Draft new Recommendation ITU-T Y.QKDN_SSNreq

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

Table of Contents

Draft new Recommendation ITU-T Y.QKDN_SSNreq

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

1 Scope

This Recommendation specifies functional requirements for integration of quantum key distribution network and secure storage network. It includes detailed description of the followings.

- functional requirements for SSN user plane
- functional requirements for SSN control plane
- functional requirements for SSN storage plane
- functional requirements for SSN management plane

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 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 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

7 Functional requirements for SSN user plane

8 Functional requirements for SSN control plane

The following functional requirements are additionally specified for SSN control plane to [ITU-T Y.3808].

The SSN controller is recommended to control distribution of shares to SSN shareholders using QKDN control information provided by the QKDN controller.

The SSN controller is recommended to control collection of shares from SSN shareholders to reconstruct the original data using QKDN control information provided by the QKDN controller.

The SSN controller is recommended to control re-sharing of shares using QKDN control information provided by the QKDN controller.

NOTE: The QKDN control information includes, but not limited to, available amount and supply rate of keys for encrypting the communication over specified shareholder link.

The SSN controller is recommended to control re-routing of shares to SSN shareholders upon request from the SSN storage plane.

9 Functional requirements for SSN storage plane

The following functional requirements are additionally specified for SSN storage plane to [ITU-T Y.3808].

The SSN shareholder is recommended to have a capability to request the SSN controller to instruct another shareholder to which the share should be transmitted.

NOTE – This may occur if a sufficient amount of keys for IT-secure encryption are not available for transition of the share to the shareholder designated by the SSN controller.

Formatted: English (United States)

10 Functional requirements for SSN management plane

_____