

Supplement

ITU-T Y Suppl. 80 (11/2023)

SERIES Y: Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities

Supplements to the Y-series Recommendations

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

ITU-T Y-SERIES RECOMMENDATIONS

Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities

GLOBAL INFORMATION INFRASTRUCTURE	Y.100-Y.999
General	Y.100-Y.199
Services, applications and middleware	Y.200-Y.299
Network aspects	Y.300-Y.399
Interfaces and protocols	Y.400-Y.499
Numbering, addressing and naming	Y.500-Y.599
Operation, administration and maintenance	Y.600-Y.699
Security	Y.700-Y.799
Performances	Y.800-Y.899
INTERNET PROTOCOL ASPECTS	Y.1000-Y.1999
General	Y.1000-Y.1099
Services and applications	Y.1100-Y.1199
Architecture, access, network capabilities and resource management	Y.1200-Y.1299
Transport	Y.1300-Y.1399
Interworking	Y.1400-Y.1499
Quality of service and network performance	Y.1500-Y.1599
Signalling	Y.1600-Y.1699
Operation, administration and maintenance	Y.1700-Y.1799
Charging	Y.1800-Y.1899
IPTV over NGN	Y.1900-Y.1999
NEXT GENERATION NETWORKS	Y.2000-Y.2999
Frameworks and functional architecture models	Y.2000-Y.2099
Quality of Service and performance	Y.2100-Y.2199
Service aspects: Service capabilities and service architecture	Y.2200-Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250-Y.2299
Enhancements to NGN	Y.2300-Y.2399
Network management	Y.2400-Y.2499
Computing power networks	Y.2500-Y.2599
Packet-based Networks	Y.2600-Y.2699
Security	Y.2700-Y.2799
Generalized mobility	Y.2800-Y.2899
Carrier grade open environment	Y.2900-Y.2999
FUTURE NETWORKS	Y.3000-Y.3499
CLOUD COMPUTING	Y.3500-Y.3599
BIG DATA	Y.3600-Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800-Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	Y.4000-Y.4999
General	Y.4000-Y.4049
Definitions and terminologies	Y.4050-Y.4099
Requirements and use cases	Y.4100-Y.4249
Infrastructure, connectivity and networks	Y.4250-Y.4399
Frameworks, architectures and protocols	Y.4400-Y.4549
Services, applications, computation and data processing	Y.4550-Y.4699
Management, control and performance	Y.4700-Y.4799
Identification and security	Y.4800-Y.4899
Evaluation and assessment	Y.4900-Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Supplement 80 to ITU-T Y-series Recommendations

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

Summary

Supplement 80 to ITU-T Y-series Recommendations consolidates quantum key distribution network (QKDN) use cases 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 QKDN use cases and provides suggestions for future standardization efforts in ITU-T SG13.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T Y Suppl. 80	2023-11-03	13	11.1002/1000/15784

Keywords

QKDN, quantum key distribution networks, use cases.

* To access the Recommendation, type the URL <https://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the standards development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this publication. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2024

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

	Page
1 Scope	1
2 References.....	1
3 Definitions	1
3.1 Terms defined elsewhere	1
4 Abbreviations and acronyms	1
5 Overview	2
5.1 The competitive advantages of using QKDN.....	3
5.2 Overview of QKDN use cases.....	4
6 Use cases.....	5
6.1 UCC1: QKD combined with other cryptographic primitives.....	5
6.2 UCC2: QKD integrated with various TCP/IP protocols	11
6.3 UCC3: QKD implemented in various network topologies.....	13
6.4 UCC4: QKD with different user device categories	18
6.5 UCC5: QKD integrated in various network forms.....	22
6.6 UCC6: QKD applied in different vertical sectors	40
Appendix I – Overview of QKDN use cases	46
I.1 UCC1: QKD combined with other cryptographic primitives.....	47
I.2 UCC2: QKD integrated with various TCP/IP protocols	47
I.3 UCC3: QKD implemented in various network topologies.....	48
I.4 UCC4: QKD with different user device categories	49
I.5 UCC5: QKD integrated in various network forms.....	49
I.6 QKD applied in different vertical sectors.....	53
Bibliography.....	55

Supplement 80 to ITU-T Y-series Recommendations

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

1 Scope

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

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

2 References

[FG QIT4N D2.2] ITU-T FG QIT4N (2022), *Quantum information technology for networks use cases: Quantum key distribution network*.

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses QKDN related terms in [b-QIT4N D2.1] and the following term defined elsewhere:

3.1.1 DRKey [b-SCION]: A symmetric cryptographic keys derived on the fly by routers from a single local secret key using a pseudo-random function in SCION architecture.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard
AKA	Authentication and Key Agreement
AS	Autonomous System
CPRI	Common Public Radio Interface
DRKey	Dynamically Re-creatable Key
EAP	Extensible Authentication Protocol
ECC	Elliptic Curve Cryptography
ECP	Encryption Control Protocol
HSM	Hardware Security Module
HTTPS	Hypertext Transfer Protocol Secure
IKE	Internet Key Exchange
KDC	Key Distribution Centre
LTE	Long Term Evolution
MAC	Message Authentication Code
mVoIP	Mobile Voice over IP

NFV	Network Function Virtualization
NGFI	Next Generation Front-haul Interface
OPoT	Ordered Proof of Transit
OTN	Optical Transport Network
OTP	One-Time Pad
PFS	Perfect Forward Security
PKC	Public Key Cryptography
PPP	Point-to-Point Protocol
PRF	Pseudo Random Function
PQC	Post-Quantum Cryptography
QKD	Quantum Key Distribution
QKDN	Quantum Key Distribution Network
QRNG	Quantum Random Number Generator
QSSE	Quantum Secure Symmetrical Encryption
RSA	Rivest-Shamir-Adleman
SECOQC	Secure Communication based on Quantum Cryptography
SCION	Scalable, Control and Isolation on Next-Generation Networks
SCMP	SCION Control Message Protocol
SDN	Software-Defined Networking
SIM	Subscriber Identity Module
SMC	Secure Multi-party Computation
TLS	Transport Layer Security
TRL	Technology Readiness Level
TSN	Time-Sensitive Networking
UC	Universally Composable
UE	User Equipment

5 Overview

This Supplement identifies foreseeable, near-term use cases of quantum key distribution network (QKDN) technologies. It lists and presents descriptive information about each of the use cases – for those applications and services based on QKDN technologies.

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:

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

- support exchange information and best practices through peer learning and knowledge dissemination processes; and
- identify possible standardization requirements in the ITU-T SG13.

5.1 The competitive advantages of using QKDN

Through quantum key distribution (QKD), the two communication parties 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.

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:

- **Quantum computing resistance:** The threats posed by quantum computing have a wide range of impacts on 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 solve these mathematical problems. As studied in [b-ETSI GR QSC 006], conventional asymmetric algorithms based on Rivest-Shamir-Adleman (RSA) and elliptic curve cryptography (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.
- **Perfect forward security (PFS):** Conventional symmetric cryptography, which is widely 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 subscriber identity module (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 threats from quantum computing attacks.

- **High performance key generation:** Most Internet security applications including hypertext transfer protocol secure (HTTPS), software update, virtual private network (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 requires 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.

5.2 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 5-1.

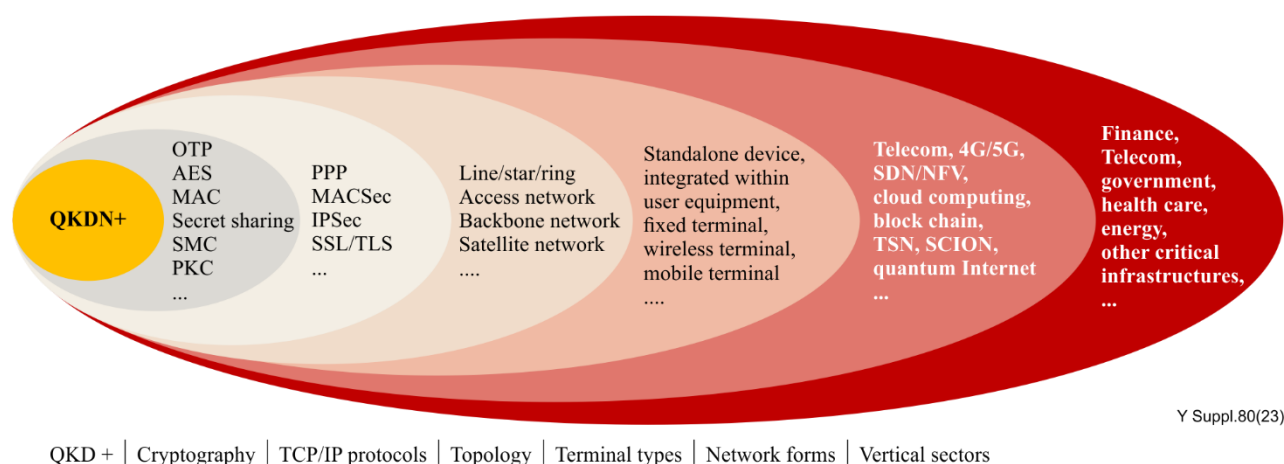


Figure 5-1 – QKDN use cases overview

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 one-time pad (OTP) or advanced encryption standard (AES) to perform symmetric encryption;
- **Message authentication:** QKD can be combined with other authentication primitives to perform message authentication functions, 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., point-to-point protocol (PPP) and MACSec protocol at MAC layer, IPSec protocol at network layer, transport layer security (TLS) protocol at transport layer.

3) UCC3: QKD implemented 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 levels, 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, time-sensitive networking (TSN), service chain and other future network evolutions, e.g., scalable, control and isolation on next-generation networks (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, healthcare, energy, telecom, critical infrastructure.

The use cases described in this Supplement provide sufficient detail on the following aspects at a level that is understandable by readers who are not experts in this specific field:

- **Use case ID:** e.g., UC-QKDN-00X.
- **Use case description:** presents a short summary, overall explanations for a use case including background, motivations, related technologies and target areas, if possible, with a diagram.
- **Problem statement:** identifies problems and/or limitations related to the use case.
- **Technical considerations:** discusses various technical issues and challenges to solve problems and/or limitations identified.
NOTE – Technology maturity: assesses the maturity of the key technical solutions required to address technical considerations above, e.g., Technology readiness level (TRL), etc.
- **Standardization considerations:** conducts gap analysis with existing standards (refer to Y.supp.QKDN-roadmap) and identifies relevant standardization items for quantum networks beyond QKDN including any suggestions for future standardization in line with the ITU-T SG13 work scope.
- **Others:**
 - 1) Benefits and impact, to describe the benefits that the use case would bring, and the impact it would have when applied.
 - 2) Application prospects, to assess the relevant application areas and potential markets, etc.

Moreover, this Supplement summarizes key findings, suggestions for further application and standardization and provides a repository of all collected use cases in Appendix I.

6 Use cases

6.1 UCC1: QKD combined with other cryptographic primitives

As QKD has the important property of being universally composable (UC) [b-Renner], it implies that QKD can be composed with other UC protocols, resulting in a composed protocol that is also UC. Some examples are listed as below:

- One-time pad (OTP) encryption is the only encryption scheme for which information-theoretic security can be proven. It is thus natural to combine it with QKD. As a consequence, when keys established by QKD are used to perform OTP encryption, the resulting protocol is an unconditionally secure message transmission protocol [b-Alléaume].
- Another frequent use case is QKD combined with a symmetric encryption scheme such as AES. This combination is the one that is currently adopted by existing commercial QKD vendors. It provides a practical solution to realize point-to-point link encryption applications with frequent key exchange.
- QKD can also be integrated with message authentication primitives, as reported in the secure communication based on quantum cryptography (SECOQC) network, which combines QKD with an efficient implementation of universal-2 hashing authentication [b-ETSI GS QKD 002].

In addition, QKD has the potential to be integrated with other cryptographic schemes to provide various security enhancement solutions, as detailed in the following use case descriptions.

6.1.1 UC-1-1: QKD combined with secret sharing

- **Use case ID:** UC-1-1.
- **Use case description**

UC-1-1 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 cryptographic means, ensure that data can be securely transported to the involved cloud providers while its integrity and confidentiality remain protected against the storage providers, other tenants of the involved storage clouds and any other non-entitled third parties.

The data is distributed among several cloud storage providers in a way that it remains available even when some cloud providers are not reachable (the minimum number of required cloud providers depends on the employed configuration).

The end user may at any time decide to exchange one cloud provider for another, without any consent or action required from the cloud provider, in a way that no exploitable information remains at the cloud provider.

- **Problem statement**

Specific data with the highest confidentiality and integrity requirements cannot be stored and archived in external public cloud services or even private cloud services without being encrypted and integrity protected. The same is also true for the data transport to and from a cloud storage. The use of encryption in a long-term storage scenario requires safeguarding of cryptographic keys for long periods of time to keep the data accessible. Furthermore, to verify that the archive can still be decrypted and the data accessed, the entire archive needs to be downloaded and decrypted.

Even if a state-of-the-art encryption primitive is used, an adversary may, sometime in the future when advanced decryption capabilities become available, be capable of accessing the plaintext.

The use of external storage providers leads to further problems; a storage provider may not be online when the data needs to be accessed, or the storage provider ceases service, or for some reason loses the data. Further problems may arise with public storage providers; the extraction of all stored data from one storage provider and the secure (i.e., complete) deletion of data when moving from one provider to another "vendor lock-in".

– **Technical considerations**

The solution is to use a cloud archive with advanced privacy and security guarantees, based on a secret sharing primitive, and secure the data links to the single storage providers with QKD links.

The secret sharing cryptographic primitive (e.g., Shamir secret sharing) allows the data to be split into multiple shares which are given to different storage providers. The secret sharing primitive has the advantage that one single share does not contain exploitable information on the original data. A minimum number of shares, the threshold, is required to access the information. The threshold (e.g., 3 out of 5 shares) can be arbitrarily selected by the data owner. Together with QKD secured transport links, such a system yields a keyless cryptographic solution with highest security and availability guarantees. Furthermore, specific protocols can remotely verify that the single storage providers have intact shares and thus the integrity of the stored data can be verified without having to download all shares and recombine them.

In a long-term scenario, single shares can be invalidated and be replaced with new shares, potentially at another cloud provider, thus solving the 'vendor lock-in' and secure deletion issues.

The use case counters some of the most severe threats in current cloud solutions and provides a distributed cloud archive with advanced data availability as well as provable long-term confidentiality and integrity guarantees.

End users receive a distributed storage solution with highest confidentiality, integrity and availability guarantees. End users may select the parameters of the secret sharing scheme (i.e., the number of shares and the threshold) as well as the storage location of the shares in private and/or public clouds according to their particular security requirements and the assumed threat level.

The secure cloud archive tolerates the loss of single shares (availability) and enables effective revocation and deletion of shares from storage providers.

Note on the security statement: The secret sharing primitive exhibits perfect secrecy, i.e., the observation of a number of shares less than the selected threshold provides exact zero information about the plaintext. Nevertheless, the security can only be guaranteed under the assumption that no number of storage providers greater or equal to the threshold collude against the end users – so that an attacker may get into the possession of enough shares to reconstruct the data (non-collusion assumption). That particular risk can be reduced if less shares than the threshold are stored in public clouds with the remaining shares being stored in private clouds of the end user.

– **Standardization considerations**

The potential standardization areas may include the integration method, the performance and security requirements and metrics to evaluate the effectiveness of QKD and secret sharing combinations.

– **Others**

– **Benefits and impact**

The use case counters some of the most severe threats in current cloud solutions and provides a distributed cloud archive with advanced data availability as well as provable long-term confidentiality and integrity guarantees. End users receive a distributed storage solution with highest confidentiality, integrity and availability guarantees. End users may select the parameters of the secret sharing scheme (i.e. the number of shares and the threshold) as well as the storage location of the shares in private and/or public clouds according to their particular security requirements and the assumed threat level.

– **Application prospects**

Individuals and organizations looking for an improved storage solution in the cloud with advanced security and privacy guarantees.

6.1.2 UC-1-2: QKD combined with secure multiparty computation (SMC)

– Use case ID: UC-1-2

– Use case description

UC-1-2 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.

For the sake of simplicity, only two entities, **A** and **B**, which are in possession of two private sequences, x_A and x_B are considered. **A** and **B** want to perform a composite signal analysis using x_A and x_B over a public database, such as a protein or genome DNA sequence database, **P**. A possible situation where the service is useful is the following: **A** and **B** want to know if both sequence x_A and x_B appear in the public sequence **P** within a certain distance but they do not want to reveal their own sequences (x_A and x_B). For this purpose, **A** and **B** need to evaluate a function to perform this analysis, but this function will operate with encrypted inputs, \tilde{x}_A and \tilde{x}_B and generate encrypted outputs, \tilde{y}_A and \tilde{y}_B . Both entities will be equipped with an encoder/decoder able to generate, \tilde{x}_A from x_A and y_A from \tilde{y}_A , respectively, and the same for entity **B**, see Figure 6-1.

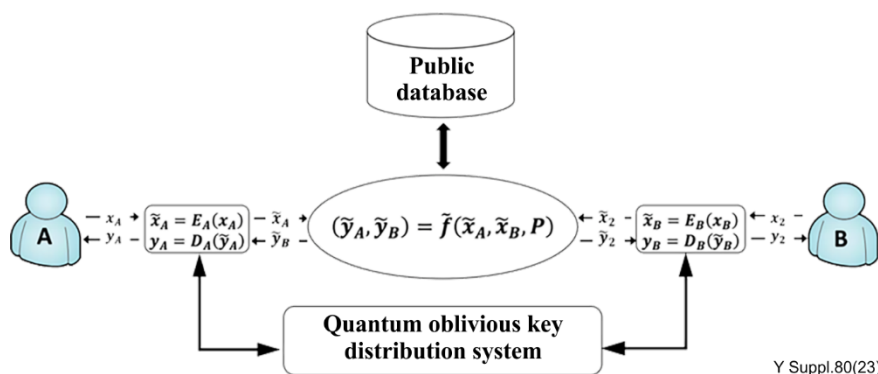


Figure 6-1 – Schema of the use case quantum enabled private recognition of composite signals

– Problem statement

Genomic information in clinical practice is gaining traction since it makes genomic medicine possible. For this new sort of medicine, genome sequence alignment is a crucial tool in the study of new diseases, viruses and drug development as well as for the development of predictive and personalized medicine. However, the process of genome sequencing and signal identification in proteins and DNA is resource-intensive, both in terms of time and capital. These signals must be validated against noise. This poses a very significant problem in the field since most of them are considerably complex because they have multiple components where each component is found by different companies/researchers. On top of that, each player in the healthcare system and drug industry collects data typically stored in private databases. Due to privacy preserving laws and commercial reasons, these databases cannot be disclosed. Indeed, the amount and wealth of information stored in a database of a certain company greatly defines how competitive it can be in terms of developing new drugs for new diseases within a useful time.

