ETSI GR QSC 004 V1.1.1 (2017-03)

GROUP REPORT

Quantum-Safe Cryptography;
Quantum-Safe threat assessment

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-004

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

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.

Introduction

Quantum Computers (QC) represent a paradigm shift in computing and the result of having any quantum computer of reasonable size, and availability, is that the existing hard problems upon which the asymmetric cryptography domain is built will not be considered hard anymore. The simple result is that asymmetric cryptography, using Elliptic Curves, or number factorization, will be invalidated. Similarly, there will be an impact on the security level afforded by symmetric cryptographic schemes. Much of the this is well known and documented in ETSI's White Paper [i.2], and in the ETSI Guide on the impact of quantum computing on business continuity [i.4] and many other places. The purpose of the present document is to expand a little on the previous publications in this field but with a general reflection that the concern (worry) regarding a quantum computing attack is not going to have the same impact across all users of quantum vulnerable cryptography.

The present document gives a very simplified consideration of the attack likelihood for when a viable QC exists and reflects that risk against the business sectors' requirements, in order to know how to use cryptographic technology in the sector. This is used to assist industry in determining how long they have to respond to the availability of QC and retain trust and security in their operations.

1 Scope

The present document presents the results of a simplified threat assessment following the guidelines of ETSI TS 102 165-1 [i.3] for a number of use cases. The method and key results of the analysis is described in clause 4.

The present document makes a number of assumptions regarding the timescale for the deployment of viable quantum computers, however the overriding assertion is that quantum computing will become viable in due course. This is examined in more detail in clause 5.

The impact of quantum computing attacks on the cryptographic deployments used in a number of existing industrial deployment scenarios are considered in clause 7.

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 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.2] Selecting Cryptographic Key Sizes, Arjen K. Lenstra and Eric R. Verheul, Journal Of Cryptology, vol. 14, p. 255-293, 2001.

[i.3] ETSI TS 102 165-1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis".

[i.4] ETSI EG 203 310 (V1.1.1): " CYBER; Quantum Computing Impact on security of ICT Systems; Recommendations on Business Continuity and Algorithm Selection".

[i.5] ISO/HL7 21731:2014 Health informatics -- HL7 version 3 -- Reference information model -- Release 4.

[i.6] Digital Living Network Alliance: DNLA Guidelines.

NOTE: Available from http://www.dlna.org/guidelines/

[i.7] Advanced Access Content System (AACS): Introduction and Common Cryptographic Elements.

NOTE: Available from http://www.aacsla.com/specifications/specs091/AACS_Spec_Common_0.91.pdf

[i.8] ETSI TS 102 940: "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management".

3 Abbreviations

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

AACS	Advanced Access Control System
AACSLA	Advanced Access Content System Licensing Authority
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
CA	Certificate Authority
CAM	Co-operative Awareness Message
CIA	Confidentiality Integrity Availability
DEM	Event Notification Message
DH	Diffie Hellman
DHCP	Dynamic Host Configuration PRotocol
DLNA	Digital Living Network Alliance
DSA	Digital Signature Algorithm
DTCP	Digital Transmission Content Protection
DTLA	Digital Transmission Licensing Authority
DTS	Datagram TLS
EAP	Extensible Authentication Protocol
EC	Elliptic Curve
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithms
EV	Extended Validation (Certificate)
HRNG	Hardware Random Number Generator
ICT	Information & Communication Technology
IKE	Internet Key Exchange
IP	Internet Protocol
ITS	Intelligent Transport System
ITS-S	Intelligent Transport System Station
LAN	Local Area Network
MAC	Message Authentication Code
PKI	Public Key Infrastructure
QC	Quantum Computer or Quantum Computing
QSC	Quantum-Safe Cryptography
RSA	Rivest Shamir Adleman
TCP	Transmission control Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
UDP	User Datagram Protocol
VPN	Virtual Private Network
WAP	Wi-Fi Protected Access
XML	eXtensible Markup Language

4 Overview of approach to threat assessment

Threat assessment in most environments consider 2 metrics: Likelihood of an attack and impact of the attack. Underlying these metrics are a further set of metrics addressing such issues as availability requirements (i.e. time needed to access the vulnerability), equipment (i.e. the complexity or cost of equipment needed to launch the attack) and so forth which are described in some detail in ETS TS 102 165-1 [i.3]. The calculation of risk is taken most often as the product of likelihood and impact and categorized as high, medium or low (different risk management systems may use more than 3 classifications but ETSI's approach has only considered 3 with a view to defining countermeasures against high and medium risk vulnerabilities).

The considerations behind the security of most cryptographic systems is that the security strength of an algorithm is optimal when the only feasible attack is brute force evaluation of the key space.

ETSI EG 203 310 [i.4] states (with some editorial extensions):

"… 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).*
- *Elliptic curve cryptography will offer no security.*
- *RSA based public key cryptography will offer no security.*
- *The Diffie-Hellman-Merkle key agreement protocol will offer no security.*

NOTE: The common practice is to refer to the key agreement protocol developed by Messrs Diffie, Hellman and Merkle as simply the Diffie-Hellman or DH protocol as the formal recognition of Merkle's role was made after DH became the accepted term.

With the advent of realizable 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."

The purpose of threat assessment is, in part, to identify where protective measures should be applied for countering the threat. The quantification of risk assists this by addressing those parts of the system most vulnerable and recommending where countermeasures should be applied. For the specific case of the impact of quantum Computing on the security of ICT systems as addressed by ETSI EG 203 310 [i.4] the broad assertion for business continuity is that systems have to be developed and deployed to be crypto-agile. The intent is to ensure that processes are in place that allow algorithms and keys to be changed across the business quickly enough to counter the viable introduction of quantum computers.

The factors to be considered in assessment of the likelihood element in determining the potential of an attack are the following:

- System knowledge:

  For the majority of crypto-systems under consideration, it should be assumed that the algorithms are public knowledge (e.g. RSA, ECC (various modes)).

- Time:

  For those systems open to attack by quantum computing, it is assumed that no new vulnerability is exposed, rather than a quantum computer invalidates the core assertion of a solution to the underlying problem is infeasible without access to the key itself. Thus the time factor for access to material to retrieve the private key of an asymmetric pair is treated as essentially null (using the formulation given in ETSI TS 102 165-1 [i.3] the term is "an attack can be identified or exploited in less than an hour").

