Draft new Supplement 79 to ITU-T Y.3800-series

Quantum key distribution networks – Role in end-to-end cryptographic services with non-quantum cryptography

Summary

Based on [ITU-T Y.3800], many study items are successfully developed and developing so far. However, in case that mobile objects (i.e., autonomous car, mobile phone, etc.) are to be supplied quantum key distribution (QKD) service, there is a difficulty to establish and maintain a quantum channel stably with them. Key supply agent-keys (KSA-keys) are not able to be supported on this situation.

For the purpose of delivery of KSA-keys generated from quantum key distribution network (QKDN) into the mobile objects, the keys can be delivered through user network using modern cryptography technology (especially key exchange protocol).

Therefore, the integration of QKDN with non-quantum cryptography will enable the QKDN and service providers, bringing its cryptography service to a much wider range of business opportunity.

For this purpose, the relationship between QKDN and end-to-end (E2E) cryptography service will be introduced. 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 in terms of further study issue will be identified.

Keywords

Quantum Key Distribution; QKD network; Modern Cryptography; Use Case.

Table of Contents

Page

Draft new Supplement 79 to 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 the overview for integration of 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 on Study Group 13

2 References

[ITU-T X.509] Recommendation ITU-T X.509 (2019), *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.*

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

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following term defined elsewhere:

3.1.1 key supply agent-key (KSA-key) [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 Technical Report

None.

4 Abbreviations and acronyms

This Recommendation 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
NIST	National Institute of Standards and Technology
PAT	Pointing, Acquisition and Tracking
PKI	Public Key Infrastructure
PQC	Post Quantum Cryptography
QKD	Quantum Key Distribution
QKDN	Quantum Key Distribution Network
TLS	Transport Layer Security

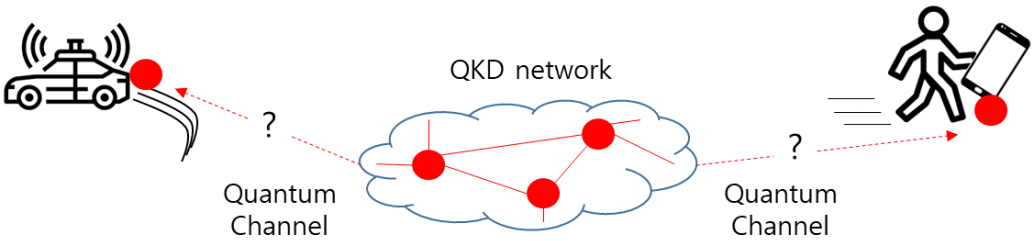
5 Conventions

None

6 Introduction

Based on [ITU-T Y.3800], many study items are successfully developed and developing so far. However, in case that mobile objects (i.e., autonomous car, mobile phone, etc.) are to be supplied QKD service, there is a difficulty to establish and maintain a quantum channel stably with them, for the purpose of KSA-keys delivery.

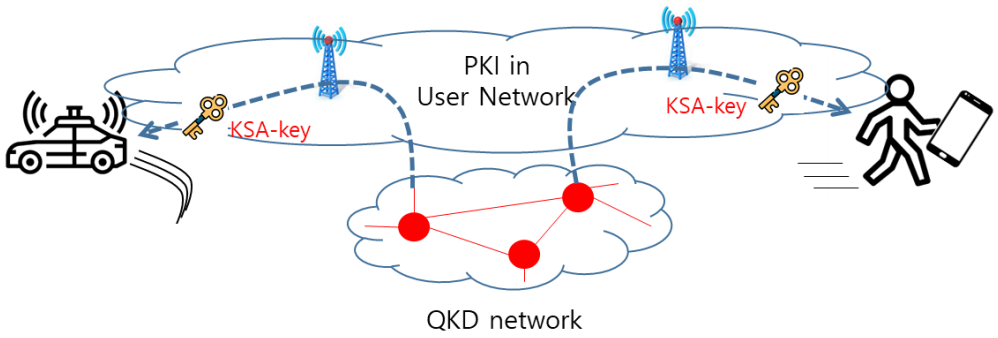
Even though Pointing, Acquisition and Tracking (PAT) technology are combined with free-space QKD modules, it is expected that the required accuracy for the quantum channel is difficult to achieve, due to the unpredictability of the movement and corresponding position of the mobile objects. It means that QKDN cannot support standalone the E2E cryptography service between the car and the mobile phone on this situation.