– Technical considerations

The proposed service allows different competitors to share information without compromising privacy or their own profits. It is based on a garbled circuit secure multiparty computation protocol. The key element of the secure multiparty computation service is the oblivious transfer protocol. The oblivious transfer protocol is implemented based on quantum generated oblivious keys. Oblivious keys are cryptographic keys in which the parties only share half of the keys. These keys are generated in a procedure similar to the generation of symmetric cryptographic keys in such a way

that, for each measurement, a commitment is performed and during basis reconciliation and error correction there is no leak to the other party about the half of the key that should be maintained oblivious. The commitments are based on classical hash functions which are assumed to be practically secure even against a quantum computer attack.

The service is a proof of concept with two competitors, **A** and **B**. Both entities have access to the raw keys of a QKD system and possess a potential component of a composite signal. With the service, the two entities can cooperate to validate their findings without leaking any sensitive information. Indeed, it allows a joint private pattern recognition of the union of their signals on public genome or protein data without revealing the content of their private patterns. This quantum enabled privacy-preserving system is going to be tested in the Madrid quantum network.

In this field trial, quantum systems from different providers are planned to be included to show that the present maturity of quantum technologies can leverage the surge of new services to end users very soon.

– **Standardization considerations**

It is important to ensure efficient management of keys between QKD and SMC. The potential standardization areas may include standards for key storage, distribution, updates, etc.

– **Others**

– **Benefits and impact**

The advantages in terms of security of quantum-based solutions rely on the fact that classical oblivious transfer solutions require some sort of public-key distribution-like scheme, usually based on the discrete logarithm problem. Thus, classical based implementations rely on the assumption that the receiver has limited computational power and is not able to compute the discrete logarithm of a random number in a useful time. It is usually believed that this is true if the attacker is restricted to the use of classical computers and large enough prime numbers are used. However, it is also known that this is not true anymore if the attacker has access to a quantum computer. Indeed, in 1995, Peter Shor published a quantum algorithm that can solve both prime factorization and discrete logarithm problems in polynomial-time. Researchers have been addressing this vulnerability following two different paths:

- 1) development of new classical public-key distribution protocols resistant to Shor's algorithm, this is known as post-quantum cryptography; and
- 2) development of protocols that make use of quantum technology.

– **Application prospects**

Health care systems and pharmaceutical industry.

6.1.3 UC-1-3: Hybrid QKD and PQC for encrypted communications

– **Use case ID:** UC-1-3.

– **Use case description**

Quantum-safe cryptography is urgently needed to protect systems with high security requirements. Even though quantum computers are not available today, data can always be saved and decrypted later by quantum computers. A practical hybrid scheme with various quantum-safe technologies for encrypted communications between data centres has been demonstrated on Alibaba's platform [b-Leilei] to enhance data transfer security.

– **Problem statement**

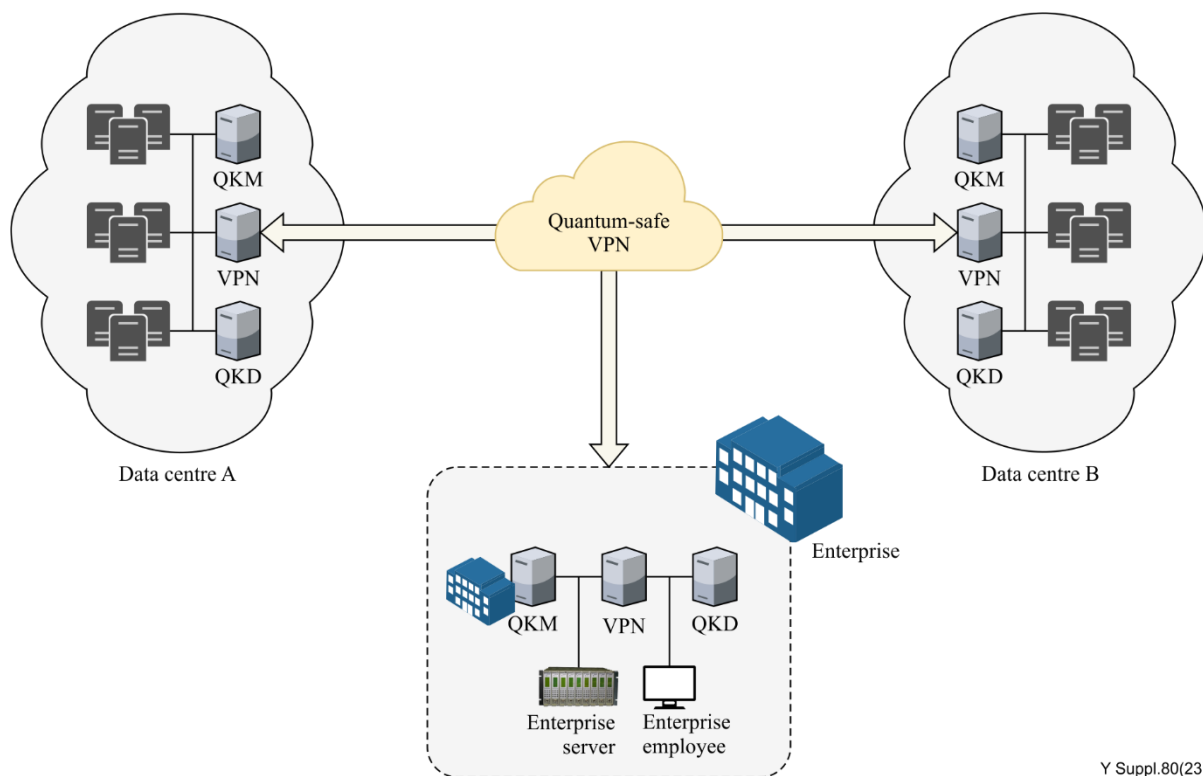
Both QKD and PQC present opportunities and obstacles. QKD can provide provably-random keys and information theoretic secure distribution of those keys. However, to deploy QKD systems in

real networks 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.

– Technical considerations

Quantum random number generators (QRNGs), QKD, post-quantum and classical cryptography algorithms are integrated in the hybrid quantum-safe scheme to enhance data transfer security. Compared to quantum cryptography and PQC solutions, the proposed triple-level security cryptographic scheme provides a layered cryptographic solution for different applications and is compatible with existing solutions, a practical implementation is illustrated in Figure 6-2.



Y Suppl.80(23)

Figure 6-2 – Practical implementation of triple-level hybrid quantum-safe scheme (classical cryptography + post quantum algorithms + QKDs)

– Standardization considerations

In a hybrid QKD and PQC scheme, the combination method of different algorithms and protocols needs to be further studied and certain specifications are required to ensure the effectiveness, efficiency and security of the hybrid quantum-safe solution.

– Others

– Benefits and impact

The hybrid quantum-safe scheme described in this use case provides a layered cryptographic solution for different applications which enhances data transfer security and is compatible with existing solutions.

– Application prospects

QKDN and PQC service providers and users.

6.2 UCC2: QKD integrated with various TCP/IP protocols

As similar to the other key exchanging algorithms in cryptography, QKD can also be applied to the data link layer, network layer, transport layer, and application layer of the TCP/IP protocol stack, which is commonly used in ICT systems, as shown in Figure 6-3.

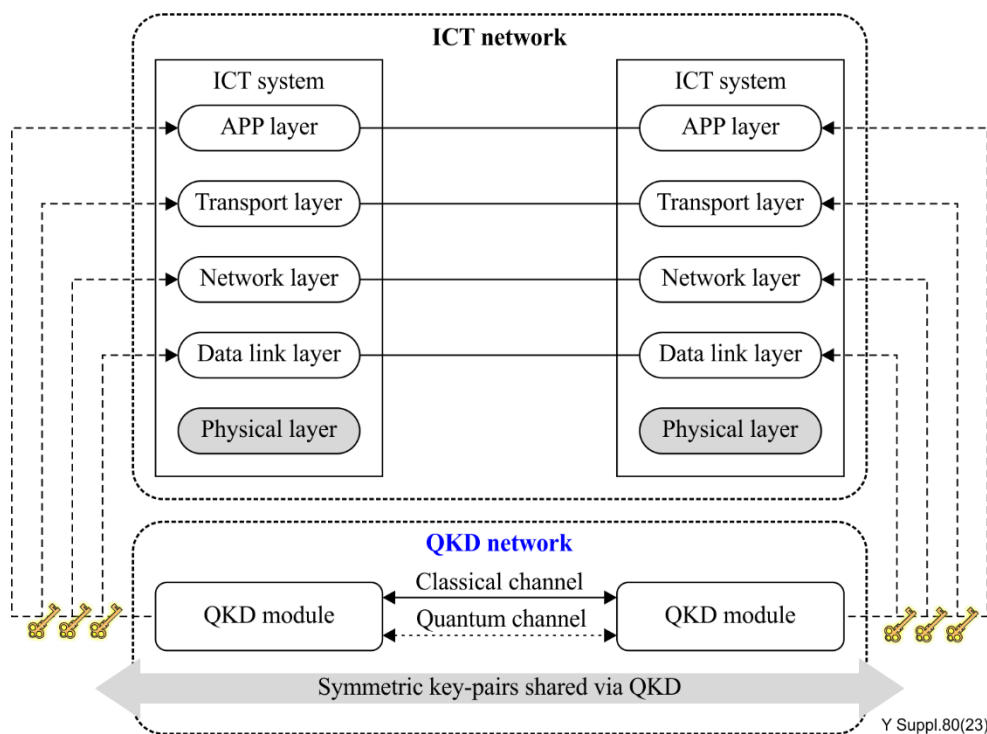


Figure 6-3 – QKDN integrated with TCP/IP protocol stack

6.2.1 UC-2-1: QKD integrated in data link layer

- **Use case ID:** UC-2-1.
- **Use case description**

On the data link layer, QKD may be used as a part of the point-to-point protocol (PPP) which is a layer 2 protocol widely used to connect two sets of nodes in a network. The encryption functionality in PPP is the encryption control protocol (ECP) [b-IETF 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 which provides a connectionless service that supports data confidentiality, integrity and authenticity for authorized systems attaching to a local area network (LAN) or interconnecting LANs.

As QKD is presently mainly implemented as a 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. A link encryptor is a network-transparent cryptographic system. A QKD link encryptor is a quantum cryptography appliance for point-to-point link encryption which may also be referred to as virtual private network (VPN) tunnel. The link encryptor usually uses the keys supplied by QKD as keys for a symmetrical block cipher (e.g., AES) or stream cipher (OTP for highest security) and can be used, for example, to encrypt traffic on an Ethernet or fibre channel links. The QKD link encryptor may be used to support communications between two adjacent network nodes employing QKD or it may provide protection for communications end-to-end across a network of nodes as a VPN tunnel. Key management is integrated in the link encryptor. For example, this solution may securely bridge two Fast Ethernet networks.

– **Standardization considerations**

Potential standardization area may include how to improve the current key management protocol to integrate QKDN for the data link layer protocols for efficient use and protection of keys.

6.2.2 UC-2-2: QKD integrated in network layer

– **Use case ID:** UC-2-2.

– **Use case description**

Internet protocol security (IPsec) is a layer 3 protocol suite for securing Internet protocol (IP) communications by authenticating and encrypting the IP packets of a data stream.

Internet key exchange (IKE or IKEv2) is the protocol used to set up a security association in the IPsec protocol suite. IKE uses a Diffie-Hellman public key exchange to set up a shared session secret, from which cryptographic keys are derived. Public key techniques or, alternatively, a pre-shared key, are used to mutually authenticate the communicating parties.

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 OTP payload encryption in a high security context.

– **Standardization considerations**

Potential standardization area may include how to improve the current key management protocol to integrate QKDN into the network layer protocols for efficient use and protection of keys.

6.2.3 UC-2-3: QKD integrated in transport layer

– **Use case ID:** UC-2-3.

– **Use case description**

Transport layer security (TLS) and its predecessor secure sockets layer (SSL) are layer 4 protocols which provide an 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 OTP 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.

– **Standardization considerations**

Potential standardization areas may include how to improve the key management protocol to integrate QKDN into the transport layer protocols for efficient use and protection of keys.

6.2.4 UC-2-4: QKD integrated in application layer

– **Use case ID:** UC-2-4.

– **Use case 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.

– **Standardization considerations**

Potential standardization areas may include how to improve the key management protocol to integrate QKDN into the application layer protocols for efficient use and protection of keys.

6.3 UCC3: QKD implemented in various network topologies

6.3.1 UC-3-1: QKDN as metropolitan access network

- Use case ID: UC-3-1.
- Use case description

This use case describes a general-purpose high security communications network between several branches and offices within an area of about 100 km in diameter (metropolitan area). The single network nodes are interconnected with dedicated optical point to point links for classical digital communication and QKD. The network uses a dedicated optical infrastructure which is completely separated from the Internet. Figure 6-4 shows a high security metropolitan area network topology.

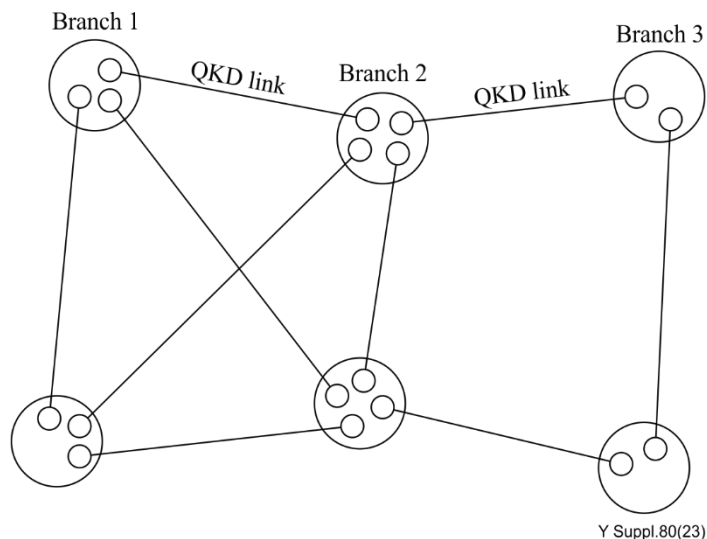


Figure 6-4 – High security metropolitan area network topology

QKD systems are used to generate symmetrical secrets in nodes connected by optical links. The secrets are used as cryptographic keys for authentication and encryption primitives with security levels fitting the purpose they are intended for. Provably secure OTP can be used for communications with the strictest long term security requirements, while other algorithms, including PQC algorithms can also be used. To increase network connectivity (between links without direct connection), and availability and/or bandwidth, a trusted repeater network solution can also be considered.

– Problem statement

Governments and other organizations with the highest communications security requirements are currently relying on communication networks which either use dedicated network infrastructures or are layered upon the Internet. In both cases, cryptography is used with an uncertain prospect with regards to current and especially long-term security.

Current cryptographic protocols and paradigms have already been subject to severe (mostly insider) attacks. Examples of such attacks include compromised random number generators making brute forcing TLS keys a trivial task, compromised root certificates for trust validation, etc. Some algorithms for securing governments' communications have later turned out to have contained deliberately introduced weaknesses; even AES is suspected to be susceptible to timing side channel attacks. Furthermore, in most jurisdictions, commercial-off-the-shelf (COTS) telecom and network hardware, e.g., network switches are required by legislation to include access mechanisms for law enforcement which have already been exploited by rogue actors.

With regards to long term security, the prospects are even worse: secrets that need to remain secure for several decades may be revealed some time in the future when advanced decryption capabilities including quantum computers become available.

– **Technical considerations**

The solution would be to use a communications network with advanced security guarantees on a dedicated optical infrastructure that is completely separated from the Internet. The advanced security is provided by QKD links delivering a continuous stream of symmetrical secrets used to authenticate and secure the communication between adjacent nodes of the network.

To increase network availability and/or bandwidth, a trusted repeater network solution may also be considered.

– **Standardization considerations**

From the perspective of future networks and emerging network technologies, it may be necessary to specify how to integrate QKD and telecom access networks, including network architecture, technical requirements, etc.

– **Others**

– **Benefits and impact**

End users can rely on the security of proper network infrastructures which produce cryptographic secrets with the high security standards of QKD.

End users can select the cryptographic security for their communication and authentication primitives according to their needs. For most sensitive communications, with the strictest long-term confidentiality requirements, encryption primitives with perfect secrecy (e.g., OTP encryption or Shamir-secret-sharing) may be used and, for communications with ephemeral confidentiality requirements, symmetric ciphers with computational security may be used.

The advantage in comparison to alternative solutions not involving QKDNs is that QKD offers key distribution with stronger security guarantees than other non-quantum key distribution primitives. The use of dedicated infrastructure not (directly) connected to the Internet ensures a relatively smaller attack surface towards attackers from the outside.

– **Application prospects**

Administrations, corporations and other organizations with branches in a metropolitan area looking for a high security communications network solution.

6.3.2 UC-3-2: QKDN as inter-city backbone network

– **Use case ID: UC-3-2.**

– **Use case description**

The backbone network consists of 32 physical nodes linearly connected by QKD links – the Beijing, Jinan, Fuli, Hefei, Nanjing and Shanghai nodes are the access points while the others are trusted repeater nodes. The backbone network has 135 links in total and two to eight multiple QKD links lie between adjacent nodes. The network rents dark fibres are deployed by China Cable Television Network Co., Ltd. and, to conserve fibre resources, the network uses quantum wavelength division multiplexing technology which combines four quantum channels into a single fibre. The distance between adjacent nodes along the backbone line varies between 34 km and 89 km with fibre loss varying from 10.3 dB to 20.5 dB.

The backbone network deploys QKD devices which implement decoy state BB84 protocol. Some of the devices integrate the up-conversion single photon detection technique and thereby achieve a 25% single photon detection rate.