- Expertise:

  There is comparatively little expertise in the programming of quantum computers even if some algorithms, like Shor's and Grover's, have been well described. However, the ability to take the data from a public key certificate and feed it into a well-defined instance of Shor's algorithm and to retrieve the private key is likely to be trivial and to tend towards the laymen end of the expertise scale.

- Opportunity:

  Only access to the public key certificate is required and this is public by default, hence there is no barrier to opportunity to the input data to an attack.

- Equipment:

  Assuming access to the input data, the barrier to breaking existing asymmetric cryptography is the existence of a viable quantum computer. For the current assessment equipment has to be categorized as at least specialized, more likely bespoke, and expensive. However there are schemes where public access to a shared quantum computer will be made available which may reduce the assessment to simply that of specialized.

The assessment of impact for any attack on cryptographic tools that a business is reliant upon is assessed as high - the dependent parties are unable to continue to operate securely. Taking account of the assessment factors above, and the impact assessment outlined in ETSI EG 203 310 [i.4], the risk to systems should be considered as critical (using the terminology of ETSI TS 102 165-1 [i.3]). However, in the absence of a quantum computer, an attack that reveals the private key, given only knowledge of the public key certificate, is infeasible with the current level of understanding. Thus the threat assessment to any vulnerable algorithm and protocol can be restricted to only understanding the timeline for deployment of a viable quantum computer that can address the factoring of very large numbers. Further consideration of the time factor is illustrated in ETSI EG 203 310 [i.4] to consider the time for which systems will be vulnerable by considering the time required to arrive at 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.
- T = the number of years it will take to develop trust in quantum-safe algorithms.

If "X + Y + T > Z" any data protected by that public key cryptographic system is at risk and immediate action needs to be taken. The Y factor is very dependent on the nature of the cryptographic deployment. Similarly, the X factor is dependent on the nature of the data being protected with some data (e.g. eHealth records) requiring protection for decades, whereas signalling data (e.g. DHCP derived IP addresses) may only require protection for a few minutes (e.g. the lease period of a DNCP derived IP address).

Some assessment is made for values to assign to the "Y" factor in clause 7. The core message however is that even with crude assessments the sum of X, Y and T will exceed Z if a viable large scale quantum computer is available in 15 or 20 years.

5 Assessment of Quantum Computing timetable

5.1 Overview

There are many approaches to quantum computation, including super-conducting qubits, ion traps, nuclear magnetic resonance, quantum annealing and others. The purpose of the present document is not to assess the relative strengths and weaknesses of each of these approaches, in particular in relation to maintenance of the support to the security suite of CIA capabilities offered by cryptography. Whilst in mid-2016 quantum computers indeed exist, they are sufficiently under-powered that they are unable to solve complex cryptographic problems in reasonable periods of time and thus 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 to say that for certain types of math problems, even small quantum computers are claimed to be far more efficient than conventional computers although some experts dispute such findings.

There is no guarantee of the time at which quantum computing will become viable, and in particular for addressing the key algorithms that are suggested to make existing public key (asymmetric) cryptography obsolete. Thus the timetable for a viable quantum computer to implement each of Shor's and Grover's algorithms is the purpose of this assessment. Based on available knowledge (see also the assessment given in ETSI's Quantum Cryptography white paper [i.1]) this will be within 15 years of publication of the present document, thus in approximately calendar year 2031.

The more difficult question is how many qubits are required for a viable quantum computer to be used against cryptographically protected data? The comparison of quantum computers to classical computers is not quite straightforward either. The general view is that an n-bit QC can work on 2^n states simultaneously whereas a classical computer can work on $2n$ states but there are many doubts regarding that view and the practicality of the calculation. For real time recovery of the private key from asymmetrically encrypted data with knowledge of the public key it is widely reported that for keys of size n a QC with at least n-qubits is required. However, one of the other questions is how vulnerable is data that has been encrypted with asymmetric keys to any form of attack via QC (i.e. not just a real time attack but an attack on data that has been captured and stored in its encrypted form in order to decrypt it when large-scale fault-tolerant quantum computing resources are available)?

5.2 QC requirements for Shor's algorithm

Shor's algorithm consists of two parts:

- A reduction, which can be done on a classical computer, of the factoring problem to the problem of order-finding.
- A quantum algorithm to solve the order-finding problem.

It should be noted that actual implementations of Shor's algorithm are few and they have not been able to prove themselves against large numbers. It is reported that Shor's algorithm has successfully factored numbers 15 (in the year 2001 using a 7-qubit machine), and 21 (in the year 2012 using a 12-qubit machine) with a true quantum computer. Thus it can be reasonably asserted that Shor's algorithm is implementable and works, what cannot be reasonably asserted for now is the ability to build a realistic machine to work with large numbers.

5.3 QC requirements for Grover's algorithm

Grover's algorithm is a search algorithm against an abstract database where for a given search input a given discrete output will be given. The impact of Grover's algorithm is generally considered a giving an increase in search times of N^2 such that a suitably sized QC will cut the time required to perform a brute force attack on key space will be substantially reduced (the crude figures suggest that the effective key size will be cut in half, from (say) 128 bits to 64 bits. There are a number of ways of assessing the number of qubits required to search a particular space but the general assertion is based on the idea that *n* bits can index 2^n items. A classical computer with *n* bits of memory can search through all 2^n inputs, using at most 2^n calls. A quantum computer with *n* qubits of memory can search through all 2^n inputs using at most $\sqrt{2^n} = 2^{n/2}$ calls.

More qubits means a faster search but as for Shor's algorithm whilst it can be asserted that Grover's algorithm is implementable and works it is unreasonable to assert when a large *n* qubit machine will exist that will outstrip current brute force search.

6 Threat assessment against aspects of QC deployments

6.1 Algorithm vulnerabilities

6.1.1 Overview

As stated in clause 4, it is seen that the cryptographic techniques that are in use today are vulnerable to the attacks using quantum computers.

Clause 4 lists symmetric cryptographic algorithms and three public key cryptosystems, Rivest-Shamir-Adelman (RSA), Elliptic Curve Cryptosystem (ECC), and Diffie-Hellman (DH). Symmetric cryptographic algorithms typically include block ciphers, stream ciphers, and hash algorithms.

