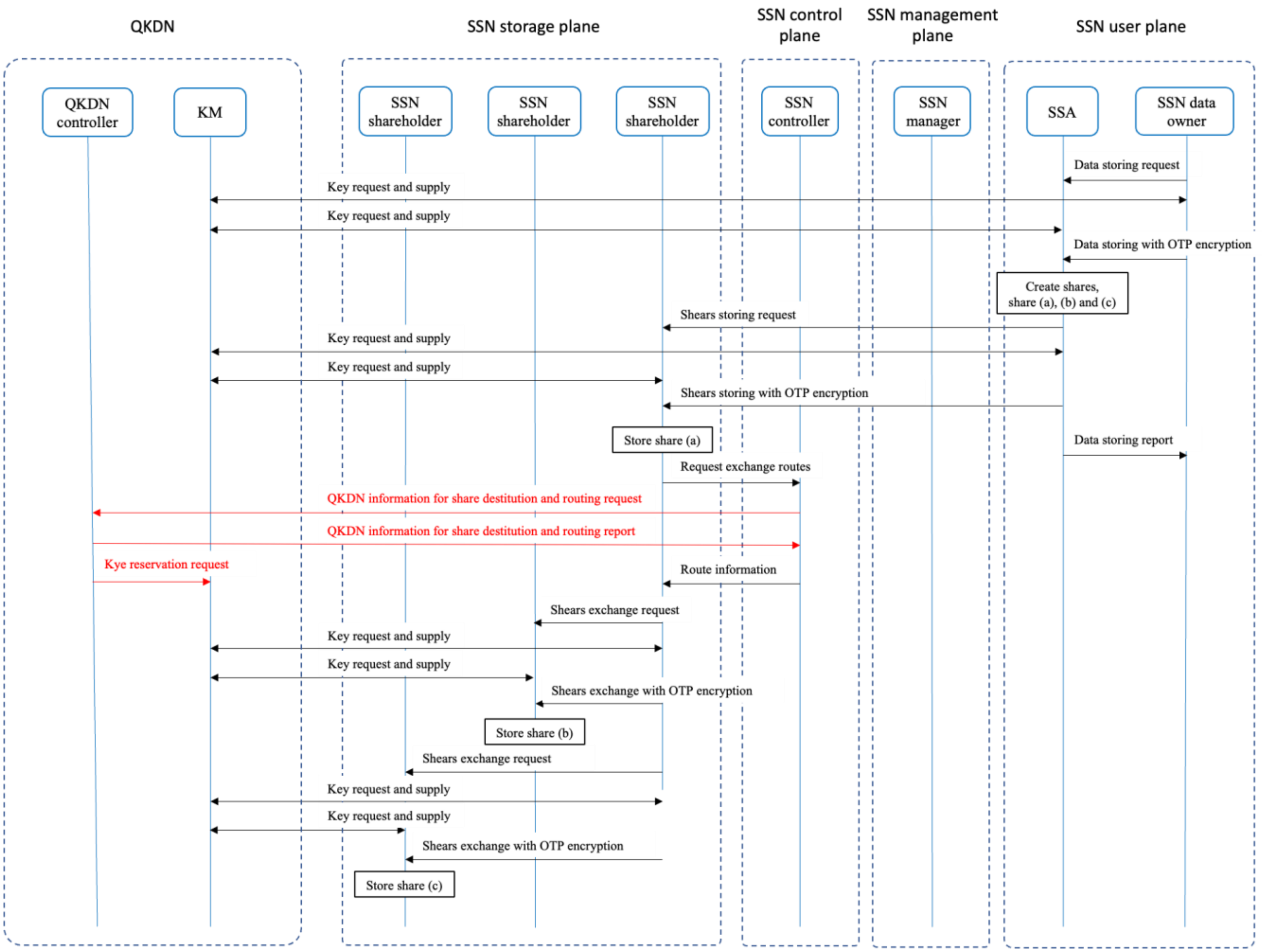


Figure 5 - An example of procedures for cooperated control between SSN and QKDN for routing of share distributing

~~12~~13 Operational procedures

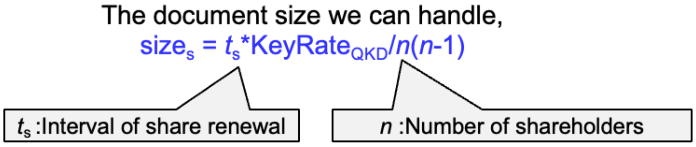
Appendix I
Further considerations on functional cooperation between QKDN and SSN

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

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.

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) .


The document size we can handle,
$\mathrm{size}_s = t_s * \mathrm{KeyRate}_{QKD} / n(n-1)$
t_s :Interval of share renewal
n :Number of shareholders