ETSI GR QSC 003 V1.1.1 (2017-02)

Quantum Safe Cryptography; Case Studies and Deployment Scenarios

Disclaimer

The present document has been produced and approved by the Quantum-Safe Cryptography (QSC) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGR/QSC-003

Keywords
algorithm, authentication, confidentiality, 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

IPRs essential or potentially essential to the present document 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.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Quantum-Safe Cryptography (QSC).

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.

1 Scope

The present document examines a number of real-world uses cases for the deployment of quantum-safe cryptography (QSC). Specifically, it examines some typical applications where cryptographic primitives are deployed today and discusses some points for consideration by developers, highlighting features that may need change to accommodate quantum-safe cryptography. The main focus of the document is on options for upgrading public-key primitives for key establishment and authentication, although several alternative, non-public-key options are also discussed.

The present document gives an overview of different technology areas; identify where the security and cryptography currently resides; and indicate how things may have to evolve to support quantum-safe cryptographic primitives. Clauses five and six discuss network security protocols, using TLS and S/MIME as typical examples. These are contrasted in clauses seven and eight by an examination of security options for IoT and Satellite use cases, which have very different requirements and constraints than traditional internet-type services. Some alternatives to public key protocols are reviewed in clause nine. Authentication requirements are discussed in clause ten and some forward-looking examples providing advanced functionality are examined in clause eleven.

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: "Quantum safe cryptography and security," ETSI White Paper No. 8, 2015.

[i.2] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2", 2008.

[i.3] Draft RCF draft-ietf-tls-tls13-09: "The Transport Layer Security (TLS) protocol version 1.3", 5 October 2015.

[i.4] C. Peikert: "Lattice Cryptography for the Internet" IACR ePrint 2014/070, 2014.

[i.5] J. W. Bos, C. Costello, M. Naehrig and D. Stebila: "Post-quantum key exchange for the TLS protocol from the ring learning with errors problem" IACR ePrint Archive 2014/599, 2014.

[i.6] V. Singh: "A Practical Key Exchange for the Internet using Lattice Cryptography" IACR ePrint 2015/138, 2015.

[i.7] E. Alkim, L. Ducas, T. Pöppelmann and P. Schwabe: "Post-quantum key exchange - a new hope" IACR ePrint 2015/1092, 2015.

[i.8] Draft IETF draft-whyte-qsh-tls13-01: "Quantum-safe hybrid (QSH) ciphersuite for Transport Layer Security (TLS) version 1.3 (draft RFC)", 20 September 2015.

[i.9] O. Garcia-Morchon, R. Rietman, L. Tolhuizen, J.-L. Torre-Arce, S. Bhattacharya and M. Bodlaender: "Efficient quantum-resistant trust Infrastructure based on HIMMO", IACR ePrint 2016/410, 2016.

[i.10] D. McGrew: "Living with post quantum security", NIST workshop on cubersecurity in a post quantum world, 2015.

[i.11] Z. Zheng, W. White and J. Schanck: "A quantum-safe circuit-extension handshake for Tor" in NIST Workshop on Cybersecurity in a Post-Quantum World, 2015.

[i.12] ETSI GR QSC 001 (V1.1.1): "Quantum-Safe Cryptography (QSC); Quantum-safe algorithmic framework".

[i.13] IETF RFC 5751: "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2", 2010.

[i.14] D. McGrew, P. Kampanakis , S. Fluhrer, S.-L. Gazdag , D. Butin and J. Buchmann: "State Management for Hash-Based Signatures" IACR ePrint, vol. 2016/357, 2016.

[i.15] Philips: "Philips Hue".

NOTE: Available at www.meethue.com.

[i.16] O. Garcia-Morchon: "Security for Pervasive Healthcare" PhD Thesis, RWTH University, 2011.

[i.17] ZigBee® Alliance.

NOTE: Available at www.zigbee.org.

[i.18] IETF RFC 7228: "Terminology for Constrained-Node Networks", 2014.

[i.19] A. Waller, A. Byrne, R. Griffin, S. La Porta, B. Ammar and D. Lund: "Case Study Specification and Requirements" 2015.

NOTE: Available at http://www.safecrypto.eu/.

[i.20] A. Menezes, P. van Oorschot and S. Vanstone: "Chapter 13: Key Management Techniques, Handbook of Applied Cryptography".

NOTE: Available at http://cacr.uwaterloo.ca/hac/.

[i.21] Kerberos® Consortium.

NOTE: Available at www.kerberos.org.

[i.22] IETF RFC 1510: "The Kerberos Network Authentication Service (V5)", 1993.

[i.23] IETF RFC 7252: "The Constrained Application Protocol (CoAP)", 2014.

[i.24] IETF RFC 4279: "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", 2005.

[i.25] O. Garcia-Morchon: "DTLS-HIMMO: Achieving DTLS certificate security with symmetric key overhead" in 20th European Symposium on Research in Computer Security (ESORICS), 2015.

[i.26] R. Blom: "Non-public key distribution" in CRYPTO 82, New York, 1983.

