QUANTUM KEY DISTRIBUTION NETWORKS FOR TRUSTED 5G AND BEYOND: AN ITU-T STANDARDIZATION PERSPECTIVE

Taesang Choi[*], Hyungsoo Kim[**], Jeongyun Kim[*], Chun Seok Yoon[**], Gyu Myoung Lee[***]*

[*]Electronic and Telecommunications Research Institute (ETRI), Korea (Rep. of), [**]KT, Korea (Rep. of), [***]Liverpool John Moores University, UK and Korea Advanced Institute of Science and Technology, Korea (Rep. of)

ABSTRACT

The introduction of Quantum Key Distribution Networks (QKDNs) into current communication networks (e.g. 5G networks) and cryptographic infrastructures brings new challenges to the design of network architecture and security considerations. This paper introduces core standards on QKDNs developed in ITU-T SG13 and pre-standardization activities in ITU-T FG-QIT4N. Then, this paper discusses key challenges and identifies potential work items for stimulating future standardization for quantum enhanced networking and services considering trustworthy networking technologies and Artificial Intelligence (AI)/Machine Learning (ML) techniques for 5G and beyond.

Keywords – Quantum key distribution network (QKDN), quantum information technology, standardization, ITU-T

1. INTRODUCTION

Quantum Key Distribution (QKD) technologies are expected to be important to secure the transmission of critical data [1][2]. QKD is based on the principles of quantum information theory and allows the establishment of information-secure cryptographic keys. A QKD protocol allows the distribution of symmetric random bit strings as a secure key that can be proven to be secure, even against an eavesdropper with unbounded computational resources under the assumptions supporting the security proof model. A QKD Network (QKDN) is a technology that extends the reachability and availability of QKD. A QKDN with multiple point-to-point QKD devices enables point-to-multipoint key distribution [3]. Ultra-security and resiliency are identified as key features for 5G and beyond [4]. Therefore, the introduction of QKDNs into current and emerging communication networks (e.g. 5G and beyond networks) and cryptographic infrastructures brings new challenges to the design of network architecture and the development of security solutions, as QKD technologies have their unique features and restrictions.

As the lead group for future networks with a focus on 5G in ITU-T, Study Group (SG) 13 has been focusing on QKDN standardization [5]. Furthermore, ITU-T established the Co-located Quantum (CQ) meeting for collaboration with SG17 on QKDN security aspects. Other Standards Development Organizations (SDOs) such as the European Telecommunications Standards Institute (ETSI) mainly targeted QKD systems with security solutions and have started to consider network aspects of QKD recently for a large-scale trusted network [1]. There are specific groups such as ETSI Industry Specification Group on Quantum Key Distribution for Users (ISG-QKD) [6], ISO/IEC JTC1/SC27 (Information security, cyber security and privacy protection) [7], and the Internet Engineering/Research Task Force (IETF/IRTF) Quantum Internet Research Group (QIRG) [8].

This paper introduces core standards on the functional requirements and architectures as well as key management, and control and management for QKDNs developed in ITU-T SG13. In addition, this paper presents standardization efforts for software defined networking control and Quality of Service (QoS) related aspects in QKDNs along with business role-based models as a guideline for applying service scenarios as well as for deployment and operation of QKDNs. It also introduces several ongoing work items (e.g. QKDN interworking, machine learning (ML)-enabled QKDN, resilience framework, etc.) recently started in ITU-T SG13.

ITU-T Focus Group on Quantum Information Technology for Networks (FG-QIT4N) [9] was established and ITU-T is developing the standardization roadmap on QKDN. Based on these activities, this paper discusses key challenges and identifies potential work items for stimulating future standardization for quantum enhanced networking and services considering trustworthy networking technologies and the adoption of Artificial Intelligence (AI)/ML techniques for 5G and beyond.

The rest of the paper is organized as follows. Section 2 summarizes standardization activities on QKDN in ITU-T. Sections 3 and 4 present recent progress for related standardization in ITU-T SG13 as well as FG-QIT4N. Section 5 discusses challenges for future standardization, along with the conclusion and future work in Section 6.

2. QKDN STANDARDIZATION IN ITU-T

QKD is a procedure or method for generating and distributing symmetrical cryptographic keys with information theoretical security based on quantum information theory. The basic elements of a QKD are a transmitter (QKD-Tx) and a receiver (QKD-Rx), each of which is referred to as a QKD module. A QKD link connects the QKD modules, potentially with the help of a quantum relay point (e.g. optical switch) for relaying quantum signals. The keys are shared via the QKD link. The QKD link usually consists of a quantum channel and a classical channel. The quantum channel for transmitting a quantum signal is reserved for quantum signals, such as a single-photon-level coherent state of light, to transmit random bit strings. The classical channel for exchanging data is reserved for synchronization and data exchange between the QKD modules.

As shown in Figure 1, the QKD systems are expanded to a QKDN comprised of two or more QKD nodes connected through QKD links. A QKDN allows sharing of keys between the QKD nodes by the key relay function providing keys between QKD nodes via intermediate QKD node(s) when they are not directly connected by a QKD link. The user network is a network in which cryptographic applications consume keys supplied by a QKDN.

