Draft new Supplement ITU-T Y.Supp.QKDN-UC

Use cases of quantum key distribution networks

Summary

Based on the deliverable (D2.2) of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N), this Supplement consolidates the QKDN use cases collected from the ITU-T FG QIT4N in the context of networking technologies as the mandate of ITU-T SG13.

Through a comprehensive analysis, the QKDN uses cases are classified into several classes and this Supplement highlights the competitive advantage of the use cases brought by QKDN and provides suggestions for future standardization efforts in ITU-T SG13.

Keywords

QKDN; Quantum key distribution networks; Use cases.

Table of Contents

Draft new Supplement ITU-T Y.Supp.QKDN-UC

Use cases of quantum key distribution networks

1   Scope

This Supplement presents use cases of quantum key distribution (QKD) networks. In particular, the scope of this Supplement includes:

- Competitive advantage brought by QKDN;
- Overview of QKDN use cases;
- Analysis of collected QKDN use cases including categorization.

2   References

TBD

3   Definitions

3.1   Terms defined elsewhere

This Supplement uses the following term defined elsewhere:

3.1.1   <Term 1> [Reference]: <optional quoted definition>.

3.1.2   <Term 2> [Reference]: <optional quoted definition>.

TBD

3.2   Terms defined in this Supplement

None.

4   Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

TBD

5   Introduction

This Supplement identifies foreseeable, near-term use cases of QKDN technologies gathered during the life of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N). It lists and presents descriptive information about each of the use cases – for those applications and services based on QKDN technologies. These use cases were submitted by individuals within organizations from around the world and FG QIT4N only considered those use cases that had reached at least a demonstrable, proof-of-concept stage.

The Supplement first introduces the potential competitive advantage brought by QKDN to various applications and services. Then, it categorizes the collected QKDN use cases into several classes and provides an overview of each use case. Finally, it summarizes key findings, provides suggestions for further standardization and industrialization and offers a repository of all collected use cases in Appendix I.

The aims of this Supplement are to:

a)   assist technology-oriented decision makers in identifying future opportunities arising from recent advances in QKDN technologies,

b)   support exchange information and best practices through peer learning and knowledge dissemination processes, and

c)   identify possible standardization requirements in the ITU-T SG13.

6   The competitive advantage of using QKDN

Through QKD, the two parties of communication can realize secure symmetric key agreement based on the transmission and processing of quantum states. Moreover, any eavesdropping behaviour will be discovered in time due to the disturbance of the quantum state.

QKD is different from conventional key distribution based on computational complexity because its information theoretical security is based on the principles of quantum mechanics. As long as an adversary does not violate the principles of quantum physics, even if they were to have a computer with arbitrary computing power such as a quantum computer, the security of QKD will not be affected.

Depending on the combination of QKD and conventional cryptography, the application of quantum secure communication can have multiple implementations, e.g.:

•   Combining QKD with an encryption scheme (such as OTP algorithm) and an authentication scheme (such as Universal-2 hash algorithm) providing information theoretic security, a quantum secure communication system with information theoretic security can be realized.

•   The combination of QKD, encryption schemes and authentication schemes that are resistant to quantum computing attacks can realize a quantum secure communication system that can resist quantum computing attacks.

As a supplementary component of cryptography, QKD has rich application scenarios. For example, it can be combined with various existing information and communication protocols at different TCP/IP layers and can also serve various industrial application scenarios to meet the highest security requirements such as providing long-term security guarantees and countering quantum computing attacks.

QKDN has the following competitive advantages:

1)   Quantum computing resistance: The threats posed by quantum computing have a wide range of impacts to various security protocols and applications based on conventional asymmetric and symmetric cryptography algorithms. As the security of these algorithms relies on the computing complexity to resolve certain difficult mathematical problems, quantum computing based on quantum algorithms such as Shor's or Grover's algorithm can effectively solves these mathematical problems. As studied in [b-ETSI GR QSC 006], conventional asymmetric algorithms based on RSA and ECC would be completely broken by Shor's algorithm. For symmetric algorithms, Grover's algorithm effectively halves the key size for these algorithms. Compared with conventional computation-complexity-based cryptography, QKD can be considered as one of the means to combat quantum computing threats by replacing traditional key exchange mechanisms.