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, Jinan and Hefei. A wide area QKD network thus has been formed and provides end users including banks, government agencies and large enterprises with versatile security services, such as video call, audio call, fax, text transmission and file transmission. The network is also scalable such that extra users can be easily added.

– **Standardization considerations**

For the scenario of a telecom backbone network, the question of how to integrate the QKDN with OTN for security enhancement still needs further standardization study, which may include technologies for transport layer, key management layer and application layer enhancements.

– **Others**

– **Application prospects**

QKD network operators directly provide QKD services to customers.

6.3.3 UC-3-3: QKDN as free-space satellite-ground or inter-satellite network

– **Use case ID:** UC-3-3.

– **Use case description**

UC-3-3 describes a high security general-purpose long-haul network based on multi-layer satellites around the world. By using satellites as relays, long-distance QKD can be realized within global metropolises.

As shown in Figure 6-5, general-purpose long-haul network based on multi-layer satellites consists of three layers of geostationary earth orbit (GEO) satellite, medium earth orbit (MEO) satellite and low earth orbit (LEO) satellite. The multi-layer satellite in orbit provides the physical basis for the application of a general-purpose long-haul network.

The general-purpose long-haul network based on multi-layer satellites can cover the whole world through satellite communication with flexible user access. It is suitable for remote areas with high costs of laying optical fibre to realize quantum key distribution. At the same time, it can solve the problem of difficult access for mobile users, such as marine mobile equipment, polar research stations, desert detection stations, etc.

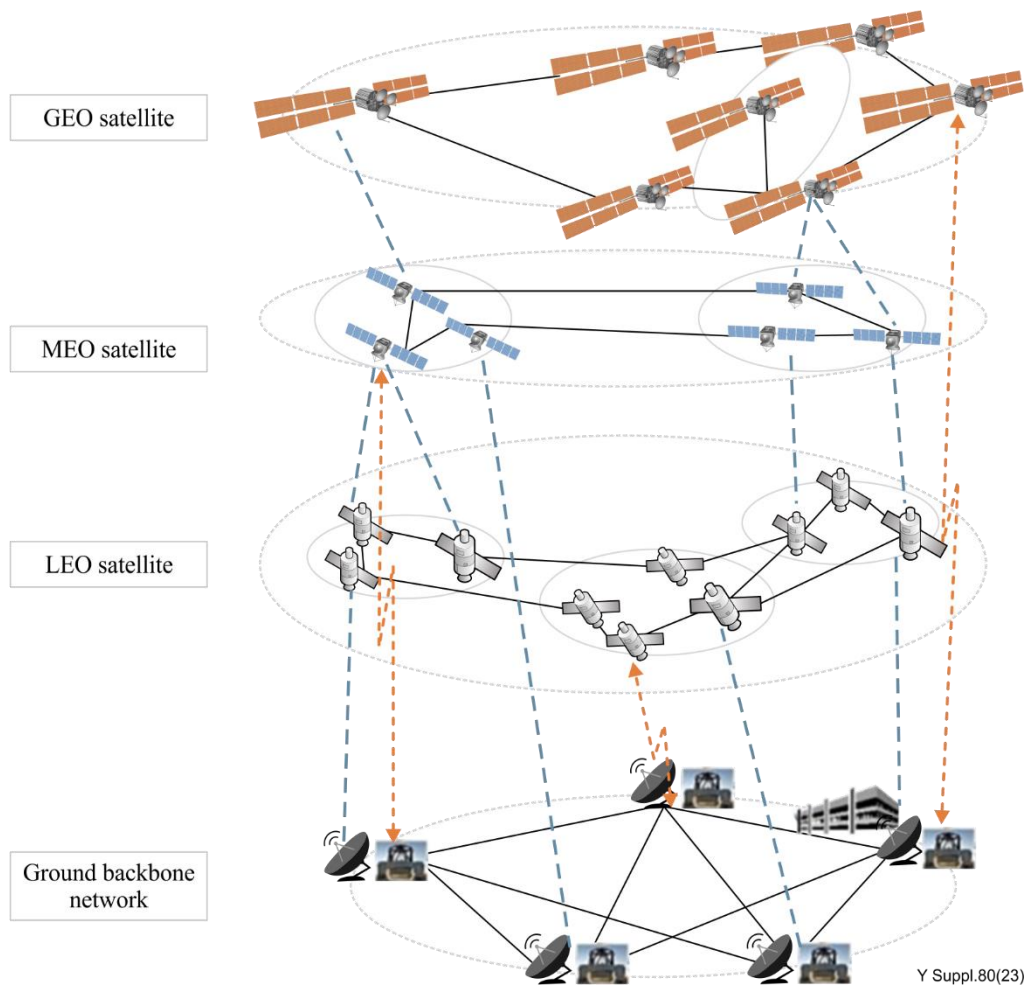


Figure 6-5 – Architecture of general-purpose long-haul network based on multi-layer satellites

Simpler satellite-based QKD networks, e.g., single layer satellite based QKDNs, may be less robust and produce less QKD keys but might still be adequate for some commercial and lower security applications.

– **Problem statement**

With the popularity of global services, the requirements for the confidentiality of information transmission are becoming higher and higher. At present, it is difficult for governments and other commercial organizations to achieve end-to-end QKD worldwide only through ground base stations.

Presently, space network attack risks are increasing, and an effective encryption method is urgently needed to ensure the communication security of the satellite network.

Due to the physical distance limitation of QKD, satellites are needed to realize end-to-end QKD globally.

– **Technical considerations**

The architecture of the general-purpose long-haul network based on multi-layer satellites (as shown in Figure 6-5) consists of three layers of GEO, MEO and LEO satellites. The global QKDN architecture based on a multi-layer satellite network is established, the centralized and distributed intelligent control mechanisms are designed and the nodes are interconnected through inter-satellite links and star-ground links.

The Micius satellite has proved the feasibility of the downlink and the performance of the uplink is constantly improving with the progress of technology. The available communication time between the ground base station and the satellite within the coverage of a single quantum satellite is about six minutes and multiple satellites in each layer of orbit can meet growing business needs. Each GEO satellite (QKDN control and management node) is responsible for key management and distribution of its respective coverage areas while the LEO and MEO satellites are QKDN transmitter and receiver terminals. The ground control node is responsible for key unified management and distribution in the whole general-purpose long-haul network, including both the satellite and ground networks.

There is a quantum key transceiver and laser devices on the satellite. As a QKD relay, it can complete the end-to-end QKD of intercontinental distances through laser communication. Through a three-layer satellite-based QKD network, it can complete multi-hop relays including satellite-to-satellite and satellite-to-ground QKD thereby achieving global end-to-end QKD.

Simpler, trusted node satellite networks can also provide global coverage if QKD links and key management is combined into LEO satellites. For example, LEO satellites can perform QKD with any ground station they pass over to generate and store private symmetric keys between that satellite and the ground station in their internal key manager. Each satellite maintains a continuous classical radio link with the ground network using only radio relay nodes in higher orbits, e.g., in geostationary orbit. When any two users on the ground (e.g., ground station A and B), need to communicate securely the network is queried for satellites that have keys stored with A and B on-board a secure key management module. Any such keys are combined using an XOR function and can be broadcast to A and B via the relay satellites with minimal latency. Station A and B can perform a reverse XOR operation to extract the key held by the other ground station and can then communicate securely. The used key for A and B is deleted from the satellites. Inter-satellite QKD links are optional in this configuration but can be used to re-distribute the key across the constellation [b-Vergoossen].

– **Standardization considerations**

A systematic standardization study is required for how to integrate QKDN into satellite networks, which should include architectural impact, technical requirements for both satellites and terrestrial stations, protocols, performance and security requirements.

– **Others**

– **Benefits and impact**

The advantages for end users, specifically the security gains include:

- General-purpose long-haul network based on multi-layer satellites that can counter space satellite network attacks and improve the defence performance of space networks.
- General-purpose long-haul network based on multi-layer satellites uses satellites as relays which can achieve end-to-end QKD between two cities worldwide and greatly enhance timeliness.
- A high security communication network can be obtained in the field of information security such as finance worldwide.
- General-purpose long-haul network based on multi-layer satellites provides wider and denser coverage and makes it easier for mobile and remote user terminals to use quantum encryption services.
- When the satellite acts as a relay, the key is XOR processed and the transport of the key from the end user to others is secured with perfect secrecy of the OTP encryption.

- The use of dedicated infrastructure (such as laser communication devices), not (directly) connected to the Internet ensures a relatively smaller attack surface towards attackers from the outside.

– Application prospects

Governments and organizations, especially end users who cannot connect to optical fibres (such as the Arctic Research Station) and those with strong mobility (such as naval ships), looking for a high security network solution for connecting different metropolises worldwide.

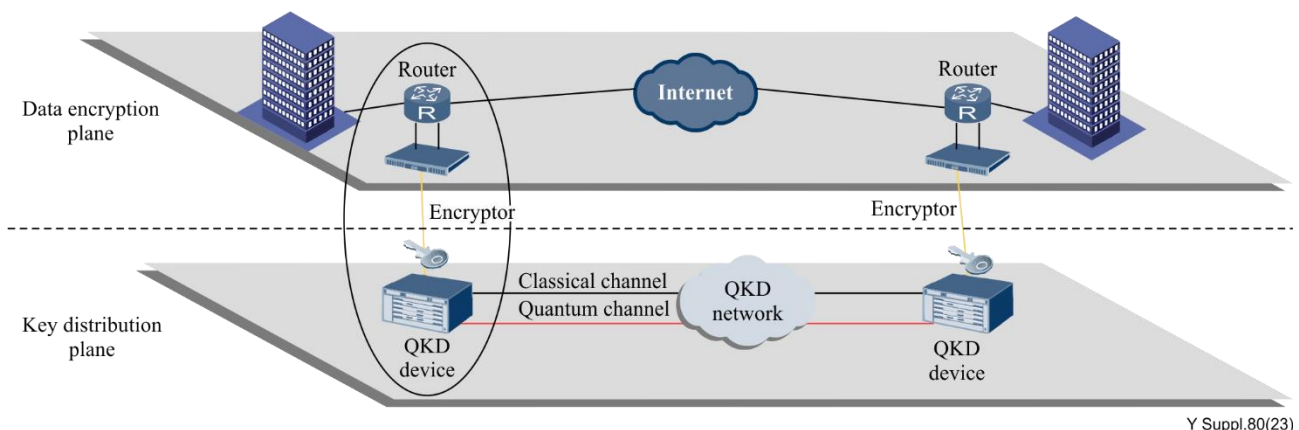
Commercial organizations whose sites are not connected to existing quantum networks or who do not trust their local quantum networks.

Network operators connecting separate quantum networks together.

6.4 UCC4: QKD with different user device categories

From a QKD end user's perspective, there are various use cases according to the different types of user devices consuming the keys provided by QKDN. The possible use cases include:

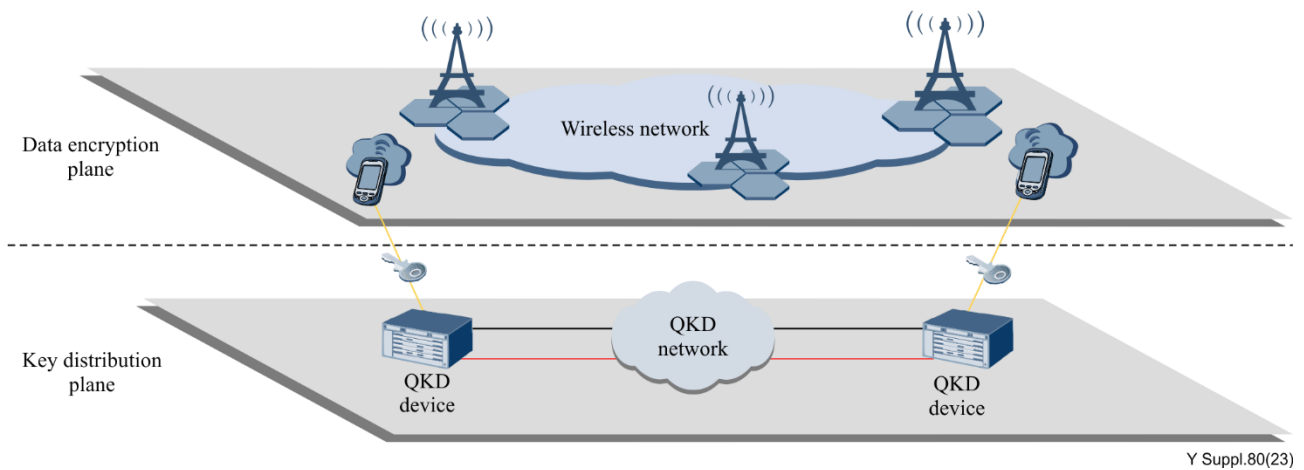
- **Fixed user device with standalone QKD module:** As current commercial QKD devices are typically bulky and require a fibre connection, the user devices placed at a user's office such as the router, the encryptor and the QKD devices are usually separate devices as shown in Figure 6-6. The encryptor connects to the QKD device with a physical connection to fetch keys and then encrypts or decrypts the data traffic passed in the router.



Y Suppl.80(23)

Figure 6-6 – QKD used via fixed user device with standalone QKD module

- **Fixed user device with integrated QKD module:** As the QKD module integration level grows, the functionality of QKD can be integrated into a router or encryptor device physically as a chipset or a peripheral component interconnect (PCI) card.
- **Wireless user device which consumes offline keys provided by QKDN:** For a wireless user device without a fibre connection to the QKDN, it can store the keys provided by QKDN into the secure storage within itself and then consume the keys for secure data communication as shown in Figure 6-7. The detailed use case description is provided in UC-4-1.



Y Suppl.80(23)

Figure 6-7 – QKD used via wireless user device with offline QKD-keys

- **Wireless user device which integrates a QKD module to consume online keys provided by QKDN:** As wireless and mobile QKD technology is developing, it is also possible to integrate a QKD module into wireless devices and perform QKD directly via wireless channels. More details on this use case are provided in UC-4-2.

6.4.1 UC-4-1: Wireless user device with offline QKD-keys

- **Use case ID:** UC-4-1.
- **Use case description**

In UC-4-1, the proposed solution is to pre-install the QKD-key pool into the mobile user and network side to enhance the security of mobile communication which is achievable with existing QKD techniques.

- **Problem statement**

The extension of QKD services to mobile terminals is envisioned to be of 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.

- **Technical considerations**

As shown in Figure 6-8, the Q-key update terminal is introduced to cache the QKD-key pool and implant the QKD-keys to mobile user equipment (which contain certain secure storage to store the keys). The key distribution centre (KDC) at the QKDN side is introduced to store the symmetric key pools and perform key management. The mobile terminals embedded with the QKD-key pool can consume the keys provided by QKDN to perform secure communication and recharge QKD-keys from the QKDN once exhausted.

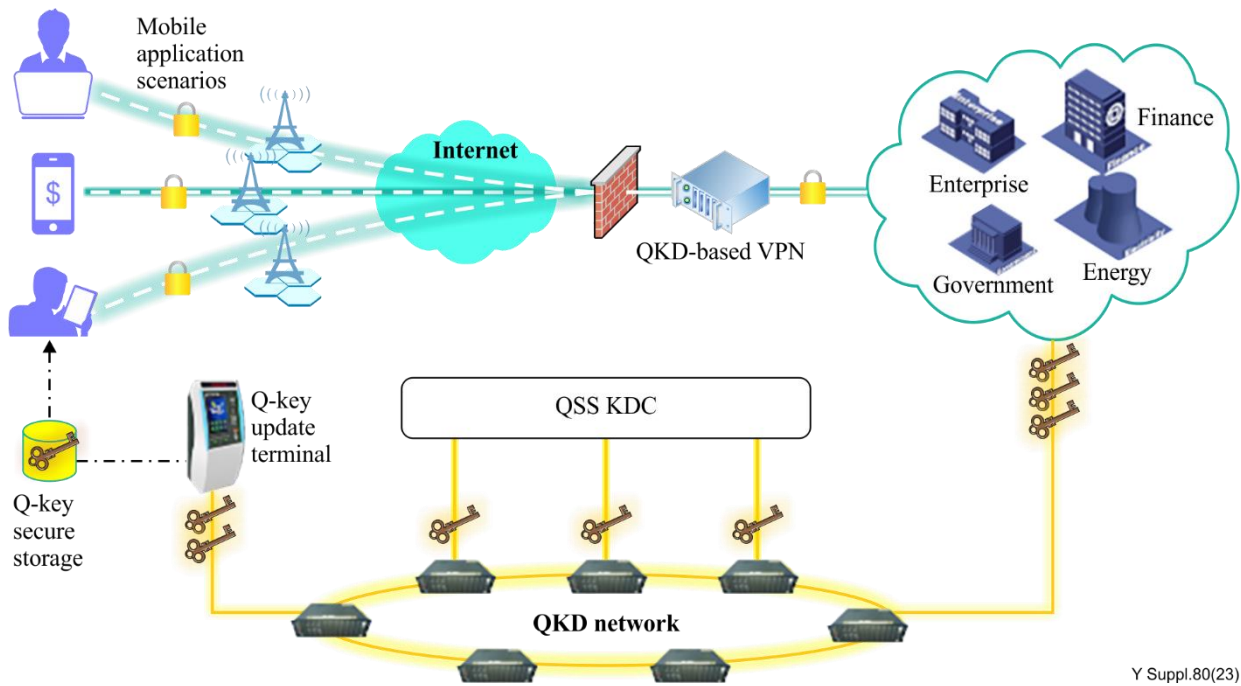


Figure 6-8 – QKD-key embedded secure mobile communication

As shown in Figure 6-9 and Table 6-1, the enhanced QKDN solution can be summarized in four steps:

- 1) First, PQC-based certificates are pre-installed in the user terminals for initial authentication.
- 2) The user terminals and the KDC can then obtain the QKD-key pool from the QKD network.
- 3) After that, the terminals with a QKD-pool storage can use symmetric QKD-keys for authentication with the KDC.
- 4) Then, the KDC can help negotiate peer-to-peer session keys for terminals A and B. With the session key generated, the terminals can perform secure communication consuming the QKD-keys in one-time manner. After the QKD-key pool is exhausted, the terminals can get updated via the Q-key update terminal from QKDN again.