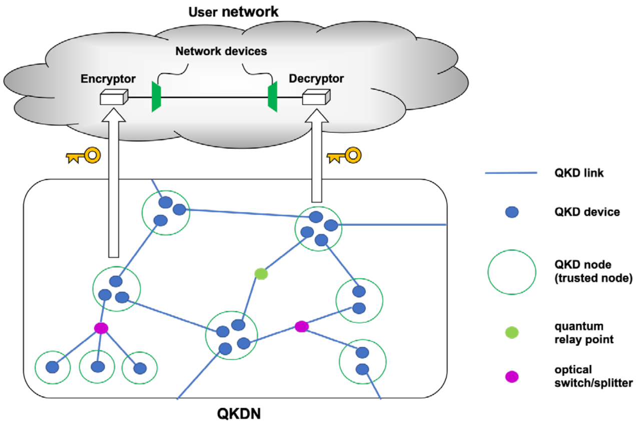


Figure 1 – QKDN concepts and their relation to a user network

Considering both the communication network and security service requirements, a QKDN as both a new kind of security solution and a new form of network infrastructure requires a systematic set of standardization work.

Taking the organization of the ITU-T as an example, the work on QKDN is already ongoing in SG13 on networking aspects and in SG17 on security aspects. Future work may involve protocols and signalling for networks, users and device interconnection (related to SG11), network operation related specifications for QKDNs (related to SG2), integration of QKD with classical optical communication networks (related to SG15) and on QKD applications in data centre interconnection and computing, Internet of Things, mobile networks, etc. (related to SG16 and SG20).

3. STANDARDS FOR QKDN IN ITU-T SG13

ITU-T SG13 started the first initiative on QKDN as a framework document in July 2018 and Recommendation ITU-T Y.3800 was approved in 2019 as the first Recommendation. So far, ITU-T SG13 has completed the development of six Recommendations and one Supplement as shown in Figure 2. There are some ongoing work items (see Table 1) including recently created new work items on interworking, ML, and resilience, etc. in QKDNs.

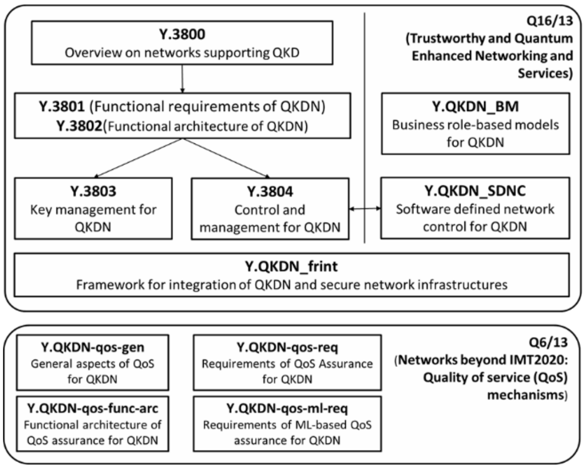

Y.3800
Overview on networks supporting QKD
Q16/13
(Trustworthy and Quantum Enhanced Networking and Services)
Y.3801 (Functional requirements of QKDN)
Y.3802(Functional architecture of QKDN)
Y.QKDN_BM
Business role-based models for QKDN
Y.3803
Key management for QKDN
Y.3804
Control and management for QKDN
Y.QKDN_SDNC
Software defined network control for QKDN
Y.QKDN_frint
Framework for integration of QKDN and secure network infrastructures
Y.QKDN-qos-gen
General aspects of QoS for QKDN
Y.QKDN-qos-req
Requirements of QoS Assurance for QKDN
Q6/13
(Networks beyond IMT2020: Quality of service (QoS) mechanisms)
Y.QKDN-qos-func-arc
Functional architecture of QoS assurance for QKDN
Y.QKDN-qos-ml-req
Requirements of ML-based QoS assurance for QKDN

Figure 2 – Core Recommendations on QKDN developed in ITU-T SG13

3.1 Core Recommendations on QKDN in ITU-T SG13

3.1.1 ITU-T Y.3800 – Overview on networks supporting quantum key distribution

ITU-T Y.3800 [10] gives an overview of the networks supporting QKD. It aims to provide support for the design, deployment, operation, and maintenance for the implementation of QKDNs, in terms of standardized technologies, along with the conceptual structures of a QKDN and a user network. As shown in Figure 3, the layered structure of QKDN consists of a quantum layer, a key management layer, a QKDN control layer and a QKDN management layer. The user network is described by a service layer and a user network management layer.

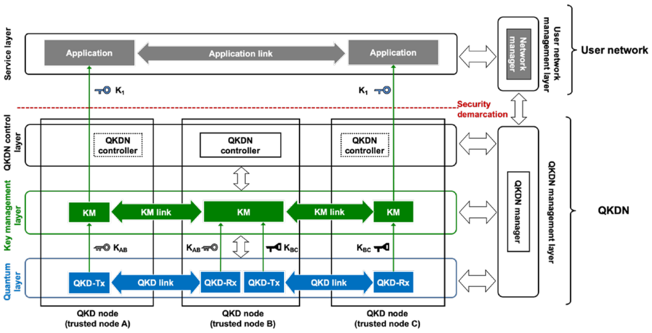


Figure 3 – The conceptual structures of a QKDN and a user network

3.1.2 ITU-T Y.3801 - Functional requirements for quantum key distribution networks

There are the most common requirements for QKDNs in terms of key rate, link length, key usage, and robustness, and so on [2]. In the context of QKDNs, ITU-T Y.3801 specifies the functional requirements for quantum layer, the key management layer, the QKDN control layer and the QKDN management layer. Based on the layered structure of QKDN shown in ITU-T Y.3800 and the functional requirements in ITU-T Y.3801 [11], the detailed functional architecture is developed in ITU-T Y.3802 [12].

