ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Supplement

ITU-T Y Suppl. 79 (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 – Role in end-to-end cryptographic services with non-quantum cryptography

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 79 to ITU-T Y-series Recommendations

ITU-T Y.3800 series – Quantum key distribution networks – Role in end-to-end cryptographic services with non-quantum cryptography

Summary

Based on Recommendation ITU-T Y.3800, many study items have been successfully developed and others are still being developed. However, in cases where mobile objects (i.e., autonomous car, mobile phone, etc.) are to be supplied with a quantum key distribution (QKD) service, there is a difficulty to establish and maintain a quantum channel with them in a stable manner. Key supply agent-keys (KSA-keys) are not able to be supported in this situation.

KSA-keys generated from a quantum key distribution network (QKDN) to mobile objects can be delivered through a user network using modern cryptography technology (especially a key exchange protocol).

Therefore, the integration of a QKDN with non-quantum cryptography will enable the QKDN and service providers to bring the cryptography service to a much wider range of businesses.

For this purpose, the relationship between the QKDN and end-to-end (E2E) cryptography services will be introduced in this Supplement. Then, relative use cases for the integration of QKDN with non-quantum cryptography will be described. Finally, based on the analysis of the detailed attributes of use cases, implications for further study will be identified.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T Y Suppl. 79	2023-11-03	13	11.1002/1000/15785

Keywords

Modern cryptography, quantum key distribution, QKD network, use case.

* 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/.

Table of Contents

Supplement 79 to ITU-T Y-series Recommendations

ITU-T Y.3800 series – Quantum key distribution networks – Role in end-to-end cryptographic services with non-quantum cryptography

1 Scope

This Supplement provides an overview for the integration of a quantum key distribution network (QKDN) with non-quantum cryptographies under three categories as follows:

– QKDN's role in end-to-end cryptography service;

– Use cases for the integration in end-to-end cryptography services with non-quantum cryptography;

– Implications for standardization activity in Study Group 13.

2 References

[ITU-T X.509] Recommendation ITU-T X.509 (2019), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.

[ITU-T Y.3800] Recommendation ITU-T Y.3800 (2019), *Overview on networks supporting quantum key distribution*.

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following terms defined elsewhere:

3.1.1 key supply agent-key (KSA-key) [b-ITU-T Y.3803]: Key data stored and processed in a key supply agent (KSA), and securely shared between a KSA and a matching KSA.

3.1.2 public-key infrastructure (PKI) [ITU-T X.509]: The infrastructure able to support the management of public keys able to support authentication, encryption, integrity or non-repudiation services.

3.1.3 quantum key distribution (QKD) [b-ETSI GR QKD 007]: Procedure or method for generating and distributing symmetrical cryptographic keys with information theoretical security based on quantum information theory.

3.2 Terms defined in this Supplement

None.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

E2E End-to-End

IKE Internet Key Exchange

IT-secured Information Theoretically-secured

KM Key Manager

KpqC	Korean post-quantum Cryptography
KSA-key	Key Supply Agent-key
PAT	Pointing, Acquisition and Tracking
PKI	Public-Key Infrastructure
PQC	Post-Quantum Cryptography
QKD	Quantum Key Distribution
QKDN	Quantum Key Distribution Network
QoS	Quality of Service
TLS	Transport Layer Security

5 Conventions

None.

6 Introduction

Based on [ITU-T Y.3800], many study items have been successfully developed and others are still being developed. However, in cases where mobile objects (i.e., autonomous car, mobile phone, etc.) are to be supplied with a quantum key distribution (QKD) service, there is a difficulty to establish and maintain a quantum channel with them in a stable manner, for the purpose of KSA-keys delivery.

Even though pointing, acquisition and tracking (PAT) technology is combined with free-space QKD modules, it is expected that the required accuracy for the quantum channel is difficult to achieve, due to the unpredictability of the movement and corresponding position of the mobile objects. This means that QKDN cannot support the end-to-end (E2E) cryptography service between the car and the mobile phone in a standalone manner in this situation.

