Final draft ETSI EG 203 310 V1.0.0 (2016-04)

CYBER;
Post Quantum Computing Impact on ICT Systems; Recommendations on Business Continuity and Algorithm Selection

Reference

DEG/CYBER-0008

Keywords

algorithm, 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

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 final draft ETSI Guide (EG) has been produced by ETSI Technical Committee Cyber Security (CYBER), and is now submitted for the ETSI standards Membership Approval Procedure.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**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 addresses business continuity arising from the concern that Quantum Computing (QC) is likely to invalidate the problems that lie at the heart of both RSA and ECC asymmetric cryptography. The present document considers the transition to the post-quantum era of how to re-assert CAs in a PKI, the distribution of new algorithms, and the distribution of new keys, and advises that business continuity planning addresses the impact of QC on ICT.

The current assumptions that underpin the security strength of RSA and ECC are that the solution to the prime factoring, and the discrete logarithm problems are infeasible without prior knowledge. It has been widely suggested that the application of quantum computing to these problems removes the assertion of infeasibility. Whilst it is not known when quantum computing will arrive or how long it will be until the factorisation and discrete logarithm problems are themselves solved the present document reviews the nature of the algorithms when subjected to QC attack and why they become vulnerable.

The present document applies to ETSI TBs undertaking work in the selection and definition of cryptographic algorithms, and to non-ETSI members who have deployed cryptographic algorithms and need to be aware of the impact of QC on ICT.

2 References

2.1 Normative 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.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

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 necessary for the application of the present document.

Not applicable.

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.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

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] ISO 22301: "Societal security -- Business continuity management systems -- Requirements".

[i.2] ETSI White Paper Quantum Safe Cryptography V1.0.0 (2014-10): "Quantum Safe Cryptography and Security; An introduction, benefits, enablers and challenges"; ISBN 979-10-92620-03-0.

[i.3] ETSI ISG QSC work programme.

NOTE: Available at https://portal.etsi.org/tb.aspx?tbid=836&SubTB=836.

[i.4] IANA: "TLS Register of cipher suites".

NOTE: Available at (https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-4).

[i.5] ISO 27000 series: "Information technology -- Security techniques -- Information security management systems".

NOTE: ISO 27000 is a multipart standard. The reference is to the body of work prepared by ISO/IEC JTC1 SC27 in the domain of Information security management systems.

[i.6] Auguste Kerckhoffs: "La cryptographie militaire" Journal des sciences militaires, vol. IX, pp. 5-83, January 1883, pp. 161-191, February 1883.

[i.7] Biography Michele Mosca.

NOTE: Available at https://services.iqc.uwaterloo.ca/people/profile/mmosca/.

[i.8] Professors Johannes Buchmann of TUD, Jintai Ding of UoC: "Post-Quantum Cryptography", Second International Workshop, PQCrypto 2008.

[i.9] Prof Seth Lloyd of MIT, MIT Review 2008.

[i.10] Prof. Johannes Buchmann, et al.: "Post-Quantum Signatures", Oct 2004, Technische Universität Darmstadt.

[i.11] Regulation (EU) N 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in the ETSI White Paper Quantum Safe Cryptography [i.2] apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in the ETSI White Paper Quantum Safe Cryptography [i.2] apply.

4 Outlining the problem

All cryptographic algorithms should be considered to have a finite lifetime, where that lifetime is determined in part by advances in cryptanalysis, by advances in computing, and by advances in the underlying mathematical knowledge that underpins cryptology. In the domain of quantum computing there is a step change in the way that computing attacks on cryptographic algorithms will occur.

In brief if the promise of quantum computing holds true then the following impacts will be immediate on the assumption that the existence of viable quantum computing resources will be used against cryptographic deployments:

- Symmetric cryptographic strength will be halved, e.g. AES with 128 bit keys giving 128 bit strength will be reduced to 64 bit strength (in other words to retain 128 bit security will require to implement 256 bit keys).
- Elliptical curve cryptography will offer no security.
- RSA based public key cryptography will offer no security.
- The Diffie-Helman-Merkle key agreement protocol will offer no security.

With the advent of realisable Quantum Computers everything that has been transmitted or stored and that has been protected by one of the known to be vulnerable algorithms, or that will ever be stored or transmitted, will become unprotected and thus vulnerable to public disclosure. Annex A summarises quantum computing, whilst Annexes B and C review the Shor and Grover algorithms and the means by which they impact existing cryptographic algorithms.

There is wide speculation on when quantum computing will be viable and whilst there is no consistency in forecasts it is reasonable to assume that quantum computers will become viable within the forecast lifetime of current cryptographic keys and algorithms.

Respected professionals in the field have speculated on the timeline as below.