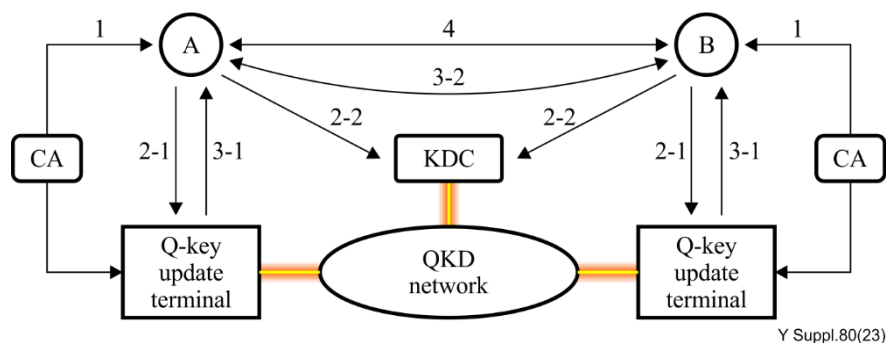


Figure 6-9 – QKD-key embedded secure mobile communication solution

Table 6-1 – QKD-key embedded secure mobile communication steps

	QKD enhanced with PQC and KDC	Vs. KDC	Vs. PKI
① Root key Pre-share	Pre-distribute PQC certificates to QKD node and terminal secure storage	Easy management	
② Identity Authentication	2-1: Use PQC certificates for QKD node and terminal initial authentication 2-2: Use symmetric Q-keys for authentication in following sessions		Q-safe
③ Session key agreement	3-1: Use QKD network to produce and distribute temporary session keys via OTP; and then Store t-session-key-pool to terminal and KDC 3-2: Use KDC to negotiate real-time session key	Forward security	Q-safe; Fast
④ Encrypted comm.	Use symmetric session key for AES encrypt/decrypt		

– **Standardization considerations**

Further standardization study is required for this solution, which may include the new key management solutions to enable QKD-keys can be used with offline mobile user devices. This will include the standardization of key generation algorithms, key storage mechanisms, and key update policies for mobile end users consuming QKD-keys.

– **Others**

– **Benefits and impact**

From an application perspective, this solution can support the extension of the QKD service to the vast mobile communication scenarios based on existing QKD techniques. Moreover, from a security perspective, this solution can provide the forward security feature for session keys compared to the KDC based scheme. It can also provide quantum-computing resistance feature compared to the traditional PKI-based scheme.

– **Application prospects**

UC-4-1 can be applied to many vertical sector scenarios, e.g., mobile working, mobile payment, industry Internet of things.

6.4.2 UC-4-2: Wireless user device with integrated QKD module

– **Use case ID: UC-4-2.**

– **Use case description**

As the QKD module can be miniaturized into chip-scale, it is possible for it to be integrated into mobile devices to perform wireless QKD service. As shown in Figure 6-10, the University of Bristol in the United Kingdom has successfully demonstrated the QKD chip transmitter integrated on the credit card, and the QKD receiver in the ATM rack to achieve free-space QKD.

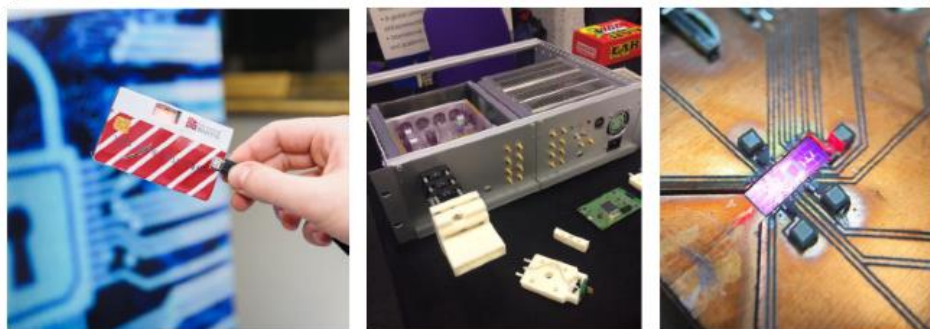


Figure 6-10 – Demo of QKD integrated credit card

Standardization considerations

The wireless QKD technology is still under development at laboratory stage. As a new paradigm for QKD usage beyond fibre-based connection, it will cause a series of standardization impacts from the physical components, networking technology and application methods from a standardization perspective.

6.5 UCC5: QKD integrated in various network forms

6.5.1 UC-5-1: QKD in 4G/5G networks

(1) UC-5-1-1: QKDN for LTE backhaul and 5G backbone

Use case ID: UC-5-1-1.

Use case description

The first commercial QKD network in Korea (Rep. of) was deployed in June 2016. This network applied QKD to LTE backhaul between Sejong central office and one of SK telecom's DU sites at Daejeon.

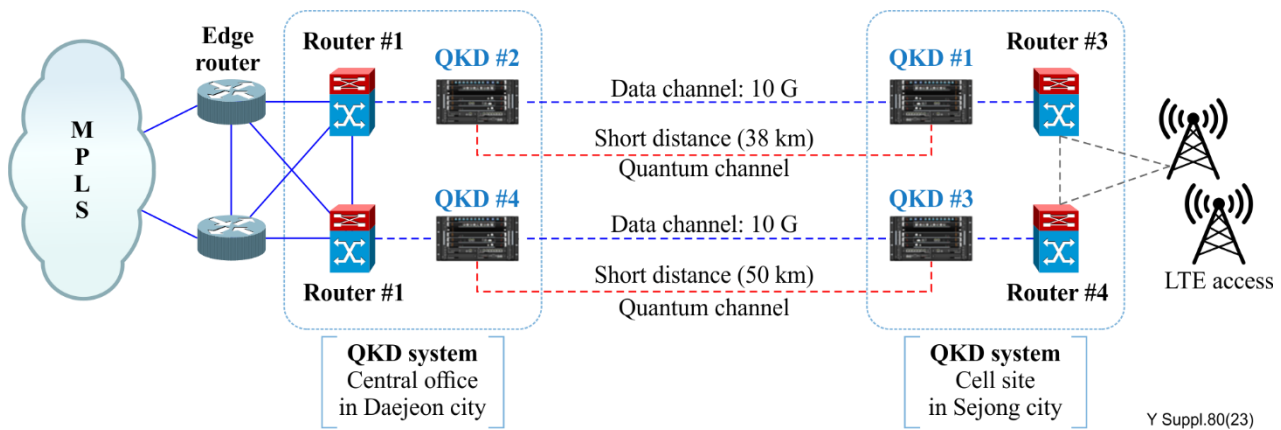


Figure 6-11 – QKD network deployment in LTE backhaul in Korea

In 2017, a trusted relay node was implemented for long distance QKDN and in 2019, the implementation and commercialization of QKD quantum cryptography for a total of 221 km of transmission line between Sungsu central office (Seoul area) and Dunsan central office (Daejeon area) of SK Telecom was accomplished. It was extended to the Taepyung central office in 2020 and this is an end-to-end distance of 380 km. Other main cities are targeted to be reached with QKD step by step. Figure 6-12 shows a long distance QKD network deployment in LTE and 5G backbone in Korea.

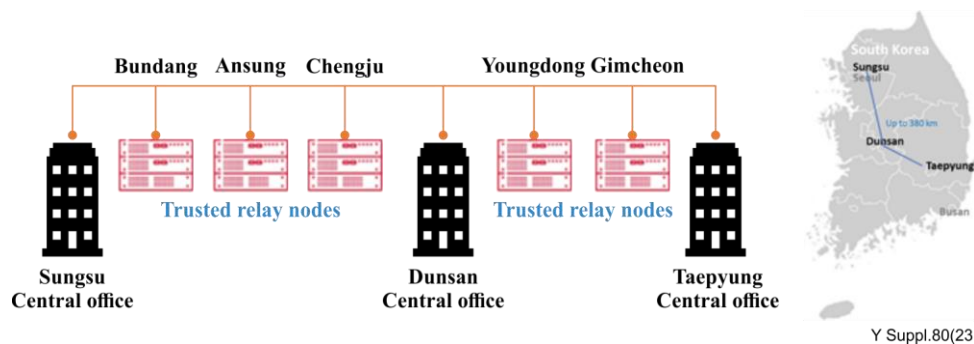


Figure 6-12 – Long distance QKD network deployment in LTE and 5G backbone in Korea¹

– **Problem statement**

As applications in Internet of things (smart cities, factories), vehicles and healthcare are expected to use 5G networks, the 5G network requires the highest level of security available when being designed and deployed. At present, SK Telecom's 5G/LTE backbone network between Sungsu through Daejeon to Taepyung takes charge of about 30% of SK Telecom's total data traffic. This data is protected using current cryptography which is expected to be vulnerable to quantum threats in the near future. So, it is critical for telecom operators to secure data traffic over their 5G/LTE backbone networks with QKD.

– **Technical considerations**

When deploying QKD over the 5G/LTE backbone network between Sungsu through Daejeon to Taepyung, trusted nodes have been deployed to extend the reach of the key exchange used by the encryptors at both ends and they are positioned in highly secure locations at SK Telecom's premises.

– **Standardization considerations**

The 5G networks and its evolutions will require a stronger security level. How to integrate QKDN with 5G backbone networks may need standardization efforts to ensure the efficient interoperability between QKDN and 5G backbone transport technologies, in order to meet the service QoS and security requirements.

– **Others**

– **Benefits and impact**

Before deploying QKD over the 5G/LTE backbone network, it was protected with TLS/IPsec (IKEv2) which is eventually expected to be broken by Shor's algorithm with quantum computing. However, by using QKD, SK Telecom can protect the data over 5G/LTE backbone from quantum attacks.

– **Application prospects**

UC-5-1-1 was developed for SK Telecom's internal use but it can be applied by any telecom operators who would like to protect their subscribers' critical data in their backbone network

(2) UC-5-1-2: Quantum secured inter-domain 5G service orchestrator

– **Use case ID: UC-5-1-2.**

– **Use case description**

¹ The designations employed and the presentation of material on this map do not imply the expression of any opinion whatsoever on the part of ITU and of the Secretariat of the ITU concerning the legal status of the country, territory, city or area or its authorities, or concerning the delimitation of its frontiers or boundaries.

In [b-Wang], it is reported that QKD technologies in combination with software-defined networking (SDN) and network function virtualization (NFV) can be applied to secure interconnections of distributed virtual network functions (VNFs) to achieve quantum secured inter-domain 5G service orchestration.

This was experimentally demonstrated via interconnecting four autonomous 5G islands simultaneously through the q-ROADM with eight optical channels using the 5GUK exchange orchestration platform. The overall concept is as shown in Figure 6-13 [b-Wang].

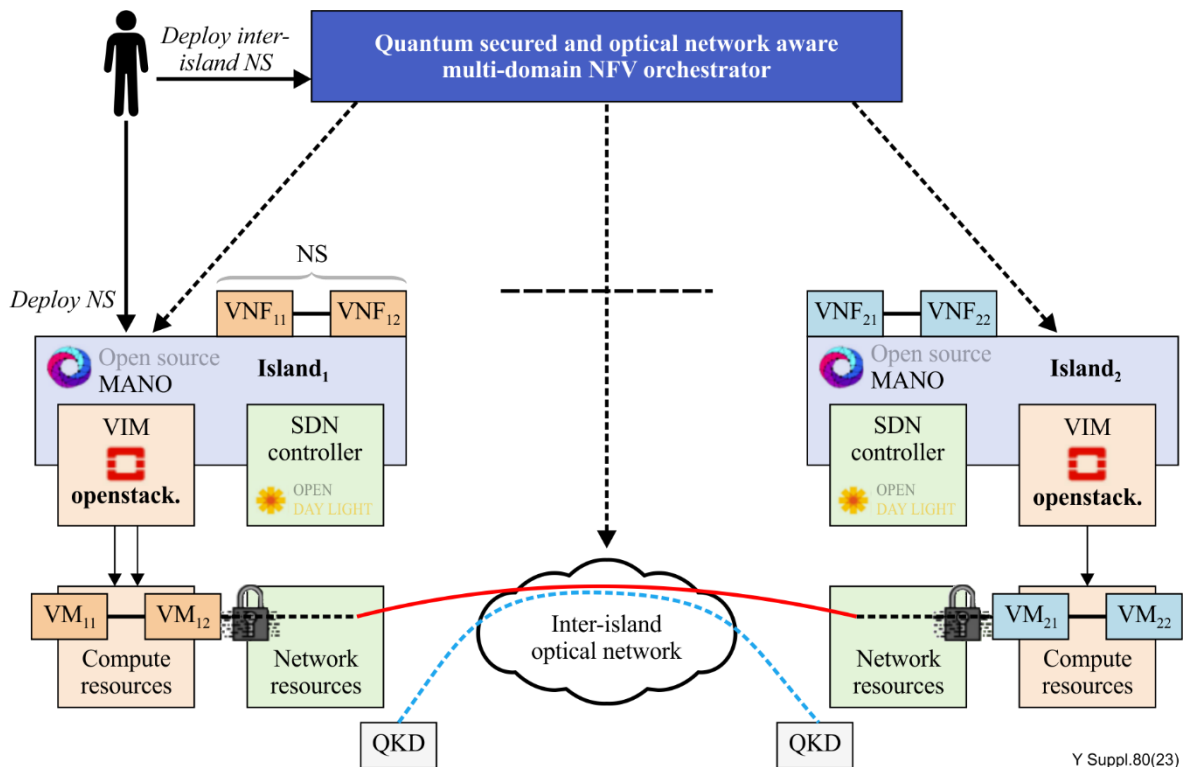


Figure 6-13 – Overall concept of QKD secured 5GUK exchange scenario

– Standardization considerations

The 5G service orchestrator is responsible for coordinating and managing cross-domain 5G services. Standardization requirements may include the protocols, interfaces and methods involving service orchestration to ensure that 5G networks can efficiently utilize QKDN services for secure provision of cross-domain services.

(3) UC-5-1-3: QKDN for 5G front-haul

- Use case ID: UC-5-1-3.
- Use case description

For 3G/4G networks, the base station (or known as eNodeB by 3GPP) is comprised of the base band unit (BBU) and the remote radio unit (RRU). The front-haul is referred to as the fibre connection between the BBU and RRU which features a high bandwidth, low latency and private common public radio interface (CPRI) interface.

For 5G, the base station (or known as gNodeB by 3GPP) functions are reallocated into three parts as RRU, distributed unit (DU) and central unit (CU), as shown in Figure 6-14.

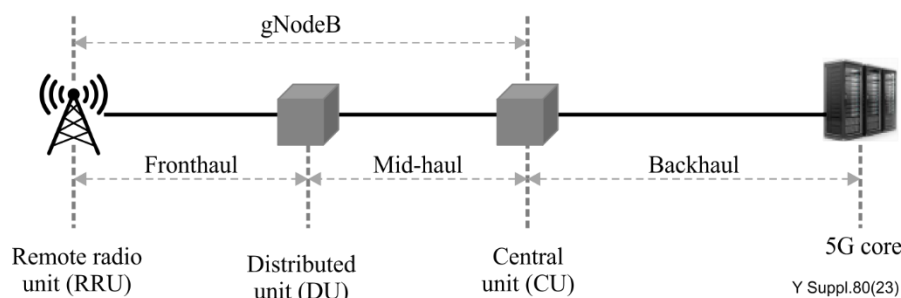


Figure 6-14 – 5G transport structure

The 5G RRU can handle certain physical layer functions of the previous BBU locally, thus, the front-haul transportation requirements can be relaxed to accommodate the surging 5G capacity. The next generation front-haul interface (NGFI) is designed for the connection between RRU and DU, as a new decoupled open interface to support RRU and DU from different vendors.

The security guarantee for 5G front-haul is an important issue which needs to satisfy high bandwidth, low latency and high-level security at the same time.

QKD is a promising solution to secure 5G front-haul which is mentioned in [b-Priem].

– **Standardization considerations**

The 5G front-haul network needs to meet the requirements of high bandwidth and extremely low latency. Standardization requirements may include the development of enhanced QKDN technology for hard real-time key provision in order to meet the stringent timing requirements of time-sensitive services including 5G front-haul.

(4) UC-5-1-4: QKDN for 5G mid-haul

– **Use case ID:** UC-5-1-4.

– **Use case description**

The mid-haul is a newly introduced concept in 5G to indicate the connection between the DU and CU.

SK Telecom (SKT) has showcased the application of QKD to the 5G mid-haul network to secure confidential data transmission from a smart factory to the cloud.

A customer of SKT, an auto parts manufacturer based in Ansan, implemented a smart factory using IoT devices and robots which generates a large volume of confidential data such as design documents transmitted over the 5G network to reach the SKT cloud. Therefore, the customer was looking for fast and secure access to the SK Telecom commercial 5G service to connect their new smart factory.

To best address this customer's security needs, SKT has secured the 5G network connectivity with the latest quantum safe technology using quantum cryptography. One 5G DU is located on the SKT's customer site in Ansan while the 5G CU is located at the central office of SKT network in Sungsoo. Since the 5G DU to CU connectivity uses a fibre optic network, it was possible to combine QKD with the encryption on the 5G mid-haul network. The deployment is illustrated in Figure 6-15.