2)   Perfect forward security (PFS): Conventional symmetric cryptography, which is vastly applied in mobile networks (including 2G/3G/4G/5G), and Kerberos-based enterprise systems usually rely on the pre-shared root keys and exchange of random numbers to refresh the session keys. It is not easy to change the root keys. For example, the root key for a mobile phone stored in the SIM card cannot be changed during the entire lifecycle. Once the root key is revealed, all the historical data can be decrypted. Compared to conventional symmetric cryptography, QKD systems can guarantee PFS since the keys are continuously refreshed and can thus only be used once. Even if some keys are revealed, the security of the entirety of historical data cannot be breached.
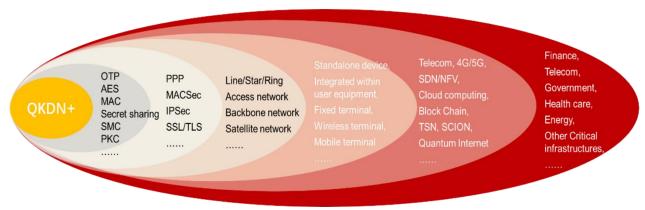
NOTE – PFS can also be achieved via asymmetric cryptography, however, conventional asymmetric cryptography may encounter the threat from quantum computing attack.

3) **High performance key generation**: Most internet security applications including HTTPS, software update, VPN, email and blockchain, etc. are based on asymmetric cryptography, also called public key cryptography (PKC). Quantum-computing-resistant PKC, also called post-quantum cryptography (PQC), is under rapid development and standardization. Certain asymmetric cryptography can also provide PFS, however, asymmetric cryptography which relies on specific hard mathematical problems usually require high overhead for computing power and processing delay. Compared to asymmetric cryptography, QKD, as the key exchange method based on quantum physics means, can provide high throughput and low latency key generation which can be one attractive option for applications which require high performance, e.g., certain time-sensitive services.

7 Overview of QKDN use cases

As key distribution is one of the fundamental cryptographic primitives, QKD has very rich application scenarios which can be classified according to various perspectives, as shown in Figure 7-1.

Figure 7-1 – QKDN use cases overview

(Editor's Note) The following six use classes are the result of FG-QIT4N. For selected use cases in this Supplement, it's necessary to review and categorize them again with different criteria in the context of ITU-T SG13.

In this Supplement, the collected QKDN use cases are classified into the following six use case classes (UCCs):

1) **UCC1: QKD combined with other cryptographic primitives**

- **Encryption**: QKD can be combined with either OTP or AES to perform symmetric encryption;

- **Message authentication**: QKD can be combined with other authentication primitives to perform message authentication function, e.g., universal-II hash functions, symmetric key based message authentication code (MAC);

- **Secret sharing**: QKD can be combined with Shamir's secret sharing algorithm to perform secure storage function;

- **Secure multi-party computation (SMC)**: QKD raw key can be used to implement oblivious key transfer to perform SMC;
- **Public key cryptography (PKC)**: QKD can be combined with PKC including PQC to provide hybrid security guarantee.

2)   UCC2: QKD integrated with various TCP/IP protocols

QKD can be integrated with TCP/IP protocols at various layers, e.g., PPP and MACSec protocol at MAC layer, IPSec protocol at network layer, TLS protocol at transport layer.

3)   UCC3: QKDN deployed in various network topologies

QKDN can be deployed with various network topologies connected via either fibre or free-space channels, e.g., line or ring or star topology, fibre-based metropolitan access network, fibre-based inter-city backbone network, free-space satellite-ground or inter-satellite network.

4)   UCC4: QKD with different user device categories

QKD can be applied in different terminal types with different integration level, e.g.,
- Fixed user device connected to a standalone QKD module;
- Fixed user device which integrates QKD module as an internal component;
- Wireless user device which consumes offline keys provided by QKDN;
- Wireless user device which integrates QKD module to consume online keys provided by QKDN.

