ETSI TR 103 619 V1.1.1 (2020-07)

CYBER;
Migration strategies and recommendations to Quantum Safe schemes

Reference
DTR/CYBER-QSC-0013

Keywords
quantum safe cryptography

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

Essential patents

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

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

Trademarks

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

Foreword

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

Modal verbs terminology

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

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

1 Scope

The present document addresses the problem of migration to an environment in a Fully Quantum Safe Cryptographic State (FQSCS) from a non-Quantum Safe Cryptographic State. The present document provides recommendations and guidance to ensure safe transition between the two (2) states.

The scope of attack considered in the present document includes those attacks against the cryptographic elements of the system. All other elements of the system that rely upon cryptography, but which are not susceptible to attack by a quantum computer, are presumed secure and are not addressed in the scope of the present document.

NOTE: The present document assumes an orderly, planned, migration. The concept of "emergency migration" wherein external events, such as the immediate availability of a viable quantum computer that is used to attack RSA or ECC entities, requiring immediate transition to a FQSCS, is not fully addressed in the present document.

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 GR QSC 004: "Quantum-Safe Cryptography; Quantum-Safe threat assessment".

[i.2] ETSI EG 203 310: "CYBER; Quantum Computing Impact on security of ICT Systems; Recommendations on Business Continuity and Algorithm Selection".

[i.3] ETSI TR 103 305-1: "CYBER; Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

[i.4] Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - The Directory: Public key and attribute certificate frameworks".

[i.5] N. Bindel, U. Heralth, M. McKague, D. Stebila: "Transitioning to a Quantum-Resistant Public Key Infrastructure", Post-Quantum Cryptography, 2017.

[i.6] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3", 2018.

[i.7] ETSI TR 103 617: "Quantum-Safe Virtual Private Networks".

[i.8] ISO/IEC 11889-1:2015: "Information Technology -- TPM Library -- Part 1: Overview".

[i.9] ISO/IEC 11889-2:2015: "Information Technology -- TPM Library -- Part 2: Design Principles".

[i.10] ISO/IEC 11889-3:2015: "Information Technology -- TPM Library -- Part 3: Structures".

[i.11] ISO/IEC 11889-4:2015: "Information Technology -- TPM Library -- Part 4: Commands".

NOTE: The above ISO/IEC documents have been made available from equivalent documents from the Trusted Computing Group through JTC1, a joint committee of the International Organization for Standardization (ISO), and IEC (International Electrotechnical Commission) who have accepted and published the Trusted Computing Group Trusted Platform Module specification Version 1.2.

[i.12] ETSI TR 103 087: "Reconfigurable Radio Systems (RRS); Security related use cases and threats".

[i.13] Bob Blakley, CITI Group, proceedings of ETSI/IQC Quantum Safe Cryptography Workshop 2019: "How can businesses respond to the quantum threat to cryptography?".

NOTE: Available at https://docbox.etsi.org/Workshop/2019/201911_QSCWorkshop/EXECUTIVE_TRACK/CITI_BLAKLEY.pdf.

[i.14] Amy M., Di Matteo O., Gheorghiu V., Mosca M., Parent A., Schanck J. (2017): "Estimating the Cost of Generic Quantum Pre-image Attacks on SHA-2 and SHA-3", In: Avanzi R., Heys H. (eds) Selected Areas in Cryptography - SAC 2016. SAC 2016. Lecture Notes in Computer Science, vol 10532. Springer, Cham.

NOTE: Available at https://link.springer.com/chapter/10.1007/978-3-319-69453-5_18.

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

crypto-agility: property that permits changing or upgrading cryptographic algorithms or parameters

Fully Quantum Safe Cryptographic State (FQSCS): state of the system wherein all cryptographic assets use Quantum Safe Cryptography (QSC)

inventory: set of cryptographic assets and processes in the system

migration: set of processes, procedures and technologies required to transition from non-QSC to FQSCS

non-Quantum Safe Cryptographic State (QSC): state wherein cryptographic assets use classical, non-Quantum Safe Cryptography (QSC)

platform configuration register: storage used for platform configuration measurements which are normally cryptographic hash values of the running code

quantum safe: not vulnerable to quantum computing attack

3.2 Symbols

Void.

3.3 Abbreviations

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

CA	Certification Authority
CSR	Certificate Signing Request
ECC	Elliptical Curve Cryptography
FAQ	Frequently Asked Questions
FQSCS	Fully Quantum Safe Cryptographic State
HBSE	Hardware Based Security Environment

HSM	Hardware Security Module
IBE	Identity Based Encryption
ICT	Information and Communications Technology
KMS	Key Management System
PEP	Policy Enforcement Point
PII	Personally Identifiable Information
PKC	Public Key Certificate
PKI	Public Key Infrastructure
PQC	Post Quantum Cryptography
QC	Quantum Computer (also Quantum Computing)
QSC	Quantum Safe Cryptography
RA	Registration Authority
RSA	Rivest Shamir Adleman
RTM	Root of Trust for Measurement
RTR	Root of Trust for Reporting
RTS	Root of Trust for Storage
RTV	Root of Trust for Verification
SCMS	Security Credential Management System
SE	Secure Element
SLA	Service Level Agreement
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TPM	Trusted Platform Module
VPN	Virtual Private Network
XACML	eXtensible Access Control Markup Language

4 Staged approach to QSC migration

The present document identifies a framework of actions that should be taken by an organization to enable migration to a Fully Quantum Safe Cryptographic State (FQSCS). The migration framework, and the migration plan that documents it, comprises the following three stages:

1) Inventory compilation.