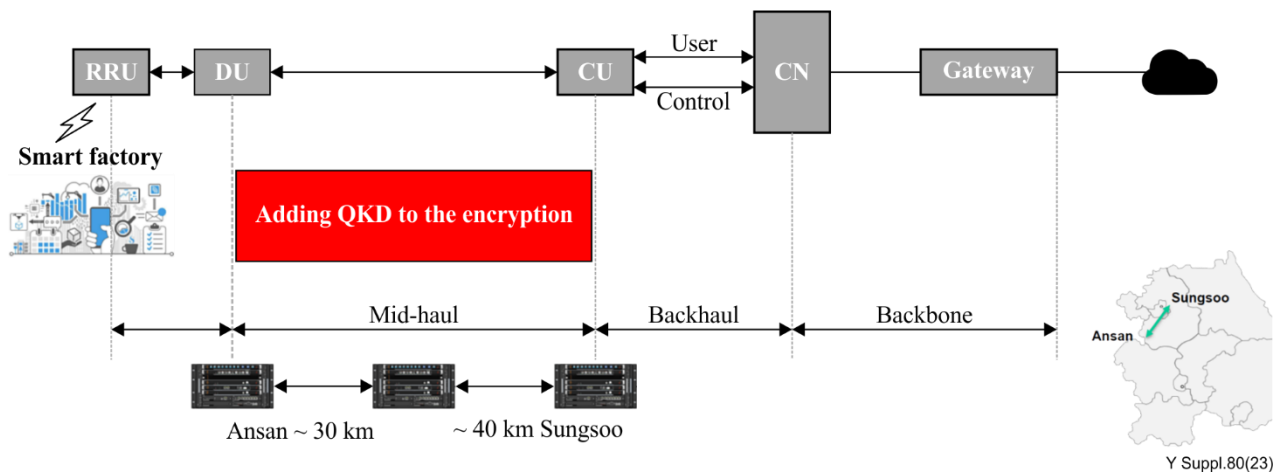


Figure 6-15 – 5G mid-haul QKD deployment for smart factory²

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

– **Problem statement**

The smart factory in Ansan generates a large volume of confidential data transmitted over 5G mid-haul to reach the SKT cloud in Sungsoo where it is processed and sent back to the machines and robots in the smart factory as input data. Consequently, it is critical to protect this data over the 5G network for their intangible property.

– **Technical considerations**

SK Telecom deployed QKD nodes in a point-to-point configuration for data transport as well as QKD key relay over the 5G mid-haul network between Ansan and Sungsoo in December 2018. Two QKD nodes are connected through a network point of presence defined as a hub for the encryption and QKD key relay.

– **Standardization considerations**

The 5G mid-haul networks involve the transmission of large amounts of data and control signals for real-time digital signal processing of 5G radio protocol stack. It may need further standardization study for the protocols, interfaces, and data formats of the enhanced mid-haul network to ensure integration and interoperability with the quantum key distribution network.

– **Others**

– **Application prospects**

Any business partners who would like to protect their data from quantum attacks can achieve this goal by using SKT cloud with QKD in SK Telecom's 5G network.

(5) UC-5-1-5: Quantum security enhancement for universal AKA authentication protocol

– **Use case ID:** UC-5-1-5.

– **Use case description**

² The designations employed and the presentation of material on this map do not imply the expression of any opinion whatsoever on the part of ITU and of the Secretariat of the ITU concerning the legal status of the country, territory, city or area or its authorities, or concerning the delimitation of its frontiers or boundaries.

Authentication verifies whether a user has the right to access a system. In the traditional authentication mode, users present valid information such as passwords to the authentication party to verify that they have the right to access the system. Authentication includes user authentication and network authentication where:

- user authentication means that the network authenticates users to prevent unauthorized users from occupying network resources; and
- network authentication allows users to authenticate networks to prevent users from accessing illegal networks and obtaining key information.

The authentication and key agreement (AKA) is a two-way authentication mechanism defined in [b-RFC 4187]; its improved version AKA' is defined in [b-RFC 5448]. Both mechanisms have been developed by IETF and adopted by 3GPP and are widely used wireless network authentication mechanisms. Figure 6-16 shows the AKA authentication protocol process.

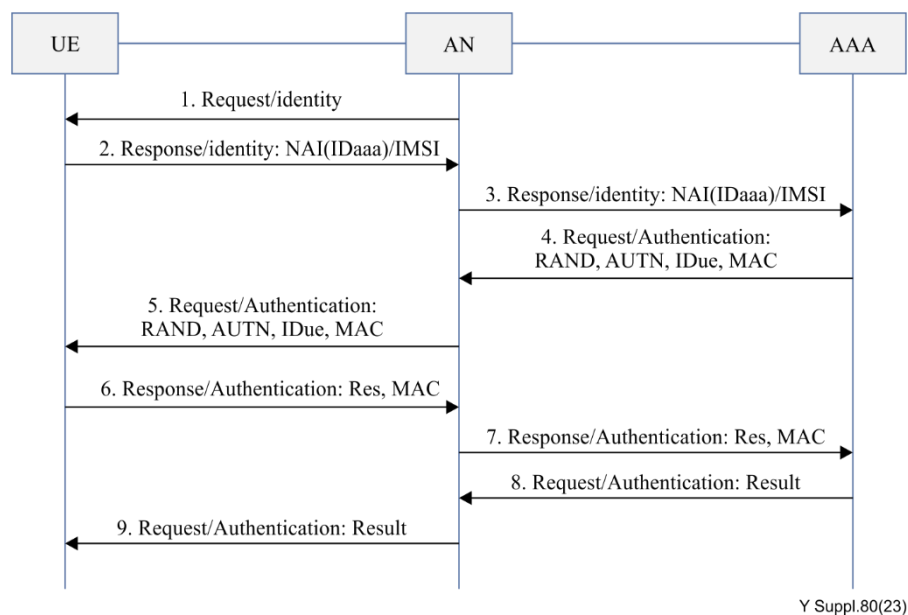


Figure 6-16 – AKA authentication protocol

- Problem statement

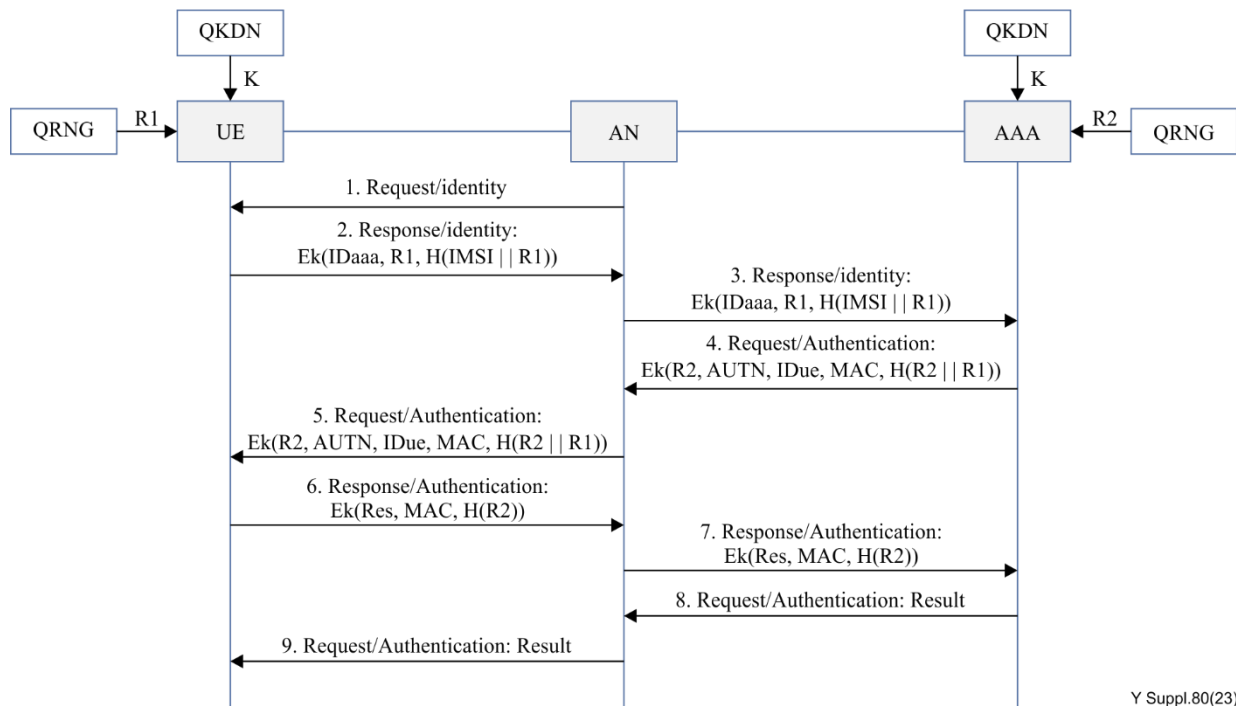
AKA authentication is considered to be a relatively safe authentication system, but it still has some shortcomings:

- If the AKA process is implemented in plaintext transmission mode, in which the interactive data is not encrypted and protected, the user ID, international mobile subscriber identity (IMSI) and other sensitive information will be disclosed and there will be risk of a middleman disguised identity attack.
- IMSI as unchangeable user information credentials should not be visible but be encrypted.
- Using a public key cryptosystem to protect data in the authentication process is not as good as using a pre-shared key symmetric encryption mechanism. The public key cryptosystem is also more difficult to operate and maintain.

– Technical considerations

The QKDN is used to realize the advantage of secure key distribution. The client UE and the authentication server authentication, authorization and accounting (AAA) use QKDN to share keys. Symmetric encryption fully ensures the security of data. The QRNG can generate enough secure true random numbers for the client and authentication server to use in the AKA process.

In the protocol improvement, the privacy of IMSI is fully considered. The client only sends the hash value of IMSI and random number, R1. The random number, R2, generated by the authentication server is not only used to generate the authentication vector (AV) but is also used with R1 generated by the client to be authentication factors of both parties. After the authentication succeeds, R1 and R2 can be used to generate new shared keys for both parties, see Figure 6-17.



Y Suppl.80(23)

Figure 6-17 – AKA authentication protocol improved by quantum security

Standardization considerations

Universal authentication and key agreement is a protocol for secure authentication and key generation. Standardization requirements may include protocols, interfaces and data formats involving authentication and key agreement to ensure integration and interoperability with quantum-safe technologies.

Others

Benefits and impact

The quantum security enhanced AKA authentication protocol can realize two-way authentication, non-disclosure of identity information of both authentication parties and multi-factor authentication. With the symmetric encryption method, it can protect the interactive data with confidentiality, integrity and authenticity. The protocol can resist attacks such as man-in-the-middle, forged identity, dictionary and replay attacks. The use of QRNG also ensures the true randomness of the generated random numbers.

Application prospects

Telecom operators and QKD service providers.

(6) UC-5-1-6: Secondary authentication protocol in 5G based on quantum security

Use case ID: UC-5-1-6.

Use case description

Network slices have been introduced in 5G to meet the differentiated needs of different industries. To prevent unauthorized users from accessing the industry's network slices, 5G proposes secondary

authentication for user access. The secondary authentication refers to the authentication between the end user and the data network outside the ISP's domain so that legitimate users can have secure access to the data network. According to [b-3GPP TS 33.501], the secondary authentication process applies between the user terminal, UE and the AAA server of the external data network (DN). The authentication protocol is based on the extensible authentication protocol (EAP) framework defined in [b-RFC 3748] and can be customized. Figure 6-18 shows secondary authentication protocol in 5G.

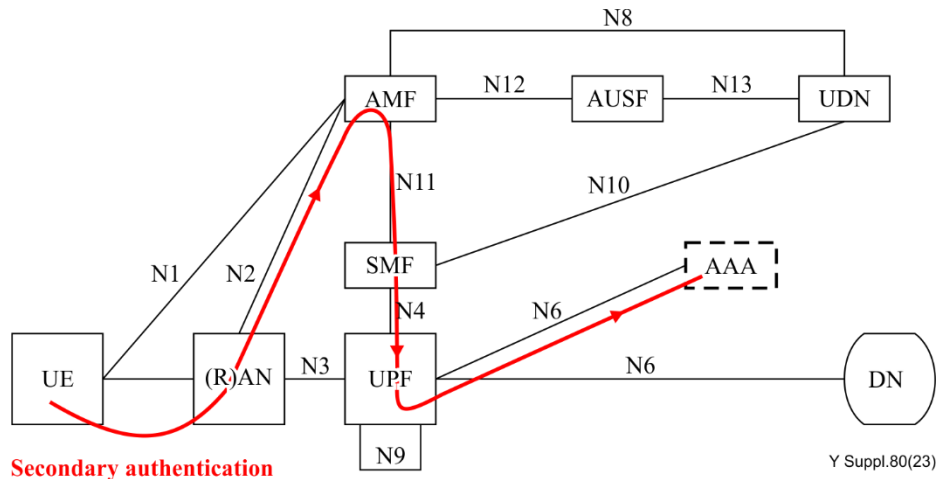


Figure 6-18 – Secondary authentication protocol in 5G

UC-5-1-6 describes two newly designed schemes; quantum secure symmetrical encryption (EAP_QSSE) and quantum secure symmetrical encryption and hash-function (EAP_QSSEH) based on quantum security. Both authentication parties use quantum random numbers as authentication factors and 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. Figure 6-19 shows secondary authentication protocol based on quantum security.



Figure 6-19 – Secondary authentication protocol based on quantum security

– Problem statement

Network development has entered the 5G era. As an enabling technology of ICT, 5G has greatly promoted the rapid development of networking and intelligence in various industries resulting in the acceleration of industrial upgrading. Applications in vertical industries will be one of the most important development directions for 5G networks in the future and there is also a diverse demand for 5G networks including security issues for 5G network device access.

5G provides different access modes and network service modes for different scenarios and supports different service delivery modes in which there are obvious differences in security requirements. For example, for the simultaneous access of resource-constrained massive IoT devices, the security authentication process requires limited computing resources; however, for the ultra-high reliable and low-latency applications such as Internet of vehicles and tele-healthcare, the access authentication process needs to be efficient and fast.

– **Technical considerations**

Under the premise of secure authentication, both authentication parties use quantum random numbers as authentication factors and 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.

– **Standardization considerations**

The mutual authentication between UE and AAA requires corresponding protocols and methods. Standardization requirements may include how to define the procedures, message formats and protocols for QKDN-based mutual authentication to ensure the integrity and security of the authentication.

– **Others**

– **Benefits and impact**

The EAP_QSSE secondary authentication protocol has the characteristics of lightweight and fast implementation. It can realize two-way authentication, non-disclosure of identity information of both authentication parties and multi-factor authentication. The EAP_QSSE protocol protects information with confidentiality, forward security and truly random numbers. It also has the function of key negotiation and can resist attacks such as man-in-the-middle, forged identity, dictionary and replay attacks.

The EAP_QSSEH can further introduce secure hash function on the basis of the EAP_QSSE to ensure the integrity of the message. It further ensures the security of the information shared by both authentication parties since they only exchange the hash values of ciphertext of the shared information rather than the ciphertext.

– **Application prospects**

Telecom operators and QKD service providers.

6.5.2 UC-5-2: QKD in SDN/NFV based network

(1) UC-5-2-1: Secure SDN and NFV control and management plane

– **Use case ID:** UC-5-2-1.

– **Use case description**

The implementation of UC-5-2-1 involves the creation of QKD keys that are combined with the usual keys in the protocols used so that the security is incremental: to break into the system, the old protocols have to be broken but also the new QKD layer. Figure 6-20 shows an abstract view of a control plane architecture including cloud/NFV and network orchestration and SDN control plane to secure by QKD

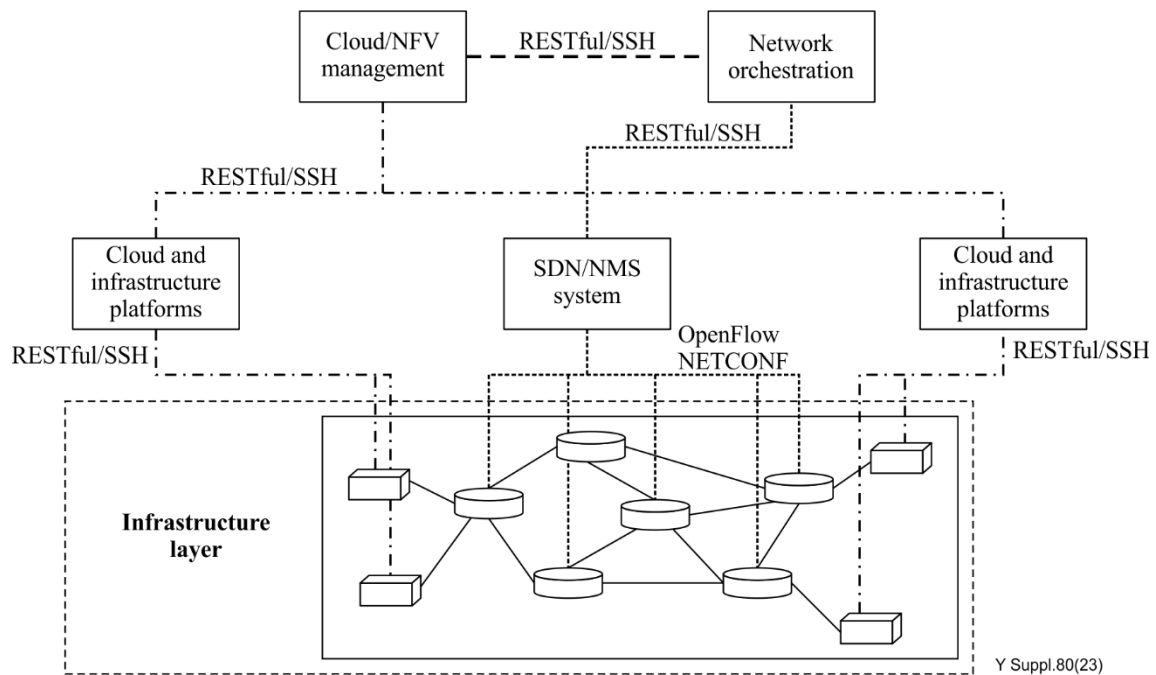


Figure 6-20 – Abstract view of a control plane architecture including cloud/NFV and network orchestration and SDN control plane to secure by QKD

A diagrammatic description of the testbed used to implement UC-5-2-1 in 2018 is depicted in Figure 6-21 with only two transponders and up to 17 classical co-propagating channels were used together with the quantum channel.

