ETSI TR 103 617 V1.1.1 (2018-09)

TECHNICAL REPORT

Quantum-Safe Virtual Private Networks

Reference

DTR/CYBER-QSC-009

Keywords

quantum cryptography, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

Recent research in the field of quantum computing has brought about a credible threat to the current state-of-the-art for protecting electronic information [i.1]. The current data protection mechanisms that typically comprise cryptographic systems rely on computational hardness as a means to protect sensitive data. This is to say that there are cryptographic problems that are difficult or impossible to solve using conventional computing.

Because of recent advances in quantum computing, the quantum computer presents a serious challenge to widely used current cryptographic techniques and assumptions. This is because the quantum computer tends to excel at certain classes of problems. Among these problem classes are:

1) the integer factorization problem, which is used by the Rivest Shamir Adleman (RSA) cryptographic system; and

2) the discrete logarithms problem, which is used by Elliptic Curve Cryptography (ECC).

Both RSA and ECC are common public-key cryptographic techniques that are used to secure much of the interchange of information over the Internet as of 2017. While the integer factorization and discrete logs problems are difficult or practically impossible to solve using a conventional computer, they become fairly trivial for a quantum computer.

Academia, industry and governments have all made large investments in building a universal quantum computer powerful enough to break currently used public-key algorithms. Therefore, new solutions based on hard problems that cannot be efficiently solved by algorithms running on a quantum computer, such as Shor's algorithm, are needed to secure the existing cryptographic protocols [i.2]. Once the appropriate replacements for currently used cryptographic primitives are selected, these protocols can be updated. There is nevertheless an immediate harvest and decrypt threat from a quantum-capable adversary.

The deployment of Virtual Private Networks (VPNs) is a common choice for governments and enterprises to securely communicate between sites or to connect employees with offices.

Figure 1 describes how the harvest and decrypt attack would work against a VPN session. Each VPN session consists of two stages:

1) the handshake; and

2) data exchange between the two parties.

During the handshake stage, the peers are authenticated, and the symmetric keys are established. Once that has been completed, the peers can begin exchanging encrypted data securely.

For example, a secure communication session over a VPN can be harvested and stored today, then decrypted by an adversary with access to a quantum computer or array of quantum computers at a later date. An adversary with a quantum computer can then break the key establishment part of the handshake and derive the symmetric keys negotiated between the peers. These symmetric keys can then be used to decrypt the encrypted data exchanged between the peers. Any data transmitted today with longer-term confidentiality requirements is already vulnerable [i.2].