Attacks by quantum computers using Grover's algorithm or Simon's algorithm are believed to reduce the security of symmetric algorithms. These quantum algorithms enable more efficient search to find the secret key, collisions, and pre-image.

Public key cryptography is also known to be vulnerable to the quantum attacks using Shor's algorithm. Shor's algorithm enables quantum computers to calculate private key, which is secret, from the public key efficiently.

6.1.2 Symmetric algorithms

For symmetric ciphers, i.e. block ciphers and stream ciphers, the quantum attack focuses on finding the secret symmetric key. Grover's algorithm shows that it is possible for a scalable quantum computer to speed up the search. Furthermore, when certain structure exists in a symmetric cipher, Simon's algorithm can be applied to improve the search. Although theoretical speed up is deemed twice, in reality, it may not be as much due to the implementation challenges. However, with conservative measures, it is recommended to double the key size to cope with quantum attacks.

For hash algorithms, the goal of attacks may be to find collision or pre-image. In the use of hash algorithm where pre-image resistance is required, such as pseudo random generation, it is deemed sufficient if the output size is doubled. In the use where collision resistance is required, such as message digest computation of a digital signature algorithm, it is already known that the output size has to be doubled even in the classical settings. Therefore, in order to achieve quantum resistance, the output size has to be four times larger. However, it should be noted that by introducing randomization, requirement of hash algorithms can be reduced from collision resistance to second pre-image resistant. Thus, addition of randomization will allow the output size to be only twice as large.

Compared with the quantum vulnerabilities of public key cryptography discussed in clause 6.1.3, symmetric cryptography algorithms seem more resistant against quantum attacks because it simply requires the key and output sizes to be doubled.

6.1.3 Public key cryptography

RSA bases its security on the difficulty of integer factorization. Currently, the best known classical attack is number field sieve, which reduces the attack complexity to sub-exponential time, which is faster than the ideal exponential time.

It is understood that integer factorization can be solved in polynomial time by using Shor's algorithm. Although the size of constant may actually have some impact on the actual time for calculation, polynomial time implies that it can be solved in short amount of time such that increase of key size does not help as much. Due to this, it is deemed dangerous to use algorithms that can be solved in polynomial time. Thus, such a quantum attack invalidates the security of RSA.

DH algorithm and Digital Signature Algorithm (DSA) base their security on the difficulties of integer discrete logarithm. Similar to RSA, the best known classical attack is number field sieve. Often the same approach such as number field sieve applies to both integer factorization and integer discrete logarithm. Since number field sieve is applicable, an integer discrete logarithm problem can be solved in sub-exponential time. For quantum attacks, Shor's algorithm allows to solve the problem in polynomial time, which invalidates the security.

Algorithms of ECC such as ECDH and ECDSA base their security on the difficulty of elliptic curve discrete logarithm. Unlike integer discrete logarithm, no sub-exponential time attack by classical computers has been found. Thus the attack complexity of ECC remains to be exponential time. Unfortunately, Shor's algorithm is also applicable to the elliptic curve discrete logarithm. Thus, the complexity is reduced to polynomial time, invalidating ECC security as well.

In conclusion, quantum attacks can invalidate security of currently used public key cryptography. Thus, it is necessary to introduce different public key cryptography that resists attacks by quantum computers.

6.1.4 Random number generation

Random number generation is a critical component to establish cryptographic security. A number of security breaches have been caused by insecure random number generation. In general, a cryptographically secure random number generator consists of good entropy sources, secure conditioner of entropy data, and cryptographic pseudo random number generator.

Security cannot be established without sufficient amount of entropy. In order to collect sufficient amount of entropy within a reasonable amount of time, it is preferred to use a dedicated hardware random number generator (HRNG).

6.2 Security Protocols

6.2.1 Introduction

There exist communication protocols that are specifically developed to provide security, such as Transport Layer Security (TLS), Internet Protocol Security (IPSec)/Internet Key Exchange (IKE), and Secure/Multipurpose Internet Mail Exchange (S/MIME). Often, these protocols are used in addition to the existing protocols to construct secure systems.

6.2.2 Transport Layer Security (TLS)

TLS is a connection oriented protocol built upon Transmission Control Protocol (TCP) that establishes secure connection between application processes. A connectionless version based TLS known as Datagram TLS (DTS) is also specified upon User Datagram Protocol (UDP). TLS is designed to provide identity authentication and confidentiality at transport/session layer. It is most commonly used by web services based on HTTPS protocol to authenticate a web server and to encrypt the communication with the server. In addition, it has a capability of client authentication in the form of mutual authentication, which is critical to some applications such as Virtual Private Network (VPN). A number of applications of TLS exist today.

TLS uses a digital signature algorithm to authenticate entities, and then establishes a shared secret using either a public key encryption algorithm or a key agreement algorithm during the connection establishment handshake. Then, the subsequent user data transmission is protected by symmetric algorithms using secret keys derived from the established shared secret. Confidentiality is provided by a symmetric cipher, and usually message integrity is achieved by using a MAC algorithm. Alternatively, an Authenticated Encryption with Associated Data (AEAD) mode of a block cipher such as Advanced Encryption Scheme Galois Counter Mode (AES-GCM) can be used to achieve both.

Most commonly used digital signature algorithm is RSA, followed by ECDSA, although it also supports DSA. For the key establishment, the use of RSA encryption algorithm is considerably reduced in favour of perfect forward secrecy provided by the key agreement algorithms, such as DH and ECDH.

In the TLS connection establishment handshake, authentication is performed first, followed by key establishment. In this manner, the public keys used in the key establishment phase can be trusted.

Since TLS has extensive use of classical public key cryptographic algorithms to establish security, both authentication and confidentiality, it is considerably vulnerable to quantum attacks. Thus, in order to cope with quantum attacks, the digital signature algorithm and key establishment algorithm has to be replaced with quantum resistant versions of algorithms to maintain its security claim. It should be noted that TLS has an option to use pre-shared secret instead of public key cryptography, although it has not been widely deployed. If pre-shared secret is used, the TLS security relies only on symmetric cryptography, which can resist quantum attacks by doubling the key size.

