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

6 functional architecture model

7 functional elements

8 reference points

9 share format and metadata

10 storage configuration

11 operational procedures

Annex A: A.1 justification

Question:	16/13	**Proposed new ITU-T Recommendation**	14-25 November 2022
Reference and title:	Recommendation ITU-T Y.QKDN_SSNarch "Functional architecture for integration of quantum key distribution network and secure storage network"		
Base text:	Annex B	**Timing:**	2Q 2024
Editor(s):	Kaoru KENYOSHI, NICT, Japan	**Approval process:**	AAP

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
- reference points
- share format and metadata
- storage configuration
- operational procedures

Summary

In several countries, proof-of-concept demonstrations of QKDNs for commercialization are becoming active. In order to widen applications and market of QKDNs, it is important to study how to integrate QKDNs and the other security infrastructures in the user networks. Secure storage network is one of applications of QKDN to protect critical data for a long-term.

This draft Recommendation will study on functional architecture and reference points for secure storage network (SSN). It includes detailed description of each function and reference point of SSN based on functional architecture model defined in Y.3808.

Relations to ITU-T Recommendations or to other standards (approved or under development):

This WI will refer to the QKDN Recommendations which are produced by Q16/13 and Q15/17 such as ITU-T Recommendation Y.3800, Y.3801, Y.3802, Y.3803, Y.3804, Y.3808 and X.1715.

This work item will collaborate with other SDOs especially on the following activities:

- Deliverables developed by FG-QIT4N;
- GSs and GRs in ETSI ISG-QKD;
- PQ-PKI, PQ-TLS in ETSI Working group Quantum safe cryptography (QSC);
- Post-quantum cryptography with ISO/IEC JTC1-SC27 WG2_SD8;

The proposed new WI will be studied in a harmonious manner with existing and ongoing works in ITU-T and other SDOs but there are no duplications identified so far.

Liaisons with other study groups or with other standards bodies:

ITU-T SG17, ETSI ISG-QKD, WG QSC, ISO/IEC JTC1-SC27

Supporting members that are committing to contributing actively to the work item:

NICT, NEC, Toshiba