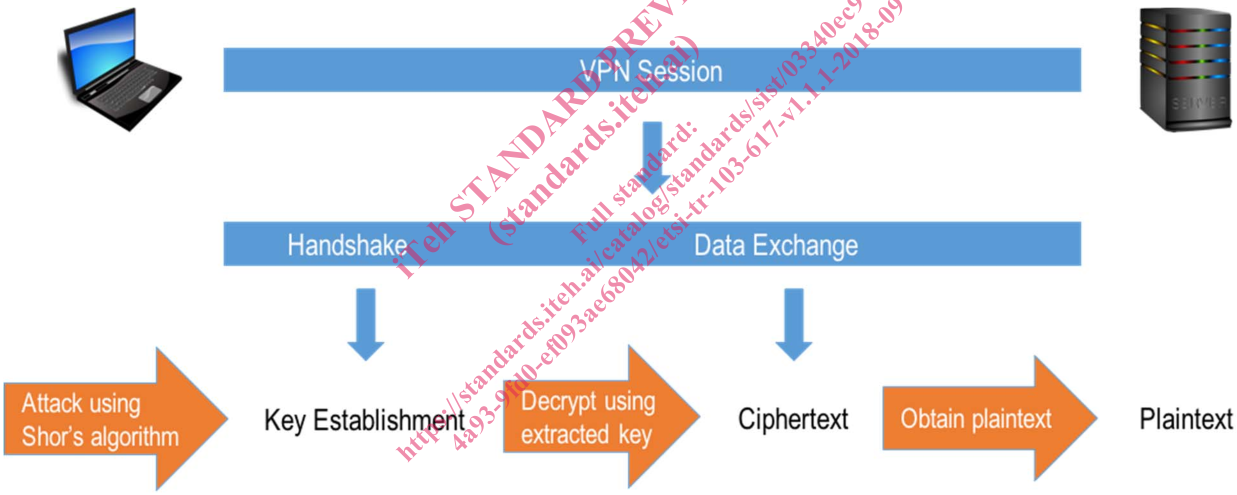

Figure 1: Harvest and Decrypt Attack by a Quantum Adversary

In 2017, quantum safe algorithm candidates were not mature enough to be used on their own. The National Institute of Standards and Technology (NIST) in the United States of America recommends an approach to address this threat today [i.13], by performing a quantum safe key establishment in parallel to a classic key establishment, and then merging the shared secrets before session key generation. In this scenario, if the classic key establishment was performed using a Federal Information Processing Standardization (FIPS) certified module, the entire system would maintain FIPS-certification. For greater assurance, two quantum-resistant schemes can be used in parallel to a classic one. These quantum-resistant schemes need to be based on different hard math problems in case an efficient quantum-based solution is found during the algorithm evaluation process for one of the problems. It should be noted that this style of hybrid cryptography is intended as an interim step, to provide protection of existing systems while the algorithm standardization takes place. Once that standards process is completed, systems are expected to shift to only use quantum safe algorithms.

Quantum safe algorithms differ noticeably from their classical equivalents. Some candidates have significantly larger keys, and in the case of key-encapsulation, larger ciphertext. Some candidates have slower key generation and cryptographic operation times, which impact protocol timing when used in an ephemeral mode for certain applications. All of these properties have an impact on underlying protocols when quantum safe algorithms are used as a replacement for classic equivalents. In the case of hybrid key establishment schemes, this impact is even greater since multiple algorithms are used instead of one.

The purpose of the present document is to clearly describe the range of protocol requirements necessary to add quantum resistance to existing or new implementations of VPNs.

1 Scope

The present document explores protocol requirements necessary to add quantum resistance to VPN technologies, including client, server and architectural considerations. Specifically, requirements around protocols and key establishment are considered, based on the multitude of systems that are at risk and require security updates before quantum computers that can attack commercial cryptography are developed.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI White Paper No. 8, ISBN No. 979-10-92620-03-0: "Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges", June 2015.

[i.2] ETSI GR QSC 004 (V1.1.1): "Quantum-Safe Cryptography; Quantum-Safe threat assessment".

[i.3] IETF RFC 4251: "The Secure Shell (SSH) Protocol Architecture".

[i.4] OpenSSH project PROTOCOL file.

NOTE: Available online at http://cvsweb.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/PROTOCOL.

[i.5] IETF RFC 4253: "The Secure Shell (SSH) Transport Layer Protocol".

[i.6] IETF RFC 4252: "The Secure Shell (SSH) Authentication Protocol".

[i.7] IETF RFC 4254: "The Secure Shell (SSH) Connection Protocol".

[i.8] IETF RFC 793: "Transmission Control Protocol".

[i.9] IETF Internet draft: "SSH Agent Protocol draft-miller-ssh-agent-00".

[i.10] IETF RFC 4255: "Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints".

[i.11] IETF Internet Draft: "Framework to Integrate Post-quantum Key Exchanges into Internet Key Exchange Protocol Version 2 (IKEv2)".

NOTE: Available online at https://tools.ietf.org/id/draft-tjhai-ipsecme-hybrid-qske-ikev2-01.txt.

[i.12] IETF Internet Draft: "Quantum-Safe Hybrid (QSH) Key Exchange for Transport Layer Security (TLS) version 1.3".

NOTE: Available online at https://tools.ietf.org/id/draft-whyte-qsh-tls13-06.txt.

[i.13] NIST Post-Quantum Cryptography FAQs.

NOTE: Available online at https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/faqs.

[i.14] IETF RFC 4301: "Security Architecture for the Internet Protocol".

[i.15] IETF RFC 7296: "The Internet Key Exchange Protocol Version 2 (IKEv2)".

[i.16] IETF Internet Draft: "Postquantum Pre-shared Keys for IKEv2".

NOTE: Available online at https://www.ietf.org/id/draft-ietf-ipsecme-qr-ikev2-02.txt.

[i.17] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[i.18] The Viability of Post-Quantum X.509 Certificates.

NOTE: Available online at https://eprint.iacr.org/2018/063.

[i.19] S. Galbraith, C. Petit, B. Shani and Y. Ti: "On The Security of Supersingular Isogeny Cryptosystems", 2016.

NOTE: Available online at https://eprint.iacr.org/2016/859.pdf.

[i.20] ETSI GR QSC 006 (V1.1.1): "Quantum-Safe Cryptography (QSC); Limits to Quantum Computing applied to symmetric key sizes".

[i.21] IETF Internet Draft: "Quantum-Safe Hybrid (QSH) Ciphersuite for Transport Layer Security (TLS) version 1.2".

NOTE: Available online at https://datatracker.ietf.org/doc/draft-whyte-qsh-tls12/.

[i.22] IETF Internet Draft: "A Transport Layer Security (TLS) Extension for Establishing An Additional Secret".

NOTE: Available online at https://datatracker.ietf.org/doc/draft-schanck-tls-additional-keyshare/.

[i.23] "The Double Ratchet Algorithm".

