



Question(s): 16/13

Geneva, 26 July 2023

TD

Source: Editors

Title: Draft Recommendation ITU-T Y.QKDN-TSNfr:“Framework for integration of quantum key distribution network and time-sensitive network” (output of interim meeting, 17-21 July 2023)

Contact: Zhangchao MA
University of Science and Technology
Beijing
China
Tel: +086-1062332374
E-mail:mazhangchao@ustb.edu.cn

Contact: Lei SUN
University of Science and Technology
Beijing
China
Tel: +086-10-62332374
E-mail: sun_lei@ustb.edu.cn

Contact: Jianquan WANG
University of Science and Technology
Beijing
China
Tel: +86-10-62332374
E-mail: wangjianquan@ustb.edu.cn

Contact: Minghan Li
CAS Quantum Network Co.,Ltd.
Beijing
China
E-mail: liminghan@qtict.com

Contact: Junsen Lai
CAICT, Ministry of Industry and
Information Technology (MIIT)
China
Tel: +86-10-62300592
E-mail: laijunsen@caict.ac.cn

Abstract: This document includes the output of Recommendation ITU-T Y.QKDN-TSNfr “Framework for integration of quantum key distribution network and time-sensitive network” based on the discussion result of the Q16/13 July meeting, 2023.

Summary

This TD is the output document for the draft Recommendation ITU-T Y.QKDN-TSNfr “Framework for integration of quantum key distribution network and time-sensitive network” based on the following input contribution and the discussion during the Q16/13 July meeting, 2023.

No.	Source	Title	Discussion results
C-137	USTB, CAS Quantum Network Co. Ltd. China Mobile	Preliminary considerations on the integration of QKDN and TSN	accepted as proposed

The updated text for draft new Recommendation ITU-T Y.QKDN-TSNfr is attached as Annex I.

Attachments:

Annex I: Updated draft Recommendation ITU-T Y.QKDN-TSNfr “Framework for integration of quantum key distribution network and time-sensitive network”

Annex I:

Draft new Recommendation ITU-T Y.QKDN-TSNfr

Framework for integration of quantum key distribution network and time sensitive network

Summary

This Recommendation specifies the framework for integration of quantum key distribution network (QKDN) and time sensitive network (TSN) including the overview and scenarios of QKDN and TSN integration, the network capabilities to support QKDN and TSN integration, the conceptual structure and basic functions of QKDN and TSN integration, and its overall operational procedures and security considerations.

Keywords

Quantum Key Distribution (QKD); QKD network (QKDN); Time Sensitive Network (TSN)

Table of Contents

1.	Scope.....	4
2.	References.....	4
3.	Terms and definitions	4
3.1.	Terms defined elsewhere.....	4
3.2	Terms defined in this Recommendation.....	5
4	Abbreviations and acronyms	5
5	Conventions	5
6	Overview and scenarios of the integration of QKDN and TSN	5
7	Network capabilities to supportQKDN and TSN integration.....	7
8	Conceptual structures for QKDN and TSN integration.....	8
9	Basic functions of QKDN and TSN integration	8
10	Overall operational procedures of QKDN and TSN integration	8
11	Security considerations	8

Draft Recommendation ITU-T Y.QKDN-TSNfr

Framework for integration of quantum key distribution network and time sensitive network

1. Scope

This Recommendation specifies the framework for integration of quantum key distribution network (QKDN) and time sensitive network (TSN).

In particular, the Recommendation covers:

- Overview and scenarios of QKDN and TSN integration
- Network capabilities to support QKDN and TSN integration
- The conceptual structure and basic functions of QKDN and TSN integration
- Overall operational procedures for the integration of QKDN and TSN
- Security considerations

2. References

[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.3802] Recommendation ITU-T Y.3802 (2020), *Functional architecture of the Quantum Key Distribution network*.

[ITU-T Y.3803] Recommendation ITU-T Y.3803 (2020), *Key management for quantum key distribution network*.

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

[ITU-T Y.3805] Recommendation ITU-T Y.3805 (2022), *Quantum Key Distribution Networks - Software Defined Networking Control*

< Others to be added >

3. Terms and definitions

3.1. Terms defined elsewhere

This recommendation uses the following terms defined elsewhere:

- 3.1.1 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.
- 3.1.2 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.

Editor's Note: More definitions will be added as work progresses

3.2 Terms defined in this Recommendation

This chapter defines all the terms used in this recommendation.

-TBD

4 Abbreviations and acronyms

This chapter describes all the abbreviations and acronyms used in the recommendation.

API	Application Programming Interface
QKD	Quantum Key Distribution
QKDN	Quantum Key Distribution Network
QoS	Quality of Service
TSN	Time Sensitive Network

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 Overview and scenarios of the integration of QKDN and TSN

~~ITU-T SG13, SG17, ETSI~~The Time-sensitive Networking (TSN) is one widely applied communication standard developed by IEEE to meet stringent latency and other SDOs have been standardizing many aspects of QKDN including QKDN architecture, key management, security timing requirements of the industrial environment.

~~TSN relies on precise time synchronization and security proof, time-aware traffic shaping and so on.~~

~~However, it is also urgent to identify the killer applications of QKDN scheduling to ensure deterministic and carry out standardization for the integration of QKDN and the user reconfigurable data transmission in Ethernet networks, in order to further promote the development of QKDN application.~~

~~The FG-QIT4N focus group has studied more than 20 application scenarios in six categories based on QKDN. Among them, the integration of QKD and TSN is one of its important application scenarios in industrial and telecommunication fields. This project will vigorously promote the standardized development of QKD and TSN integrated applications.~~

~~TSN, as a key enabler for IT/OT convergence, TSN is expected to provide new solutions for the next generation of industrial networks.~~

~~A centralized TSN model is as shown in Fig.1. The control signalling interaction between the centralized network configurator (CNC) and TSN switches, the data delivery between TSN endpoints and switches and the time synchronization messages all need highly secure and real-time security protection measures.~~

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

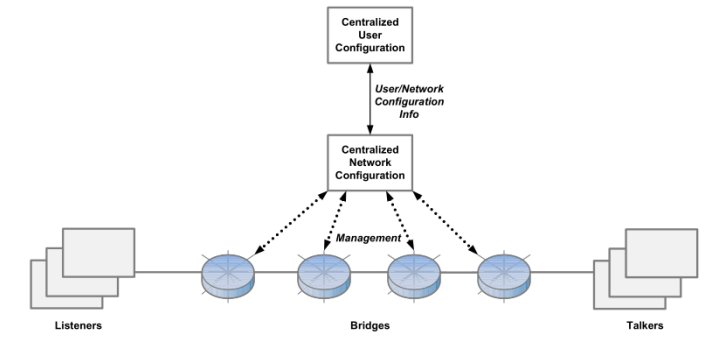


Fig. networks1 Fully centralized TSN model

Formatted: English (United States)

Ensuring cybersecurity is an important requirement in life-critical control systems for which industrial TSN will provide communication service. Traditional key exchange methods (i.e., either manually pre-shared keys or public key exchange), which will require more computing resources and mobile fronthaul networks, while it also raises sever security concerns. It is still challenging cause additional latency, are discouraged for traditional computing complexity based cryptography to provide efficient high-speed real-time encryption to ensure security for TSN. As the TSN targeted scenario.

As QKD can generate out-of-band high-speed symmetric keys based on quantum physics principle, it is envisioned to be an important solution for TSN security enhancement.

As shown in Fig. 1, the TSN as a user network can be secured by QKDN. The QKDN TSN integrated functions may include:

- QKDN secured time synchronization message delivery between TSN grandmaster clock and slave clocks;
- QKDN secured TSN control signalling interaction between CNC/CUC and endpoint bridges;
- QKDN secured packet transportation between talker and listeners;
- TSN controller aware of QKDN key resource to schedule data paths with security guarantee;
- QKDN controller aware of TSN requirements to generate key resource along TSN links;

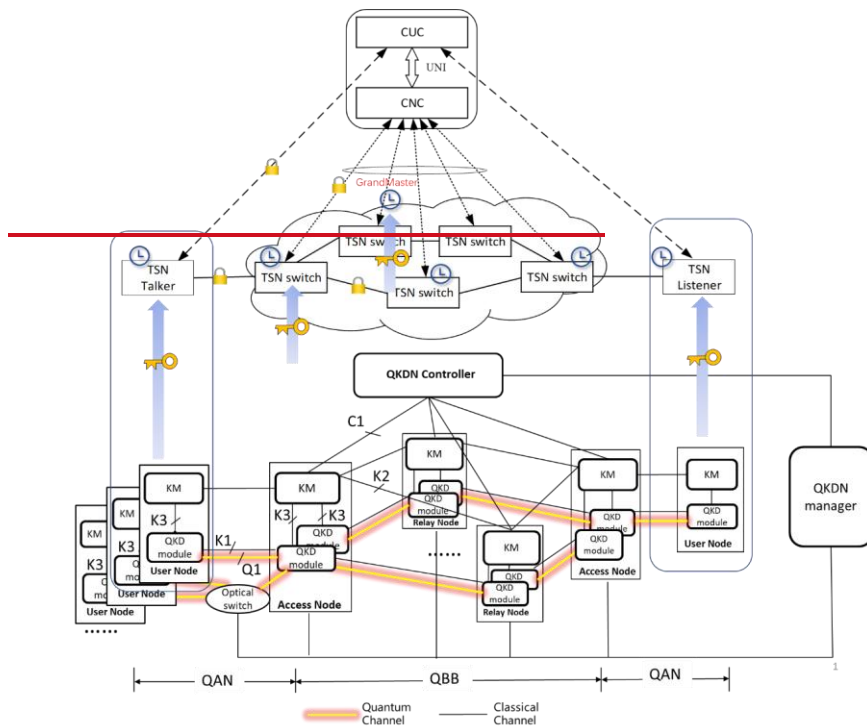


Fig. 1 TSN as a user network secured by QKDN

Formatted: English (United States)

This Recommendation aims to provide a framework to facilitate the integration of QKDN and TSN and to ensure the efficient security enhancement of TSN based on QKDN.

Editor's Note: Further descriptions will be added for the concept of QKDN and TSN integration as work progresses.

7 Network capabilities to support QKDN and TSN integration

Editor's Note: network capabilities to support QKDN and TSN integration considering the various integration scenarios, including QKD protected time synchronization and packet delivery, QKD and TSN coordination etc, will be described.

The basic network capabilities to support QKDN-TSN integration may include:

- QKDN-secured time synchronization message delivery between TSN grandmaster clock and slave clocks;
- QKDN-secured TSN control signalling interaction between CNC/CUC and endpoint/bridges.
- QKDN-secured packet transportation between talker and listeners.
- TSN controller aware of QKDN key resource to schedule data paths with security guarantee;
- QKDN controller aware of TSN requirements to generate key resource along TSN links.

Formatted: Left

8 Conceptual structures for QKDN and TSN integration

Editor's Note: The conceptual structures of QKDN and TSN integration will be described.

The TSN as a user network can be secured by QKDN. The conceptual structure for the integration of QKDN and TSN is as shown in Fig. 2.

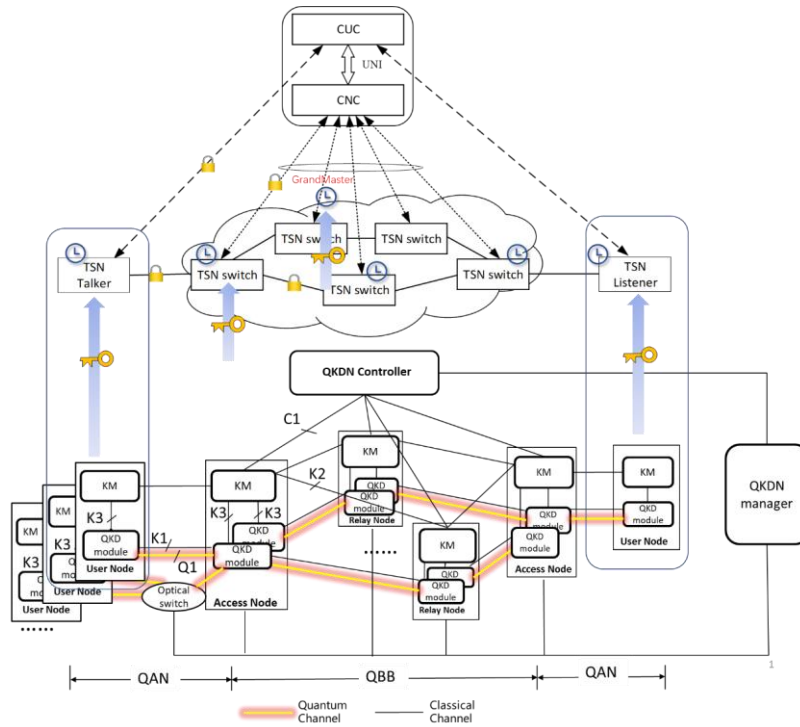


Fig. 1 Conceptual structure of TSN integrated with QKDN as a user network

Formatted: English (United Kingdom)

9 Basic functions of QKDN and TSN integration

Editor's Note: Basic functions and relevant functional entities to implement the integration of QKDN and TSN will be described.

10 Overall operational procedures of QKDN and TSN integration

Editor's Note: Operational procedures to implement the coordination and integration of the QKDN and TSN for use cases will be described.

11 Security considerations

Editor's Note: General security perspective are addressed here for QKDN and TSN integration, however, the details of security are outside of scope of this recommendation

Bibliography

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