6.2.3 Internet Protocol Security (IPSec)/Internet Key Exchange (IKE)

IPSec/IKE is designed to provide network layer security. IPSec accomplishes data confidentiality using symmetric algorithms. The symmetric keys of IPSec are derived from the shared secret established by IKE. IKE was built upon key agreement, such as DH, or ECDH, for the generation of shared secret, and symmetric cryptography with pre-shared secret for authentication. IKE also allows to use digital signature or public key encryption for authentication. However, most deployments use a pre-shared secret.

In IKE, shared secret generation with a key agreement is followed by authentication. This means that it uses unauthenticated key agreement, which is different from TLS. One of the reasons for this is that this allows to hide the identity of the communicating parties by performing authentication over an encrypted channel. Along with that it is a network layer protocol, this provides some important features to construct a VPN.

The shared secret generation of IKE is vulnerable to quantum attacks. Therefore, it has to be replaced by a quantum resistant key exchange algorithm. For the authentication, unless a digital signature is used, doubling the key sizes of symmetric algorithms should suffice. If a digital signature algorithm is used, it has be replaced by a quantum resistant equivalent to retain its security level.

6.2.4 Secure/Multipurpose Internet Mail Exchange (S/MIME)

S/MIME is a security protocol for electronic mail (e-mail). It uses digital signature for authentication and public key encryption for secrecy. Unlike TLS or IPSec/IKE, a secure e-mail protocol has to be one pass. This is the reason for the use of public key encryption algorithm instead of key agreement. Although S/MIME allows key agreement such as DH or ECDH, the key agreement is used to construct public key encryption by using a static key pair for the receiver side and an ephemeral key pair for the sender side. S/MIME sacrifices perfect forward secrecy to accomplish one pass protocol.

S/MIME uses public key cryptography for its security. Therefore, it is also vulnerable to quantum attacks. It is necessary to replace these public key cryptographic algorithms with quantum resistant equivalents in order to cope with the threats by quantum computers.

6.2.5 Public Key Infrastructure (PKI)

Digital signature algorithms are not sufficient to establish entity authentication because a public key may not be trusted. PKI is a mechanism to authenticate a public key by a trusted third party. It uses a digital signature algorithm to achieve cryptographic security. A trusted third party referred to as a Certificate Authority (CA) validates the identity of an entity and its public key, compose a digital certificate that contains the identity and the public key of the entity, and digitally signs the certificate. An entity presents it digital certificate, and generate signature on a random challenge to prove its identity, while the recipient verity the digital signature on the challenge to confirm the possession of private key corresponding the public key in the certificate, and validate the certificate by verifying the CA's signature on the certificate. PKI is essential in establishing authentication in protocols such as TLS and S/MIME.

Most PKI systems of today uses RSA for the digital signature algorithm, and some use ECDSA. Quantum computers invalidate the security of these algorithms. Therefore, a quantum-safe digital signature algorithm is needed to build PKI systems that is safe against quantum attacks.

6.2.6 Application of security protocols

Security protocols such as TLS and IPSec/IKE are in used in a number of applications. Most notable among such applications are VPN and Wi-Fi. Since these applications rely their security on the underlying security protocols, such as TLS or IPSec/IKE, they are vulnerable to quantum attacks unless these underlying security protocols are upgraded to cope with quantum attacks.

Most VPN is constructed upon IPSec/IKE or TLS. IPSec/IKE is particularly popular among location-to-location VPN. One of the reasons is that IPSec/IKE allows to hide the entities on the Local Area Network (LAN) within a location. An eavesdropper can capture the packets between the two locations to observe the network addresses of source and destination as those of gateways of each location, but the source and destination entities within each LAN that are actually communicating cannot be identified. TLS based VPN is more popular among endpoint-to-location VPN, partly because the configuration of TLS based VPN is simpler.

Security of Wi-Fi is established by Wi-Fi Protected Access (WAP) or Wi-Fi Protected Access II (WAP2). WAP and WAP2 can achieve confidentiality and authentication by symmetric cryptography, typically along with pre-shared secret. Additionally, WAP and WAP2 Enterprise support TLS in Extensible Authentication Protocol (EAP).

7 Industry specific issues

7.1 Banking and e-commerce

NOTE 1: This clause does not provide an exhaustive list of industries that may be affected by the advent of Quantum Computing as a threat to security but is indicative of such industries.

E-commerce and online banking are domains that inherit many of the PKI problems. For some instances, particularly in online banking, there has been a move towards 2-factor authentication schemes as part of access control, and a move to adopt a symmetric key based ComSec facility. Other schemes to counter robot access using tools such as Captchas have been taken across many sites and the rigours of compliance to the various data protection directives and privacy protection laws have lent the e-commerce and online banking world a sheen of good security practices. E-commerce, as exemplified by large online shopping outlets are dominated by RSA based signature schemes:

- Amazon.co.uk:
  - Signature: SHA-256 with RSA Encryption
  - Public key: 2 048-bit RSA
- Facebook.com:
  - Signature: SHA-256 with RSA Encryption
  - Public key: 256-bit Elliptic Curve
- Google.com:
  - Signature: SHA-256 with RSA Encryption
  - Public key: 2 048-bit RSA
- Co-operative Bank UK:
  - Signature: SHA-256 with RSA Encryption
  - Public key: 2 048-bit RSA

NOTE 2: The examples given above are given for illustration of the capabilities used in public and well known e-commerce and banking sites and do not imply any preference or favour to the holding organisations by ETSI.

The list above is obviously a very curtailed list. The Certificates are commonly issued with a lifetime of 12 months and are increasingly moving towards EV certs. The root certificates (the top of the PKI tree) however tends to have much longer lifetimes associated to their key pairs and certificates. The risk is to a large extent dependent on what is protected. For web-systems where data is protected in transit the risk is that such data is captured for future analysis.

The end points of most e-commerce systems are the commercial web-browsers, or smartphone based apps. Modern browsers rely on underlying mechanisms and libraries to implement their security mechanisms, for the ComSec aspects the security is afforded by TLS that is not currently quantum-safe and for any of the larger signature sizes is not currently able to support the signature field natively (there are methods to expand the signature space although current implementations tend not to support this).