3.1.3 ITU-T Y.3802 - Quantum key distribution networks – Functional architecture

ITU-T Y.3802 defines a functional architecture model of the QKDN, as shown in Figure 3. It specifies detailed functional elements and reference points, architectural configurations and basic operational procedures of the QKDN.

The functional architecture model includes the following architectural components: 1) Layered structure (i.e. Figure 3); 2) With a cryptographic application, a user network manager, and an application link in the user network, basic functions and links in the QKDN as follows:

- QKD module: a set of hardware and software components that implement the cryptographic functions and quantum optical processes, including QKD protocols, synchronization, and distillation for key generation. It is contained within a defined cryptographic boundary to demarcate one layer's responsibility on the keys.
- Key Manager (KM): a functional module located in a QKD node to perform the functions for key management in the key management layer.
- QKDN controller: a functional module, which is located in the QKDN control layer to control a QKDN.
- QKDN manager: A functional module, which is located in the QKDN management layer to monitor and manage a QKDN.
- QKD link: a communication link between two QKD modules to operate the QKD.
- KM link: a communication link connecting KMs to perform key management.

3) Functional elements: Subfunctions contained in each basic function (e.g. a routing control function under the QKDN controller); and 4) Detailed reference points. More specifically:

- In the quantum layer, a pair of QKD modules connected by a QKD link generates quantum key distribution keys (QKD-keys) by using QKD protocols.
- In the key management layer, the KM function is to receive and manage keys generated by QKD modules and QKD links, relay the keys, and supply the keys to cryptographic applications.
- In the QKDN control layer, a QKDN controller function is to control QKDN resources to ensure secure, stable, efficient, and robust operations of a QKDN.
- In the QKDN management layer, a QKDN manager function is to manage Fault, Configuration, Accounting, Performance, and Security (FCAPS) aspects of a QKDN as a whole, and support user network management.
- In the service layer, a cryptographic application function consumes the shared key-pairs provided by a QKDN and performs secure communications between remote parties.
- In the user network management layer, a user network manager function performs FCAPS management features of a user network.

Based on the architecture, there are multiple possible network configurations of interconnecting various entities. It illustrates 1) a distributed QKDN; 2) a centralized QKDN; 3) a centralized QKDN with hierarchical QKDN nodes; and 4) a centralized QKDN with a centralized key relay. In addition, it describes basic operational procedures for service provisioning and system initialization, key generation, key request and supply, key relay, and key relay rerouting.

3.1.4 ITU-T Y.3803 - Quantum key distribution networks – Key management

ITU-T Y.3803 [13] provides help for the design, deployment, and operation of key management of a QKDN to fulfill the requirements specified in ITU-T Y.3801.

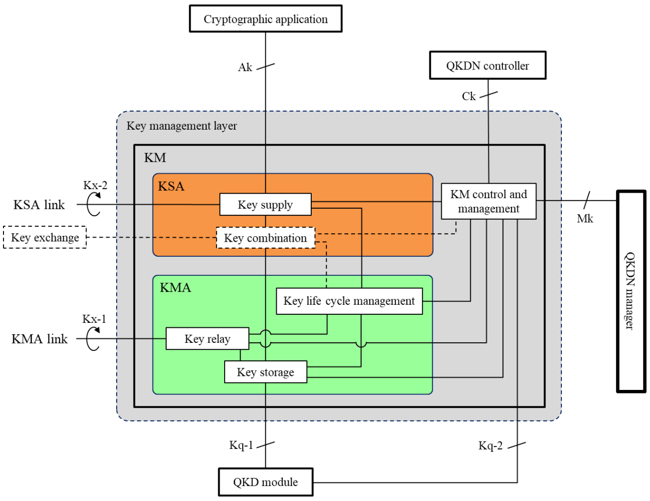


Figure 4 – Functional architecture model of the key management layer

As shown Figure 4, the KM consists of a Key Management Agent (KMA), a Key Supply Agent (KSA), and a KM control and management function. In addition, a KM link is divided into the KMA link (Kx-1) and the KSA link (Kx-2) corresponding to their independent roles. ITU-T Y.3803 presents basic key management operations in a QKDN. Each pair of QKD modules connected by a QKD link generates keys in its own way. Generated keys are transferred to KMs. The KMs manage the keys and supply them to cryptographic applications in the service layer of the user network. The keys can be relayed via KMs and shared between any designated QKD nodes. The QKDN controller performs routing control of key relay. The QKDN manager monitors the status of the whole of the QKDN and supports key life cycle management for the KMs, as well as routing and rerouting control of key relay for the QKDN controller.