[i.27] T. Matsumoto and H. Imai: "On the key predistribution system - A practical solution to the key distribution problem" in CRYPTO 87.

[i.28] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro and M. Yung: "Perfectly-secure key distribution for dynamic conferences" in CRYPTO 92, 1992.

[i.29] W. Zhang, M. Tran, S. Zhu and G. Cao: "A Random PerturbationBased Pairwise Key Establishment Scheme for Sensor Networks" in ACM MobiHoc, 2007.

[i.30] M. Albrecht, C. Gentry, S. Halev and J. Katz: "Attacking cryptographic schemes based on "perturbation polynomials" in 16th ACM conference on Computer and communications security (CCS '09), 2009.

[i.31] O. Garcia-Morchon, R. Rietman, L. Tolhuizen, J.-L. Torre-Arce, S. Moon, D. Gomez-Perez, J. Gutierrez and B. Schoenmakers: "Attacks and parameter choices in HIMMO" IACR ePrint 2016/152, 2016.

[i.32] TUD: "Practical hash based signatures", 2016.

NOTE: Available at www.pqsignatures.org.

[i.33] IEEE 1609.2-2013™: "Wireless Access in Vehicular Environments", 2013.

[i.34] NIST: "The keyed-hash Meassage Authentication Code (HMAC)" FIPS-198-1, 2008.

[i.35] ISO/IEC 9797 parts 1 and 2: "Message Authentication Codes (MACs)", 1999.

[i.36] L. Ducas, V. Lyubashevsky and T. Prest: "Efficient identity-based encryption over NTRU lattices," IACR ePrint 2014/794, 2014.

[i.37] D. Apon, X. Fan and F.-H. Liu: "Fully secure lattice-based IBE as compact as PKE" IACR ePrint 2016/125, 2016.

[i.38] S. Agrawal, D. Boneh and X. Boyen: "Lattice basis delegation in fixed dimension and shorter ciphertext hierarchical IBE" in EUROCRYPT 2010 Volume 6110 of the series Lecture Notes in Computer Science pp 553-, 2010.

[i.39] D. Cash, D. Hofheinz, E. Kiltz and C. Peikert: "Bonsai Trees, or How To Delegate a Lattice Basis" Journal of Cryptology October 2012, vol. 25, no. 4, pp. 601-609, 2012.

[i.40] KLU: "HEAT project".

NOTE: Available at https://heat-project.eu/.

[i.41] K. Xagawa: "Improved (hierarchical) inner-product encryption from lattices" IACR ePrint 2015/249, 2015.

[i.42] S. Argawal, D. Freeman and V. Vaikuntanathan: "Functional encryption for inner product predicates from learning with errors" IACR ePrint 200/410, 2011.

[i.43] C. Gentry, A. Sahai and B. Waters: "Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based" IACT ePrint 2013/340, 2013.

[i.44] Z. Barkerski, C. Gentry and V. Vaikuntanathan: "(Leveled) fully homomorphic encryption without bootstrapping" IACR ePrint 2011/277, 2011.

[i.45] NIST: "Report on Post Quantum cryptography" NISTER 8105, 2016.

3 Abbreviations

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

6LoWPAN	Ipv6 over Low power Wireless Personal Area Networks
ABE	Attribute-based Encryption
AES	Advanced Encryption Standard
CoAP	Constrained Application Protocol
COTS	Commercial Off The Shelf
DH	Diffie-Hellman
DSA	Digital Signature Algorithm
DTLS	Datagram Transport Layer Security
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
FHE	Fully Homomorphic Encryption
HEAT	Homomorphic Encryption Applications and Technology
HFE	Hidden Field Equations
HIBE	Hierarchical Identity-Based Encryption
HIMMO	Hiding Information Mixing Modular Operations
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force

IKE	Internet Key Exchange
IoT	Internet of Things
IPsec	Internet Protocol Security
KDC	Key Distribution Centre
KMS	Key Management Server
KTC	Key Translation Centre
LoRA™	Low Power Wide Area Network for IoT
LTE™	Long Term Evolution
MAC	Message Authentication Codes
MIT	Massachusetts Institute of Technology
oneM2M	Standards for machine to machine
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
PSK	Pre-shared key
QSC	Quantum-Safe Cryptography
QSH	Quantum Safe Hybrid
RFC	Request For Comments
RSA	Rivest Shamir Adleman
S/MIME	Secure/Multipurpose Internet Mail Extensions
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
V2X	Vehicle to everything
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
W3C	Worldwide Web Consortium

4 QSC deployment scenarios

Cryptography is already widely-used and is rapidly becoming ubiquitous, appearing in everything from internet and mobile applications to emerging technologies such as the Internet of Things (IoT). Over the past 20 to 30 years, information storage has transitioned from a paper-based society, where physical copies of sensitive documents were once locked in filing cabinets and safes, to one where sensitive documents are now stored electronically. Although not obviously visible, this migration continues to occur. More information is now stored on databases within cloud environments, completely off-site to where the data originated. This poses an interesting problem for the future: how to keep sensitive data from unauthorised access both while being transferred over a network and while stored electronically.

Furthermore, quantum computers are no longer the thought experiments they once were not very long ago. There are many approaches to quantum computation, including super-conducting qubits, ion traps, nuclear magnetic resonance, quantum annealing and others. As of this date, small quantum computers exist in laboratories, although they are sufficiently under-powered to solve complex cryptographic problems in reasonable periods of time.

While these small quantum computers pose no threat to information security at present, it is already possible to observe their efficiency in solving certain classes of mathematical problems. This is why there is an increased priority by industry and governments on quantum computer research. This priority is evidenced by the propensity for increased investment in recent years. This is also why there is an increased priority on investments in quantum safe cryptography.

The wide range of applications being built today is accompanied by a diversity of security, efficiency and policy requirements and a variety of different computing platforms ranging from highly constrained devices to high end computing; so it seems unlikely that there would be a single one-size fits all solution for quantum resistance. The document presents some real-world use cases of where cryptography is deployed today and investigates how things may need change to migrate to quantum-safe cryptography.

The present document gives an overview of different technology areas, identify where the security and cryptography currently resides, and indicate how things might have to evolve or change to support quantum-safe cryptographic primitives. More detailed analysis of these examples may appear as separate ISG documents.

NOTE: The present document is a survey and should not be treated as an official ETSI endorsement of any products or standards mentioned below. Nor is it the intention of the document to prescribe how protocols defined and maintained by any other standards bodies should evolve. The intention is simply to discuss the consequences of using certain primitives in some typical example use-cases.

5 Network security protocols

5.1 Introduction

An over-simplified but stereotypical model for public key-based communications is the following. Two parties wish to establish a secure and authenticated communications link across a network. One or both parties obtain signed certificates from a trusted Public Key Infrastructure (PKI) containing the identity and public key of the other party with whom they wish to communicate. After verifying the validity of the certificate and the counterpart's identity, a public-key based handshake protocol is used to establish a secret session key known only to the two parties, and this session key is typically input to a block cipher to encrypt the subsequent communications between the pair.

Most current public-key-based communications are designed to be secure against *classical* adversaries. This means that the handshake mechanism allows two authenticated parties to agree on a secret session key that is secure against attackers with traditional computing resources. It is widely accepted that most currently-deployed public-key based communications will become vulnerable to a future attacker with access to large-scale quantum computers. For this reason, a growing body of research is being focused on developing quantum-safe public-key based handshake protocols.

Protocols such as Internet Protocol Security (IPsec), Internet Key Exchange (IKE), Transport Layer Security (TLS) protocol, Hypertext Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP) and others are ubiquitous internet or application level protocols used to secure a host of modern communications applications including web browsing, e-mails, Virtual Private Networks (VPNs), Voice over Internet Protocol (VoIP), instant messaging, etc. chapter 4 of the ETSI whitepaper [i.1] gives an overview of the sorts of changes that would need to be considered to incorporate quantum-safe primitives into common network protocols such as these.

Most of these protocols are defined and maintained by the Internet Engineering Task Force (IETF), Worldwide Web Consortium (W3C) or similar groups and it is not in the remit of ETSI ISG QSC to decide how these protocols should evolve. However, given the ubiquitous nature of these protocols, it is necessary to have some understanding of the compatibility of any ETSI recommended primitives with the wider commercial infrastructure.

Clauses 5.2 to 5.3.3 focus on TLS as an important example of a real-world use case. They look at some specific proposals in the literature for ways to upgrade TLS to be quantum secure. The TLS [i.2] and [i.3] protocol suite provides a cryptographic layer through which network application protocols such as Hypertext Transfer Protocol Secure (HTTPS) (used for web browsing), SMTP (e-mail) and VoIP (voice) can be securely tunnelled. TLS is widely used to underpin the security of many of the other technology areas discussed in the remainder of the present document.

5.2 TLS

5.2.1 TLS cryptography

TLS version 1.2, defined in [i.2] and its intended upgrade, still in draft at [i.3], make wide use of public-key cryptography supported by PKI to provide key establishment and authentication services. These are currently based on the well-known factoring or discrete logarithm primitives Rivest Shamir Adelman (RSA), Diffie-Hellman (DH), Digital Signature Algorithm (DSA), Elliptic Curve Diffie-Hellman (ECDH) and Elliptic Curve Digital Signature Algorithm (ECDSA) and it is precisely these primitives that need to be upgraded to be quantum-safe. Since TLS is so widely used, it is here that the best and most modern primitives to provide secure and efficient quantum-safe replacements for the current Public Key Cryptographic (PKC) protocols will need to be deployed.

TLS also makes use of symmetric cryptography e.g. the block cipher Advanced Encryption Standard (AES) for data encryption and the Secure Hash Algorithm (SHA) for digital signatures and certificate verification. Since these primitives may be regarded as already quantum-safe, or easily upgraded to be quantum-safe by increasing key or block sizes, they will not be discussed further here and the focus will instead be on the public-key primitives.