5)   UCC5: QKD integrated in various network forms

QKD can be integrated in various ICT network forms which require high security guarantee, e.g., 4G/5G, SDN/NFV-based, cloud computing, blockchain, TSN, service chain and other future network evolutions, e.g., SCION, quantum internet.

6)   UCC6: QKD applied in different vertical sectors

QKD can be applied in various vertical sectors which require high level and long-term security, e.g., finance, government, health care, energy, telecom, critical infrastructure.

8   Use Cases

(Editor's Note) After reviewing the use cases from the FG-QIT4N in the Appendix, it's necessary to select QKDN related use cases in the context of networking technologies as the mandate of ITU-T SG13. Then, the selected use cases will be moved into this clause with details.

<TBD>

Appendix I

Overview of QKDN use cases

(Editor's Note) This Appendix is the collection of QKDN use cases as the result of FG-QIT4N. New use cases can be identified and reviewed. Contributions are invited.

This Appendix provides an overview of the QKDN use cases considered by the Focus Group on Quantum Information Technology for Networks.

I.1 UCC1: QKD combined with other cryptographic primitives

I.1.1 QKD combined with secret sharing

Use case ID	UC-1-1
Short description	This use case describes a distributed cloud archive for long term storage of digital data with advanced security and privacy guarantees.
	QKD links, as well as other technical and other cryptographic means ensure that the data can securely be transported to the involved cloud providers, and remains integrity protected, as well as confidentiality protected against the storage providers, other tenants of the involved storage clouds, as well as other non-entitled third parties.

I.1.2 QKD combined with SMC

Use case ID	UC-1-2
Short description	This use case describes quantum enabled private recognition of composite signals in proteins and genome.
	It consists of a service which enables quantum secure multiparty computation to perform private recognition of composite signals. The generation and distribution of quantum oblivious keys are the basis of this novel service. The quantum oblivious keys are generated from the raw keys of a QKD system.
	This use case is based on use cases UC-5-2-1 and UC-5-2-2.

I.1.3 Hybrid QKD and PQC for encrypted communications

Use case ID	UC-1-3
Short description	Quantum-safe cryptography is urgently needed to protect systems with high security requirements, as data today can be saved and decrypted later by quantum computers.
	Both QKD and PQC present opportunities and obstacles. QKD can provide provably-random keys and information theoretic secure distribution of those keys. However, to deploy a QKD system in the real-world, the technology must overcome the transmission distance problem as well as restrictions of point-to-point links, high manufacturing and maintenance cost, and lack of scalability.
	PQC, on the other hand, is similar to classical cryptography that is algorithm-based. However, deploying a new cryptosystem incurs potentially high cost, with the time and energy consumed by cryptographic computations. In addition, PQC in principle still faces the risk of potential attacks by future mathematical breakthroughs.
	QKD and PQC can be integrated in the hybrid quantum-safe scheme to enhance data transfer security.

I.2 UCC2: QKD integrated with various TCP/IP protocols

I.2.1 QKD integrated in data link layer

Use case ID	UC-2-1
Short description	On the data link layer, QKD may be used as a part of the Point-to-Point Protocol (PPP) protocol. The encryption functionality in PPP is the Encryption Control Protocol (ECP - RFC 1968) which allows the use of encryption in PPP frames. QKD may be used as a key exchange protocol for PPP. QKD may also be used to provide keys for the IEEE 802.1 MACsec layer 2 protocol. As QKD is today mainly implemented as point-to-point link involving two endpoints connected by a quantum channel, it is reasonable to combine a QKD link with a link encryptor to form a QKD link encryptor. Key management is integrated in the link encryptor. For example, this solution may securely bridge two Fast Ethernet networks.

I.2.2 QKD integrated in network layer

Use case ID	UC-2-2
Short description	QKD may be used by a modified IKE protocol to provide the shared secret for IPsec payload encryption. The shared secret provided by QKD may either be used in a conventional block or stream cipher for One-Time-Pad payload encryption in a high security context.

I.2.3 QKD integrated in transport layer

Use case ID	UC-2-3
Short description	Transport Layer Security (TLS) and its predecessor Secure Sockets Layer (SSL) are layer 4 protocols, which provide end-to-end security for network communication services. A session key, usually established with public key exchange, is used e.g. to secure the transmission of credit card information in e-commerce transactions. In a scenario involving QKD, the session key may be replaced by a QKD key, or the QKD keys may immediately be used for One-Time-Pad encryption of transmission data. QKD keys may also be used for message authentication, replacing Hash-based Message Authentication Codes (HMACs) as used in TLS, or the pseudo-random functions of standard SSL.

I.2.4 QKD integrated in application layer

Use case ID	UC-2-4
Short description	Above the transport layer, QKD systems may be integrated in layer 7, the application layer of the OSI model. This may be useful for applications using pre-shared keys for user authentication or for the acquisition or certain rights, or as encryption keys for payload transmission between instances of the application.

I.3 UCC3: QKD implemented in various network topologies

I.3.1 QKDN as metropolitan access network

Use case ID	UC-3-1
Short description	This use case describes a general-purpose high security communications network between several branches and offices within an area of about 100km in diameter (metropolitan area). The single network nodes are interconnected with dedicated optical point to point links for classical digital communication and quantum key distribution. The network uses a dedicated optical infrastructure, which is completely separated from the internet.

I.3.2 QKDN as inter-city backbone network

Use case ID	UC-3-2
Short description	In September 2017, the 2000 km Beijing-Shanghai backbone QKD network was put into operation. The backbone network consists of 32 physical nodes linearly connected by QKD links and has 135 links in total. Two to eight multiple QKD links lie between adjacent nodes. The backbone network is designed to function as a high bandwidth channel that feeds quantum keys between metropolitan and QKD networks located in different cities. The backbone network has been connected to four metropolitan QKD networks already established in Beijing, Shanghai, Jian and Hefei.

I.3.3 QKDN as free-space satellite-ground or inter-satellite network

Use case ID	UC-3-3
Short description	This use case describes a high security general-purpose long-haul network based on multi-layer satellites around the world. By using satellite as relay, long-distance QKD can be realized within the global metropolises.

I.4 UCC4: QKD with different user device categories

I.4.1 Wireless user device with offline QKD-keys

Use case ID	UC-4-1
Short description	This use case describes QKD-key embedded secure mobile communication. To extend QKD service to the mobile terminals is envisioned with high value, but the current physical layer limitations still restrict the direct application of QKD via the air interface between mobile user equipment and base stations. In this use case, the proposed solution is to pre-install the QKD-key pool into the mobile user and network side to enhance security of mobile communication which is achievable with existing QKD techniques.

I.4.2   Wireless user device with integrated QKD module

Use case ID	UC-4-2
Short description	As QKD module being miniaturized into chip-scale, it is possible to be integrated into mobile devices to perform wireless QKD service. This use case describes a successful demonstration, by the University of Bristol in the United Kingdom, of the QKD chip transmitter integrated on the credit card, and the QKD receiver in the ATM rack to achieve the free-space quantum key distribution.

I.5   UCC5: QKD integrated in various network forms

I.5.1   QKD in 4G/5G networks

I.5.1.1   QKDN for LTE backhaul and 5G backbone

Use case ID	UC-5-1-1
Short description	This use case describes a network applying QKD to LTE backhaul between Sejong central office and one of SK Telecom's DU site at Daejeon.
	A trusted relay node was implemented for long distance QKD networks in 2017. Implementation and commercialization of QKD quantum cryptography for a total of 221km of transmission line between Sungsu central office (Seoul area) and Dunsan central office (Daejeon area) of SK Telecom was accomplished in 2019. It will be extended to Taepyung central office and this will make the end to end distance 380km. Other main cities will be reached with QKD step by step.

I.5.1.2   Quantum secured inter-domain 5G service orchestrator

Use case ID	UC-5-1-2
Short description	This use case describes QKD technologies in combination with SDN and NFV and their application in securing interconnections of distributed VNFs to achieve quantum secured inter-domain 5G service orchestration.
	And it was experimentally demonstrated via interconnecting four autonomous 5G islands simultaneously through the q-ROADM with eight optical channels using the 5GUK Exchange orchestration platform.

I.5.1.3   QKDN for 5G front-haul

Use case ID	UC-5-1-3
Short description	The security guarantee for 5G fronthaul is an important issue which need to satisfy high bandwidth, low latency and high-level security at the same time.
	QKD is a promising solution to secure 5G fronthaul and this use case describes the application of QKD to secure the 5G fronthaul.

I.5.1.4   QKDN for 5G mid-haul

Use case ID	UC-5-1-4
Short description	The mid-haul is one newly introduced concept in 5G to indicate the connection between DU (Distributed Unit) and CU (Centralized Unit). SK Telecom has showcased the application of QKD to the 5G mid-haul network, in order to secure the confidential data transmission from a smart factory to the cloud.
	This use case describes how SKT has secured the 5G network connectivity with the latest quantum safe technology using quantum cryptography to best address a customer's

security need. This solution combines the latest technology available ensuring high-speed, stability and security for the customer data connectivity.

I.5.1.5 Quantum security enhancement for universal AKA authentication protocol

Use case ID	UC-5-1-5
Short description	QKDN is used to realize the advantage of secure key distribution. The client UE and the authentication server AAA use QKDN to share keys. Symmetric encryption fully ensures the security of data. The quantum random number generator (QRNG) can generate enough secure true random numbers for the client and authentication server to use in AKA process.

I.5.1.6 Secondary authentication protocol in 5G based on quantum security

Use case ID	UC-5-1-6
Short description	This use case describes two newly designed schemes EAP_QSSE (Quantum Secure Symmetrical Encryption) and EAP_QSSEH (Quantum Secure Symmetrical Encryption and Hash-function) based on quantum security. Both authentication parties use quantum random numbers as authentication factors, and quantum key distribution network (QKDN) to share keys, for two-way authentication of UE and AAA, to achieve lightweight and fast 5G network secondary authentication in a symmetrical encryption authentication manner.

I.5.2 QKD in SDN/NFV based network

I.5.2.1 Secure SDN and NFV Control and Management Plane

Use case ID	UC-5-2-1
Short description	The adoption of SDN and NFV technologies brings many benefits to the network, like the reduction of the complexity and costs of operating the entire infrastructure or the reduction of vendor's block-in in the systems layer (e.g., NMSs). However, the network can be affected by some threats that were not present before, as the configuration of the network elements and the images of VNFs must be transferred from central offices, network controllers and orchestration platforms. To tackle this issue, QKD can be seen as an additional security layer that runs in parallel (or also integrated) to the transport network. QKD can help to mitigate such threats, securing the communications in the control and management plane.

I.5.2.2 Quantum encryption for end-to-end services

Use case ID	UC-5-2-2
Short description	As SDN and NFV technologies are being progressively adopted in transport networks, they also open the market for new capabilities and services to be provided by the operators. SDN allows new technologies and solutions to be integrated in the network at a faster pace. One of the most demanded capabilities is an increase on the security standards of network services, as big corporations have to transfer data between their secure headquarters and data centres. These services (usually enterprise VPNs for business to business -B2B- communications) rely in underlying security protocols that are at risk of future attacks, more when speaking about data meant to have everlasting security. Also, depending on the service being deployed, the security can be implemented at different layers (e.g., IPsec, MACsec, Optical Transport Network - OTN). Quantum key distribution can be seen as a measure to provide such future-proof security, if it is appropriately used by other security systems (e.g., HSMs, VNFs, network cards, etc.) and automated via management systems. This use-case combines QKD systems to secure end-to-end (E2E) services (e.g., transport tunnels, VPNs) between remote premises. Protocols like PCEP (Patch Computation element Protocol) and MPLS (Multiprotocol Label Switching) are used and modified to use QKD.

I.5.2.3 Quantum security for service chaining

Use case ID	UC-5-2-3
Short description	The changing behaviour of current network services is forcing operators to evolve from traditional/legacy, non-scalable and rigid networks towards new flexible architectural solutions. The lead on this evolution comes from multiple sources, being Network Functions Virtualization (NFV) one of the most radical and popular trends. But the flexibility brought by these new networking trends carry associated vulnerabilities and implications. For instance, in a virtualized environment, several functions might be deployed in distributed locations for composing a service function chain (SFC). Both control and data communications must be appropriately secured, as any attempt to compromise a virtual function or its behaviour can compromise the entire infrastructure.
	A wide-spread concern about virtualized network elements is related to traffic attestation. Any network device deployed in a production network must be capable of assessing if a specific traffic flow passes through it and is correctly forwarded. If a node cannot guarantee this capability, it won't be accepted for production deployment.
	By progressively changing physical network functions (PNFs) by virtual network functions (VNFs), this task becomes harder. As the traffic traverses multiple intermediate nodes (possibly, out of the control of the VNF operator), it could eventually bypass a critical node within the SFC (e.g. a firewall). In order to mitigate this issue, a proof-of-transit technique has been developed to verify if a packet has traversed all the nodes within a path. QKD is used to provide order to the proof of transit as well as a security enhancement. Having also the continuous flow of keys provided by QKD and the speed of symmetric encryption also reduces the overhead and higher flows can be managed.

I.5.3 QKD in blockchain network

I.5.3.1 Quantum-secured blockchain

Use case ID	UC-5-3-1
Short description	It is well known that blockchain encounters severe security threat from quantum computing as its security is based on public key exchange algorithm, e.g., ECC.
	This use case describes a one quantum-safe blockchain solution based on QKD proposed by authors from RQC. The main idea is to replace the PoW based consensus mechanism with the Byzantine algorithm based one. For the new consensus mechanism, it does not need public key exchange for authentication, but it relies on QKD to realize information-theoretically secure authentication for pairwise nodes within the blockchain network. Due to the abandon of public key algorithm, it can be considered as quantum-safe blockchain.

I.5.3.2 Quantum vault for blockchain

Use case ID	UC-5-3-2
Short description	ID Quantique and its partners have proposed one quantum vault solution to utilize QKD and QRNG to enhance the security of blockchain.
	It is considered that the major pain point of blockchain technology is the secure storage of private keys. the vault is the traditional popular solution for managing blockchain private keys which is based HSM.
	Hereby the quantum vault solution utilizes QRNG to produce true random number as secret key seeds and uses Shamir key sharing algorithm to split the keys into multiple elements, and then use QKD to securely distribute the key elements to distributed distant key storage nodes.

I.5.4   QKD in TSN network

Use case ID	UC-5-4
Short description	The Time-sensitive Networking (TSN) is one widely applied communication standard developed by IEEE to meet the stringent latency and timing requirements of industrial environment.
	Ensuring cybersecurity is also an important requirement in life-critical control systems for which industrial TSN will provide communication. While private key exchange which requires manually pre-sharing keys and public key exchange which requires more computing resources are discouraged for the TSN targeted scenario, QKD can be one possible solution for TSN.

I.5.5   QKD in SCION

Use case ID	UC-5-5
Short description	Despite the fast advancement of internet-based services, the architecture and core protocol have remained mostly the same for decades since the internet's inception. However, to accommodate ever increasing and diverse data services more efficiently and securely, a new architecture is necessary, and several efforts have been made for a next-generation internet architecture.
	QKD can play an important role in a new internet architecture for enhancing the security which is one of the main the concern that today's internet is facing.
	One example use case introduced here is the QKD integration with SCION (Scalable, Control and Isolation on Next-Generation Networks) which is a research project lead by researchers at ETH Zurich. SCION aims to offer a communication infrastructure that remains highly available even in the presence of adversaries.

I.6   QKD applied in different vertical sectors

I.6.1   QKDN for smart factory

Use case ID	UC-6-1
Short description	A commercial QKD network for smart factory is being deployed in Korea. This network applied QKD to leased line between Hyundai Robotics and KT office in Daegu.
	Hyundai Robotics manufactures industrial robots, applies them to overseas industrial facilities, and remotely operates through various ICT infrastructure such as IoT device, leased line and servers. In this process, a malicious hacking threat on optical cable of leased line may cause production disruption due to confidential leaks.
	To prevent such problems, the QKD network is installed to protect corporate information and to enhance security.

I.6.2   QKDN for social safety

Use case ID	UC-6-2
Short description	A commercial QKD network for social safety is being deployed in Korea. This network applied QKD to drone communication between two adjacent local governments in Gangwon-do.
	Local governments operate drone-based surveillance system for public safety. In particular, since it is necessary to be careful about information leakage in areas adjacent to military camps, QKD networks are applied to drone communication.
	By injecting the quantum encryption key supplied from QKD into the drone, not only the drone control signal is protected, but also the video signal from the drone is encrypted and protected to improve security.

I.6.3   QKDN for medical centre

Use case ID	UC-6-3
Short description	A commercial QKD network for medical centre was deployed in Korea. This network applied QKD to leased line between St. Mary's Hospitals and their data centre in Seoul.
	In St. Mary's Hospital, a large medical institution, the central medical data server manages the medical data of branches located in various regions, and the branches share medical data such as patient information, medical records through the central medical data server. In this sharing process, there is a possibility that medical information, which is personally sensitive information, may be leaked by hacking.
	To prevent such threats, a QKD network is applied between medical data servers to encrypt medical data and improve security.

I.6.4   QKDN for secure mVoIP

Use case ID	UC-6-4
Short description	A commercial QKD network for secure mVoIP was deployed in Korea. This network applied QKD to VoIP communication between two smart phones.
	In mVoIP, there are threats of hacking such as voice terminal wiretapping, voice network wiretapping, and session hijacking attack.
	The KSA key is received from QKDN and injected into the secure communication devices. The mVoIP voice call data is encrypted through the devices.

Bibliography

[b-ETSI GR QSC 006]

TBD

Annex A

A.13 Justification for proposed draft new Supplement Y.Supp.QKDN-UC

Question:	16/13	**Proposed new ITU-T Supplement**	Geneva, 14-25 November 2022	
Reference and title:	Y.Supp.QKDN-UC – "Use cases of quantum key distribution networks"			
Base text:	Annex B		**Timing:**	Q4 2023
Editor(s):	Chang-Yui Shin, Korea University, realmine@korea.ac.kr Zhangchao Ma, CAS Quantum Network Co., Ltd., mazhangchao@qtict.com Xiaosong Yu, BUPT, xiaosongyu@bupt.edu.cn Junsen Lai, MIIT, laijunsen@caict.ac.cn		**Approval process:**	Agreement

Purpose and scope (Define what this document will address and its intent or objectives in order to indicate the limits of its applicability):

This Supplement presents use cases of quantum key distribution (QKD) networks. In particular, the scope of this Supplement includes:

- Competitive advantage brought by QKDN;
- Overview of QKDN use cases;
- Analysis of collected QKDN use cases including categorization.

Summary (provides a brief overview of the proposal):

Based on the deliverable (D2.2) of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N), this Supplement consolidates the QKDN use cases collected from the ITU-T FG QIT4N in the context of networking technologies as the mandate of ITU-T SG13.

Through a comprehensive analysis, the QKDN uses cases are classified into several classes and this Supplement highlights the competitive advantage of the use cases brought by QKDN and provides suggestions for future standardization efforts in ITU-T SG13.

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

ITU-T Recommendation Y.3800 series – Quantum key distribution networks

Liaisons with other study groups or with other standards bodies:

ITU-T SG11, SG17, ETSI ISG-QKD

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

Korea (Rep. of), KT Corp, ETRI, KAIST, Korea University, CAS Quantum Network Co., Ltd., QuantumCtek Co., Ltd. , BUPT

_____