3.1.5 ITU-T Y.3804- Quantum key distribution networks – Control and management

To realize secure, stable, efficient, and robust operations of and services by a QKDN, as well as to manage a QKDN as a whole and support user network management, ITU-T Y.3804 [14] specifies functions and procedures for QKDN control and management based on the requirements specified in ITU T Y.3801. More specific functions are:

- control and management specific functions (e.g. path computation for routing control, session control including access traffic steering/switching/splitting for session control, QoS and charging policy control, FCAPS management for each layer);
- control and management reference points among/between control and management functional components and those of other layers;
- control and management orchestration functions of multilayers. QKDN management layer includes multiple functional components responsible for multilayers (quantum, key management, and QKDN control layers) and cross-layer management orchestration;
- interworking functions with external management systems especially user network management systems, the management capability exposure function, etc.

Each layer has a layer specific control and management function associated with a corresponding management function in the QKDN management layer. Each layer specific control and management function provides a management agent capability between each layer management function of the QKDN manager and its respective layer functions. A cross-layer management orchestration function provides orchestration capability among multiple layer management functions. Reference points are defined as standard interfaces between the QKDN controller(s) and the functional components under control for the purpose of QKDN control, as well as standard interfaces between the QKDN manager and the functional components under management for the purpose of QKDN management.

3.1.6 ITU-T Y.3805- Quantum Key Distribution Networks - Software Defined Networking Control (Y.QKDN-SDNC)

ITU-T Y.3805 [15] specifies the requirements, a functional architecture, reference points, a hierarchical Software Defined Networking (SDN) controller and overall operational procedures of SDN control. SDN [16] has several advantages over traditional communication networks. On the one hand, the SDN controller supports centralized, programmable, and hierarchical control; on the other hand, it can provide fast services for applications by opening northbound interfaces between the control layer and the service layer. The change of a control method by SDN in a QKDN provides an alternative method to realizing control functionalities by introducing logically centralized and programmable control of network resources through standardized interfaces and protocols.

Figure 5 illustrates the hierarchical SDN controller in a QKDN. Under such scenarios, SDN controllers are organized in a hierarchical way, and the functions and implementations of each SDN controller is independent of each other. The hierarchical controller is responsible for service provisioning within its control range. The SDN controller of each layer has its northbound interface to communicate with the service layer, and the first layer has a southbound interface for controlling the controllable elements and collecting information from the key management layer and the quantum layer.

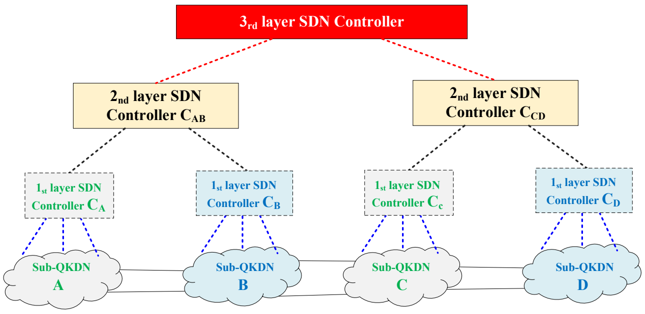

3_{rd} layer SDN Controller
2_{nd} layer SDN Controller C_{AB}
2_{nd} layer SDN Controller C_{CD}
1_{st} layer SDN Controller C_A
1_{st} layer SDN Controller C_B
1_{st} layer SDN Controller C_c
1_{st} layer SDN Controller C_D
Sub-QKDN A
Sub-QKDN B
Sub-QKDN C
Sub-QKDN D

Figure 5 – Hierarchical SDN controller in a QKDN

Unlike other traditional operational procedures of QKD network functions without SDN control, the operational procedures of SDN control in a QKDN reduce the time for provisioning different services using SDN control by skipping the QKDN manager. The SDN controller can also provide more efficient key resource utilization by deciding the end of key generation and controlling the management monitor in a global view. In addition, the SDN technology improves the flexibility of service provisioning and provides services for applications in a fast way by opening the north-bound interface between the QKDN control layer and the service layer. With regard to a SDN-enabled QKDN, ETSI has published the specification on a control interface for SDN in a QKDN [17].

3.1.7 ITU-T Y.3806 – Quantum key distribution networks – Requirements for QoS assurance (Y.QKDN-qos-req)

ITU-T Y.3806 [18] specifies the high-level and functional requirements of QoS assurance for a QKDN. The functional requirements include QoS planning, QoS monitoring, QoS optimization, QoS provisioning, QoS protection and recovery, etc.

For the end-to-end QoS assurance of the QKDN, it is essential to define the scope of the QoS in association with a QKDN, taking into consideration the relationship between end-to-end QKDN QoS and its associated network performance of underlying QKDNs. End-to-end QoS depends upon network performance of different sub-QKDNs: ingress and egress QKDN Access Networks (QAN) and a QKDN Backbone Network (QBN).