2) Preparation of the migration plan.

3) Migration execution.

The present document describes the activities that fulfil each of these stages. The rationale for, and purpose of, migration is to mitigate the existential risk from Quantum Computing to cryptographic assets that is documented in ETSI GR QSC 004 [i.1] and in ETSI EG 203 310 [i.2].

NOTE 1: Annex A of the present document provides a series of checklists that summarize in tabular form the stages outlined in the remainder of the present document. Annex A is derived from a presentation made to the 2019 ETSI QSC Workshop [i.13].

NOTE 2: Annex B offers a review of the threat landscape and rationale for migration in the form of a Frequently Asked Questions (FAQ) table.

5 Stage 1 - Inventory compilation

5.1 Starting and end states of migration

The present document addresses migration of systems that use non-Quantum Safe Cryptography for various purposes, including, but not limited to: confidentiality and integrity of data at rest or in transit; authentication of users or other system elements; access control to resources of the system. Migration to a FQSCS prevents a cryptographic attack that would be aided or enabled by quantum computing.

In order to consider migration the present document identifies and defines two explicit states:

- Non-Quantum Safe Cryptographic State - the "initial state" wherein cryptographic assets use classical, non-Quantum Safe Cryptography (QSC).
- Fully Quantum Safe Cryptographic State (FQSCS) - the target "end state" of the system wherein all cryptographic assets use QSC.

5.2 Inventory compilation

NOTE 1: As identified in the definition of the term inventory, cryptographic assets and processes in the system are likely to present in a number of forms, in which the cryptographic dependency may or may not be immediately apparent. In addition many of the cryptographic assets have dependencies on organizational assets, or on specific hardware or software infrastructures, that have to be identified in the inventory.

Migration cannot be planned without prior knowledge of the assets in the organization that will be impacted by a Quantum Computer and the application of quantum computing. Thus the first stage of migration is to identify the set of cryptographic assets and processes in the system (the inventory). The assets can be present in a number of forms, including hardware and software. To identify the assets of the system, and assist in the compilation of the system inventory, at least one of the following resources should be used:

1) the questions contained in clause A.1 of the present document; or
2) the methods described in ETSI TR 103 305-1 [i.3].

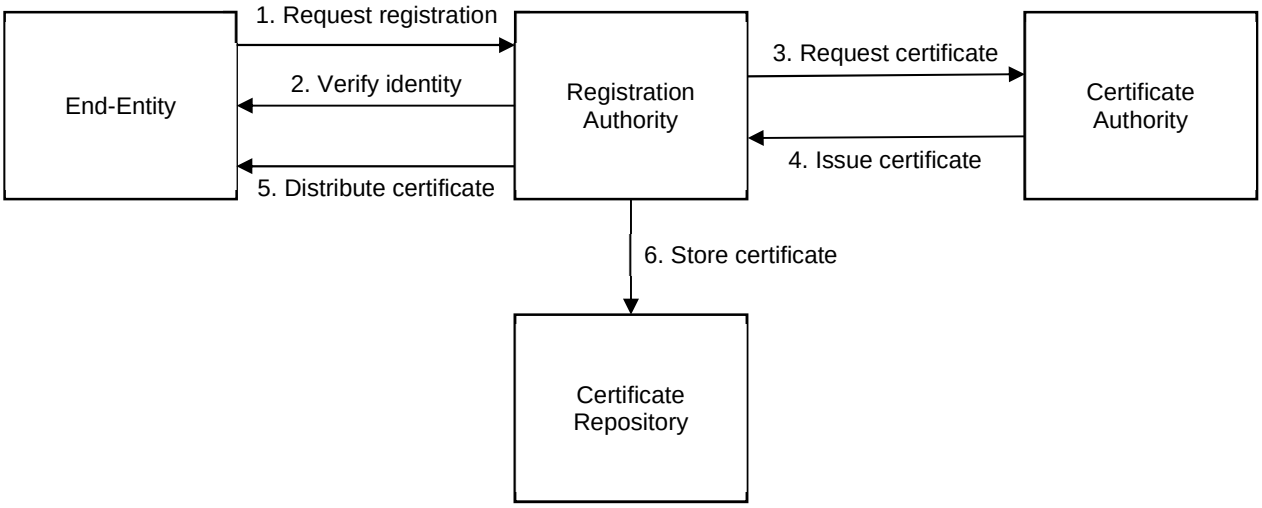
NOTE 2: The resources listed above are complimentary and can be used in combination.