Professors Johannes Buchmann of TUD, Jintai Ding of UoC, "Post-Quantum Cryptography", Second International Workshop, PQCrypto 2008 [i.8]: "*Some physicists predicted that within the next 10 to 20 years quantum computers will be built that are sufficiently powerful to implement Shor's ideas and to break all existing public key schemes. Thus we need to look ahead to a future of quantum computers, and we need to prepare the cryptographic world for that future.*"

Prof Seth Lloyd of MIT, MIT Review 2008 [i.9]: "*My colleagues at MIT and I have been building simple quantum computers and executing quantum algorithms since 1996, as have other scientists around the world. Quantum computers work as promised. If they can be scaled up, to thousands or tens of thousands of qubits from their current size of a dozen or so, watch out!*"

Prof. Johannes Buchmann, et al [i.10]: "Post-Quantum Signatures", Oct 2004, Technische Universität Darmstadt: "*There is a good chance that large quantum computers can be built within the next 20 years. This would be a nightmare for IT security if there are no fully developed, implemented, and standardized post-quantum signature schemes.*"

From this small sample it can be predicted that viable quantum computing will be added to the arsenal of cryptanalysts in or around 2030. However, research is rapid evolving in quantum computing and this timetable is more likely to shrink than expand as the underlying physics problems of quantum computing are overcome and the further development of QC becoming an engineering rather than a science problem.

The number of qubits required to make a meaningful attack on cryptosystems is still significant. Most commentators suggest that if the key length is L that between L and L^2 qubit machines are required. The state of the art in 2015 of a true QC was less than 20 qubits.

The ETSI White Paper [i.2] suggests that Quantum safe communication techniques are not compatible with techniques incumbent in products vulnerable to quantum attacks. In a well-ordered and cost efficient technology transition, there is a period of time where the new products are gradually phased in and legacy products are phased out. Currently, quantum safe and quantum vulnerable products can co-exist in a network; in some cases, there is time for a well-ordered transition. However, the window of opportunity for orderly transition is shrinking and with the growing maturity of QC research, for data that needs to be kept secret for decades into the future, the window for transitioning may already be closed.

5 Business continuity considerations

5.1 Overview

A very simple equation outlines the extent of the problem of evolution to a QC safe deployment of cryptography:

- X = the number of years the public-key cryptography needs to remain unbroken.
- Y = the number of years it will take to replace the current system with one that is quantum-safe.
- Z = the number of years it will take to break the current tools, using quantum computers or other means.

If "X + Y > Z" any data protected by that public key cryptographic system is at risk and immediate action needs to be taken. Thus if Z is estimated as 15 years then both X and Y have to be significantly less than 15 years, and the sum of X and Y also has to be less than 15 years, to be safe.

Whilst the advent of quantum computing will represent a step change in the ability of attackers to directly attack encrypted data, or to determine a collision for existing hash functions, the normal development of computing power and cryptanalysis suggests that there is no status quo and that reasonable steps have to be taken in the normal course of events to counter this continual development. The threat of quantum computing is significant only insofar as existing algorithms for e-commerce, digital signature and authentication will be immediately weakened or invalidated whereas with non-quantum computing development an organisation can make longer term maintenance level plans to re-key and re-secure their assets. The conventional case may be considered by evolving from a DES like solution through 3DES, AES-128 to AES-256 on a long term cycle.

The level of threat formed by quantum computing is inconsistent as purely algorithmic measures are not going to be the only security level deployed. A physically isolated and cryptographically protected database is probably at less risk of compromise than an open data store on a cloud service provider. However, any user of asymmetric cryptography cannot afford to be complacent and has to acknowledge as a first step that cryptographic protection cannot be applied once and forgotten.

For data that has been encrypted once with a non-quantum safe algorithm that data would need to be re-encrypted with a new quantum safe algorithm and key. Identification of candidate data in this case is non-trivial and as shown in clause 5.3 there is no consensus to date on suitable algorithms. The immediate concern here is that industry has to develop trust in quantum safe algorithms before quantum computers are available and deploy them in advance of the threat vector being realisable. It takes a number of years to validate an algorithm and to build trust through reliable cryptanalysis in its capability. This has to be factored into the deployment and business continuity model. In the simplified equation given at the start of this clause an additional variable has to be added:

- T = the number of years it will take to develop trust in quantum safe algorithms

This modifies the equation to determine safety to $(X + Y + T > Z)$. The obvious view is that Y is a function of T.

It is suggested in clause 4 that security should not be dependent only on the algorithm and as Kerchoffs [i.6] has stated "A cryptosystem should be secure even if everything about the system, except the key, is public knowledge" but this pre-supposes that the first clause of his statement is true and quantum computing defeats this pre-condition. Where quantum computing works is that whilst in conventional systems there is no way to get the private key from knowledge of the public key and some crypto-text, this is not true for a quantum computing attack. Thus knowledge of the public key and some crypto-text will allow an adversary to recover the private key, hence all the security of the system is broken. For conventional symmetric cryptography where Grover's algorithm comes into play the security of the system still lies in the key although the strength of the cryptosystem is reduced with recovery to the same cryptographic strength requiring a doubling of key size (e.g. from 128 bits to 256 bits). Grover's algorithm is also claimed to significantly impact the strength and trust of hashing algorithms.

Key generation schemes and the provision of entropy in the system may also be impacted by quantum computing based attacks. There is still debate and research in this field but generally for the creation of randomness the Shannon based measure that with knowledge of what has happened in the past I cannot predict the next value with greater than 50 % reliability (in a two state system) then the output is random. Pending further study the general rules for random number generation should be followed and the rule of thumb that the source of entropy should be random over a similar range to the expected output is critical (i.e. do not rely on achieving 128-bit security when the source of randomness for the system is only within (say) a 4-bit range). In short, good randomness that leads to high entropy, or sources of entropy that lead to true randomness, cannot be ignored. If the underlying source of randomness is weak (i.e. not really random or random over a very small range) then any dependent security function is going to be weakened. The attacker is not going to try and break the crypto engine and the protocols if he can use weak randomness as an attack vector.

5.2 Existing standards (ISO 22301)

Business Continuity Management (BCM) in the face of an attack to the cryptographically protected assets of the organisation has to be considered as part of the planning and risk analysis aspects of ISO 22301 [i.1]. The extension to be highlighted is that whilst BCM and Security Management frameworks such as those from ISO 27001 [i.5] apply it is essential that where cryptographic technologies are applied in the business appropriate review of the continuing validity of such technologies should be built into the risk analysis and planning, and that process should review such issues as key transition, algorithm transition and trust management.

The worst case scenario in BCM from the evolution of QC is that variable Z is met before the organisation has managed to satisfy variable Y. In such a case the business and its partners can no longer trust the cryptographically protected assets of the business.

5.3 Algorithm change

There are many candidates for quantum safe algorithms in the asymmetric crypto domain but there is no consensus on their suitability. Irrespective of what is ultimately determined to be the QSC algorithms of choice the systems that require cryptographic protection require to be crypto-agile. The purpose of crypto-agility is that the entire set of business processes that rely on cryptographic security are able to do the necessary management to change keys and algorithms.

NOTE: If symmetric algorithms are used the ability of the algorithm to work in a new mode with longer keys is not guaranteed and if longer keys are not supported (e.g. moving from 80 to 160 bits, or 128 to 256 bits) a new algorithm suited to the new key size should be selected.

Support of QSC algorithms has a significant impact on processing and memory resource for the authentication, signature and key exchange protocols, and on the carriage of resultant signatures and keys in protocols. Whilst it is not the purpose of the present document to specify which algorithms should be selected the following notes are provided as indicative of the approaches being examined in bodies such as ETSI ISG QSC [i.3].

QSC algorithms for asymmetric cryptographic application may take a number of forms as below:

- Lattice based algorithms
- Code base algorithms
- Hash based algorithms, etc.

The impact of such algorithms on core elements such as key size, signature size and so forth to give equivalence to a classical algorithm of approximately 128-bit strength is outlined in table 1.

Table 1: Key and signature size comparison for common QSC algorithms (from [i.3])

Type	Scheme	Security	Public key	Signature
Lattice	Lyubashevsky	---	1 664 bytes	2 560 bytes
	NTRU-MLS	128 bits	988 bytes	988 bytes
	Aguilar et al	128 bits	1 082 bytes	1 894 bytes
	Güneysu et al	80 bits	1 472 bytes	1 120 bytes
	BLISS	128 bits	896 bytes	640 bytes
	Ducas et al	80 bits	320 bytes	320 bytes
	HIMMO	128 bits	32 bytes	---
MQ	Quartz	80 bits	72 237 bytes	16 bytes
	Ding	123 bits	142 576 bytes	21 bytes
	UOV	128 bits	413 145 bytes	135 bytes
	Cyclic-UOV	128 bits	60 840 bytes	135 bytes
	Rainbow	128 bits	139 363 bytes	79 bytes
	Cyclic-Rainbow	128 bits	48 411 bytes	79 bytes
Code	Parallel-CFS	120 bits	503 316 480 bytes	108 bytes
	Cayrel et al	128 bits	10 920 bytes	47 248 bytes
	Cyclic-Cayrel et al	128 bits	208 bytes	47 248 bytes
	RankSign	130 bits	7 200 bytes	1 080 bytes
	Cyclic-RankSign	130 bits	3 538 bytes	1 080 bytes
Hash	Merkle	128 bits	32 bytes	1 731 bytes
	Leighton-Micali	128 bits	20 bytes	668 bytes
	XMSS	256 bits	64 bytes	8 392 bytes
	SPHINCS	256 bits	1 056 bytes	41 000 bytes
Isogeny	Jao-Soukharev	128 bits	768 bytes	1 280 bytes
	Sun-Tian-Wang	128 bits	768 bytes	16 bytes

The figures above are for guidance only but compare to equivalent public key sizes for ECC of 256 bits (32 bytes) and for RSA of 3 192 bits (399 bytes).

For carriage and identification of parameters it is clear that common protocols such as TLS need to be updated to be able to refer to QSC algorithms (the current list of ciphersuites is found at IANA [i.4]).