3.2 Ongoing work items on QKDN in ITU-T SG13

Table 1 – Ongoing work items on QKDN

SG/Q	Work item
Q16/13	Y.QKDN_BM : Quantum key distribution networks – Business role-based models
	Y.QKDN_frint : Framework for integration of QKDN and secure storage network
	Y.QKDN-iwfr : Quantum key distribution networks – interworking framework
	Y.QKDN-ml-fra : Quantum key distribution networks – Functional requirements and architecture to enable machine learning
	Y.QKDN-rsfr : Quantum key distribution networks – resilience framework
	Y.supp.QKDN-roadmap : Standardization roadmap on Quantum Key Distribution Networks
Q6/13	Y.QKDN-QoS-pa: Quantum key distribution networks – QoS parameters
	Y.QKDN-QoS-fa: Functional architecture of QoS assurance for quantum key distribution networks
	Y.QKDN-QoS-ml-req: Requirements of machine learning based QoS assurance for quantum key distribution networks

3.2.1 QKDN – Business role-based models

Y.QKDN_BM describes business roles, business role-based models, and service scenarios in a QKDN from different deployment and operation perspectives. Especially, Y.QKDN_BM identifies various business models that require security application services with a QKDN and exiting user networks.

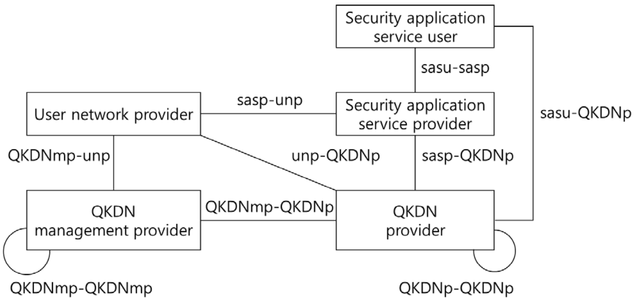


Figure 6 – The owners of business roles in a QKDN

Y.QKDN_BM can be used as a guideline for applying service scenarios that utilize a QKDN from business points of view as well as for deployment and operation of a QKDN from telecommunication operators' points of view.

Telecommunication operations, QKDN operators, or other relevant stakeholders can act as players of QKDN business roles. Players are involved in security application service-related business activities with the QKDN environment. Each player has at least one business role. In some cases, however, one player can have more than one business role at the same time. The identified security application service-related business roles are shown in Figure 6.

3.2.2 Integration of QKDN and secure storage network

The purpose of introducing the QKDN into current communication networks and cryptographic infrastructures is to enhance their security level by supplying highly secure symmetric keys to cryptographic applications. A Secure Storage Network (SSN) consists of multiple data servers and is supported by a secret sharing scheme. A Public Key Infrastructure (PKI) plays an essential role again to realize authentication, access control, and integrity protection in the SSN. Y.QKDN_frint shows a concept of integration of the QKDN with the PKI and the SSN. It also specifies functional requirements, a functional architecture model, reference points and operational procedures for SSNs.

3.2.3 QKDN - Interworking framework

Constructing a large-scale QKDN which covers a wide area, may consist of multiple QKDNs and they are interworking with each other. Therefore, Y.QKDN-iwfr mainly focuses on the interworking between QKDNs supported by multiple QKDN providers. Figure 7 shows a conceptual interworking model between QKDNs.

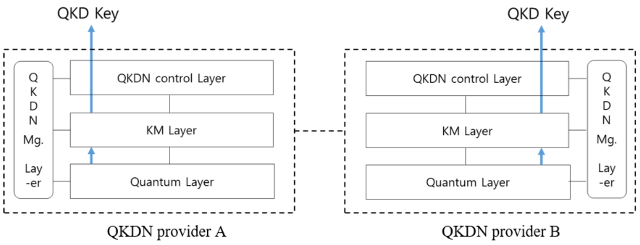


Figure 7 – Interworking between QKDNs

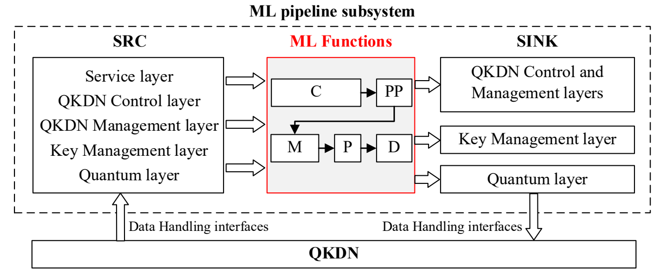
There are several issues to be standardized for interworking between QKDNs with different technologies. Here, different technologies can be used in QKDNs such as key relay encryption methods, key relay schemes, key relay alternatives, configurations of the QKDN controller, and protocols in the key management layer, the QKDN control layer and the QKDN management layer.

3.2.4 QKDN - Applications of machine learning

ITU-T published Supplement 70 [19] to present the applications of ML in QKDNs as follows:

- Applications of ML in the quantum layer of a QKDN: ML-based quantum channel performance prediction (QL01), QKD system parameter optimization (QL02), and remaining use life (RUL) prediction of components in a QKD system (QL03).
- Applications of ML in the key management layer of a QKDN: ML-based key formatting (KM01), key storage management (KM02), and suspicious behavior detection in the key management layer (KM03).
- Applications of ML in the control and management layers of a QKDN: ML-based data collection and data preprocessing (CML01), routing (CML02), and QKDN fault prediction (CML03).

The ML pipeline subsystem in a QKDN is shown in Figure 8. The ML functional elements in the ML pipeline subsystem include a Collector (C), a Preprocessor (PP), a Model (M), a Policy (P) and a Distributor (D). The ML functions enable us to collect input data from the Source of data (SRC) through data handling interfaces. The SRC can be in multiple layers of QKDNs (see Figure 3). The target of the ML output (SINK) can be elements in the quantum layer, the key management layer and QKDN control and management layers. More details related to the ML pipeline subsystems can be found in [20].