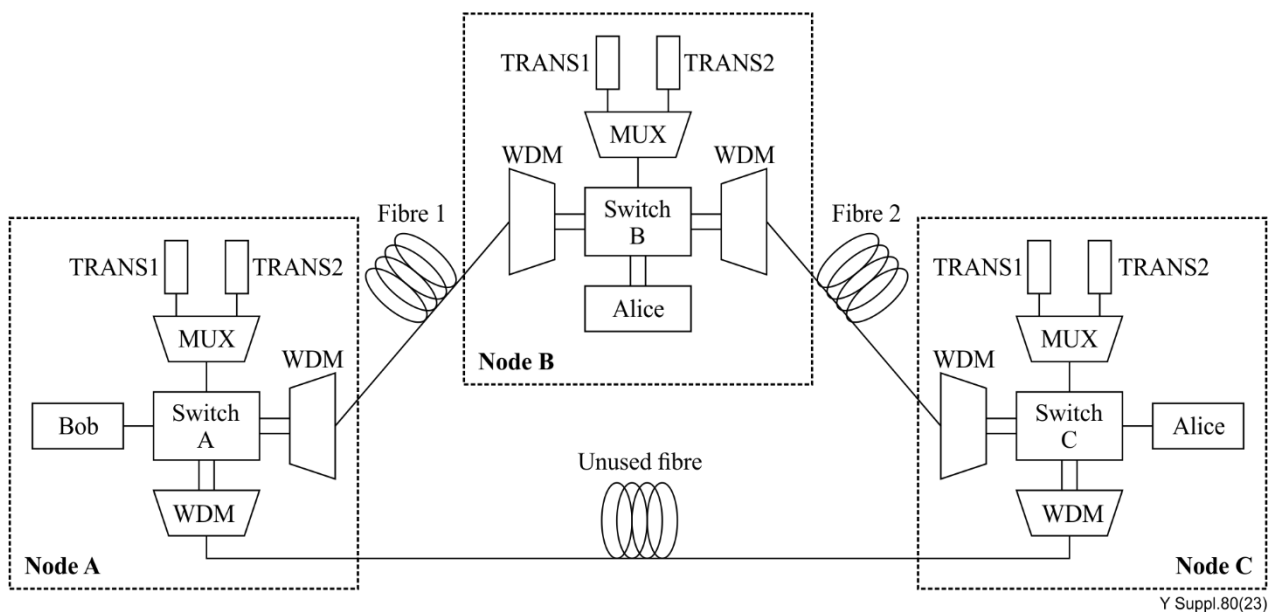


Figure 6-21 – Diagrammatic description of the testbed used to implement the use-case in 2018

– Problem statement

Integrating SDN and NFV technologies can affect networks by introducing new 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. This is a key problem since a compromised control and management plane would affect the entire infrastructure and services.

– **Technical considerations**

To tackle this issue, QKD can be seen as an additional security layer that runs in parallel (or is also integrated) to the transport network. QKD can help to mitigate such threats; securing the communications in the control and management plane.

– **Standardization considerations**

The standardization impact may include how to standardize the interfaces and protocols to enhance the authentication and authorization in SDN and NFV control planes with QKDN to ensure that only legitimate entities can access and control network resources.

– **Others**

– **Benefits and impact**

The adoption of SDN and NFV technologies brings many benefits to networks such as the reduction of the complexity and cost of operating the entire infrastructure or the reduction of vendor lock-in in the systems layer (e.g., NMSs). QKDN will greatly enhance the security of the SDN and NFV control plane which is key for its service provision.

– **Application prospects**

Typical vertical applications of UC-5-2-1 are for network security and self-healed network management.

(2) UC-5-2-2: QKD keys for end-to-end services

– **Use case ID:** UC-5-2-2.

– **Use case description**

UC-5-2-2 combines QKD systems to secure end-to-end (E2E) services e.g., transport tunnels, VPNs between remote premises. Protocols like path computation element protocol (PCEP) and multiprotocol label switching (MPLS) are used and modified to use QKD. Figure 6-22 shows the MPLS/PCEP workflow for setting up a quantum encryption service.

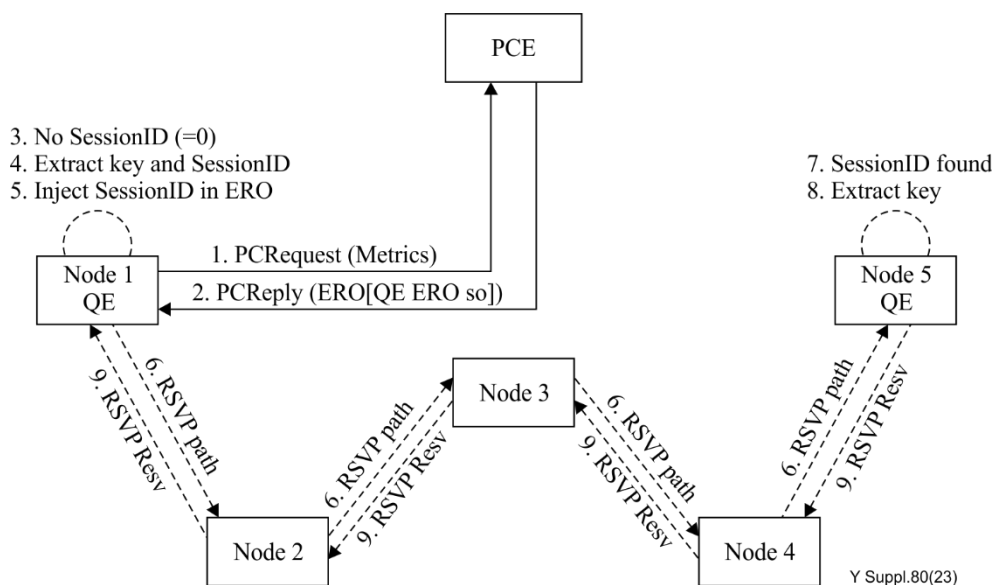


Figure 6-22 – MPLS/PCEP workflow for setting up a quantum encryption service

Figure 6-23 illustrates a logical scheme describing the network used for the E2E quantum encryption service via IPsec. The left part shows the DC management and data networks, with a QKD domain (Bob) and a virtual router connected to a PCE while the right part shows the local

network connecting another virtual router to the remote PCE and another QKD domain (Alice). The intermediate area exposes the packet/optical network.

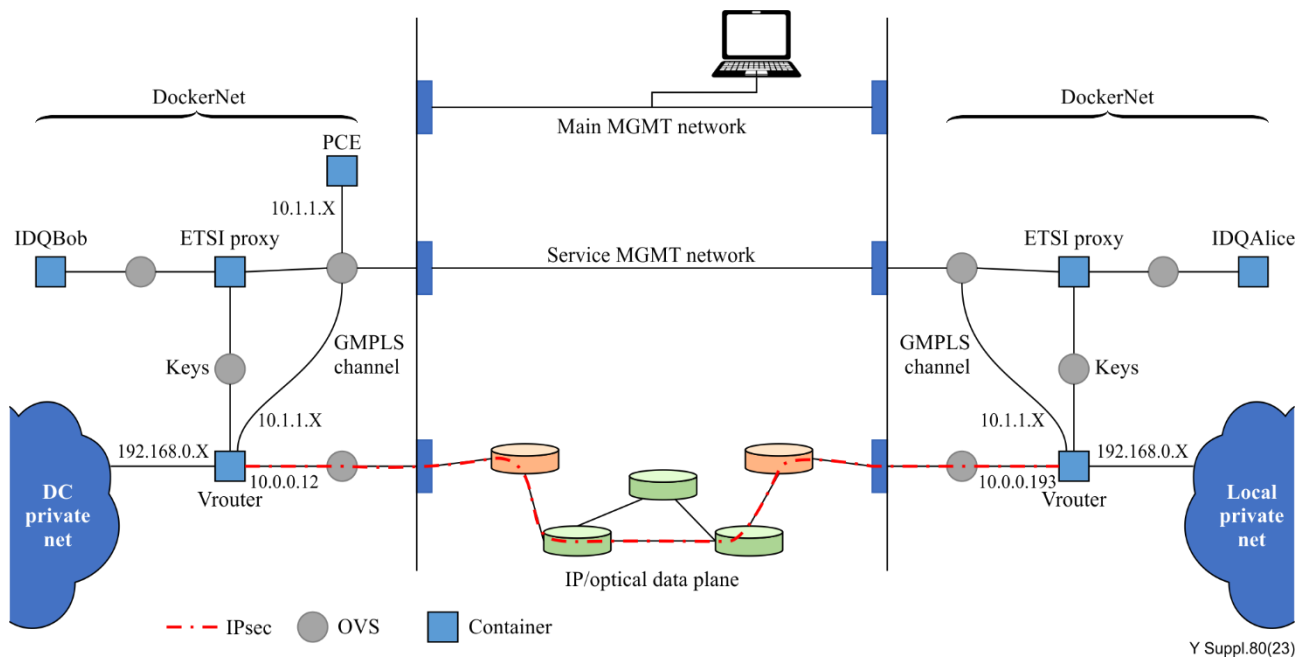


Figure 6-23 – Logical scheme describing the network used for the E2E quantum encryption service via IPsec

– Problem statement

One of the most demanded capabilities is an increase on the security standards of network services as big corporations have to transfer data securely between their headquarters and data centres. These services rely on underlying security protocols that are at risk of future attacks, more so 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).

– Technical considerations

QKD can be seen as a measure to provide such future-proof security if it is appropriately used by other security systems e.g., hardware security modules (HSMs), VNFs, network cards, etc. and automated via management systems.

– Standardization considerations

To develop a QKD-based encryption solution for end-to-end services to ensure data security involves the specification of how to integrate QKDN with various service protocols while maintaining the flexibility for an end-to-end service integration.

– Others

– Benefits and impact

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.

– Application prospects

Typical vertical applications of UC-5-2-2 are for network security, enterprise VPNs for business to business (B2B) communications and 5G networks.

(3) UC-5-2-3: Quantum security for service chaining

- Use case ID: UC-5-2-3.
- Use case description

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 security enhancement. Figure 6-24 illustrates a representation of an ordered proof of transit scheme in a network. The input and output nodes are connected by a chain of nodes that each packet must travel.

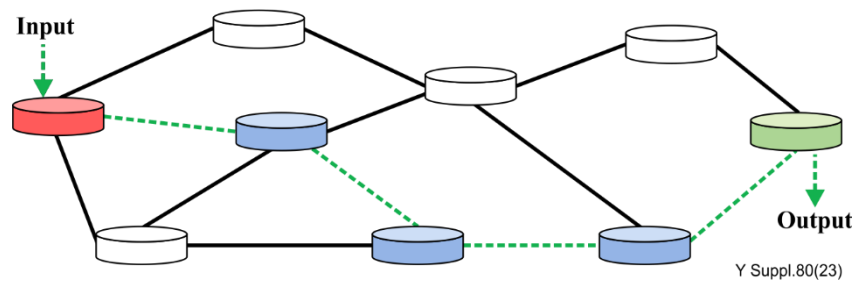


Figure 6-24 – Representation of an ordered proof of transit (OPoT) scheme in a network

Figure 6-25 illustrates the setup for the ordered proof of transit (OPoT) to secure service chaining as it was used in the Madrid quantum network [b-Aguado-3]. Two logical layers are shown: the QKD layer (lower part) and the data, OPoT layer (upper part).

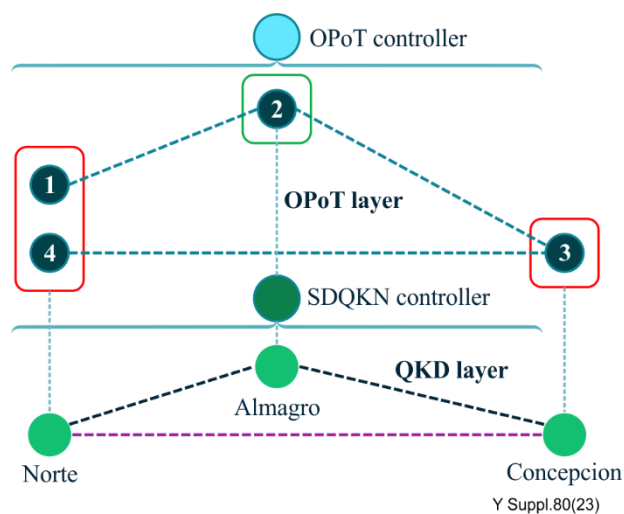


Figure 6-25 – OPoT-DEM: setup for the ordered proof of transit to secure service chaining as was used in the Madrid quantum network

- Problem statement

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 with NFV being one of the most radical and popular trends. It relies on computing virtualization concepts to encapsulate network elements functionalities, or VNFs, in virtual machines or instances which are placed in commodity data centres or cloud computing infrastructure. However, the flexibility brought by these new networking trends also carries 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 will not be accepted for production deployment.

By progressively replacing physical network functions (PNFs) with VNFs, this task becomes harder. As 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.

- **Technical considerations**

QKD is used to exchange information between elements within the chain, providing order and an extra layer of security. 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.

- **Standardization considerations**

It may need to develop standards to ensure that network functions, applications and resources used in service chains can achieve quantum-safe security with the integration of QKDN for data transmission, authentication and access control.

- **Others**

- **Benefits and impact**

This trend allows network resources to be dynamically allocated per-user/service and on demand, thus, permitting a new degree of flexibility in network management, reducing the time-to-market of new network functions, installation time of new services and cost of scaling and operating a network.

- **Application prospects**

Typical vertical applications of UC-5-2-3 are for network security and attestation, QKD as a cloud service, critical infra-structure protection, QKD for B2B and 5G networks.

6.5.3 UC-5-3: QKD in blockchain network

(1) UC-5-3-1: Quantum-secured blockchain

- **Use case ID:** UC-5-3-1.

- **Use case description**

[b-Kiktenko] proposes a quantum-safe blockchain solution based on QKD.

- **Problem statement**

It is well known that blockchain faces a severe security threat from quantum computing as its security is based on a public key exchange algorithm, e.g., ECC.

- **Technical considerations**

The main idea is to replace the proof of work (PoW) based consensus mechanism with the Byzantine algorithm which does not need public key exchange for authentication. Instead, it relies on QKD to realize information-theoretically secure authentication for pairwise nodes within the blockchain network.

- **Standardization considerations**

It may need to standardize the QKDN-enhanced algorithms for protecting data, transactions, and smart contracts in blockchains. This includes encryption and signature algorithms based on quantum key distribution.

- **Others**
- **Benefits and impact**

Due to the abandonment of the public key algorithm in this use case, the blockchain network can be considered as "quantum-safe blockchain".

- **Application prospects**

Blockchain service providers.

(2) UC-5-3-2: Quantum vault for blockchain

- **Use case ID:** UC-5-3-2.
- **Use case description**

In [b-Huttner], ID Quantique and its partners propose a quantum vault solution to utilize QKD and QRNG to enhance the security of blockchain.

- **Problem statement**

The major pain point of blockchain technology is considered to be the secure storage of private keys. The vault is a traditional popular solution used to manage blockchain private keys based on HSM.

- **Technical considerations**

The quantum vault solution uses QRNG to produce true random numbers as secret key seeds and uses the Shamir key sharing algorithm to split the keys into multiple elements and then uses QKD to securely distribute the key elements to distributed distant key storage nodes. The solution is illustrated in Figure 6-26.

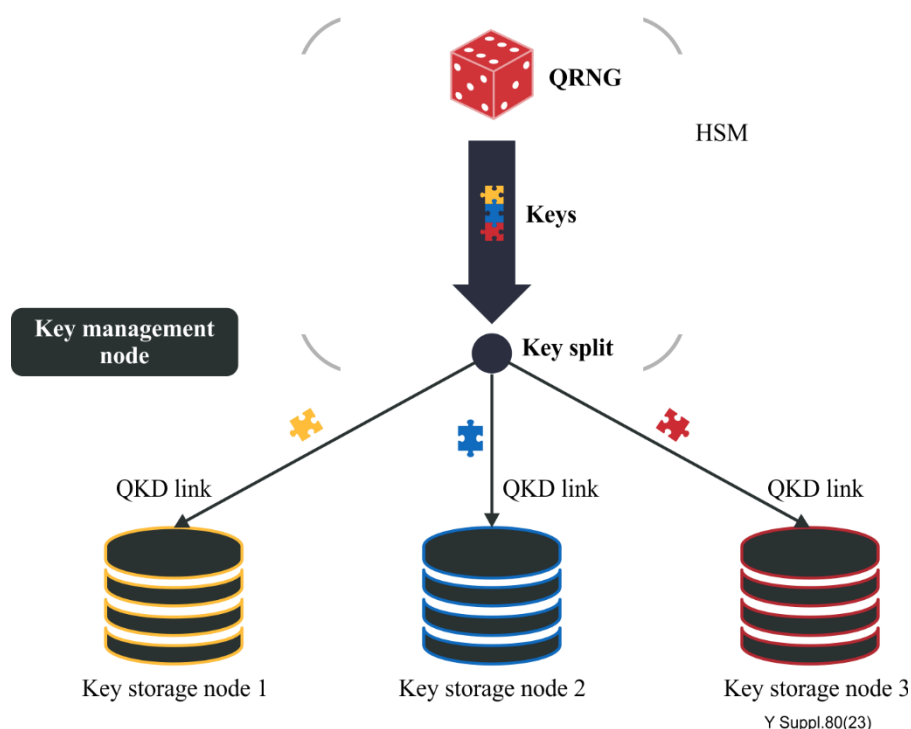


Figure 6-26 – QKD in a quantum-secured blockchain vault

- **Standardization considerations**

It may need to specify the security standards for nodes and communications in blockchain networks, including quantum-safe communications between nodes.

- **Others**

- **Benefits and impact**

UC-5-3-2 enhances the security of blockchain by using QKD to securely distribute its private key segments to the distributed key storage nodes.

- **Application prospects**

Blockchain service providers.

6.5.4 UC-5-4: QKD in TSN network

- **Use case ID:** UC-5-4.

- **Use case description**

Time-sensitive networking (TSN) is one widely applied communication standard developed by IEEE to meet stringent latency and timing requirements of the 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, as manifested in [b-Avnu].

- **Standardization considerations**

It may need to specify the standardized interfaces and integration methods required to integrate QKD into time-sensitive networks. This includes communication interface standards between QKD devices and TSN network devices.

- **Others**

- **Application prospects**

Industrial manufacturers

6.5.5 UC-5-5: QKD in SCION

- **Use case ID:** UC-5-5.

- **Use case 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 the 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 to enhance the security, which is one of the main concerns that today's Internet is facing.

One example use case introduced here is the QKD integration with scalable, control and isolation on next-generation networks (SCION) which is a research project led by researchers at ETH Zurich. SCION aims to offer a communication infrastructure that remains highly available even in the presence of adversaries.

Some typical vertical applications of QKD in SCION include for high-availability communication such as financial networks and industrial control systems used for power distribution. Governments can also use this architecture for critical communication infrastructure such as law enforcement communication.