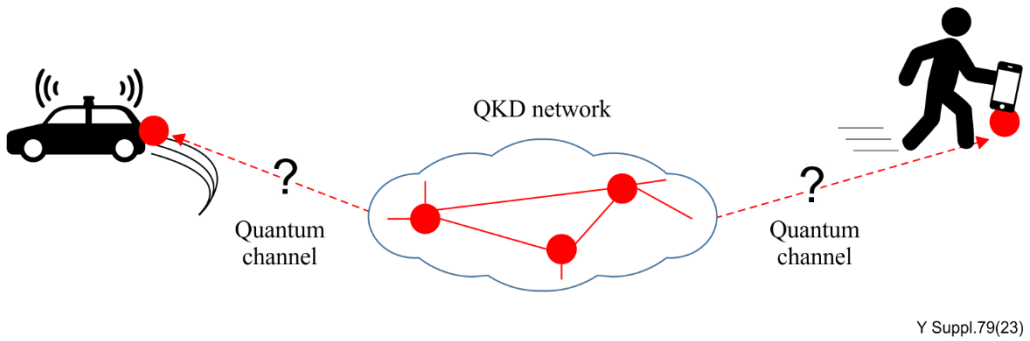


Figure 1 – An example of QKD network in the mobile object environment

Public-key infrastructure (PKI) architecture in modern cryptography is considered a security aspect for the extension of QKD applications. The combination between key generation/distribution of QKDN and other PKI-related functions is essential in the user network.

In order to overcome the difficulty for mobile objects, some additional functions for existing cryptography architecture can be used. For the purpose of delivery of KSA-keys generated from QKDN into the mobile objects, the keys can be delivered through a user network with PKI technology (especially key exchange protocol), instead of the extension of quantum channel.

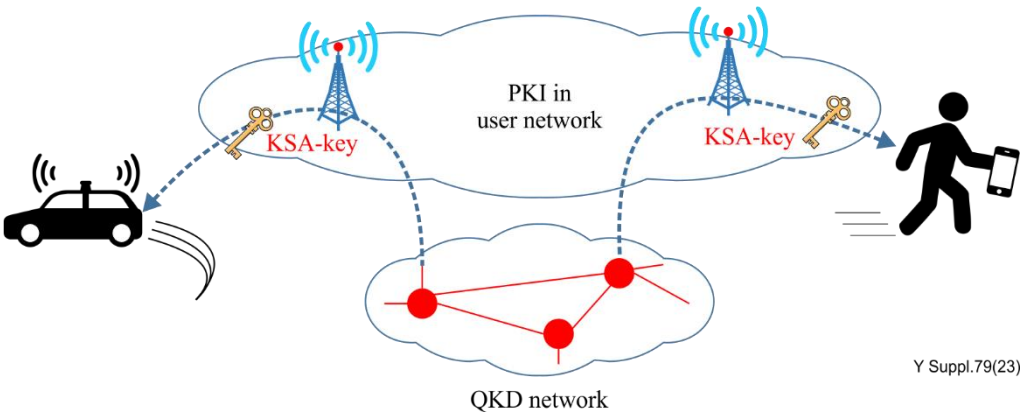


Figure 2 – KSA-keys delivery through PKI in user network

However, this approach causes a problem in countering a quantum computer's attack, since cryptographic algorithms in existing PKI architecture are known to be non-quantum-safe. To address this issue with quantum-safe algorithms, overhauling existing PKI architecture will be required as existing algorithms become obsolete.

Fortunately, some ongoing standardization projects such NIST Post-Quantum Cryptography (PQC) and KpqC (Korean PQC) are currently aiming to standardize a set of post-quantum secure encryption/key exchange algorithms and digital signature algorithms.

NOTE – The study of PQC is out of scope of this Supplement.

From this point of view, it is recommended that the integration of QKDN and PKI with a PQC algorithm should be studied for the extension of QKD service availability and market penetration for QKD service providers. Considering this study is just one of several possibilities, other possible approaches should be studied as well. In addition to those approaches, architecture and functional requirements can be further studied.