<Figure 1. An example of QKD network in the mobile object environment >

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

In order to overcome the difficulty for the 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 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 makes a problem against quantum computer's attack, since cryptographic algorithms in existing PKI architecture are known as non-quantum safe. To address quantum-safe, overhauling existing PKI architecture is required as existing algorithms become obsolete.

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

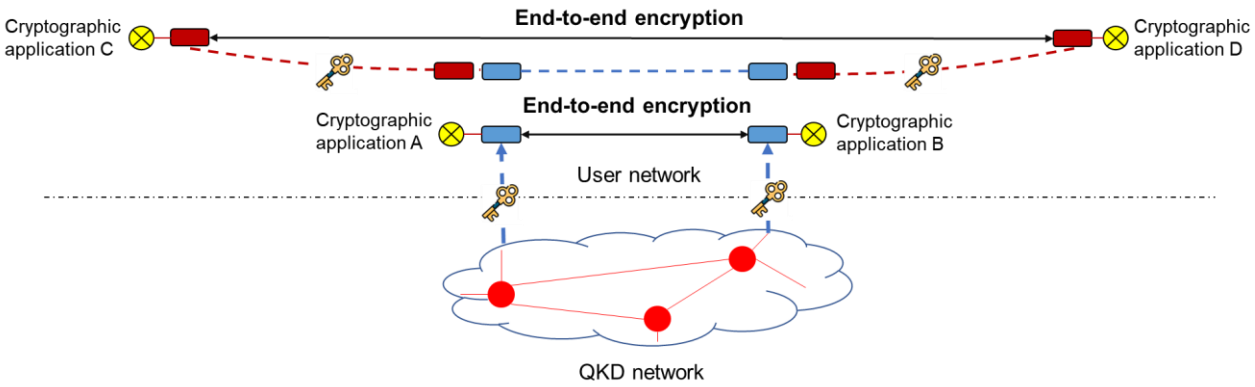
Note - The study of PQC is out of scope of this document.

From this point of view, it is recommended that the integration of QKDN and PKI with PQC algorithm should be studied for the extension of QKD service availability and market penetration for QKD service provider. Considering this study is just one of 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 the QKDN and QKD service providers, bringing its cryptography service to a much wider range of business opportunity.

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

Figure 3 shows the QKDN's role in 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 cyber-attacks 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 end-to-end cryptography service.>

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

Note: How to generate and distribute cryptographic keys is out of scope in this Supplement.

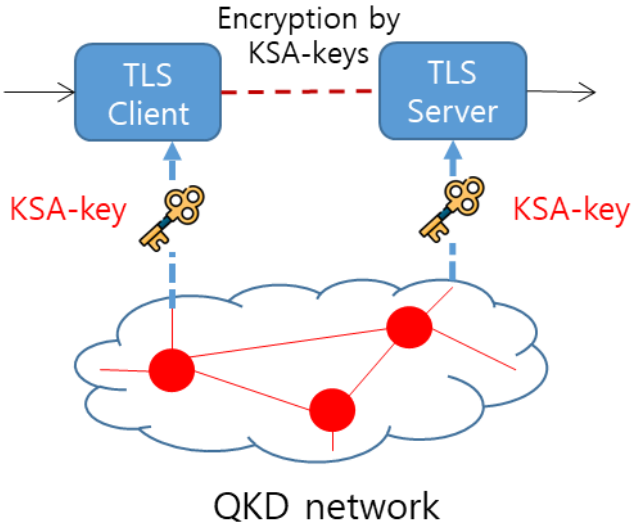
From modern cryptographic technology's perspective, 3 types of cryptographic service are possible. They are E2E encryption by KSA-keys, E2E encryption by classical keys, and E2E cryptographic services combining both encryption by KSA-keys and encryption by other classical keys.

- E2E encryption by KSA-keys (including where hybrid with other classical keys); In this type, QKDN should provide KSA-keys in each end-point of the cryptographic service in the User Network. This type is the basic assumption of ITU-T Y.3800-series.
- E2E encryption by classical keys; This type has been specified in many modern cryptographic technology-related ITU Recommendations and other SDOs standards including [ITU-T X.805].
- 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 in end-to-end cryptography services with non-quantum cryptography

8.1 Use Case 1

In this use case, KSA-keys generated from QKDN supply to 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, so called TLS handshake.



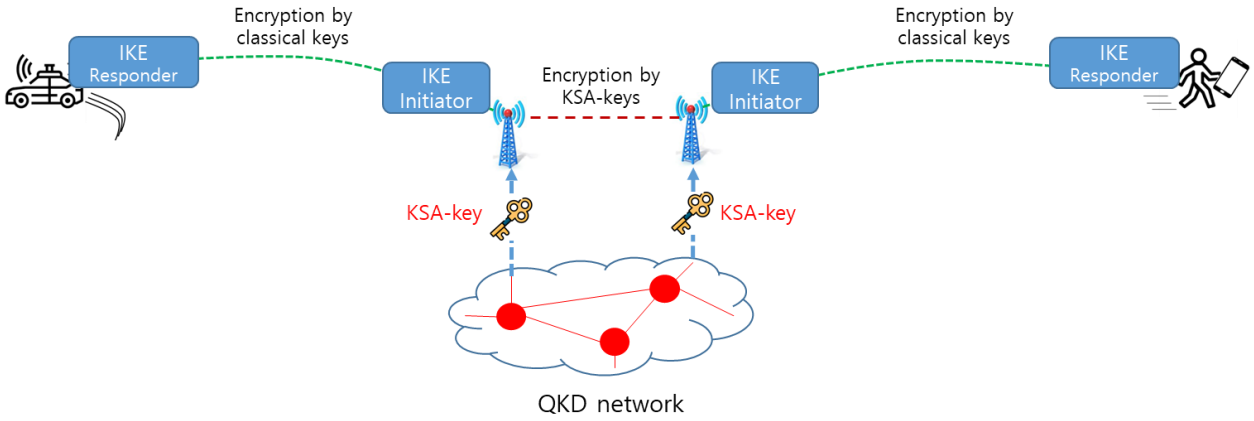
<Figure 4. Configuration of Use case 1>

NOTE 1 – It is assumed that TLS client and server, and QKD module and key manger (KM) are located in the same trusted node together. 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 illustration of the conceptual structures of a QKDN and a Use Network. But, in this Figure 3, cryptographic application is not a part of Trusted Node in align with QKDN.

8.2 Use Case 2

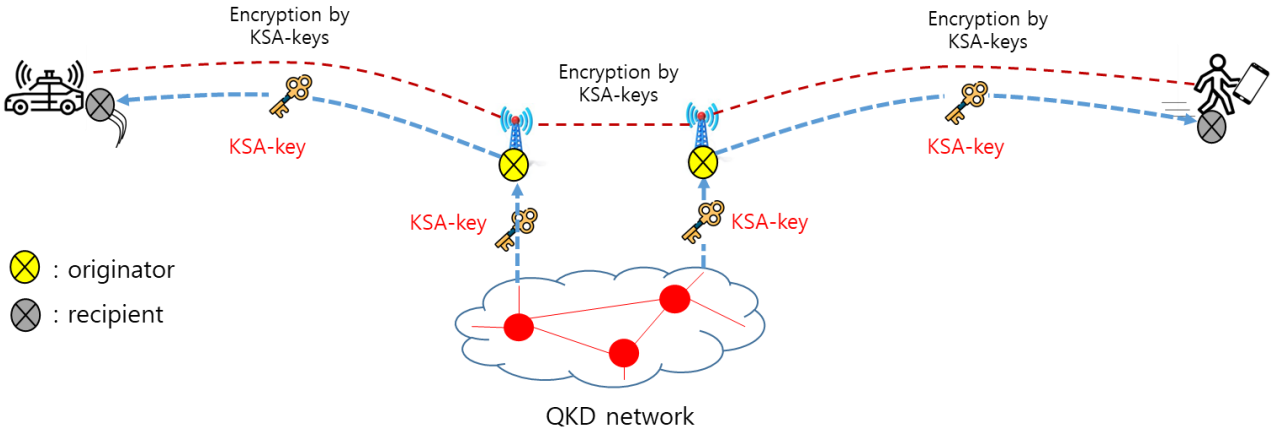
In this use case, KSA-keys generated from QKDN supply only to the corresponding portion for encryption by KSA-keys. The other end portions are encrypted by the cryptographic keys derived from modern cryptography, i.e., IKE protocol.



<Figure 5. Configuration of Use case 2>

8.3 Use Case 3

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



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 in the same Trusted Node together, 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.