Taking account of the "Y" factor, the time to replace vulnerable systems with quantum-safe alternatives requires the changes to flow down from the root of the PKI system.

7.2 Intelligent Transport Systems

There are a number of examples of Intelligent Transport Systems in development and for those that rely on classical symmetric cryptography the primary threat is that the effective strength of any operation is significantly reduced. The more concerning domains are those, exemplified by the ETSI and ISO specifications for Co-operative ITS (C-ITS), that have adopted an asymmetric cryptographic solution for authentication and authorization.

C-ITS involves the regular transmission (by all actors) of "co-operative awareness messages", or CAMs, that indicate the current location of an ITS actor (represented as an ITS-Station or ITS-S). The CAMs are broadcast and contain sufficient information to allow local identification over a short time period of distinct ITS-Ss.

From a security perspective the receiver has to be confident that the ITS-S is a genuine ITS-S of the type declared in the CAM. The confidence or assurance is achieved by signing the contents of the package and transmitting a public key certificate attesting to the validity of the key by a trusted entity. The key-pair is bound to the identity of the ITS-S but for prevention of "stalking" attacks has been marked as "short term" and is only used a small number of times before being discarded (these short term identities are treated as discardable pseudonyms). Every "new" identity (pseudonym) is tied to a new key pair and a new certificate.

In addition to CAMs there are Event Notification Messages (generally known as DEM for historic reasons) that inform of specific events - accidents, weather events and so on. These messages are similarly geo-located, time-located and identifiable to a single ITS-S.

The current crypto-solution of C-ITS is to use ECC to sign transmissions and to use 2 key structures at any one time in the ITS-S, with certificates of 2 types generated by 2 non-colluding authorities. Authority 1 attests the long term identity of the ITS-S, Authority 2 attests the short term identities. Authority 2 should have no knowledge of the long term identity, and Authority 1 should not be able to link the short term identity to the long term identity. However, if the authorities are able to collude (perhaps by a lawful request) it is possible to map the long term and short term identities (giving rise to reversible pseudonyms) and thus to identify the actor in any particular exchange (e.g. in an accident where one or more of the vehicles leaves the scene it may be possible by analysis of any retained CAM/DEM transmissions to identify the missing vehicles). In particular it is required that CAM and DEM transmissions from the same vehicle should be un-linkable (they refer to different forms of information). The overall PKI architecture of C-ITS is shown in figure 1.

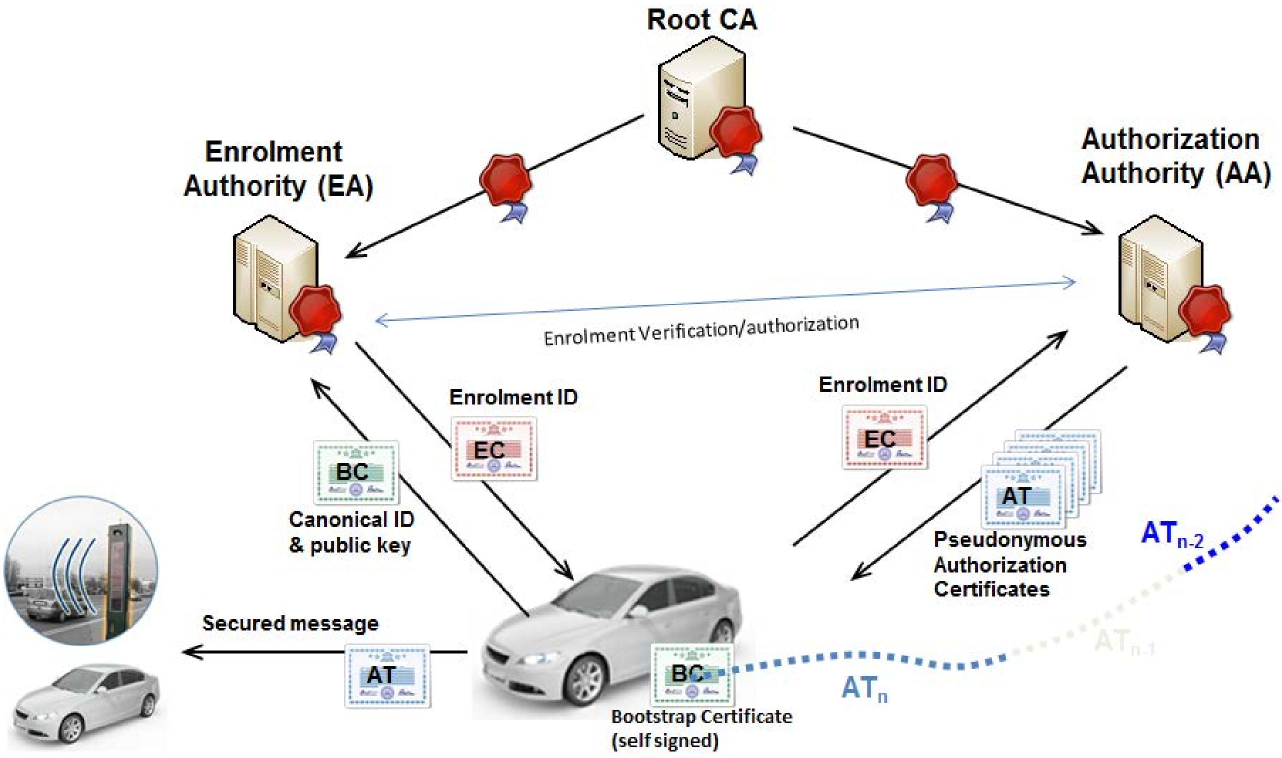

Root CA
Enrolment Authority (EA)
Authorization Authority (AA)
Enrolment Verification/authorization
Enrolment ID
EC
Enrolment ID
EC
BC
Canonical ID & public key
AT
Pseudonymous Authorization Certificates
AT_{n-2}
AT_{n-1}
AT_n
Secured message
AT
BC
Bootstrap Certificate (self signed)

Figure 1: PKI architecture (from ETSI TS 102 940 [i.8])

On the assumption that the C-ITS architecture is maintained then the QSC challenge is in defining and specifying algorithms that meet certain criteria for key pair generation rate and certificate generation rate between the ITS-S and the AA (this is where the pseudonyms and the authorization they are tied to be enforced). The characteristics of C-ITS are such that an ITS-S will receive 10s or 100s or even 1 000s of signed transmissions per second that should all have their signatures verified.

The attack scenario for C-ITS is that the root key of the signing authority is compromised. As a consequence, the authority of the systems, hence the trust of actors in the system, is nullified.

The consequence is that a rogue actor may be able to introduce data that appears to be authoritative to the system and may force real world accidents - in the ETSI requirements a check for plausibility of message content has been identified but not specified that may assist in filtering out rogue data although if the trust mechanism has been compromised this may be difficult to manage.

It is suggested in clause 4 that all systems developed and likely to be in use at the time when viable quantum computers exist (as an attack vector) have to be "crypto-agile". In C-ITS where the technology may be embedded into vehicles with a potential on-road life of 20 years (or more) and built to lowest cost principles there is a risk that such crypto-agility will not be realized. In a mixed community of crypto-agile and non-crypto-agile devices there is a reasonably high probability.

For consideration of the "Y" factor the greatest issue in ITS is the number and nature of ITS devices and their ability first to exhibit crypto-agility facilities, and secondly to attach to an update network. Where devices are crypto-agile, but where that agility is not accessible "over the air", devices have to be physically accessed and the nature of ITS in general is that service points able to perform this kind of work either do not exist or are only routinely accessed at long intervals (12 monthly or greater). However it is noted that in C-ITS the data transmitted is not confidential but rather the attributes of authenticity and integrity are protected but that protection only has to be valid over a relatively short period of time.

7.3 eHealth

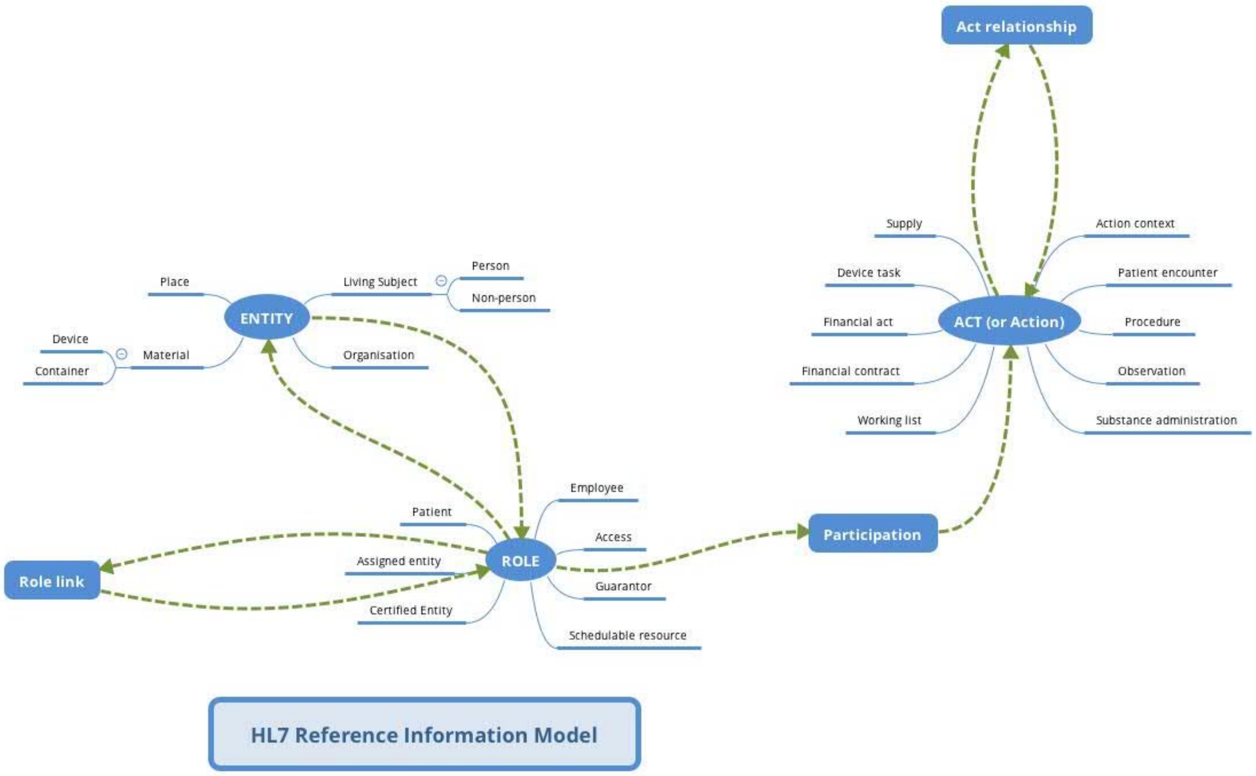
eHealth is, like ITS, a complex and multi-faceted industry. There is a data driven element in the context of health records, there are domain such as tele-medicine, tele-health-diagnostics, tele-health monitoring, and so on that all have distinct security requirements. For the case of health records in eHealth a health record is created not long after development of the foetus and 'belongs" initially to the health record of the mother, with links to the father's health record. The health record is transferred to the child when born and remains with that individual throughout the life of the individual, and is maintained for some time after death as part of the genetic and familial health record for assistance in treating offspring and siblings and close societal members (if incidents are geo-tagged and the location of individuals are known then responses to outbreaks can be geo-tracked too).

The contents of a health record are confidential but need to be accessed by many parties over the lifetime of the record. The record is highly dynamic and is added to by many parties over the life of the patient. Not all parts of the record should be readable by all parties to the record. Additionally, there are limited parties who will be able to write to the record. Not all of the parties will be known in advance and many may not exist at the time of creation of the record. It is worth noting that as advances in crypto technology will occur over the life of the record that different crypto technologies will apply over the life of the record. Access control may be by role, by attribute, by name and may be restricted by location, time or other contextual information.

Access control may also be overridden completely for a record to allow for emergency intervention and treatment (killing a patient by giving treatment proscribed in the health record because that data was not accessible is not going to be a valid defence).

Each part of the record and the entirety of the record has to be able to attest to its integrity.

A health record is not a single document and the overall structure has been standardized by HL7 (a simplification of the normative content of the information model is shown in Figure 2 derived from information available in ISO/HL7 21731 [i.5]).



NOTE: Adapted from ISO/HL7 21731 [i.5].

Figure 2: HL7 reference information model

The messaging protocol for HL7v3, as it is a normal XML structure, is presumed to be protected (for comSec) using conventional XML transfer security functions.

There are many threats in eHealth when it extends beyond the health record and for now ignoring the privacy angle (working on the assumption that private data has to be made available without always being able to get explicit consent) there are certainly threats from hijack of sensors and actuators, from false data injection and from modification or deletion of data.

The protection thus has to address at least the following:

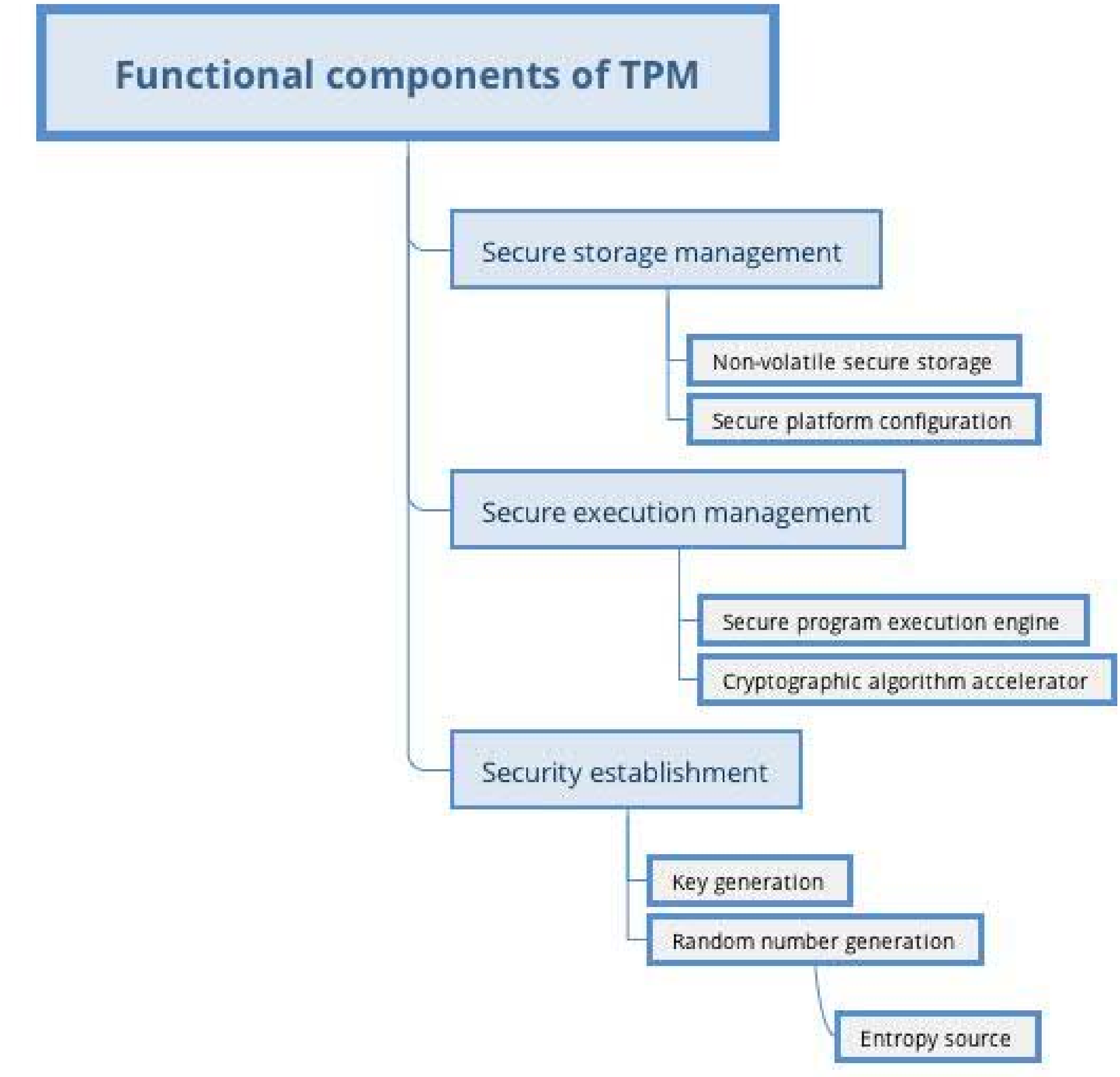
- Multi-party read and write access
- Very long confidentiality period
- All records and transmissions to be confidential but any single actor should be unable to see all of the record
- Inference attacks have to be protected against (part of the identity management requirements set)

There may be cases in eHealth where homomorphic encryption will apply - for instance modifying a dose of drugs, or altering the date of an appointment, without decrypting and re-encrypting data. It may be reasonable to assert that operations on encrypted data will be required and that confidentiality will need to be retained thus any QSC capability should be able to support such homomorphic encryption capabilities.

In practice eHealth systems are inherently complex as the X factor (time that encrypted data needs to be unbroken) for stored records is very long, and the number of devices and records is very large (tens or hundreds of billions) and very geographically distributed, which leads to very high values assigned to the Y factor. Thus the vulnerability of such systems and the need to ensure long term crypto-agility is managed will be essential.

7.4 Trusted Platform Modules

The Trusted Computing Group prepares a number of standards for embedded modules to address platform security and a summary of the capabilities is given in Figure 3. As of the most recent version of the TPM platform specification the algorithms supported are not quantum-safe, however TPM 2.0 does support crypto-agility that suggests that compatible implementations will be in a position to migrate to QSC in due course. However the scope of current TPM crypto-agility has not explicitly addressed the primitives for quantum-safe cryptographic primitives.


Functional components of TPM
Secure storage management
Non-volatile secure storage
Secure platform configuration
Secure execution management
Secure program execution engine
Cryptographic algorithm accelerator
Security establishment
Key generation
Random number generation
Entropy source

NOTE: Adapted from material found in http://www.trustedcomputinggroup.org/.

Figure 3: TPM architecture

For many domains, e.g. ITS, eHealth, the adoption of a crypto-agile TPM may be a recommended step in achieving quantum-safe behaviour.

7.5 Digital Media and Content Protection

7.5.1 System overview

Digital media content yearly revenue is measured in the trillions of dollars. All of these systems' content protection scheme, and so the revenue stream, is predicated on the security of the elliptic curve discrete log problem. It is now well known or understood that EC is invalidated by Quantum Computing thus the revenue of the digital media delivery industry is at risk (i.e. removing content protection becomes trivial and thus copyright violation and revenue bypass becomes an increasingly relevant threat).

The number of deployed devices, estimated as in excess of 4 billion certified devices, represents a not insignificant endeavour to continue to secure this trillion dollar revenue scheme. The impact of the number of devices, and the number of entities involved in the supply chain, suggest that management of the "Y" factor will be critical in making a safe transition to quantum-safe crypto platforms for media protection.

7.5.2 Digital Transmission Licensing Authority (DTLA)

The *Digital Transmission Licensing Authority (DTLA)* exists to define and license the use of the Digital Transmission Content Protection (DTCP) specifications. DTCP is a secure connection specification for audio-visual content for transmission between other network devices that can authenticate compliance with DTCP.

DTCP uses Elliptic Curve Digital Signature Algorithms (ECDSA) to authenticate devices using a digital certificate. In addition, these devices use an Elliptic Curve Diffie-Hellman (ECDH) key exchange to establish a shared authentication key between certified devices, which ultimately is used to protect digital content during transmission between devices.

Typical use cases supported by the DTCP specifications are the following:

- View Content Anywhere in the Home:
    - DTCP allows consumers to network DTCP certified devices to seamlessly share digital content between devices on a home network.
- Record for Personal Enjoyment:
    - DTCP has defined content protection mechanisms that allows a legitimate consumer to make copies of broadcast or subscription media. In addition, it provides mechanisms like copy once, or no copy possible, ensuring the devices that can play protected media will not make un-authorized copies of the content.
- A High Degree of Interoperability:
    - A key mission of the DTCP is develop an eco-system of interoperable customer devices to proliferate the utility of in-home digital media networking.

7.5.3 Digital Living Network Alliance (DLNA®)

The *Digital Living Network Alliance (DLNA®)* is an industry standards consortium focused on delivering interoperable consumer products for the connected home. In addition to developing the standards, DLNA has defined a certification program for conformance to their published guidelines [i.6]. There are over 4 billion certified DLNA devices at the time of this writing as reported by DLNA. The DLNA Link Protection uses DTCP-IP and relies on the same ECDSA and ECDH schemes to protect content during transmission.

7.5.4 Advanced Access Content System Licensing Authority (AACSLA)

Advanced Access Content System Licensing Authority (AACSLA) publishes the *Advanced Access Control System (AACS)* specification. This defines the underlying content protection system that is used to protect Blu-Ray™ media. The specification defines a method for licensed drives and hosts to authenticate and perform a key agreement scheme utilizing ECDSA and ECDH, to derive a BusKey to secure content between a drive and host [i.7].

8 Summary, conclusions and recommendations

As is noted in ETSI EG 203 310 [i.4] a very simple equation outlines the extent of the problem of evolution to a QC safe deployment of cryptography:

- X = the number of years that 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 cryptographic toolkit, using quantum computers or other means.
- T = the number of years it will take to develop trust in quantum-safe algorithms.

If "X + Y + T > Z" any data protected by that public key cryptographic system is at risk and immediate action needs to be taken. There is some limited ability to control T once a set of primitives are developed and put into applications, there is also some ability to assess Y but the value assigned to Y is very dependent on the nature of the cryptographic deployment and the visibility of the enabled devices. The research community in developing quantum computers, and in developing new mathematical analysis of existing algorithms, will always seek to minimize the value assigned to Z which puts increasing pressure on managing the Y factor to ensure that the simplified equation is always in favour of those at risk.

As noted in ETSI EG 203 310 [i.4] the most pressing recommendation is that all users of cryptography are able to document and to trial the business continuity scenarios surrounding migration of their entire cryptographically protected set of assets to new, quantum-safe protection. This will give a clear, by industry or by sector, assessment of the Y factor, and steps should be taken to ensure that as far as is possible that Y is minimized.

Annex A: Authors & contributors

The following people have contributed to the present document:

Rapporteur:
Mr Scott Cadzow, Cadzow Communications Consulting Ltd.

NOTE: Contributions made by the rapporteur have in part been supported by EU projects i-locate (grant number 621040), SUNSHINE (grant number 325161) and UNCAP (grant number 643555).

Annex B: Bibliography

- Shannon, Claude E. (July/October 1948). "A Mathematical Theory of Communication". Bell System Technical Journal 27 (3): 379-423.

- Proos and Zalka: "Shor's discrete logarithm quantum algorithm for elliptic curves", quant-ph/0301141.

Annex C: Change History

Date	Version	Information about changes
June/July 2015	0.0.1	Initial table of contents and placeholders for contributions and discussions. Submitted to QSC#2 for discussion.
December 2015	0.0.2	Change marked contribution to QSC#04 (January 2016) for review.
July 2016	0.0.3	Updates tying more to the content of QSC-001, the white paper, and business use case analysis.
August 2016	0.0.4	Simplification of text. Stress on the crypto-agility countermeasure requirement. Additional background text added. Deletion of data that can be found in the white paper.
October 2016	0.0.5	Accepted output from QSC#07. Extension of text for Grover's algorithm. Extension of use case for Media delivery. Proposed as final draft for publication. Change of deliverable type to GR with corresponding change of template.
October 2016	0.0.6	Minor updates addressing comments received in review prior to publication approval.
November 2017	0.0.7	Rewrite of entire clause 6 addressing comments received in review.
January 2017	0.0.8/9	Correction of version numbering to align to ETSI Portal Drafts folder. Removal of Annex A. Update of ToC.
January 2017	0.0.10	Addition of key words to cover material. Removal of hanging paragraph in clause 6. Removal of all instances of the word "must" with text that is not considered as establishing a normative requirement. Some additions to the abbreviations clause.
January 2017	0.0.11	Removal of hanging paragraph, keywords change, removing change bars, rewording suggestions.

History

Document history		
V1.1.1	March 2017	Publication