As a conclusion, the integration of QKDN with non-quantum cryptography will enable QKDN and QKD service providers to bring cryptography services to a much wider range of businesses.

7 QKDN's role in an end-to-end cryptography service

Figure 3 shows the QKDN's role in an E2E cryptography service. The E2E cryptography service requires cryptographic keys for the E2E encryption of messages between two end users. QKDN provides a secure way of establishing symmetric keys between two users for end-to-end data encryption. E2E encryption, which helps prevent data breaches and cyberattacks, is important for data security and privacy, especially for sensitive and confidential information, such as business documents, financial details and medical conditions. The E2E encryption can be realized between the cryptographic applications in the user network by applying QKDN or applying the integration of QKDN and non-quantum cryptographies.

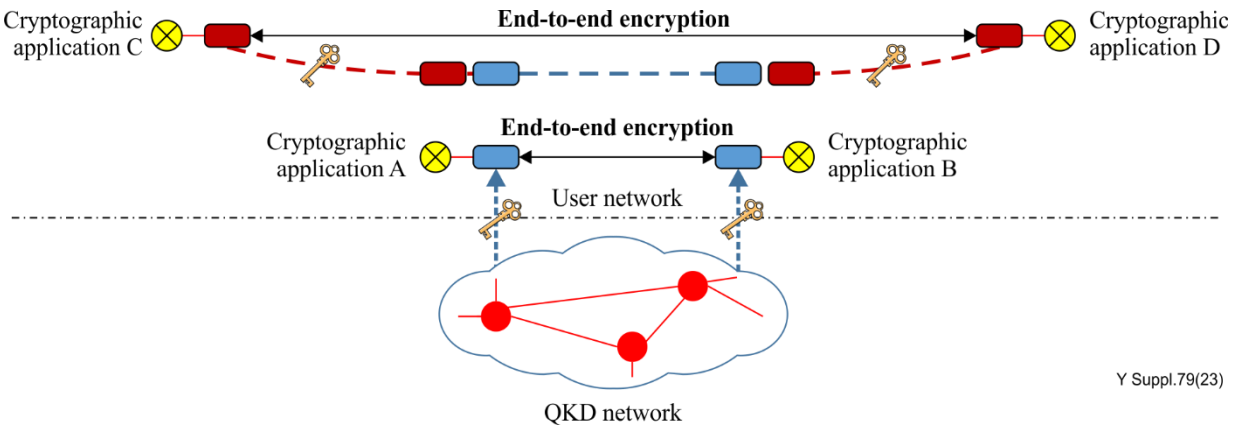


Figure 3 – QKDN's role in an end-to-end cryptography service

Figure 3 of [ITU-T Y.3800] shows a relation between three layers in QKDN and a service layer in the user network. The service for QKD technology in the service layer is a cryptography service that is encrypted and decrypted by symmetric KSA-keys from QKDN (encryption by KSA-keys). On the other hand, PKI architecture can be introduced in the service layer as well. The service is encrypted and decrypted with classical asymmetric cryptographic keys from a modern cryptographic module (encryption by classical keys).

NOTE – How to generate and distribute cryptographic keys is out of the scope of this Supplement.

From modern cryptographic technology's perspective, three types of cryptographic service are possible. They are: E2E encryption by KSA-keys; E2E encryption by classical keys; and E2E cryptographic services combining both encryption by KSA-keys and encryption by other classical keys.

- E2E encryption by KSA-keys (including, where hybrid, with other classical keys): In this type, the QKDN should provide KSA-keys in each end-point of the cryptographic service in the user network. This type is the basic assumption of the ITU-T Y.3800-series.
- E2E encryption by classical keys; This type has been specified in many modern cryptographic technology-related ITU Recommendations, including [ITU-T X.805], and by other standards development organizations.
- E2E cryptographic services combining both encryption by KSA-keys and encryption by other classical keys: This type has not been specified in terms of how to design, deploy, operate and maintain. The relevant aspects for use cases and implications for further standardization activity are within the scope of this Supplement to support its implementation.

8 Use cases for the integration of end-to-end cryptography services with non-quantum cryptography

8.1 Use Case 1

In this use case, KSA-keys generated from the QKDN supply to the TLS (Transport Layer Security) client and server symmetrically. TLS communication between client and server can be encrypted and decrypted thorough the keys. Therefore, a public-key exchange procedure may not be required during the initiation process, the so-called TLS handshake. The configuration of this use case is shown in Figure 4.

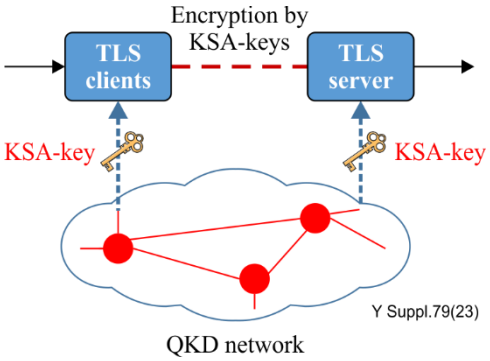


Figure 4 – Configuration of Use case 1

NOTE 1 – It is assumed that the TLS client and server, and QKD module and key manager (KM) are located together in the same trusted node. Based on this assumption, the delivery connectivity from QKDN to TLS functions is considered to be IT-secured.

NOTE 2 – Figure 3 of [ITU-T Y.3800] specifies the conceptual structures of a QKDN and a use network. However, in this Figure 3, cryptographic application is not a part of trusted node in alignment with QKDN.

8.2 Use Case 2

In this use case, KSA-keys generated from the QKDN supply only to the corresponding portion for encryption by KSA-keys. The other end portions are encrypted by the cryptographic keys derived from modern cryptography, i.e., the Internet key exchange (IKE) protocol. The configuration of this use case is shown in Figure 5.

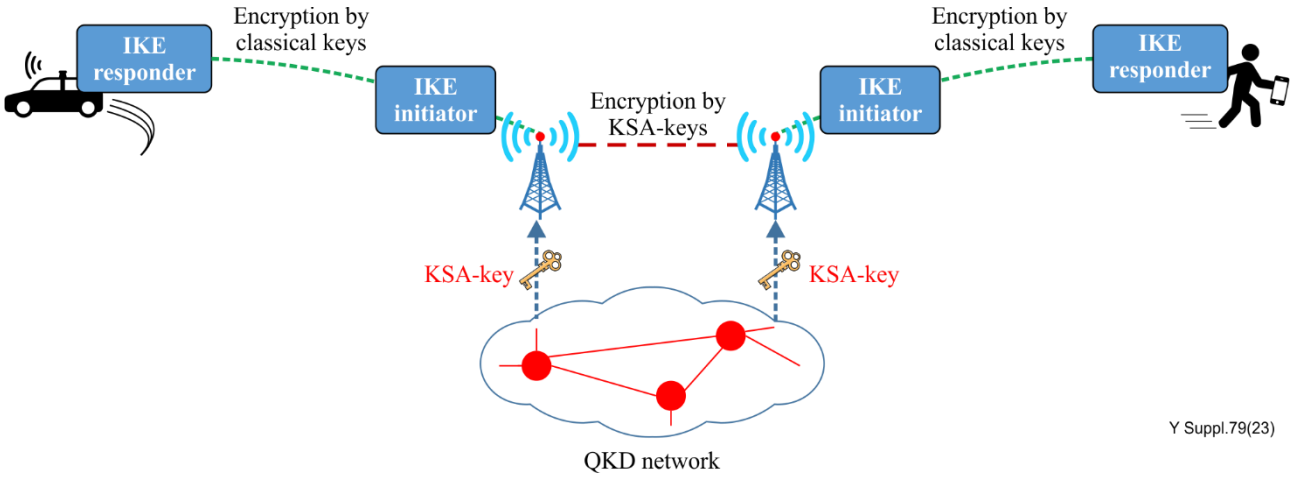
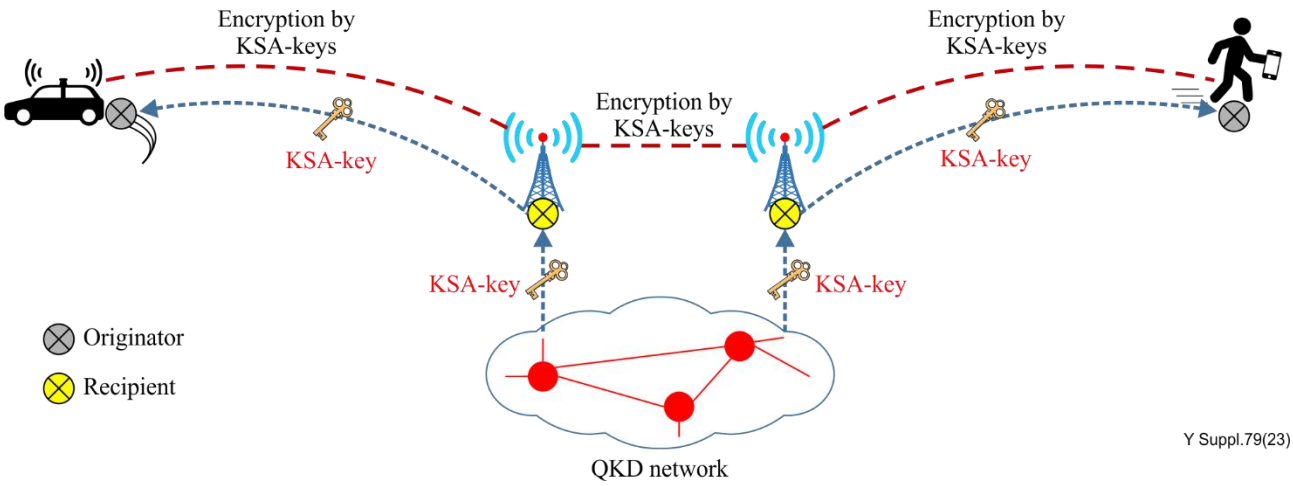


Figure 5 – Configuration of Use Case 2

8.3 Use Case 3

In this use case, KSA-keys generated from the QKDN supply to the corresponding portion. Then the keys deliver to both ends of connectivity through the key exchange function of modern cryptography. The communication between both ends can be encrypted by the received KSA-keys. The configuration of this use case is shown in Figure 6.



NOTE – The terminology of originator and recipient are derived from [ITU-T X.509].

Figure 6 – Configuration of Use Case 3

9 Implications for standardization activity on Study Group 13

9.1 General implications for standardization activity

9.1.1 Use Case 1

If the TLS client and server and QKD module and key manager are not located together in the same trusted node, the connectivity from QKDN to TLS functions should be further secured.

The potential use of non-quantum but quantum-resistant cryptography can be further studied. For the protection of user data within cryptographic applications (e.g., by the TLS protocol) removal of public-key generation and exchange procedure can be studied.

9.1.2 Use Cases 2 and 3

In Use Case 2, there are no specific technical consideration points. However, the security threat into physical concatenation between encryption by KSA-keys and encryption by classical keys connectivity might be further studied.

In Use Case 3, modern cryptography should take into account KSA-keys as one of the keys to be exchanged between originator and recipient. Relevant additional interface and procedure between the QKDN and modern cryptography could be required.

9.1.3 Control and management implications of use cases

The integration of the QKDN and modern cryptography introduces some control and management implications. The QKDN control and management architecture defines QKDN-related control and management capabilities and PKI architecture also provides its own control and management functionality. In order to guarantee the quality of key delivery across the integrated environment, cooperation of control and management capabilities needs to be further studied. Figure 7 illustrates the boundary and role of control and management in the integrated environment.

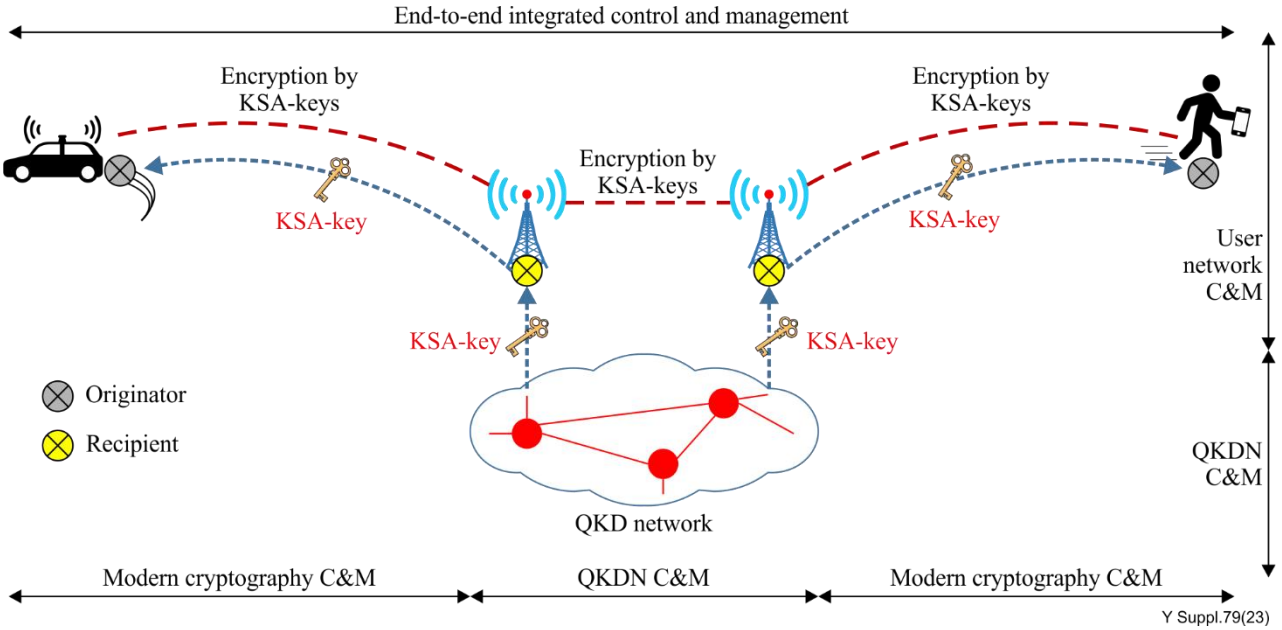


Figure 7 – The boundary and role of control and management in the integrated environment

9.1.4 Quality of service (QoS) aspect

From the QKDN quality of service (QoS) perspective, [b-ITU-T Y.3806] specifies the requirements including QoS planning, QoS monitoring, QoS optimization, QoS provisioning, QoS protection and recovery. In addition, [b-ITU-T Y.3807] describes QoS and network performance (NP) on QKDN and specifies the associated relative parameters for QoS and their definitions. Finally, [b-ITU-T Y.3811] specifies the functional architecture of QoS assurance and basic operational procedures for QKDNs. With these Recommendation, the QKDN QoS is well addressed in terms of only QKDN, not considering user networks and end-devices. The cryptographic applications can be end-devices.

On the other hand, there are several types of use network, meaning non-quantum networks, and the Recommendations for user network QoS are addressed. For example, [b-ITU-T Y.1540] defines the parameters that may be used in specifying and assessing the performance of speed, accuracy, dependability, and availability of Internet protocol (IP) packet transfer of IP data communication services. [b-ITU-T Y.3106] specifies the QoS requirements for the IMT-2020 network.

When KSA-keys are delivered between two cryptographic applications, they pass through both the QKDN and user network. Otherwise, the encrypted data goes through the user network. Figure 8 shows end-to-end QoS domain for cryptographic applications. In order to support end-to-end QoS, two types of QoS are considered in choosing a path between the cryptographic applications. Therefore, the QoS coordination and mapping are necessary between QKDN and the user network.