Achievable security levels: A network is considered secure if it can achieve the desired properties even in the presence of an active adversary. One such prominent property is availability, i.e., the

control-, data-, management-, and configuration-planes should be protected such that an adversary cannot disrupt basic communication connectivity.

– **Problem statement**

Since all the E2E symmetric keys are driven from the local secret key in SCION architecture, managing the local secret is critical. As security is one of the main concerns, security enhancements can be added to the SCION architecture by integrating QKD with SCION and using QKD in the making of the local key.

– **Technical considerations**

As the first integration model for a QKD-equipped SCION architecture, QKD is applied to the DRKey setup protocol (one of the SCION extension protocols) which enables network entities to derive symmetric cryptographic keys on the fly from the local secret key.

In DRKey setup protocols, an autonomous system (AS) uses one local secret key to derive a symmetric key for another AS or end host on the fly using an efficient key generation function, pseudo-random function (PRF).

The main advantage of this approach is that the authentication process is extremely efficient. A router can efficiently derive a key for any AS and use it to authenticate packets to this AS. Moreover, it does not need coordination within an AS. If all routers within an AS share a secret SCION control message protocol (SCMP) key, each of them can locally and efficiently re-create the SCMP key using the DRKey protocol for any destination AS without any additional communication and without storing any per-AS state.

Assumptions made are:

- **Initial PKI Infrastructure:** it is assumed that each entity has a public/private key pair (K_i^+ , K_i^-), and that the public keys are correctly distributed to all other parties.

Figure 6-27 illustrates a high-level overview of the SCION-QKD integration model, which consists of two main components in addition to the server and client:

- 1) SCION certificate service (CS) which initiates the DRKey protocols, and
- 2) QKD that ensures the secure key distribution amongst ASes.

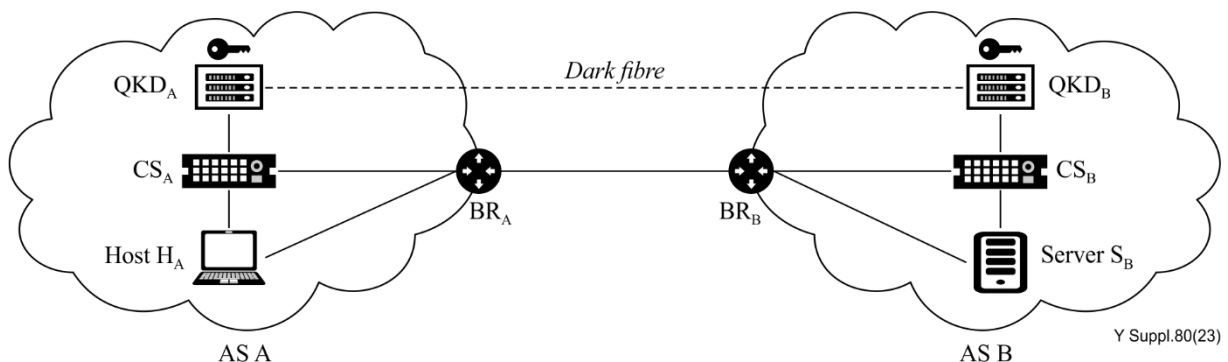
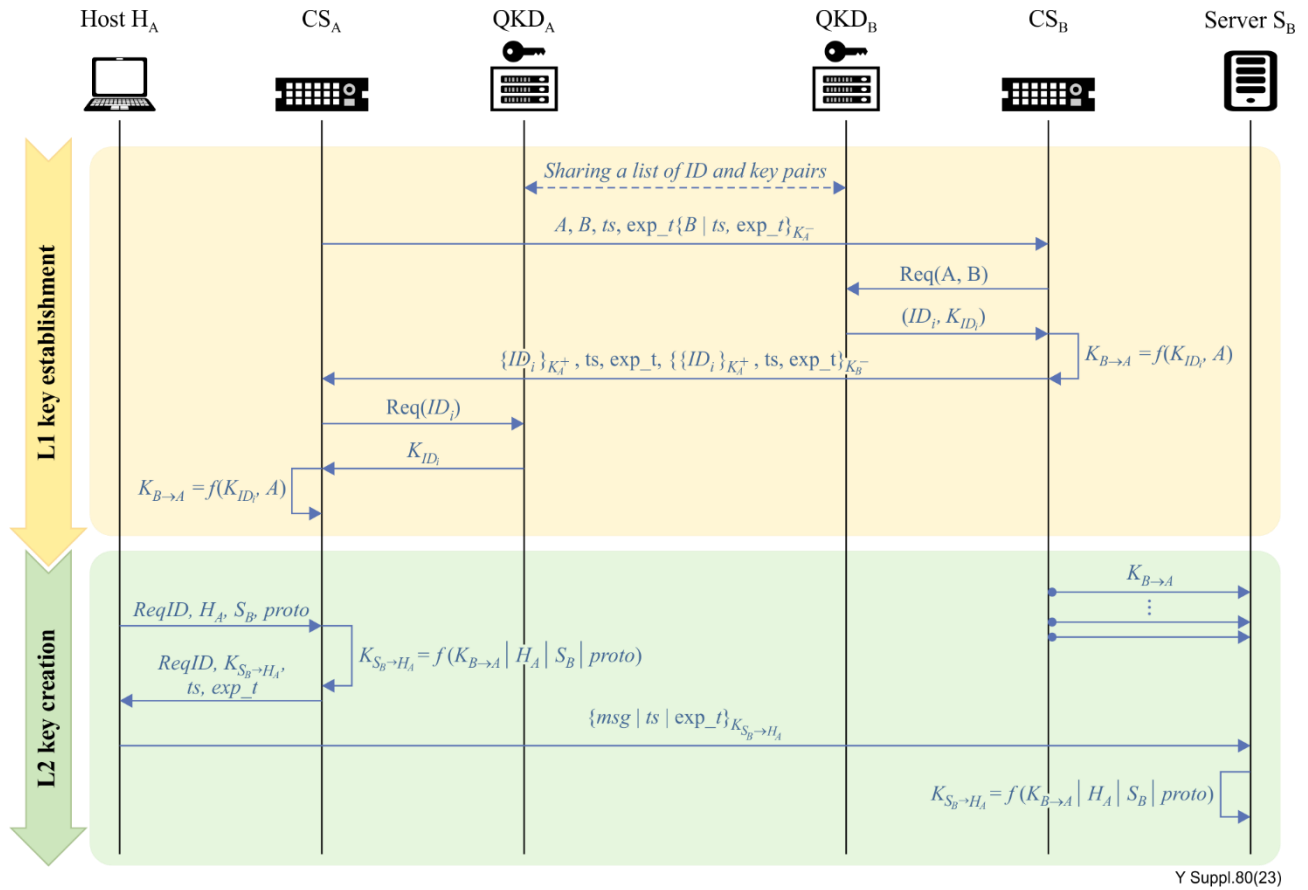


Figure 6-27 – High-level overview of the SCION-QKD integration model

In this integrated model, DRKey distribution process is illustrated in Figure 6-28.



Notations:

- $K_B \rightarrow A$: Symmetric key shared between AS B and AS A
- $K_{B:S_B} \rightarrow A:H_A$: Symmetric key shared between Server S_B in AS B and Host H_A in AS A

Figure 6-28 – DRKey distribution process

The detailed steps of the L1 and L2 DRKey distribution process are as follows:

- 1) Local CS (CS_A) initiates the L1 Key establishment protocol to the remote CS (CS_B).
- 2) With the help of QKDs, CS_B generates a symmetric key ($K_{B \rightarrow A}$) and delivers it to CS_A .
- 3) CS_B also frequently shares the newly generated L1 keys with all the entities within the AS (e.g., S_B).
- 4) A local client (H_A) requests an L2 Key from CS_A for communication with S_B .
- 5) CS_A creates a new symmetric key (L2 Key: $K_{B:S_B \rightarrow A:H_A}$) using $K_{B \rightarrow A}$ and replies it to H_A .
- 6) H_A starts communication using $K_{B:S_B \rightarrow A:H_A}$.
- 7) S_B also creates $K_{B:S_B \rightarrow A:H_A}$ by itself upon packet arrival, and verifies the validity of the packets.

This architecture can be deployed to ISPs' or any end users' (e.g., business or university) network.

Some specific functional requirements include:

- **Latency guarantees:** due to the complexity of inter-domain networks and interactions between high numbers of flows, latency guarantees are very challenging to achieve even in non-adversarial contexts. The key distribution latency for an end-to-end key sharing should be minimal.
- **Global time synchronization:** time-synchronization within a few seconds is required among all entities in the network (i.e., hosts, certificate services, QKDs).

Some standards relevant to UC-5-5 include [b-ETSI GS NGP 001] and [b-ETSI GS NGP 005].

– **Standardization considerations**

It may need to specify the standardized interfaces and methods required to integrate QKD technology into next-generation network equipment and architecture. This includes communication interface standards between QKD devices and network devices, as well as integration standards with network control and management systems.

– **Others**

– **Benefits and impact**

QKD can be integrated into the candidate of the next Internet architecture, i.e., SCION which is one research project that aims to realize this to add the advanced security measures. QKD keys can be used for local secret keys to drive all the E2E symmetric keys and, in turn, the security enhancements can be added to the SCION architecture as follows:

- **Security in key exchange:** to exchange a first-level key, the certificate services of corresponding ASes need to perform a key-exchange protocol via a secure channel, e.g., using TLS. With QKD, only the key ID is exchanged instead of the key, eliminating threats of on-path adversaries.
- **Key-fetching performance:** to be able to derive second-level keys without additional delay, an AS needs to keep the frequently contacted AS's first-level key proactively. For ASes that are not contacted regularly, on-demand key exchange is required. The QKD-based instant key establishment can reduce the additional delay.
- **Management scalability:** today's Internet consists of more than 71 K active ASes, which is expected to increase. Since QKD supports an instant key establishment, ASes do not need to perform AS-to-AS key establishment, increasing key-management scalability.

– **Application prospects**

UC-5-5 can be deployed by ISPs and/or B2B users (e.g., enterprises, universities, etc.).

6.6 UCC6: QKD applied in different vertical sectors

QKD can be applied in various vertical economic sectors that require high level and long-term security which may include, but are not limited to, the following:

- Finance
- Government and public sectors
- Healthcare, e.g., to secure genome data
- Telecom networks, e.g., to secure 5G network
- Industry networks
- Other critical infrastructures

6.6.1 UC-6-1: QKDN for smart factory

– **Use case ID:** UC-6-1.

– **Use case description**

Hyundai Robotics manufactures industrial robots, applies them to overseas industrial facilities and remotely operates through various ICT infrastructures such as IoT devices, 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, a commercial QKDN for the smart factory has been installed to protect corporate information and to enhance security. This network applies QKD to a leased line between Hyundai Robotics and KT Corp. office in Daegu, see Figure 6-29 for an illustration.

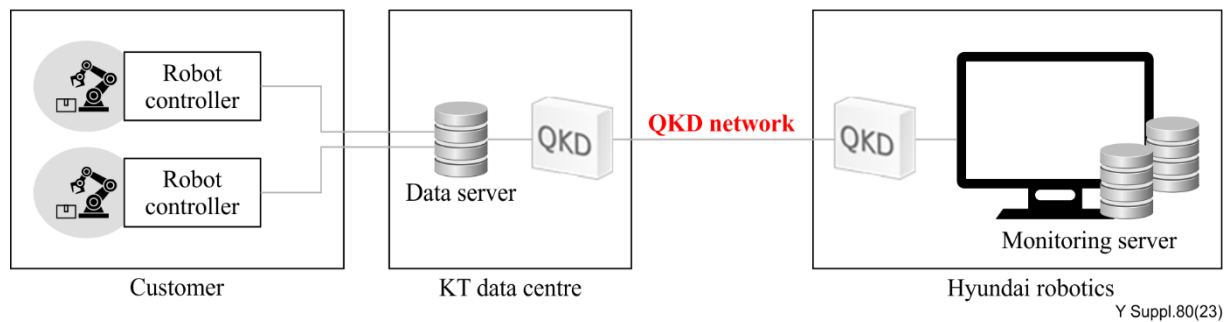


Figure 6-29 – QKDN for smart factory

– Problem statement

The main concern for global manufacturing industries is how to support secure remote management and administration since the relative data is related to their know-how and is business sensitive. Existing remote communication between the data centre and customer side is based on legacy telecommunication technologies, such as leased-line, VPN, e-MTC, etc. These communication methods are open to malicious hacking threats to the optical cable, mobile/satellite communication.

– Technical considerations

Monitoring and control data requiring the highest security is stored in the data centre of the KT Corp. office; one of KT's business model is the co-located cloud service. The leased line based on optical cable provides connectivity between the KT office and Hyundai Robotics' control centre. A set of QKD systems is installed in both sites (trusted node – secured by each site's own security policy) and supports the QKD-based security (quantum cryptography) for the optical cable.

– Standardization considerations

It may need to specify the integration methods, performance and stability requirements when using QKD in a smart factory environment, including standards for quantum key generation rates, communication delays, etc.

– Others

– Benefits and impact

The effort of global manufacturing industries to manage and administrate their products in remote locations through telecommunication technologies should take the security into account. Highly secured communication technology can remove this kind of threat from business/corporate management strategy. This solution can also be applied to secure mobile and satellite communication-based leased line on wireless and very long distance leased line service.

– Application prospects

Telecom operators and industrial manufacturers.

6.6.2 UC-6-2: QKDN for social safety

– Use case ID: UC-6-2.

– Use case description

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.

Korea (Rep. of) is deploying a commercial QKDN for social safety and this network applied QKD for drone communication between two adjacent local governments in Gangwon-do, see Figure 6-30.

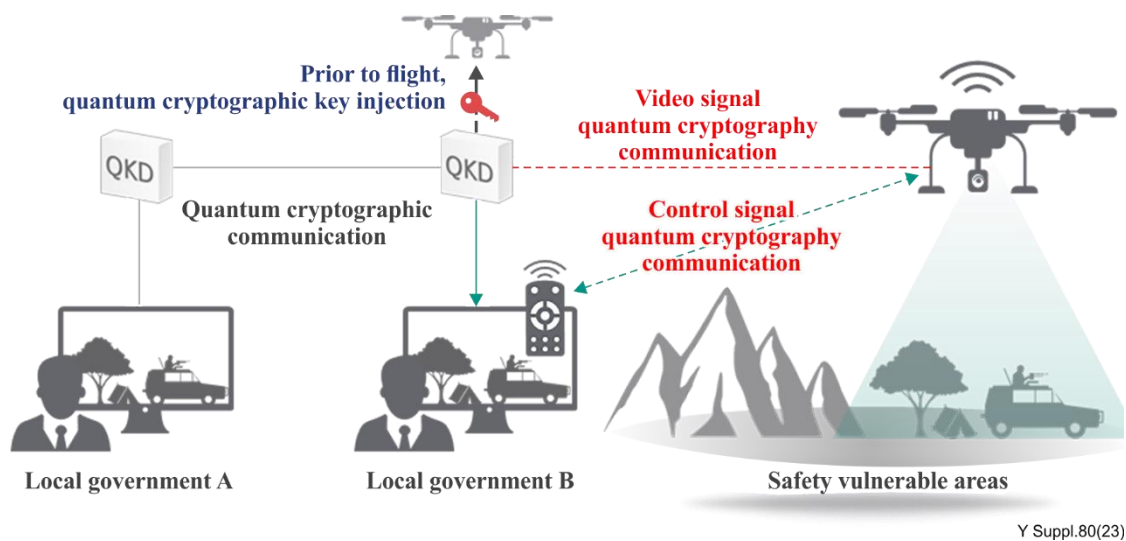


Figure 6-30 – QKDN for social safety

By injecting the quantum encryption key supplied from QKD into the drone, not only is the drone control signal protected, but also the video signal from the drone is encrypted and protected to improve security.

– **Problem statement**

Video data captured from a flying drone requires the highest security to be delivered to the local government. The wireless communication provides connectivity between the drone and the local government's monitoring centre. A set of QKD systems is installed at both ends of the leased-line and supports the QKD-based security (quantum cryptography) into the optical cable. However, the drone is located out of side of QKD connectivity.

– **Technical considerations**

The QKD key generated from QKD systems is injected into the drone prior to it leaving and flying from its mooring position. Then, the drone can communicate the data through quantum encrypted format.

– **Standardization considerations**

It may need to specify the integration methods, the performance and stability requirements when using QKD in the field of social security, including standards for quantum key generation rate, communication delay, etc.

– **Others**

– **Benefits and impact**

Wireless QKD technologies have not been commercially implemented yet as it is challenging for mobile objects such as drones, airplanes, vehicles, etc. QKD key injection in a trusted node/location can compensate this weakness. Before fully wireless QKD technology is realized, this approach could be tentatively acceptable for the security of mobile objects.

– **Application prospects**

Telecom operators and local government.

6.6.3 UC-6-3: QKDN for medical centre

– Use case ID: UC-6-3.

– Use case description

In St. Mary's Hospital, a large medical institution in Korea (Rep. of)., 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 and 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 commercial QKDN has been applied between medical data servers to encrypt medical data and improve security. This network applied QKD to a leased line between St. Mary's Hospital branches and their data centre in Seoul, see Figure 6-31.

