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

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.