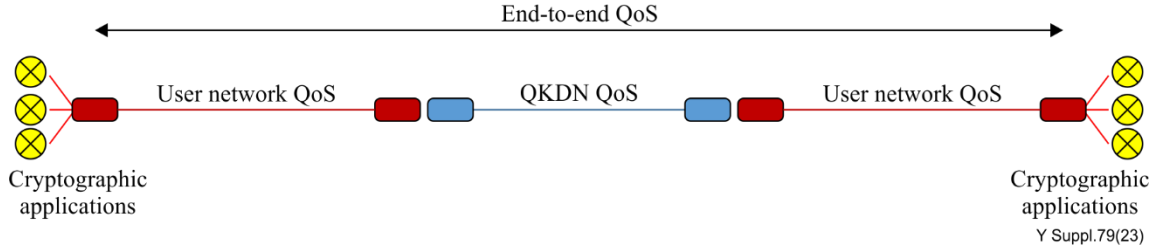


Figure 8 – End-to-end QoS domain for cryptographic applications

9.2 Implications for Study Group 13

9.2.1 Secure delivery of KSA-keys from QKDN to user network

A cryptographic application in the user network ideally has a point of presence within each of the QKD nodes (trusted nodes) it receives keys from. The interfaces and links implementing the Ak interface can then benefit from the protection of a QKD node. Such presence can be temporary, e.g., while receiving keys for later use outside the QKD node in the case of dynamic entities. Figure 3 in [ITU-T Y.3800] does not indicate the cryptographic application shown as having any part within a QKD node (trusted node). Much of the associated series of Recommendations considers cases where cryptographic applications do have such points of presence. Otherwise, it should be considered with other ITU-T SGs and SDOs how the Ak interface between a QKDN and a user network should be secured (e.g., including the use of modern cryptography with PQC algorithms).

9.2.2 Hybrid control and management capabilities between the QKDN and user network

The control and management capabilities associated with safe and reliable E2E key delivery need to be studied in Q16/13 and Q6/13 of SG13. Since Q16/13 is responsible for QKDN control and management, the integrated control and management can be under its responsibility. QoS control and management for integrated E2E QKD can be studied in Q6/13. Control and management in the integrated environment may need the support of the PKI architecture.

9.2.3 Quality of service for supporting non-quantum cryptographies.

From E2E QoS assurance, it is considered how the QoS coordination and mapping are performed and what the impact on existing Recommendations are.

Due to the different QoS assurance ways of QKDN and non-quantum cryptographies, as well as the various cryptography services, it is challenging to assure the E2E QoS for the encryption by KSA-keys and encryption by classical keys services under the integration of QKDN and non-quantum cryptographies. Q6 in SG13 focuses on the QoS aspects related to QKDNs. It is appropriate to study the E2E QoS assurance for the integration of QKDN and non-quantum cryptographies, such as the overview, QoS assurance requirements, QoS parameters and QoS assurance architecture.

Bibliography

[b-ITU-T Y.1540] Recommendation ITU-T Y.1540 (2019), *Internet protocol data communication service – IP packet transfer and availability performance parameters*.

[b-ITU-T Y.3106] Recommendation ITU-T Y.3106 (2019), *Quality of service functional requirements for the IMT-2020 network*.

[b-ITU-T Y.3803] Recommendation ITU-T Y.3803 (2020), *Quantum key distribution networks – Key management*.

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

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

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

[b-ETSI GR QKD 007] ETSI Group Report QKD 007 V1.1.1 (2018), *Quantum key distribution (QKD); Vocabulary*.

[b-IETF RFC 4306] IETF RFC 4306 (2005), *Internet Key Exchange (IKEv2) Protocol*.

[b-IETF RFC 8446] IETF RFC 8446 (2018), *The Transport Layer Security (TLS) Protocol Version 1.3*.

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

Published in Switzerland
Geneva, 2024