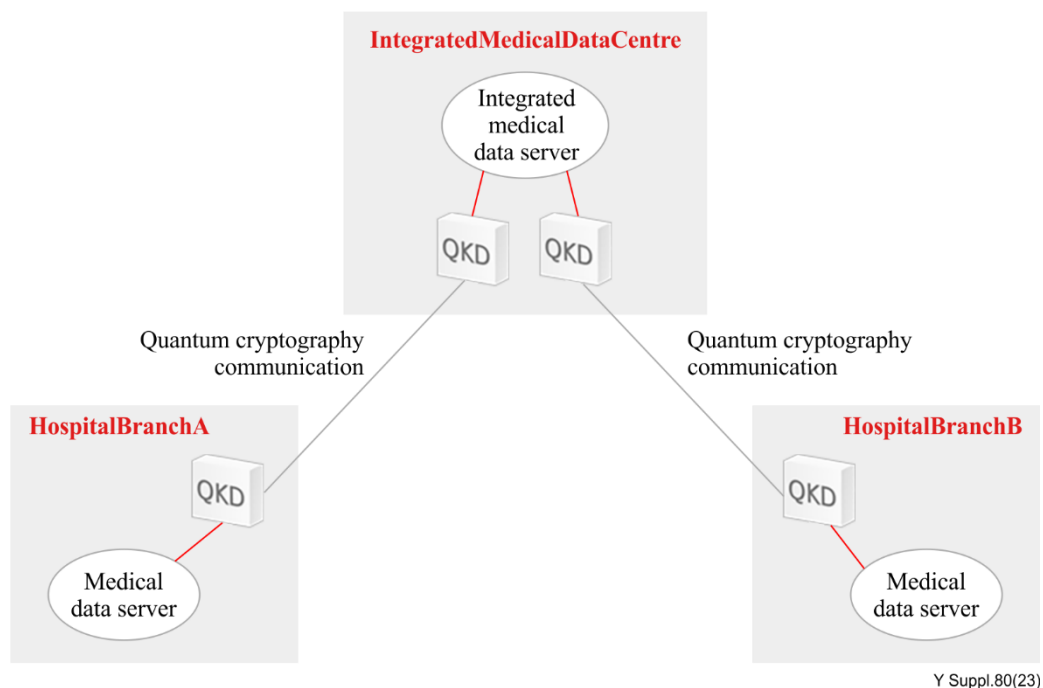


Figure 6-31 – QKDN for medical centre

– Problem statement

A main concern for the smart medical industry is that of how to support secure remote management and administration between data services and medical centres since the relative data is related to patient privacy. Existing remote communication between the data centre and customer side is based on legacy telecommunication technologies, such as leased-line, VPN, MPLS, etc. These communication methods are open to malicious hacking threats on optical cable, mobile/satellite communication.

– Technical considerations

Privacy-sensitive data, such as patient information and medical records, require the highest security when shared between branches of medical centres and their data centres. The leased-line based on optical cable provides the connectivity between them and a set of QKD systems is installed in multiple sites (trusted node – secured by each site's own security policy) which support the QKD-based security (quantum cryptography) for the optical cable.

– **Standardization considerations**

It may need to specify the standards for generating, distributing, storing, and updating quantum keys to ensure the confidentiality and integrity of medical data. This also includes key management integration standards for medical information systems.

– **Others**

– **Benefits and impact**

The medical industry's effort to manage and administer their data in remote data servers through telecommunication technologies should take the security into account. Highly secure communication technology can eliminate this kind of threat from business/corporate management strategy. This solution can also be applied to secure mobile and satellite communication-based leased line on wireless and very long distance leased line service.

– **Application prospects**

Telecom operators and medical centres.

6.6.4 UC-6-4: QKDN for secure mVoIP

– **Use case ID:** UC-6-4.

– **Use case description**

For mobile voice over IP (mVoIP), there are threats of hacking such as voice terminal wire-tapping, voice network wire-tapping, and session hijacking attack. To prevent such threats, a commercial QKDN for secure mVoIP was deployed in Korea (Rep. of). This network applies QKD to VoIP communication between two smart phones, see Figure 6-32.

The KSA key is received from the QKDN and injected into the secure communication devices and the mVoIP voice call data is encrypted through the devices.

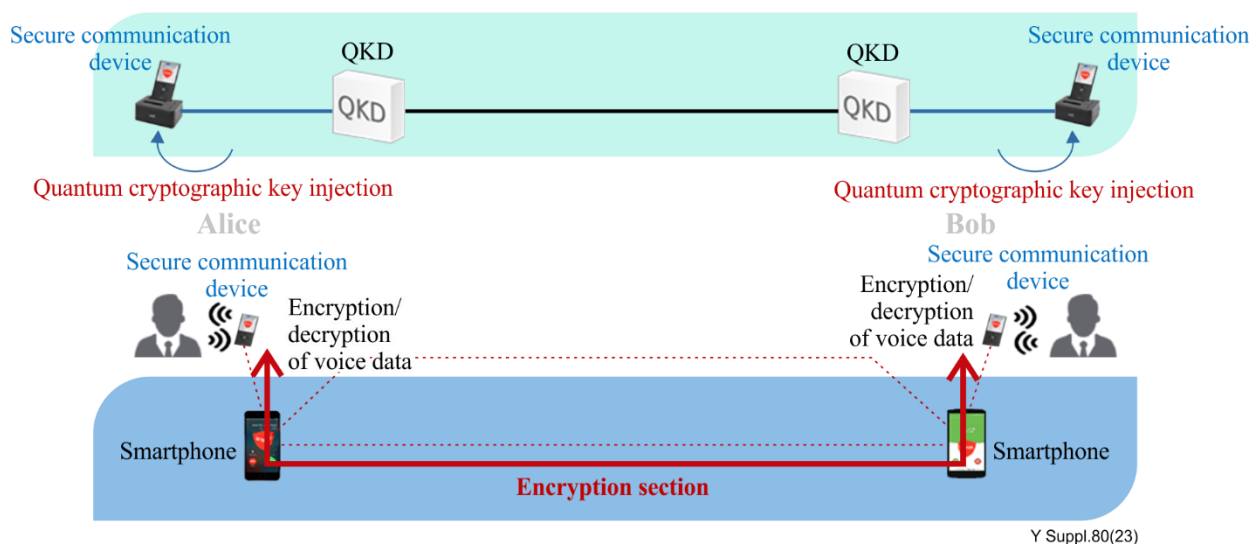


Figure 6-32 – QKDN for secure mVoIP

– **Problem statement**

Voice data requires the highest security when exchanged between smart phones and wireless communication provides connectivity between them.

A set of QKD systems is installed at both ends of the leased-line which supports the QKD-based security (quantum cryptography) into the optical cable, but the smart phones are located outside of QKD connectivity.

– **Technical considerations**

The QKD key generated from the QKD systems is injected into smart phones from charging stations, then, the smart phone can communicate the voice data in a quantum encrypted format.

– **Standardization considerations**

It may need to specify the standards for ensuring the security of call content and keys in QKDN networks and mVoIP calls, including protection requirements against quantum attacks.

– **Others**

– **Benefits and impact**

Wireless and portable QKD technologies have not been commercially implemented yet as it is challenging for mobile objects such as smart phone, drones, airplanes, vehicles, etc. QKD key injection in trusted nodes/locations can compensate for this weakness. Before fully wireless QKD technology is realized, this approach could be considered as tentatively acceptable for the security of mobile objects.

– **Application prospects**

Telecom operators and secure communication service providers.

Appendix I

Overview of QKDN use cases

This appendix provides a short description of each use case in clauses I.1 to I.6. Use the following table to select use cases and related SGs.

Clause no.	Use cases	Related SG
I.1	UCC1: QKD combined with other cryptographic primitives	
I.1.1	QKD combined with secret sharing	SG13, SG17
I.1.2	QKD combined with SMC	SG13, SG17
I.1.3	Hybrid QKD and PQC for encrypted communications	SG13, SG17
I.2	UCC2: QKD integrated with various TCP/IP protocols	
I.2.1	QKD integrated in data link layer	SG13, SG17
I.2.2	QKD integrated in network layer	SG13, SG17
I.2.3	QKD integrated in transport layer	SG13, SG17
I.2.4	QKD integrated in application layer	SG13, SG17
I.3	UCC3: QKD implemented in various network topologies	
I.3.1	QKDN as metropolitan access network	SG13
I.3.2	QKDN as inter-city backbone network	SG13
I.3.3	QKDN as free-space satellite-ground or inter-satellite network	SG13
I.4	UCC4: QKD with different user device categories	
I.4.1	Wireless user device with offline QKD-keys	SG13, SG17
I.4.2	Wireless user device with integrated QKD module	SG13
I.5	UCC5: QKD integrated in various network forms	
I.5.1	QKD in 4G/5G networks	SG13
I.5.2	QKD in SDN/NFV based network	SG13
I.5.3	QKD in blockchain network	SG13, SG17
I.5.4	QKD in TSN network	SG13
I.5.5	QKD in SCION	SG13
I.6	UCC6: QKD applied in different vertical sectors	
I.6.1	QKDN for smart factory	SG13
I.6.2	QKDN for social safety	SG13
I.6.3	QKDN for medical centre	SG13
I.6.4	QKDN for secure mVoIP	SG13

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	<p>This use case describes a distributed cloud archive for long term storage of digital data with advanced security and privacy guarantees.</p> <p>QKD links, as well as other technical and other cryptographic means ensure that the data can be securely 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.</p>

I.1.2 QKD combined with SMC

Use case ID	UC-1-2
Short description	<p>This use case describes quantum enabled private recognition of composite signals in proteins and genomes.</p> <p>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.</p> <p>This use case is based on use cases UC-5-2-1 and UC-5-2-2.</p>

I.1.3 Hybrid QKD and PQC for encrypted communications

Use case ID	UC-1-3
Short description	<p>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 costs, and lack of scalability.</p> <p>PQC, on the other hand, is similar to classical cryptography that is algorithm-based. However, deploying a new cryptosystem incurs potentially high costs, 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.</p> <p>QKD and PQC can be integrated in the hybrid quantum-safe scheme to enhance data transfer security.</p>

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	<p>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) [b-IETF RFC 1968] which allows the use of encryption in PPP frames. QKD may be used as a key exchange protocol for PPP.</p> <p>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.</p>

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 100 km 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	<p>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.</p> <p>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.</p>

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	<p>This use case describes QKD-key embedded secure mobile communication.</p> <p>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.</p> <p>In this use case, the proposed solution is to pre-install the QKD-key pool into the mobile user and network side to enhance the security of mobile communication which is achievable with existing QKD techniques.</p>

I.4.2 Wireless user device with integrated QKD module

Use case ID	UC-4-2
Short description	<p>As QKD modules are being miniaturized into chip-scale, it is possible that they 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 onto the credit card, and the QKD receiver in the ATM rack achieves free-space quantum key distribution.</p>

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	<p>This use case describes a network applying QKD to a LTE backhaul between Sejong central office and one of SK Telecom's DU sites at Daejeon.</p> <p>A trusted relay node was implemented for long distance QKD networks in 2017. Implementation and commercialization of QKD quantum cryptography for a total of 221 km of the 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 380 km. Other major cities will be reached with QKD step by step.</p>

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

Use case ID	UC-5-1-2
Short description	<p>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.</p> <p>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.</p>

I.5.1.3 QKDN for 5G front-haul

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

I.5.1.4 QKDN for 5G mid-haul

Use case ID	UC-5-1-4
Short description	<p>The mid-haul is one newly introduced concept in 5G to indicate the connection between a distributed unit (DU) and a centralized unit (CU). 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.</p> <p>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 needs. This solution combines the latest technology available ensuring high-speed, stability and security for the customer data connectivity.</p>

I.5.1.5 Quantum security enhancement for universal AKA authentication protocol

Use case ID	UC-5-1-5
Short description	<p>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 an AKA process.</p>

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

Use case ID	UC-5-1-6
Short description	<p>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.</p>

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	<p>The adoption of SDN and NFV technologies brings many benefits to the network, such as the reduction of the complexity and costs of operating the entire infrastructure or the reduction of the 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.</p> <p>To tackle this issue, QKD can be seen as an additional security layer that runs in parallel (or is also integrated) to the transport network. QKD can help to mitigate such threats, securing the communications in the control and management plane.</p>

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

Use case ID	UC-5-2-2
Short description	<p>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.</p> <p>One of the most demanded capabilities is an increase in 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 on underlying security protocols that are at risk of future attacks, and more so 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, OTN).</p> <p>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 such as patch computation element protocol (PCEP) and multiprotocol label switching (MPLS) are used and modified to use QKD.</p>

I.5.2.3 Quantum security for service chaining

Use case ID	UC-5-2-3
Short description	<p>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, network functions virtualization (NFV) being 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.</p> <p>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 will not be accepted for production deployment.</p> <p>By progressively replacing 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.</p>

I.5.3 QKD in blockchain network

I.5.3.1 Quantum-secured blockchain

Use case ID	UC-5-3-1
Short description	<p>It is well known that blockchain encounters severe security threats from quantum computing as its security is based on public key exchange algorithm, e.g., ECC.</p> <p>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 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.</p>

I.5.3.2 Quantum vault for blockchain

Use case ID	UC-5-3-2
Short description	<p>ID Quantique and its partners have proposed one quantum vault solution to utilize QKD and QRNG to enhance the security of blockchain.</p> <p>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.</p> <p>Here 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 uses QKD to securely distribute the key elements to distributed distant key storage nodes.</p>

I.5.4 QKD in TSN network

Use case ID	UC-5-4
Short description	<p>Time-sensitive networking (TSN) is one widely applied communication standard developed by IEEE to meet the stringent latency and timing requirements of industrial environments.</p> <p>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.</p>

I.5.5 QKD in SCION

Use case ID	UC-5-5
Short description	<p>Despite the rapid 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.</p> <p>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.</p> <p>One example use case introduced here is the QKD integration with SCION scalable, control and isolation on next-generation networks (SCION) 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.</p>

I.6 QKD applied in different vertical sectors

I.6.1 QKDN for smart factory

Use case ID	UC-6-1
Short description	<p>A commercial QKD network for smart factory is being deployed in Korea. This network applied QKD to leased line between Hyundai Robotics and the KT office in Daegu.</p> <p>Hyundai Robotics manufactures industrial robots, applies them to overseas industrial facilities, and remotely operates through various ICT infrastructures 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.</p> <p>To prevent such problems, the QKD network is installed to protect corporate information and to enhance security.</p>

I.6.2 QKDN for social safety

Use case ID	UC-6-2
Short description	<p>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.</p> <p>Local governments operate a 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.</p> <p>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.</p>

I.6.3 QKDN for medical centre

Use case ID	UC-6-3
Short description	<p>A commercial QKD network for medical centres was deployed in Korea. This network applied QKD to leased line between St. Mary's Hospital branches and their data centre in Seoul.</p> <p>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, and 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.</p> <p>To prevent such threats, a QKD network is applied between medical data servers to encrypt medical data and improve security.</p>

I.6.4 QKDN for secure mVoIP

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

Bibliography

- [b-Aguado-3] Aguado, A., López, D. R., Pastor, A., López, V., Brito, J. P., Peev, M., Poppe, A. and Martín, V. (2020), *Quantum cryptography networks in support of path verification in service function chains*. *Journal of Optical Communications and Networking* Vol. 12, No. 4, pp. B9-B19.
- [b-Alléaume] Alléaume R, Branciard C, Bouda J, et al., *Using quantum key distribution for cryptographic purposes: A survey[J]*. *Theoretical Computer Science*, 2014, 560: 62-81.
- [b-Avnu] Avnu Alliance White Paper (2018), *Industrial Wireless Time-Sensitive Networking: RFC on the Path Forward*.
<https://avnu.org/wp-content/uploads/2014/05/Industrial-Wireless-TSN-Roadmap-v1.0.3-1.pdf>
- [b-3GPP TS 33.501] Technical specification (TS) 3GPP V18.30.0 (2023), *Security architecture and procedures for 5G System*.
- [b-ETSI GR QSC 006] Group Report ETSI GR QSC 006 V1.1.1 (2017), *Quantum-Safe Cryptography (QSC); Limits to Quantum Computing applied to symmetric key sizes*.
- [b-ETSI GS NGP 001] Group Specification ETSI GS NGP 001 V1.3.1 (2019), *Next generation protocols (NGP); scenario definitions*.
- [b-ETSI GS NGP 005] Group Specification ETSI GS NGP 005 V1.1.1 (2017), *Next generation protocols (NGP); next generation protocol requirements*.
- [b-ETSI GS QKD 002] Group Specification ETSI GS QKD 002 (2010), *Quantum Key Distribution (QKD); Use Cases*.
- [b-IETF RFC 1968] IETF RFC 1968, *The PPP Encryption Control Protocol (ECP)*.
- [b-Kiktenko] Kiktenko, E. O., Pozhar, N. O., Anufriev, M. N., Trushechkin, A. S., Yunusov, R. R., Kurochkin, Y. V., Lvovsky, A. I. and Fedorov, A. K. (2018), *Quantum-secured blockchain*. *Quantum Science and Technology*, Vol. 3, No. 3.
- [b-Leilei] Leilei, H., Feng, K. and Xie, C. (2020), *A practical hybrid quantum-safe cryptographic scheme between data centers*. In *Proceedings Volume 11540, Emerging Imaging and Sensing Technologies for Security and Defence V and Advanced Manufacturing Technologies for Micro- and Nanosystems in Security and Defence III*; 1154008.
- [b-Priem] Priem, X. (2020), *Bristol Smart Internet Lab's Future Networks 2030 Vision*. In *sixth ITU Workshop on Network 2030 and Demo Day*, Lisbon, Portugal. Available at:
https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20200113/Documents/Xavier_Priem.pdf
- [b-QIT4N D2.1] Deliverable FG-QIT4N D2.1 (2021), *Quantum information technology for networks terminology: Quantum key distribution network*.
- [b-RFC 3748] RFC 3748 (2004), *Extensible Authentication Protocol (EAP)*.
- [b-RFC 4187] RFC 4187 (2006), *Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)*.
- [b-RFC 5448] RFC 5448 (2009), *Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')*.

- [b-Renner] Renner, R. (2008), *Security of quantum key distribution*. *International Journal of Quantum Information*, Vol. 6, No. 1, pp. 1-127.
- [b-SCION] Perrig, A., Szalachowski, P., Reischuk, R. M. and Chuat, L. (2017), *SCION: A Secure Internet Architecture*.
<https://scion-architecture.net/pdf/SCION-book.pdf>
- [b-Vergoossen] Vergoossen, T., Loarte, S., Bedington, R., Kuiper, H. and Ling, A. (2020), *Modelling of satellite constellations for trusted node QKD networks*. *Acta Astronautica*, Vol. 173, pp. 164-171.
- [b-Wang] Wang, R., Tessinari, R. S., Salas, E. H., Bravalheri, A., Uniyal, N., Muqaddas, A. S., Guimaraes, R. S., Diallo, T., Moazzeni, S., Wang, Q., Kanellos, G., Nejabati, R. and Simeonidou, D. (2020), *End-to-End Quantum Secured Inter-Domain 5G Service Orchestration Over Dynamically Switched Flex-Grid Optical Networks Enabled by a q-ROADM*. *Journal of Lightwave Technology*, Vol. 38, No. 1, pp. 139-149.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems