International Telecommunication Union

ITU-T Technical Report

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(20 May 2022)

XSTR-HYB-QKD

Overview of hybrid approaches for key exchange with quantum key distribution

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.

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.

Technical Report ITU-T XSTR-HYB-QKD

Overview of hybrid approaches for key exchange with quantum key distribution

Summary

This Technical Report provides a landscape of the standardization activities on hybrid approaches for migration towards quantum-safe algorithms or protocols within international, regional and national organizations. The hybrid approach that is covered by this Technical Report is for key exchange.

Hybrid approaches for key exchange consist of generating a key exchange functionality by combining at least two different key exchange methods.

This Technical Report studies the possible way forward to accommodate quantum key distribution protocols in the context of hybrid approaches for key exchange. This compatibility is studied for generic hybrid key exchange and hybrid key exchange that is specific to certain communication protocols.

Keywords

Hybrid approaches, QKD, QKDN.

Table of Contents

		Page
1	Scope	1
2	References	1
3	Definitions	2
	3.1 Terms defined elsewhere	2
4	Abbreviations and acronyms	2
5	Introduction to hybrid approaches to quantum-safe security methods	3
6	Overview of standardization activities on hybrid approaches for key exchange mechanisms	5
	6.1 Standards addressing concepts of hybrid approaches for key exchange	5
	6.2 Standards allowing hybrid approaches for key exchange in protocols	7
7	Gap analysis of compatibility of keys provided by QKD networks with hybrid key exchange methods	8
	7.1 Standards addressing concepts of hybrid approaches for key exchange	9
	7.2 Standards allowing hybrid approaches for key exchange in protocols	10
Bibliography		13

Technical Report ITU-T XSTR-HYB-QKD

Overview of hybrid approaches for key exchange with quantum key distribution

1 Scope

This Technical Report describes:

– an overview on various hybrid approaches for migration towards quantum-safe algorithms or protocols that have been developed or are still under development within SDOs (hybrid approaches for key exchange consist of generating a key exchange functionality by combining at least two different key exchange methods);

– a study of the compatibility of usage of symmetric keys provided by quantum key distribution (QKD) networks with these hybrid approaches (this study will include approaches for key exchanges);

– an identification of possible missing aspects in standards to use QKD with certain secure communication protocols.

2 References

[ITU-T X.1714] Recommendation ITU-T X.1714 (2020), *Key combination and confidential key supply for quantum key distribution networks.*

[BSI TR-02102-1] BSI Technical Guideline TR-02102-1 (2022), *Cryptographic Mechanisms: Recommendations and Key Lengths.*

[ETSI GS QKD 004] ETSI group Specification GS QKD 004 V2.1.1 (2020), *Quantum Key Distribution (QKD); Application Interface.*

[ETSI GS QKD 014] ETSI Group Specification GS QKD 014 V1.1.1 (2019), *Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API.*

[ETSI TS 103 744] Technical Specification ETSI TS 103 744 V1.1.1 (2020), *CYBER; Quantum-safe Hybrid Key Exchanges.*

[IEEE 802.1AE] IEEE Std 802.1AE-2018, *802.1AE: MAC Security (MACsec).*

[IETF IKEv2] IETF IKEv2 (2022), *Multiple Key Exchanges in IKEv2 draft-ietf-ipsecme-ikev2-multiple-ke-05.*

[IETF IKEv2(03)] IETF IKEv2(03) (2022), *Multiple Key Exchanges in IKEv2 draft-ietf-ipsecme-ikev2-multiple-ke-03.*

[IETF PQ KEM] IETF PQ KEM (2021), *Hybrid Post-Quantum Key Encapsulation Methods (PQ KEM) for Transport Layer Security 1.2 (TLS) draft-campagna-tls-bike-sike-hybrid-07.*

[IETF RFC 5246] IETF Standard RFC 5246 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2.*

[IETF RFC 7296] IETF Standard RFC 7296 (2014), *Internet Key Exchange Protocol Version 2 (IKEv2).*

[IETF RFC 8784] IETF Standard RFC 8784 (2020), *Mixing Pre-shared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security.*

[NIST SP 800-56A Rev.3] NIST Special Publication 800-56A Revision 3 (2018), *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography*.

[NIST SP 800-56B Rev.3] NIST Special Publication 800-56B Revision 3 (2014), *Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography*.

[NIST SP 800-56C Rev.2] NIST Special Publication 800-56C Revision 2 (2020), *Recommendation for Key-Derivation Methods in Key-Establishment Schemes*.

[NIST SP 800-133 Rev.2] NIST Special Publication 800-133 Revision 2 (2020), *Recommendation for Cryptographic Key Generation.*

3 Definitions

3.1 Terms defined elsewhere

This Technical Report uses the following terms defined elsewhere:

3.1.1 cryptographic key [ETSI TS 103 744]: Binary string used as a secret by a cryptographic algorithm

3.1.2 key agreement scheme [ETSI TS 103 744]: Key-establishment procedure in which the resultant secret keying material is a function of contributions of the entities participating, such that no entity can predetermine that value of the secret keying material independently of the other entities' contributions

3.1.3 key derivation [ETSI TS 103 744]: Process to derive key material from one or more shared secrets.

3.1.4 key encapsulation mechanism [ETSI TS 103 744]: Method to secure the establishment of a cryptographic key for transmission using public key cryptography.

3.1.5 key establishment/exchange method [ETSI TS 103 744]: Cryptographic procedure by which cryptographic keys are established between two parties.

3.1.6 public key [ETSI TS 103 744]: Key in an asymmetric cryptographic scheme that can be made public without loss of security.

3.1.7 private key: Key in an asymmetric cryptographic scheme that is kept secret.

3.1.8 public key cryptography [ETSI TS 103 744]: Cryptographic system that utilizes a pair of keys, a private key known only to one entity and a public key which can be openly distributed without loss of security.

3.1.9 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.

3.1.10 shared secret [ETSI TS 103 744]: Secret value that has been computed using a key-establishment scheme.

4 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

DH Diffie-Hellman

ECC Elliptic Curve Cryptography

ECDH	Elliptic Curve Diffie-Hellman
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
HMAC	Hash-based Message Authentication Code
IKE	Internet Key Exchange
IPsec	Internet Protocol security
KEM	Key Encapsulation Mechanism
MACsec	Medium Access Control security
OSI	Open System Interconnection
OTN	Optical Transport Network
PPP	Point to Point Protocol
PQC	Post-Quantum Cryptography
QKD	Quantum Key Distribution
QKDN	Quantum Key Distribution Networks
RSA	Rivest, Shamir and Adelman
SDO	Standards Development Organization
SIKE	Supersingular Isogeny Key Encapsulation
SSL	Secure Session Layer
TLS	Transport Layer Security
VPN	Virtual Private Network
XOR	Exclusive-Or

5 Introduction to hybrid approaches to quantum-safe security methods

Quantum computing has become a serious threat to the security of existing and future communication networks. It could solve certain computational problems, such as integer factorization (which underlies the Rivest, Shamir and Adelman (RSA) encryption) and discrete logarithm (which underlies the Diffie-Hellman key sharing), substantially faster than classical computers. The migration of legacy networks to quantum-safe (i.e., secure against quantum computing) networks is a complex task that needs to be well prepared. In this context, several standards development organizations (SDOs) have developed or are developing standards on the topic of quantum-safe security.

SG17 has been studying work items for security requirements for quantum key distribution network (QKDN) and X.1710 [b-ITU-T X.1710] and X.1714 [ITU-T X.1714] have been published. X.1710 is for the security framework for QKDN and specifies overall requirements for QKDN. X.1714 describes key combination methods for QKDN and specifies security requirements for both key combinations and confidential key supplies from QKDN to cryptographic applications.

There has been intensive standardization activity on post-quantum cryptography aiming to evaluate and standardize quantum-resistant public-key cryptographic algorithms including from 2017 under the NIST post-quantum cryptography (PQC) standardization process.

However, several gaps are identified as follows:

Most standardization activities on hybrid key exchange schemes have been envisioned and performed by experts in post-quantum cryptography. In spite of the QKD protocols being key exchange protocols the resulting standards and those under development that are compatible with the QKD have not yet been verified. Hence, hybrid approaches for key exchanges consist of generating key

exchange functionalities by combining at least two different key exchange methods that can be considered. Nevertheless, these hybrid approaches for key exchange might not be directly applicable to QKD based on the existing standards.

To overcome these gaps, various efforts have been made to exploit QKD in existing communication networks to improve their security. Much research has also integrated QKD with protocols in different layers of the open system interconnection (OSI) model.

While the use of QKD in fiber optical networks has advanced significantly in recent years, research and development on applications of QKD within different OSI layers are still at an early stage. QKD establishes shared secret keys, so that it can potentially be substituted for other symmetric key primitives in appropriate use cases. Compared with physical layer implementations such as the optical transport network (OTN), protocols in higher layers are more likely to have been designed to permit the replacement of cryptographic primitives.

Examples of such research efforts are the integration of QKD point-to-point protocol (PPP) [b-Ghernaouti-Hélie 2005] and a medium access control security (MACsec) [b-Cho 2021] at the data link layer (i.e., OSI layer 2), and the integration of QKD with the Internet protocol security (IPsec) [b-Sfaxi 2005] at the network layer (i.e., OSI layer 3). Furthermore, integration of QKD at the transport layer (i.e., OSI layer 4) with a secure session layer (SSL) / TLS [b-Mink 2009] has also been attempted.

On the data link layer, QKD can be used as a key exchange protocol for PPP which is a data link protocol that connects two nodes [b-Ghernaouti-Hélie 2005].

Medium access control security (MACsec) is an IEEE 802.1AE standard [IEEE 802.1AE] for secure communication on Ethernet links. MACsec ensures the confidentiality, integrity and origin of the authenticity of the Ethernet frames in the local area networks. The secrecy of MACsec stems from a root key that is either configured as a pre-shared key or derived from a mutual authentication protocol.

QKD can be used in MACsec for secure Ethernet networks [b-Cho 2021].

For the network layer and transport layer, both Internet protocol security (IPsec) and the transport layer security (TLS) develop a shared secret and then use it to compute keys for encryption and integrity protection.

Internet protocol security (IPsec) is a suite of protocols that provides security to the Internet protocol (IP) communications at the network layer by authenticating and encrypting IP data packets. IPsec is often used to provide a virtual private network (VPN), either between two locations or between a remote device and an enterprise network. IPsec can also provide end-to-end security. Internet key exchange (IKE) is the protocol used to set up a security association in the IPsec protocol suite. IKE uses a Diffie-Hellman (DH) 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.

Transport layer security (TLS) is a transport layer protocol which provides end-to-end security for network communication services. TLS is based on the earlier secure sessions layer (SSL) protocol and is explicitly invoked by an application. Although it is widely used in various applications, its most common use is to encrypt traffic between a web server and a browser.

QKD keys can be used as a shared secret for a TLS session. In this case, QKD keys would replace the Diffie-Hellman (DH) shared secret thereby eliminating the need to calculate a DH shared secret [b-Mink 2009].

The above approaches help in moving towards the utilization of QKD technologies for enhancing the security of modern computing applications on the Internet.

6 Overview of standardization activities on hybrid approaches for key exchange mechanisms

This clause describes the landscape of activities of various SDOs on hybrid approaches for key exchange mechanisms.

6.1 Standards addressing concepts of hybrid approaches for key exchange

NOTE – 'Concepts of hybrid approaches for key exchange' should be understood as the cryptographic mechanisms specified in the standards which allow the establishment of cryptographic keys resulting from two or more key exchange methods.

6.1.1 International standards

6.1.1.1 ITU-T X.1714

[ITU-T X.1714] describes key combination methods for QKDN and specifies security requirements for both key combinations and key supplies from QKDN to the cryptographic applications. In particular, this Recommendation addresses the following points:

– security of the combination of keys exchanged through a QKDN and keys exchanged through other key exchange methods;

– security of the key supply from a QKDN to the cryptographic applications.

6.1.2 Regional standards

6.1.2.1 European standards

There are three European SDOs: CEN, CENELEC and ETSI. At the time of the writing (May 2022), standardization activities on hybrid approaches for key exchanges could be found only within the ETSI technical committee CYBER QSC.

6.1.2.1.1 ETSI TS 103 744, Quantum-safe hybrid key exchanges

ETSI TC CYBER QSC published a technical specification on quantum-safe hybrid key exchanges in December 2020. This technical specification addresses the concept of hybrid approaches for key exchanges by specifying two methods for deriving cryptographic keys from multiple shared secrets. These shared secrets might be established either by using a quantum-safe, an unsafe quantum-safe cryptographic method or by any other means for establishing a pre-shared secret.

[ETSI TS 103 744] specifies that one of the key agreement schemes [shall] be elliptic curve Diffie-Hellman as defined in clause 5.7.1.2 of [NIST SP 800-56A Rev.3]. This standard specifies several cryptographic primitive algorithms that are used e.g., hash functions, pseudorandom functions or key derivation functions.

Two types of hybrid key agreement schemes are specified by TC CYBER QSC. The first scheme is called 'concatenate hybrid key agreement scheme', the second is the 'cascade hybrid key agreement scheme'.

The first scheme consists of running all the key agreement schemes in parallel. The messages exchanged between the initiator and the responder are the result of the concatenation of the messages generated by each key agreement scheme at each step of the hybrid key agreement scheme. Furthermore, the shared secret that will be used as an input of the key derivation function is the result of the concatenation of the secrets established with each key agreement scheme and one optional pre-shared key.

The second scheme consists of running the key agreement schemes sequentially. In this case, each message exchanged between the initiator and the responder will be related to one step of one of the key agreement schemes. The final key material is computed by applying as many iterations of the key derivation function as the number of key agreement schemes composing the hybrid key agreement

scheme. The results of each iteration of the key derivation function are a secret and includes some key material. The input secret of the *ith* iteration is obtained with the secret exchanged by the *ith* key agreement scheme and the secret that has been computed at the (i-1)th iteration. At the first iteration, the input secret may be obtained with the secret exchanged by the first key agreement scheme and a pre-shared secret.

[ETSI TS 103 744] indicates that a pre-shared key for the first scheme (concatenate hybrid key agreement scheme) and the second scheme (cascade hybrid key agreement scheme) may be established using a previous session or an alternative key-establishment method like the QKD.

NOTE – TC CYBER QSC was initiated in June 2021 to revise [ETSI TS 103 744].

6.1.3 National standards

NOTE – At the time of writing, activities on hybrid key exchange schemes can be found only in the United States of America (USA) and the Federal Republic of Germany.

6.1.3.1 NIST standards (USA)

NIST has no standard dedicated to hybrid key exchanges. However, NIST provides recommendations on various options to securely generate symmetric keys from several symmetric keys or values ([NIST SP 800-133 Rev.2]), and on one way to combine several secrets established by various key exchange schemes, to generate, from multiple secrets, one secret that is used as input for a key derivation method. ([NIST SP 800-56C Rev.2]).

6.1.3.1.1 Clause 6.3 of [NIST SP 800-133 Rev.2]

[NIST SP 800-133 Rev.2] is a recommendation for cryptographic key generation. The 2nd revision of this recommendation was published in June 2020. Clause 6.3 of this document is dedicated to symmetric keys produced by combining (multiple) keys and other data. The combination schemes that are described in clause 6.3 can serve to generate a symmetric key from the keys established by multiple key exchanges.

NOTE – In the context of [NIST SP 800-133 Rev.2], 'keys' are the cryptographic keys that are established by key exchange schemes approved by the NIST. While 'other data' are strings that might either be secret or not. In particular, 'other data' might be keys that are established with key exchange schemes that are not approved by NIST, such as the ones based on all quantum-safe cryptographic algorithms or QKD.

Three methods are recommended by NIST to generate symmetric keys from the combination of keys and other data. One important requirement of the keys and other data that are combined is that they are independent from each other.

1) The first method consists of the concatenation of two or more keys. The length of the generated key equals the sum of the lengths of the keys that have been concatenated.

   NOTE – This method does not allow the use of other data (e.g., keys exchanged with not approved key exchange methods).

2) The second method consists of the XOR (exclusive-or)ing keys and items of data. The length of each key or item that is used as input [shall] be equal to the required length of the resulting symmetric key.

3) The third method consists of a key extraction process. The final symmetric key results from a hash-based message authentication code (HMAC) function applied on the concatenation of the (multiple) keys and the other data. The hash result might be truncated to generate a final key with a length matching the required key length.

6.1.3.1.2 Clause 2 of [NIST SP 800-56C Rev.2]

[NIST SP 800-56C Rev.2] is a recommendation for key derivation methods in key establishment schemes. The 2nd revision of this recommendation was published in August 2020. Clause 2 is dedicated to the scope and purpose of the document. Clause 2 introduces the structure of hybrid shared secrets that can be used as input for key derivation methods.

This standard allows the use of a hybrid shared secret, called Z', that results from the concatenation of a shared secret, called Z, established using a secret establishment scheme approved by the NIST and of an auxiliary shared secret, called T, established using some other methods. The key derivation methods specified in SP 800-56C Rev.2 process Z' is in the same manner as Z. This means that a cryptographic key can be derived from a secret generated using two different secret establishment methods.

NOTE – In [NIST SP 800-56C Rev.2], there is no restriction on the method that can be used to generate the auxiliary shared secret T.

6.1.3.2 BSI standards (Germany)

BSI has no standard dedicated to hybrid key exchanges. However, BSI provides recommendations on one option for the use of quantum-safe cryptographic key exchanges ([BSI TR-02102-1]).

6.1.3.2.1 Clause 3.2 of [BSI TR-02102-1]

[BSI TR-02102-1] is a technical guideline assessing the security and long-term orientation for BSI selected cryptographic mechanisms. Version 2022-01 of this technical guideline was published in January 2022. Clause 3.2 provides technical statements and recommendations on quantum-safe cryptography. It addresses the combination of classical and PQC security.

[BSI TR-02102-1] recommends the use of quantum-safe cryptographic algorithms only when they are combined with classical elliptic curve cryptography (ECC) – or an RSA-based key exchange or key transport. The secret generated with one classical key establishment method [should] be combined with the secret generated with one quantum-safe key establishment method using a key derivation method specified in section B.1.1 of the same document.

NOTE – BSI recommends only the use of FrodoKEM-976, FrodoKEM-1344 and Classical McEliece as quantum-safe cryptographic algorithms.

6.2 Standards allowing hybrid approaches for key exchange in protocols

NOTE 1 – 'Hybrid approaches for key exchange in protocols' should be understood as variations of certain protocols specified in the standards allowing the establishment of cryptographic keys resulting from two or more key exchange methods.

NOTE 2 – Although IETF Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time according to IETF. All the Internet Drafts were analysed at the time of writing to give gap analysis which is the purpose of this Technical Report and there is no intention to propose any use of any specific IETF Internet-Drafts for key exchange in protocols.

6.2.1 International standards

NOTE – No standard, published or under study within ISO, IEC, or ITU, introducing the concept of hybrid approaches can be found at the time of writing.

6.2.1.1 IETF RFC 8784

[IETF RFC 8784] is an IETF standard for mixing pre-shared keys in the Internet exchange protocol version 2 (IKEv2) for post-quantum security. This IETF standard was published in June 2020. This document describes an extension of IKEv2 to allow it to exploit alternative key exchange mechanisms by using pre-shared keys.

[IETF RFC 8784] was written under the assumption that each IKE peer has a list of pre-shared keys along with their associated identifiers that can be shared using any kind of post-quantum key exchange method. [IETF RFC 8784] also introduces notifications that allow the initiator and the responder to either use or not pre-shared keys in their IKEv2 transaction. The decision not to use pre-shared keys can be taken by one of the two parties that are present in the several steps of the protocol. In this case, the initiator and the responder use the conventional IKEv2 protocol. When a pre-shared key is used, they are combined with the three subkeys generated from the conventional IKEv2

protocol specified in [IETF RFC 7296]. The combination of the subkeys with the pre-shared keys is performed with a pseudorandom function.

NOTE – [IETF RFC 8784] does not specify the key exchange methods that can be used to exchange the pre-shared secrets.

6.2.1.2 IETF draft-ietf-ipsecme-ikev2-multiple-ke-05 (work in progress)

IETF draft-ietf-ipsecme-ikev2-multiple-ke-05 [IETF IKEv2] is an IETF draft for multiple key exchanges in IKEv2. Its fifth draft will expire in September 2022. This document describes an extension of IKEv2 to allow multiple key exchanges while computing a shared secret during a security association setup.

[IETF IKEv2(03)] aims at updating [IETF RFC 7296] by giving the possibility of using alternative key exchange methods in addition to the Diffie-Hellman key exchange methods specified in [IETF RFC 7296]. The different key exchange methods are performed successively. The secrets established from each key exchange are combined to generate a shared secret that will be used in the same manner as the way the shared secret established with a Diffie-Hellman key exchange is used in [IETF RFC 7296]. The secret established with the n^{th} key exchange is combined with the intermediate keys resulting from the (n-1) first key exchanges using the pseudorandom functions.

NOTE – [IETF IKEv2] does not specify the additional key exchange methods. However, algorithms resistant to quantum computer attacks are mentioned as a possibility.

6.2.1.3 IETF draft-campagna-tls-bike-sike-hybrid-07 (work in progress)

IETF draft-campagna-tls-bike-sike-hybrid-07 [IETF PQ KEM] is an informative IETF draft for hybrid post-quantum key encapsulation methods (PQ KEM) for the transport layer security 1.2 (TLS). Its seventh draft expired in March 2022. This document is intended to define hybrid key exchanges in sufficient detail to allow independent experimentations to interoperate.

[IETF PQ KEM] describes additions to TLS to support PQ hybrid key exchanges, applicable to TLS version 1.2 [IETF RFC 5246]. The defined hybrid key exchange combines the shared secrets established by two key exchange methods. One key exchange method is based on the elliptic-curve Diffie-Hellman ephemeral (ECDHE). The other can be based either on a supersingular isogeny key encapsulation (SIKE) or Kyber. These three algorithms are part of the 3^{rd} round of the NIST standardization process of key exchange algorithms that are resistant to quantum computer attacks. The hybrid premaster secret that will serve as TLS 1.2 [IETF RFC 5246] pre-master secret results from the concatenation of both shared secrets.

6.2.2 Regional standards

NOTE – No standard, published or under study within regional SDOs, introducing hybrid key exchange methods for protocols, can be found at the time of writing.

6.2.3 National standards

NOTE – No standard, published or under study within national SDOs, introducing hybrid key exchange methods for protocols, can be found at the time of writing.

7 Gap analysis of compatibility of keys provided by QKD networks with hybrid key exchange methods

This clause describes a study of the compatibility of keys provided by QKD networks with these hybrid approaches for key exchanges identified in clause 6 and the related gap analysis.

7.1 Standards addressing concepts of hybrid approaches for key exchange

7.1.1 Introduction

Several standards specifying cryptographic mechanisms for implementation of hybrid key exchanges have been published recently or are still under study. Those standards are mainly written with an objective to combine currently used cryptographic algorithms (e.g., Diffie-Hellman) with emerging cryptographic algorithms that are considered as robust against quantum computing. QKD technologies offer an alternative method for exchanging keys in a secure manner under the quantum computing threat. Therefore, the combination of key exchange cryptographic algorithms with QKD technologies might not always be allowed by the standards addressing the concepts of hybrid approaches for key exchange that have been described previously.

The following subclauses evaluate the compatibility of QKD keys and technologies with those standards. In case there is incompatibility, additional standards are suggested to reach compatibility.

7.1.2 [ETSI TS 103 744] Quantum-safe hybrid key exchanges

[ETSI TS 103 744] is a European standard that mentions QKD as one possible key-establishment method in relation to quantum-safe key exchanges. The standard is based on the assumption that hybrid key agreement schemes will employ key exchange mechanisms that will utilise public keys and QKD is not in this class of cryptographic mechanisms. However, the key derivation function takes an optional pre-shared secret and QKD is mentioned as a possible key establishment method for the pre-shared secret key.

QKD cannot be used to establish the shared secrets between the initiator and the responder as part of the communications specified within the hybrid key agreement schemes. However, QKD keys can be combined with keys from public-key methods under [ETSI TS 013 744] by using them as pre-shared secret keys.

This limitation does not significantly impact the interoperability between QKD networks and applications consuming QKD keys. Indeed, QKD is a quantum-safe key establishment mechanism that typically establishes keys out-of-band from secure applications using a quantum channel in addition to the classical communications channel(s).

In summary, [ETSI TS 103 744] has been designed primarily for quantum-safe public key exchange mechanisms. However, it allows the use of QKD as one option to establish pre-shared secret keys for use in a hybrid key agreement scheme.

7.1.3 Clause 6.3 of [NIST SP 800-133 Rev.2]

[NIST SP 800-133 Rev.2] is a US standard that is written in a way that allows the use of secret keys established with unapproved key exchange mechanisms. In this case, these secret keys are called 'other data'. NIST considers that this 'other data' can be secret or not. Secret keys established with approved key exchange mechanisms are called 'keys' in NIST standards. QKD technologies are considered by NIST as unapproved key exchange mechanisms. Therefore, QKD keys can only play the role of the 'other data' when implementing [NIST SP 800-133 Rev.2].

NOTE – In the context of NIST standards, 'approved' algorithm or technique is an algorithm or technique that is either 1) specified in a Federal Information Processing Standard (FIPS) or NIST Recommendation, or 2) adopted in a FIPS or NIST Recommendation.

As described in clause 6.1.3 of this Technical Report, only the second and third methods specified in clause 6.3 of [NIST SP 800-133 Rev.2] allow the use of 'other data'. The second method consists of XORing all the keys and other data to generate the resulting key. The third method consists of extracting the resulting key from a secret consisting in the concatenation of all keys and other data. In both cases, keys and other data are used in the same manner.

In summary, two methods specified in [NIST SP 800-133 Rev.2] allow the use of QKD technologies to implement quantum-safe hybrid key exchanges in combination with at least one approved key exchange mechanism.

7.1.4 Clause 2 of [NIST SP 800-56C Rev.2]

[NIST SP 800-56C Rev.2] is a US standard that specifies two key derivation methods. These methods can be applied to a shared secret resulting from the concatenation of several shared secrets. The NIST standards are written in a way that allows the use of shared secrets, called 'auxiliary secrets', established with not-approved methods. The methods for establishment of shared secrets that are approved by NIST are specified in [NIST SP 800-56A] and [NIST SP 800-56B].

QKD technologies do not match the specifications given by [NIST SP 800-56A] and [NIST SP 800-56B]. Therefore, QKD keys can only be used as an 'auxiliary secret'. 'Auxiliary secrets' are treated in the same manner as 'shared secrets' in [NIST SP 800-56C Rev.2].

In summary, an implementation of [NIST SP 800-56C Rev.2] allows the use of the QKD keys as an 'auxiliary secret'. This allows the implementation of quantum-safe hybrid key exchanges with QKD technologies as long as at least one approved method for the establishment of shared secrets is used.

7.1.5 Clause 3.2 of [BSI TR-02102-1]

[BSI TR-02102-1] is a German technical guideline specifying the hybrid key exchange mechanisms and the key exchange mechanisms, including the quantum-safe mechanisms, approved by BSI. QKD technologies are not part of the approved quantum-safe key exchange mechanisms in the current version but BSI plans to make recommendations on protocols, authentication and the use of QKD in the medium-term once necessary preconditions are met. Furthermore, this technical guideline does not give any options to combine a key exchanged through an approved key exchange mechanism with another key exchanged through a not-approved key exchange mechanism.

In summary, [BSI TR-02102-1] does not allow the implementation of hybrid quantum-safe hybrid key exchanges with QKD technologies. This situation might stay unchanged as long as BSI does not approve QKD technologies as one option for key exchange mechanisms.

7.2 Standards allowing hybrid approaches for key exchange in protocols

7.2.1 Introduction

The compatibility of QKD technologies with key exchange protocols is more complex to study because QKD keys are established between the applications in an out-of-band manner. Indeed, the QKD keys are exchanged within the QKDN and are then delivered by nodes from this QKDN to applications.

The typical steps that should be considered when allowing the use of QKD keys within key exchange protocols are represented in Figure 1. In this figure, the lines with double arrows represent the interactions between two entities without any considerations if these interactions are bidirectional or unidirectional.

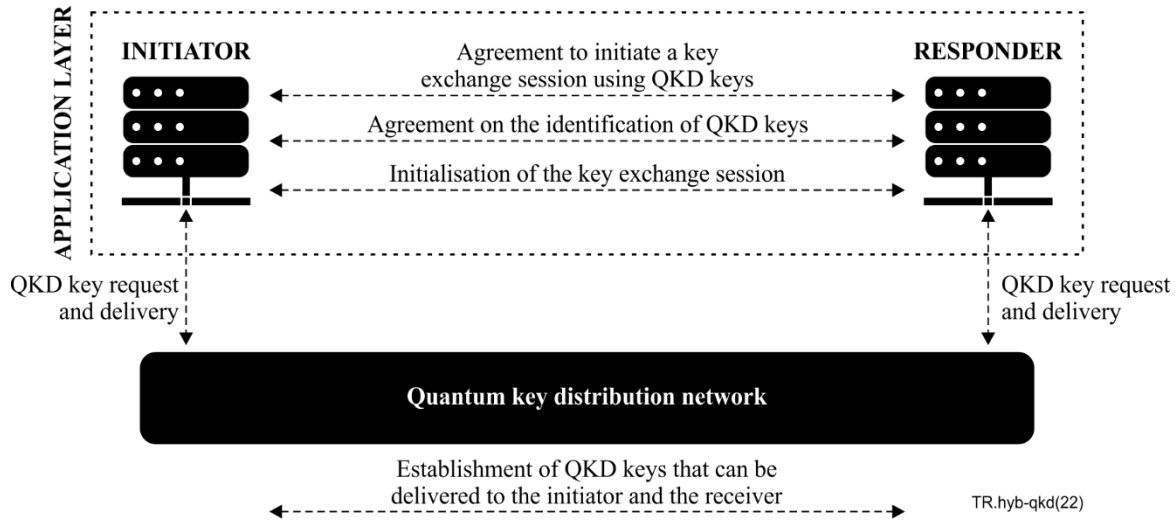

Figure 1 – Typical steps to consider when allowing the use of QKD keys within key exchange protocols

In the application layer represented in Figure 1, an initiator aims at exchanging a key with a responder via a key exchange protocol. If the initiator and the responder want to use the QKD keys in their protocol, they need to agree on the use of QKD keys and the identification of these QKD keys before initiating the key exchange session. The QKDN is in charge of establishing QKD keys that match the requests from the applications and delivering these keys to these applications. The compatibility evaluations in the following subclauses will be performed based on the protocol steps identified in Figure 1.

7.2.2 IETF RFC 8784

[IETF RFC 8784] is an IETF standard for mixing pre-shared keys in the Internet exchange protocol version 2 (IKEv2) for post-quantum security. Clause 3 of [IETF RFC 8784] specifies the notifications on the use of post-quantum pre-shared keys. These notifications are exchanged between the initiator and the responder. Depending on the notification of the responder, the applications may decide to abort, to use the standard IKEv2 protocol or to use the variation of IKEv2 with post-quantum pre-shared keys. In the latter case, the initiator sends a notification on the identifier of the post-quantum pre-shared key to the responder. The method to mix the post-quantum pre-shared keys with the secret exchanged with Diffie-Hellman exchange (as specified in [IETF RFC 7296]) is specified in clause 3 too.

The methods to exchange these pre-shared keys are not defined. Therefore, QKD is one option supported by this standard. However, the method proposed in [IETF RFC 8784] is limited to an initiator and a responder that is configured with fixed lists of pre-shared keys and pre-shared key identifiers. This standard does not cover dynamic changes of the pre-shared keys.

In summary, IETF RFC 8784 allows the use of the QKD technologies in the IKEv2 protocol. Nevertheless, QKD technologies can only be used as one method to create fixed lists of post-quantum pre-shared keys and key identifiers between the applications.

7.2.3 IETF draft-ietf-ipsecme-ikev2-multiple-ke-05 (work in progress)

IETF draft-ietf-ipsecme-ikev2-multiple-ke-05 [IETF IKEv2] is an IETF draft for multiple key exchanges in IKEv2. Its clause 3.2.1 specifies notifications to announce the alternative key exchange methods supported by the initiator and the responder. These notifications are exchanged between the initiator and the responder. When the initiator and the responder agree on one or more alternative key exchange methods, these alternative key exchange methods are mixed with Diffie-Hellman exchange (as specified in [IETF RFC 7296]) as specified in clause 3.2.2.

The alternative key exchange methods are not specified in [IETF IKEv2(03)] and should be specified in other standards. This makes QKD technologies one of the possible options for alternative key exchange methods in this potential update of IETF RFC 7296 (namely the standard IKEv2). To make this possibility concrete, standards on how applications can request and receive QKD keys from a QKDN need to be developed. This development can be based on one of the published standards specifying QKD key interfaces between applications and QKDN: [ETSI GS QKD 014] and [ETSI GS QKD 004].

7.2.4 IETF draft-campagna-tls-bike-sike-hybrid-07 (work in progress)

IETF draft-campagna-tls-bike-sike-hybrid-07 [IETF PQ KEM] is an IETF draft describing hybrid post-quantum key encapsulation methods (PQ KEM) for transport layer security 1.2 (TLS) [IETF RFC 5246]. This IETF draft proposes a TLS 1.2 extension that allows the use of one of the three post-quantum key encapsulation mechanisms BIKE, Kyber and SIKE in the combination of the standard elliptic curve Diffie-Hellman (ECDH) algorithm. The hybrid approach consists in the concatenation of the secret exchanged with ECDH and of the key exchange with the chosen post-quantum key encapsulation mechanism.

As the aim of [IETFPQ KEM] is to provide interoperability between different experiments, all the details of the proposed extension are very well specified. As QKD technologies are not part of the chosen quantum-safe key exchange methods, [IETF PQ KEM] is not compatible with QKD keys. Nevertheless, this IETF draft could serve as an example for the development of future TLS extensions that would give the possibility to use QKD keys. One way is to introduce QKD technologies as one of the supported quantum-safe key exchanges in [IETF PQ KEM]. This introduction should be preceded by the development of standards on how applications can request and receive QKD keys from a QKDN.

Bibliography

[b-ITU-T X.1710] Recommendation ITU-T X.1710 (2020), *Security framework for quantum key distribution networks.*

[b-ETSI GR QKD 007] ETSI GR QKD 007 (2018), *Quantum Key Distribution (QKD); Vocabulary*.
<https://www.etsi.org/deliver/etsi_gr/QKD/001_099/007/01.01.01_60/gr_qkd007v010101p.pdf>

[b-Cho 2021] Cho, J.Y. and Sergeev, A. (2021), *Using QKD in MACsec for secure Ethernet networks*.
<https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/qtc2.12006>

[b-Ghernaouti-Hélie 2005] Ghernaouti-Hélie, S. and Sfaxi, M.A. (2005), *Upgrading PPP security by Quantum Key Distribution*. Part of the IFIP – The International Federation for Information Processing book series (IFIPAICT, volume 229).
<https://link.springer.com/chapter/10.1007/978-0-387-49690-0_4>

[b-Mink 2009] Mink, A., Frankel, S., and Perlner, R. (2009), *Quantum Key Distribution (QKD) and Commodity Security Protocols: Introduction and Integration*. International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 2.
<https://airccse.org/journal/nsa/0709s9.pdf>

[b-Sfaxi 2005] Sfaxi, M.A., Ghernaouti-Hélie, S., Ribordy, G., and Gay, O. (2005). *Using Quantum Key Distribution within IPSEC to secure MAN communications*.
<https://www.researchgate.net/publication/236200262_Using_Quantum_Key_Distribution_within_IPSEC_to_secure_MAN_communications>