C: collector; PP: preprocessor; M: model; P: policy; D: Distributor; SRC: source of data; SINK: target of ML output

Figure 8 – ML pipeline subsystem in a QKDN

For the functional requirements and architectures for an ML-enabled QKDN, Y.QKDN-ml-fra specifies the roles of ML in a QKDN. In particular, Y.QKDN-ml-fra includes functional requirements and a functional architecture model of the ML-enabled QKDN. To specify the functional architecture to enable ML in a QKDN, it applies the high-level architecture specified in [20] to fulfill the requirements for the ML-enabled QKDN. The functional architecture for the ML-enabled QKDN includes three subsystems: QKDN-related ML pipeline; QKDN-related ML sandbox; and QKDN-related Machine Learning Management Subsystem (MLMS). Further considerations on locations of ML-related functions will be discussed with detailed procedures.

3.2.5 QKDN - Resilience framework

For resilience in a QKDN, Y.QKDN-rsfr specifies the framework of resilience in a QKDN including the conceptual models of QKDN protection and recovery scenarios. It also provides typical use cases of resilience and related requirements of resilience schemes supported by the quantum layer, the key management layer, and QKDN control and management layers, respectively. Y.QKDN-rsfr considers the following typical scenarios of resilience in a QKDN: 1) resilience in a QKDN supported by 1+1 protection, 2) resilience in a QKDN supported by 1:1 or 1:n recovery, and 3) resilience in a QKDN supported by re-routing.

3.2.6 QoS aspects in QKDN

There are three work items for QoS aspects in QKDN as follows:

- Y.QKDN-QoS-pa: It covers the descriptions of QoS and network performance in a QKDN, classification of performance concerns for which parameters may be needed, QoS parameters of a QKDN and network performance supporting factors.
- Y.QKDN-QoS-fa: It gives an overview of QoS assurance for a QKDN, a functional architecture of QoS assurance for a QKDN, reference points of functional architecture and procedures of QoS assurance for a QKDN.
- Y.QKDN-QoS-ml-req: It first provides an overview of requirements of ML-based QoS assurance for QKDN. It also describes a functional model of ML-based QoS assurance followed by associated high level and functional requirements of ML-based QoS assurance.

3.2.7 Standardization roadmap on QKDN

Y.supp.QKDN-roadmap provides the standardization roadmap on QKDNs. It describes the landscape with related technical areas of trust technologies from an ITU-T perspective and list of related standards and publications developed in other SDOs.

4. PRE-STANDARDIZATION ACTIVITIES IN ITU-T FG-QIT4N

A Quantum Information Network (QIN or Quantum Internet) is expected to connect quantum information processing nodes, including QKD nodes, quantum computers and quantum sensors, via quantum communication technologies such as quantum teleportation and quantum repeating, to realize quantum information transmission and networking. QIN has the potential to provide a series of new applications, such as distributed quantum computing and quantum sensor networks with the following technologies:

- Quantum computing: a new computation model that follows the laws of quantum mechanics to control quantum information units.

- Quantum communication: a class of novel communication technologies that is based on the transmission of quantum signals, such as QKD, quantum teleportation, quantum repeater.
- Quantum sensing & metrology: the study of measurement techniques that give higher resolution and sensibility in measurements of physical parameters than the same measurement performed in a classical framework.

Considering evolution and applications of Quantum Information Technology (QIT) as the fusion of quantum physics and information technology for networks, ITU-T FG-QIT4N was created in 2019 to provide a collaborative platform for pre-standardization aspects of QIT for networks, with the following topics (see Figure 9):

- Telecom/network aspects of QKDNs that are identified in close coordination with ITU-T SG13 and SG17 as not within the scope of SG13 (QKDN architecture aspects) and SG17 (security aspects of QKDNs and applications of Quantum Random Number Generation (QRNG) for security)
- QIN technology and network evolution.

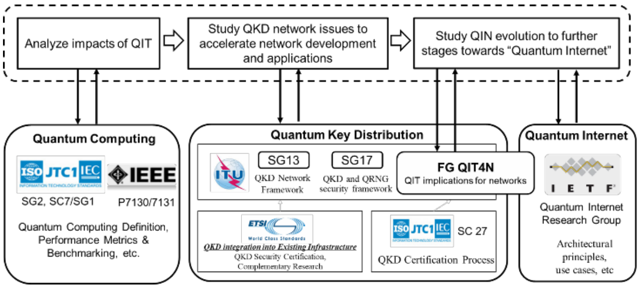

Analyze impacts of QIT
Study QKD network issues to accelerate network development and applications
Study QIN evolution to further stages towards "Quantum Internet"
Quantum Computing
ISO JTC1 IEC
IEEE
SG2, SC7/SG1
P7130/7131
Quantum Computing Definition, Performance Metrics & Benchmarking, etc.
Quantum Key Distribution
ITU
SG13
QKD Network Framework
SG17
QKD and QRNG security framework
FG QIT4N
QIT implications for networks
ETSI World Class Standards
QKD integration into Existing Infrastructure
QKD Security Certification, Complementary Research
ISO JTC1 IEC
SC 27
QKD Certification Process
Quantum Internet
IETF
Quantum Internet Research Group
Architectural principles, use cases, etc

