A.1 justification for proposed draft new Recommendation ITU-T Y.QKDN_da "Quantum key distribution networks –Dependability assessment"

Question:	Q6/13	**Proposed new ITU-T Recommendation**	Geneva, 23 October - 3 November 2023	
Reference and title:	ITU-T Y.QKDN_da "Quantum key distribution networks – Dependability assessment"			
Base text:			**Timing:**	2025, Nov
Editor(s):	Na Chen, China Telecom; Jianjun Tang, China Telecom; Taesang Choi (ETRI); Zhangchao Ma, USTB; Junsen Lai, CAICT, MIIT China.		**Approval process:**	AAP

Scope (defines the intent or object of the Recommendation and the aspects covered, thereby indicating the limits of its applicability):

This draft Recommendation specifies dependability assessment for quantum key distribution network (QKDN). In particular, the scope of this Recommendation includes:

- Introduction of dependability assessment for QKDN;
- Conceptual model of dependability assessment for QKDN;
- QKDN dependability assessment indicators;
- Dependability assessment process in QKDN;
- Security considerations.

Summary (provides a brief overview of the purpose and contents of the Recommendation, thus permitting readers to judge its usefulness for their work):

With the increasing services supported by QKDN, and various requirements for the interoperation and coordination between QKDN and corresponding user networks, it is urgent to discuss QKDN robustness and carry out necessary standardization works.

QKDN users expect continuously stable keys supply supported by QKDN, which brings strict requirements for robust QKDN operation. Network dependability assessment of QKDN is to evaluate the availability performance and its influencing factors, such as reliability, maintainability of network functions and components, quality of connections, so as to avoid destructive failures in QKDN. Besides, it can improve the level of effectiveness, precision and automation of the QKDN management in QKDN operation and maintenance.

Thus, this Recommendation will carry out standardization study and specify QKDN dependability assessment conceptual model, indicators, and dependability assessment process.

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 SG13 and SG17 such as ITU-T Recommendation Y.3800, Y.3801, Y.3804, Y.3806, Y.3807, Y.3811, Y.3812 and X.1710.

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;

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 SG2, SG12, ETSI ISG-QKD

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

China Telecom (China); ETRI (Korea); University of Science and Technology Beijing (China); MIIT China; CAS Quantum Network Co., Ltd. (China).

Annex B: Proposed initial draft of Y.QKDN_da

Draft new Recommendation ITU-T Y.QKDN_da

Quantum key distribution networks –dependability assessment

Summary

With the increasing services supported by QKDN, and various requirements for the interoperation and coordination between QKDN and corresponding user networks, it is urgent to discuss QKDN robustness and carry out necessary standardization works.

QKDN users expect continuously stable keys supply supported by QKDN, which brings strict requirements for robust QKDN operation. Network dependability assessment of QKDN is to evaluate the availability performance and its influencing factors, such as reliability, maintainability of network functions and components, quality of connections, so as to avoid destructive failures in QKDN. Besides, it can improve the level of effectiveness, precision and automation of the QKDN management in QKDN operation and maintenance.

This Recommendation will carry out standardization study and specify QKDN dependability assessment conceptual model, indicators, and dependability assessment process.

Keywords

Dependability assessment, QKD (quantum key distribution), QKDN (QKD network)

Table of Contents

Draft new Recommendation ITU-T Y.QKDN_da

Quantum key distribution networks – dependability assessment

1 Scope

This draft Recommendation specifies dependability assessment for quantum key distribution network (QKDN). In particular, the scope of this Recommendation includes:

- Introduction of dependability assessment for QKDN;
- Conceptual model of dependability assessment for QKDN;
- QKDN dependability assessment indicators;
- Dependability assessment process in QKDN;
- Security considerations.

2 References

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

[ITU-T Y.3800] Recommendation ITU-T Y.3800 (2019), *Framework for Networks to support Quantum Key Distribution*.

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

[ITU-T Y.3804] Recommendation ITU-T Y.3804 (2020), *Control and Management for Quantum Key Distribution Network*.

[ITU-T Y.3806] Recommendation ITU-T Y.3806 (2021), *Quantum key distribution networks – requirements for quality of service assurance*.

[ITU-T Y.3807] Recommendation ITU-T Y.3807 (2022), *Quantum key distribution networks – Quality of service parameters*.

[ITU-T Y.3811] Recommendation ITU-T Y.3811 (2022), *Quantum key distribution networks – Functional architecture for quality of service assurance*.

[ITU-T Y.3812] Recommendation ITU-T Y.3812 (2022), Quantum key distribution networks – Requirements for machine learning based quality of service assurance.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 **reliability** [b-ITU-T E.800]: The probability that an item can perform a required function under stated conditions for a given time interval.

3.1.2 **availability** [b-ITU-T E.802]: Availability of an item to be in a state to perform a required function at a given instant of time or at any instant of time within a given time interval, assuming that the external resources, if required, are provided.

3.1.3 **dependability** [b-ITU-T Y.3514]: The availability performance and its influencing factors on reliability performance, maintainability performance and maintenance support performance.

3.1.4 **Indicator** [b-ITU-T E.800]: Value calculated from observed attribute/s of a measure.

3.1.5 **network performance** [b-ITU-T E.417]: The performance of a portion of a telecommunications network that is measured between a pair of network-user or network-network interfaces using objectively defined and observed performance parameters.

3.1.6 **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.

3.1.7 **user network** [ITU-T Y.3800]: A network in which cryptographic applications consume keys supplied by a quantum key distribution (QKD) network.

3.1.8 **quantum key distribution link (QKD 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.

3.1.9 **quantum key distribution module (QKD 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).

3.1.10 **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.

3.1.11 **quantum key distribution network controller (QKDN 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.

3.1.12 **quantum key distribution network manager (QKDN 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.

3.1.13 **quantum key distribution node (QKD 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).

< Others to be added>

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

E2E	End to End
IT-secure	Information-theoretically secure
KM	Key Management
KML	Key Management Layer

KPI	Key Performance Indicator
NP	Network Performance
QCL	Quantum Control Layer
QKD	Quantum Key Distribution
QKDN	QKD Network
QKDNM	Quantum Key Distribution Network Manager
QL	Quantum Layer
QoS	Quality of Service

< Others to be added>

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 of dependability assessment for QKDN

ITU-T SG13, SG17, ETSI and other SDOs have been standardizing many aspects of QKDN including QKDN framework, architecture, key management, security requirements, machine learning and SDN enhancements and so on. With the increasing services supported by QKDN, and considering various requirements for the interoperation and coordination between QKDN and corresponding user networks, it is urgent to discuss QKDN robustness and carry out necessary standardization works.

QKDN users expect stable operation and reliable keys supplies of QKDN for secure communication services. Quality of service of QKDN is influenced by many factors which are correlated with network performance aspects, as shown in Fig. 1, network performance related standardization should be considered. Besides, [ITU-T Y. 3807] mentions that network performance is measured in terms of parameters which are meaningful to the QKDN provider and are used for the purpose of design, configuration, control and management of QKDN.

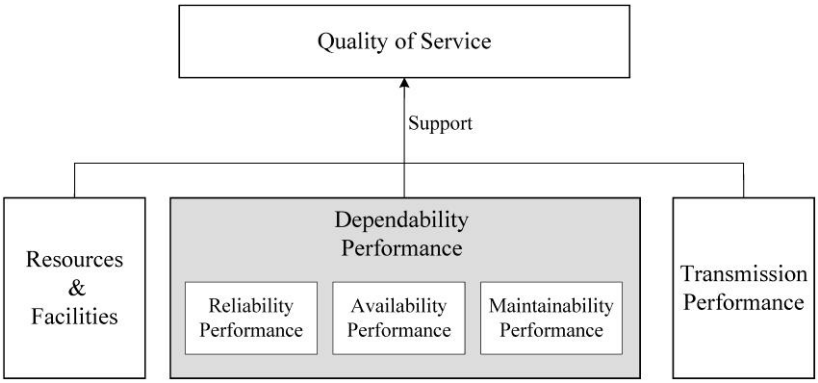

Fig. 1 Relationships between Quality of Service and dependability performance of QKDN

Network dependability assessment of QKDN is to evaluate the availability performance and its influencing factors, such as reliability, maintainability of network functions and components, quality of connections, so as to avoid destructive failures in QKDN. Besides, when a network failure occurs, QKDN dependability assessment can provide guidance for identifying precise fault locations, fault types, reasons, etc, so as to achieve rapid response to system anomalies and troubleshoot faults with

minimal time and economic costs. Therefore, dependability assessment can improve the level of effectiveness, precision and automation of the QKDN management in QKDN operation and maintenance.

<Editor's Note: Further descriptions will be added.>

7 Conceptual model of dependability assessment for QKDN

<TBD>

8 QKDN dependability assessment indicators

<TBD>

9 Dependability assessment process in QKDN

<TBD>

10 Security considerations

<TBD>

Bibliography

[b-ITU-T E.417] Recommendation ITU-T E.417 (2005), *Framework for the network management of IP-based networks*.

[b-ITU-T E.800] Recommendation ITU-T E.800 (2008), *Definitions of terms related to quality of service*.

[b-ITU-T E.802] Recommendation ITU-T E.802 (2007), *Framework and methodologies for the determination and application of QoS parameters*.

[b-ITU-T Y.3514] Recommendation ITU-T Y.3514 (2017), *Cloud computing - Trusted inter-cloud computing framework and requirements*.

[b-ETSI GR QKD 007] ETSI GR QKD 007 (2018), *Quantum Key Distribution (QKD) – Vocabulary*.

_____