NOTE: Available online at https://www.signal.org/docs/specifications/doubleratchet/.

[i.24] IEEE 802.1AE-2006^{TM}: "Local and Metropolitan Area Networks: Media Access Control (MAC) Security".

[i.25] IEEE 802.1AEbn-2011^{TM}: "Local and metropolitan area networks--Media Access Control (MAC) Security Amendment 1: Galois Counter Mode--Advanced Encryption Standard-- 256 (GCM-AES-256) Cipher Suite" (Amendment to IEEE Std 802.1AE-2006).

[i.26] IEEE 802.1AEbw-2013^{TM}: "Local and metropolitan area networks-Media Access Control (MAC) Security Amendment 2: Extended Packet Numbering" (Amendment to IEEE Std 802.1AE-2006).

[i.27] IEEE 802.1X-2010^{TM}: "Local and metropolitan area networks--Port-Based Network Access Control".

[i.28] IEEE 802.1Xbx-2014^{TM}: "Local and metropolitan area networks -- Port-Based Network Access Control Amendment 1: MAC Security Key Agreement Protocol (MKA) Extensions" (Amendment to IEEE Std 802.1X-2010).

[i.29] IEEE 802.1Xck^{TM}: "Local and Metropolitan Area Networks - Port-Based Network Access Control Amendment: YANG Data Model". (DRAFT).

NOTE: Available online at https://standards.ieee.org/develop/project/802.1Xck.html.

[i.30] IETF RFC 3394: "Advanced Encryption Standard (AES) Key Wrap Algorithm".

[i.31] IETF RFC 3748: "Extensible Authentication Protocol (EAP)".

[i.32] IETF RFC 5216: "The EAP-TLS Authentication Protocol".

[i.33] IEEE 802.1AR^{TM}: "Local and metropolitan area networks-Secure Device Identity".

[i.34] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AES	Advanced Encryption Standard
AESKW	Advanced Encryption Standard Key Wrap
AUTH	Authentication
CA	Certificate Authority
CAK	Connectivity Association Key
CERT	Certificates
CKN	Connectivity association Key Name
DA	Destination Address
DH	Diffie-Hellman
EAP	Extensible Authentication Protocol
EAPoL	Extensible Authentication Protocol over LAN
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithms
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standardization
HDR	High Data Rate
HTTP	HyperText Transfer Protocol
ICK	Integrity Check Key
ICV	Integrity Check Value
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IKEv1	Internet Key Exchange version 1
IKEv2	Internet Key Exchange version 2
IP	Internet Protocol
IPsec	Internet Protocol security
KDF	Key Derivation Function
KE	Key Exchange
KEK	Key Encryption Key
KEM	Key Encapsulation Mechanism
KN	Key Number
LAN	Local Area Network
LHL	Leftover Hash Lemma
LWE	Learning With Errors
MAC	Message Authentication Code
MACsec	Media Access Control security
MIs	Member Identifiers
MKA	Media access control security Key Agreement
MKPDU	Media access control security Key agreement Protocol Data Unit
MSK	Master Session Key
MTU	Maximum Transmission Unit
NATs	Network Address Translators
NIST	National Institute of Standards and Technology
PKI	Public Key Infrastructure
PPK	Post-quantum Pre-shared Key
PRF	PseudoRandom Function
PSK	Pre-Shared Key
QSC	Quantum-Safe Cryptography
QSH	Quantum Safe Hybrid
QS_SA	Quasi Steady - State Approximation
QS_KE	Quantum-Safe - Key Exchange
RFC	Request For Comments
RSA	Rivest Shamir Adleman
RTT	Round Trip Time
SA	Security Association
SAK	Security Association Key

SC	Secure Channel
SIDH	Supersingular Isogeny Diffie–Hellman
SK	Secret Key
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSHFP	Secure Shell key Fingerprint
TCP	Transmission Control Protocol
TLP	Transport Layer Protocol
TLS	Transport Layer Security
US	United States (of America)
VPN	Virtual Private Network

4 General Virtual Private Network (VPN) requirements

4.1 Background

The primary purpose of a VPN is to provide a secure connection between two end points. While the specific technologies used to accomplish this can vary widely, the general goals are similar. A VPN then is the technology used to construct a private network over public channels. Large organizations typically consist of different locations that are geographically widespread. Each location can have its own Local Area Network (LAN) within which many servers and client computers interconnect. Nonetheless, it would be necessary to connect LANs of different locations, and some remote entities, to provide a single network service for the entire organization. Different locations can be connected by separate, dedicated, and well-protected communication lines. However, as the number of sites increases, and they become more physically separated, such a solution becomes cost prohibitive. Supporting access to this private network by remote entities, such as traveling employees, can become infeasible since the number is extremely large and remote entities can move. VPN allows the use of public networks to connect all these locations and entities as a single private network.

Often, sensitive data is transmitted over a private network among internal servers, or between an internal server and an internal client. Therefore, the security of data in transit over a VPN is critical. Since current VPN technologies utilize public key cryptography extensively for its security, they are vulnerable against quantum attacks.

VPN architectures are often categorized into two connection types: Site-to-site VPN and Remote Access VPN. Because of the different characteristics of these two types of VPN, the requirements differ.

Site-to-Site VPN

The site-to-site VPN establishes a secure tunnel between the local private networks of two physically separated locations over public networks, such that the network behaves as if it is a single private network. An outsider of the VPN can observe the existence of data traffic between the two sites, but cannot see who is connecting with whom, or read the information in the data traffic. VPN was originally developed for this purpose. In addition, the VPN provides authentication between the two parties.

The site-to-site VPN connects two sites semi-permanently, therefore, tunnel establishment might not be performed frequently. Since the tunnel is spanned between only two gateways, flexibility to meet the needs of different deployments is often preferred over the cost of complexity. Also, it is usually not overly difficult to set up a shared secret between the two gateways or static self-signed certificates.

Remote Access VPN

The remote access VPN allows a personal device to connect into the organization's private network over the public network such that the computing resources on this private network become available to the remote device. An outsider can see the data traffic between the remote device and the gateway but cannot identify which computing resource in the private network the remote device is connecting to or read or modify the information in the data traffic.

In contrast with site-to-site VPN, tunnel establishments occur very frequently in the remote access VPN. Also, client (device) authentication is critical for remote access VPN. This is, in part, because when the number of client devices is large, there is key management required to securely share secrets between the devices and the gateway.

Underlying Security Protocols and Quantum Vulnerabilities

VPN achieves cryptographic security by the underlying security protocols. These include Internet Protocol Security (IPSec) and Internet Key Exchange (IKE); Transport Layer Security (TLS); Media Access Control Security (MACsec); Secure Shell (SSH), and others.

Some VPN protocols are used to establish security between network entities, i.e. at the network layer level, and some between applications. All protocols accomplish data confidentiality and authentication using symmetric algorithms. Most protocols accomplish entity authentication and key establishment using public key cryptography, while some rely on pre-shared secrets. While public key based key establishment algorithms are typically negotiated between peers and make phased system upgrades possible, the authentication algorithms are not typically negotiated with as much flexibility since public key certificates contain only one public key type which makes system upgrades difficult. However, some protocols have introduced more flexibility here such as TLS 1.3 [i.34].

Generally speaking the needs of each protocol listed above are relatively similar at a base level - confidentiality and authentication - but how those are implemented may be very different depending on the use case. For example, when TLS is used to establish a VPN between multiple corporate users and the head office, it may require client authentication while TLS used between a web client and a public web server may only require server authentication. Some of these specific needs are addressed in the relevant clauses later.

Public Key Infrastructure (PKI)

Presenting a public key with a digital signature only proves that the sender owns the corresponding private key and is not sufficient to establish entity authentication. It is necessary to construct a system that can prove or assure that the presented public key belongs to a legitimate entity. PKI is developed to provide such a mechanism of public key-based authentication. Digital signature algorithm is the foundation of PKI used to achieve cryptographic security. In PKI, a trusted third party, a Certificate Authority (CA), vets the identity of an entity and its public key. It then composes a digital certificate that contains the identity and the public key of the entity, and digitally signs the certificate. An entity can then present its digital certificate and use the corresponding private key to generate a signature on a random challenge to prove its identity. The questioning party can then verify the digital signature on the challenge to confirm the entity has possession of the private key, associated with the certificate. They can also validate the certificate by verifying the CA's signature on the certificate. PKI is essential for establishing authentication in many protocols. While it is possible to pre-install all certificates on entities in a closed environment, a PKI is still necessary for effective certificate revocation checking.

4.2 Requirements for hybrid use cases

Security, authenticity and forward secrecy against classical computers are inherent from the classical handshake mechanism. In this transition period as the new quantum-safe algorithms are standardized, there is a desire to keep the properties offered by existing classical handshakes but adding protection from quantum computers. As a result, the use of a hybrid scheme then provides quantum security and quantum forward secrecy while maintaining the classical handshake properties.

Broadly speaking, the two main areas of concern from a quantum computer are in regard to confidentiality and authentication. Confidentiality is of a higher priority risk due to the threat of "harvest and decrypt" and so requires changes early. Authentication is a lower priority concern today but may involve a complex migration path. This priority is also highlighted by the fact that confidentiality risk today is from a passive attacker, utilizing a quantum computer in the future, while the authentication threat is from an active attacker with a quantum computer.