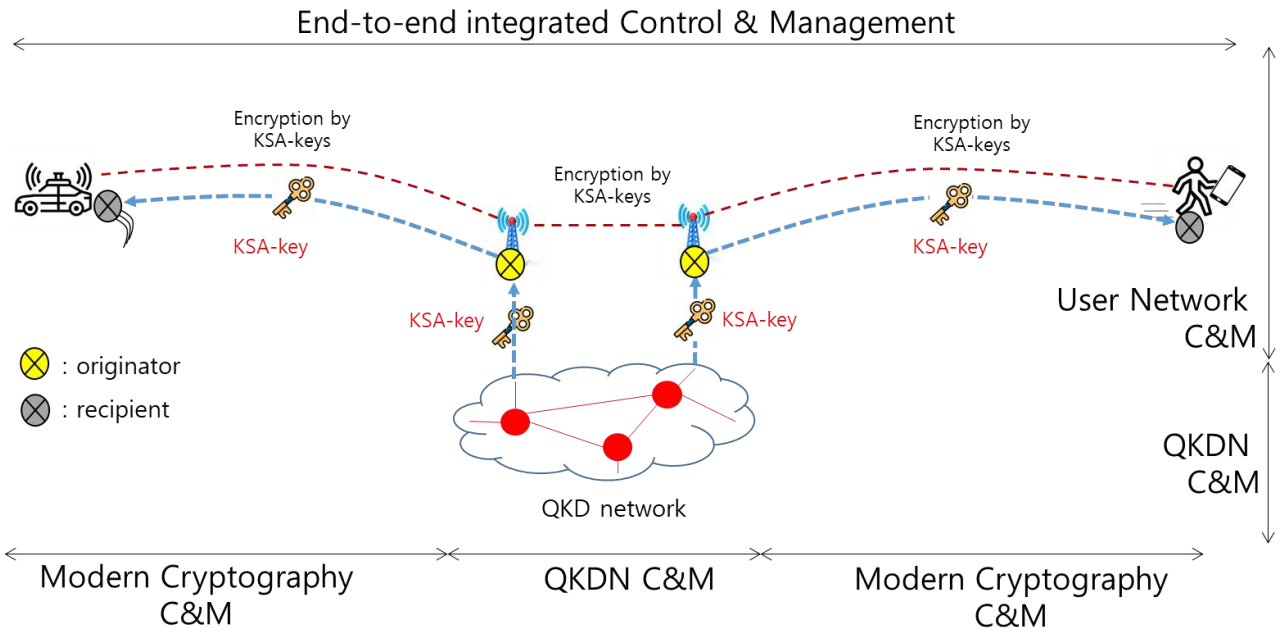
9.1.2 Use Case 2 & 3

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

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

9.1.3 Control and management implications of Use Cases

The integration of QKDN and modern cryptography introduces some control and management implications. 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 QoS aspect

From the QKDN 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, which means non-quantum network, 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, it passes through both 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 user network.

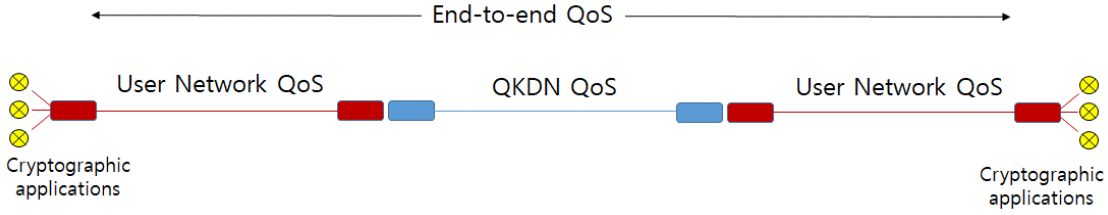


Figure 8. End-to-end QoS domain for cryptographic applications

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 QKDN and User Network

Control and management capabilities associated with safe and reliable E2E key delivery need to be studied in Q.16 and Q.6 of SG13. Since Q.16 is responsible for QKDN control and management, the integrated control and management can be under its responsibility. And QoS control and management for integrated E2E QKD can be studied in Q.6. Control and management in the integrated environment may need 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 to 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 suitable 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-ETSI GR QKD 007] ETSI Group Report QKD 007 V1.1.1 (2018), Quantum key distribution (QKD); Vocabulary

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

[b-IETF RFC 4306] IETF RFC 4306 (2005), Internet Key Exchange (Kev2) Protocol

[b-ITU-T Y.3806] Quantum key distribution networks – Requirements for quality of service assurance

[b-ITU-T Y.3807] Quantum key distribution networks – Quality of service parameters

[b-ITU-T Y.3811] Quantum key distribution networks – Functional architecture for quality of service assurance

[b-ITU-T Y.1540] Internet protocol data communication service – IP packet transfer and availability performance parameters

[b-ITU-T Y.3106] Quality of service functional requirements for the IMT-2020 network

_____