Figure 9 – A landscape of QIT standardization activities and the position of FG-QIT4N

Table 2 – FG-QIT4N planned deliverables

WG	Deliverables	
WG0 (Coordination committee)	D0.1	QIT4N standardization landscape and outlook
WG1 (Network aspects of QIT)	D1.1	QIT4N terminology part 1: Network aspects of QIT
	D1.2	QIT4N use case part 1: Network aspects of QIT
	D1.3	Implications of quantum information technology on networks
	D1.4	QIT4N standardization outlook and technology maturity part 1: Network aspects of QIT
WG2 (QKDN)	D2.1	QIT4N terminology part 2: quantum key distribution network
	D2.2	QIT4N use case part 2: quantum key distribution network
	D2.3.1	QKDN protocols part I: Quantum layer
	D2.3.2	QKDN protocols part II: key management, QKDN control layer and management layer
	D2.4	QKDN transport technologies
	D2.5	QIT4N standardization outlook and technology maturity part 2: quantum key distribution network

As illustrated in Figure 10, the implications of QITs for networks can be classified into two levels: 1) the development of QITs has an impact and benefits for existing and emerging networks, which may include security enhancement, precision time synchronization, boosting signal and data processing capabilities, etc., and 2) the development of QITs could forge new QINs via connecting various types of quantum information processing nodes (e.g. quantum computers, quantum sensors, QKD nodes) by quantum communication technologies and providing new services (e.g. distributed quantum computing and sensing).

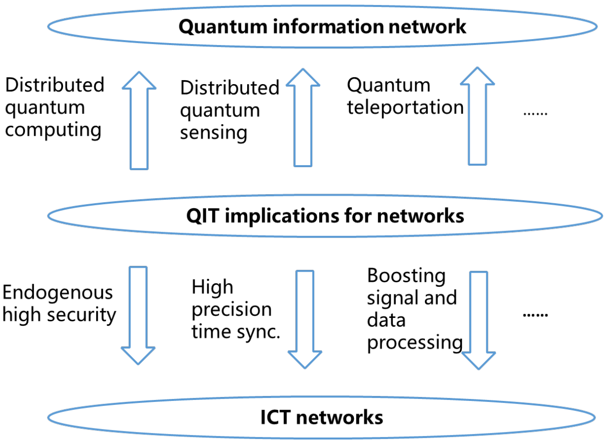

Quantum information network
Distributed quantum computing
Distributed quantum sensing
Quantum teleportation
......
QIT implications for networks
Endogenous high security
High precision time sync.
Boosting signal and data processing
......
ICT networks

Figure 10 – Implications of QIT for networks

In addition, ITU-T FG-QIT4N considers standards relevant to: 1) QIT as building blocks for QINs, 2) QIT for which the network plays an intrinsic role, and 3) QIT to provide ICT network functions and/or performance improvement.

All deliverables (see Table 2) from ITU-T FG-QIT4N will be transferred to relevant study groups in ITU-T for making them formal ITU Recommendations or Supplements, etc.

5. CHALLENGES FOR FUTURE STANDARDIZATION

A QKDN is still a continuously evolving technology. The challenges for QKDN standardization exist from near-term issues (e.g. how to ensure security and interoperability of trusted relay based QKDNs) to medium and long-term issues (e.g. how to reduce costs via integration of quantum and classical telecommunication networks, how to extend the applications of QKD, how to scale up the network via quantum relay) (see Figure 11).

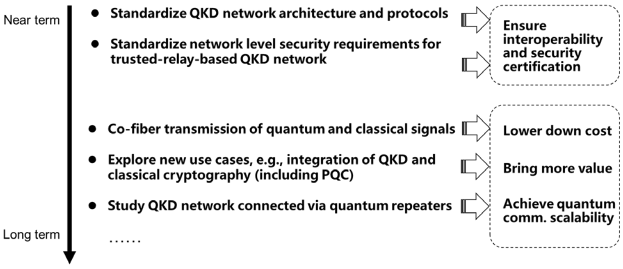

Near term
Standardize QKD network architecture and protocols
Standardize network level security requirements for trusted-relay-based QKD network
Ensure interoperability and security certification
Co-fiber transmission of quantum and classical signals
Lower down cost
Explore new use cases, e.g., integration of QKD and classical cryptography (including PQC)
Bring more value
Study QKD network connected via quantum repeaters
Achieve quantum comm. scalability
Long term
......

Figure 11 – Near-term to long-term QKDN standardization perspective [ITU-T FG-QIT4N]

Furthermore, ITU-T SG13 will continue to develop Quantum Enhanced Networking and Services (QENS) covering a broad range of QIT while supporting emerging user networks (e.g. 5G and beyond) for cryptographic applications, taking into consideration the importance of trustworthy networking and services as long-term issues.

Future work on QKDNs and QENS standardization may cover the following potential work items that could address the challenges highlighted below.

- Support of QKDN interoperability: Many different scenarios for interworking with QKDNs have been identified with possible directions to make progress on QKDN architectures and reference points in the interworking framework of SG13 and the QKDN protocol framework of SG11. Therefore, it's necessary to develop interoperable solutions among multiple providers and different technologies.
- Specifications of QKDN protocols: From a QKD system perspective, most protocols have been developed. For a QKDN perspective, these protocols should be extended to support a network with many nodes and new protocols for control and management should be newly developed in line with the functional architecture model shown in Figure 3.
- Synchronization: Frequency and time synchronization plays a fundamental supporting role in networks. Therefore, specific requirements and related protocols for synchronization should be standardized.
- Multiprotocol connectivity: There is a lack of detailed schemes to effectively coordinate different QKD devices of manufacturers and regions under multiprotocol. It is necessary to establish QKDNs based on multiple QKD devices to provide quantum key service for more users, since a QKD device can only provide quantum keys for a communication pair [21].
- The adoption of AI/ML to a QKDN: It is very important to use AI/ML for improving network performance while supporting QoS. Based on ongoing efforts discussed in Sections 3.1.7 and 3.2.6, architecture models, and mechanisms for end-to-end QoS support also need to be specified with detailed scenarios.
- Integration of user networks (e.g. 5G and beyond) with a QKDN: While identifying new use cases of a QKDN to facilitate the possible further standardization with more valuable scenarios, developing standards to support emerging QKD applications in user networks with a QKDN are necessary.
- Trusted-relay-based QKDN: Trustworthy networking is fundamentally important to ensure security and privacy with legal compliance. The efforts for related security solutions on a QKDN should be continued in alignment with architectural frameworks to be developed.
- Scale up QKDN: Feasible approaches for building up a large-scale QKDN and its cost-effective deployment for user networks should be investigated with candidate technical solutions (e.g. with quantum relay).
- Towards QENS from QKDN: Technical solutions for QKDN are necessary to be expanded for supporting QENS with QITs. QENS basically need QIN and its services with advanced features from quantum computing and communication as well as quantum sensing and metrology.

6. CONCLUSION

As the introduction of a QKDN into the current networks brings new challenges to the design of the network architecture and security considerations, we have introduced standardization activities in ITU-T SG13 and FG-QIT4N. We have also identified key challenges and potential work items for stimulating future standardization for QENS considering trustworthy networking technologies and AI/ML techniques for cryptographic applications in 5G and beyond. For future work, we need to stimulate QKDNs and QENS standardization activities while addressing challenges to be resolved for supporting trustworthy networking and services, as well as cryptographic applications through tightly integrating with 5G networks and beyond as user networks with QKD and QITs.

ACKNOWLEDGEMENT

This work was supported by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korean government (MSIT) (No.2020-0-00557, Development of Standards for Quantum Information Technology).

REFERENCES

[1] ETSI, Quantum Key Distribution, https://www.etsi.org/technologies/quantum-key-distribution

[2] Miralem Mehic, et. al., "Quantum key distribution: a networking perspective," ACM Computing Surveys, vol.53, no.5, pp 1-41, October 2020.

[3] Mehrdad Dianati, et. al., “Architecture and protocols of the future European quantum key distribution network,” Security and Communication Networks, vol.1, issue 1, pp 57-74, January 2008.

[4] Akihiro Nakao, “Beyond 5G/6G telecommunication ensuring continuity in business, research and education,” ITU Kaleidoscope 2020, December 2020.

[5] ITU-T SG13, https://www.itu.int/en/ITU-T/studygroups/2017-2020/13/Pages/default.aspx .

[6] ETSI ISG-QKD, https://www.etsi.org/committee/1430-qkd .

[7] ISO/IEC JTC1/SC27, https://www.iso.org/committee/45306.html .

[8] IETF/IRTF QIRG, https://datatracker.ietf.org/group/qirg/about/.

[9] ITU-T FG-QIT4N, https://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/default.aspx .

[10] Recommendation ITU-T Y.3800, “Overview on networks supporting quantum key distribution,” October 2019.

[11] Recommendation ITU-T Y.3801, “Functional requirements for quantum key distribution networks,” April 2020.

[12] Recommendation ITU-T Y.3802, “Quantum key distribution networks - Functional architecture,” December 2020.

[13] Recommendation ITU-T Y.3803, “Quantum key distribution networks – Key management,” December 2020.

[14] Recommendation ITU-T Y.3804, “Quantum key distribution networks - Control and management,” September 2020.

[15] Recommendation ITU-T Y.3805, “Quantum Key Distribution Networks - Software Defined Networking Control,” under AAP, July 2021 (consented).

[16] Recommendation ITU-T Y.3300, “Framework of software-defined networking,” June 2014.

[17] ETSI GS QKD 015 v1.1.1, “Quantum key distribution (QKD); control interface for software defined networks,” March 2021.

[18] Recommendation ITU-T Y.3806, “Quantum key distribution networks – Requirements for quality of service assurance,” September 2021.

[19] Supplement ITU-T Y.Suppl.70, “ITU-T Y.3800-series – Quantum key distribution networks - Applications of machine learning,” July 2021.

[20] Recommendation ITU-T Y.3172, “Architectural framework for machine learning in future networks including IMT-2020,” June 2019.

[21] ITU-T, “Living list – Multi-protocol connectivity in quantum key distribution networks,” SG13-TD518/WP3, December 2020.