If assets identified in the inventory are not in the control of the organization but need to be migrated to achieve FQSCS, the dependency, including the party liable to assure migration of the asset, should be clearly indicated in the inventory.

EXAMPLE 1: A software asset is obtained from an "app-store" and is signed by a 3rd party with a classical (quantum vulnerable) algorithm that asset's cryptographic protections (e.g. signature) details need to be listed in the inventory and the liable party for updating the signature noted.

Many assets listed in the inventory will have dependencies on management processes and procedures that may be retained in whole or in part at the FQSCS. The most obvious of these dependencies are the means by which keys are managed.

EXAMPLE 2: Management of keys for an asymmetric cryptographic system is enabled using a PKI system, such as shown in Figure 1. This forms part of the key management entity. There are parts of the PKI system that are not strictly vulnerable to attack by a Quantum Computer.



NOTE: The ordering of steps 5 and 6 is not strict and can be taken in either order or performed in parallel.

Figure 1: Example public key architecture and registration process

The inventory compilation should capture the abstract entities and functions that deliver cryptographic protections that will be subject to migration.

EXAMPLE 3: The role of entities such as Certificate Authorities do not necessarily change as a result of the migration process but the means by which to implement their role can change.

EXAMPLE 4: The abstract meaning of messages such as those shown in Figure 1 do not change as a result of migration, but the means by which these messages are implemented can change.

Many of the assets that will be identified in the inventory require a trust management framework, and/or a credential management framework. For such entities that rely on specific roots of trust, the inventory should include identification of the root of trust of the asset. A summary of various trust models can be found in clause G.4 of ETSI TR 103 087 [i.12] and the form should be identified in the inventory along with the trust chain and function it contains. Forms of roots of trust include the following:

- Root of Trust for Verification (RTV) - this provides a cryptographic accelerator to verify digital signatures associated with software/firmware and creates assertions based on the results.
- Root of Trust for Storage (RTS) - this provides a protected repository and a protected interface to store and manage keying material.

NOTE 3: The RTS often maintains the Platform Configuration Registers (PCR) output from secure boot and configuration processes.

- Policy Enforcement Engine - to enforce the capabilities of the security policy (can be considered as analogous to the combination of Policy Administration Point, Policy Decision Point and Policy Enforcement Point (PEP) in protocols such as XACML).
- Root of Trust for Measurement (RTM) - to undertake the measurement of system state, typically taking a cryptographic hash of the particular platform element.
- Root of Trust for Reporting (RTR) - for use in services such as remote attestation.

NOTE 4: The root of trust can be implemented in a number of ways including specific chipsets or by specific combinations of software and chipsets.

NOTE 5: The term "root of trust" is nearly but not quite synonymous with the term "trust anchor" and both terms are used throughout the present document. The distinction that most often applies is that a service is anchored, thus for example RTV is a service that will be implemented at a trust anchor, where the anchor is the physical entity such as an HSM.

In normal asymmetric encryption practice the principal creates a key pair. As part of the inventory and closely related to the preparation of the migration plan there should be an assessment of the ability of devices (acting on behalf of the principal) to generate and store a key pair for the Quantum Safe Cryptography solution that will ultimately replace the non-Quantum Safe solution.

NOTE 6: For the particular case of Functional Encryption systems such as in Identity Based Cryptography the public key remains constant (e.g. an email address in IBE) across the non-QSC and QSC states. However the underlying algorithms, and secret key generation, are mutable between the non-QSC and QSC state.

NOTE 7: The cryptographic primitives of the Trusted Platform Module (TPM) model from the Trusted Computing Group (TCG) are not, in level 2 [i.8], [i.9], [i.10], [i.11], fully cryptographically Quantum Safe but there is some provision for cryptographic agility within the same or similar families.

EXAMPLE 5: Many HSMs offer the ability to update cryptographic parameters, such as changing the curve in elliptical curve cryptography and have crypto-agility only within the same cryptographic model.

5.3 Business process requirements for stage 1

As a business process the compilation of the inventory should be carefully managed.

1) Appointment of a migration inventory manager:

   - A single manager should be appointed with responsibility for compiling the inventory.

   - The migration inventory manager should report to the migration planning manager.

2) Allocation of budget for inventory compilation:

   - The compilation of the inventory can incur significant cost (financial, temporal, organizational and for technical provisions) if no equivalent inventory already exists.

NOTE: Whilst most organizations have some form of asset inventory this may need to be extended to address the specific aspects of an asset that are required to plan migration.

Figure 2 illustrates an example of the form of organization chart. The roles for migration identified here and in clauses 6.8 and 7.3 should be integrated to the existing organization such that it is clear the migration is a board level activity (i.e. senior strategic management).

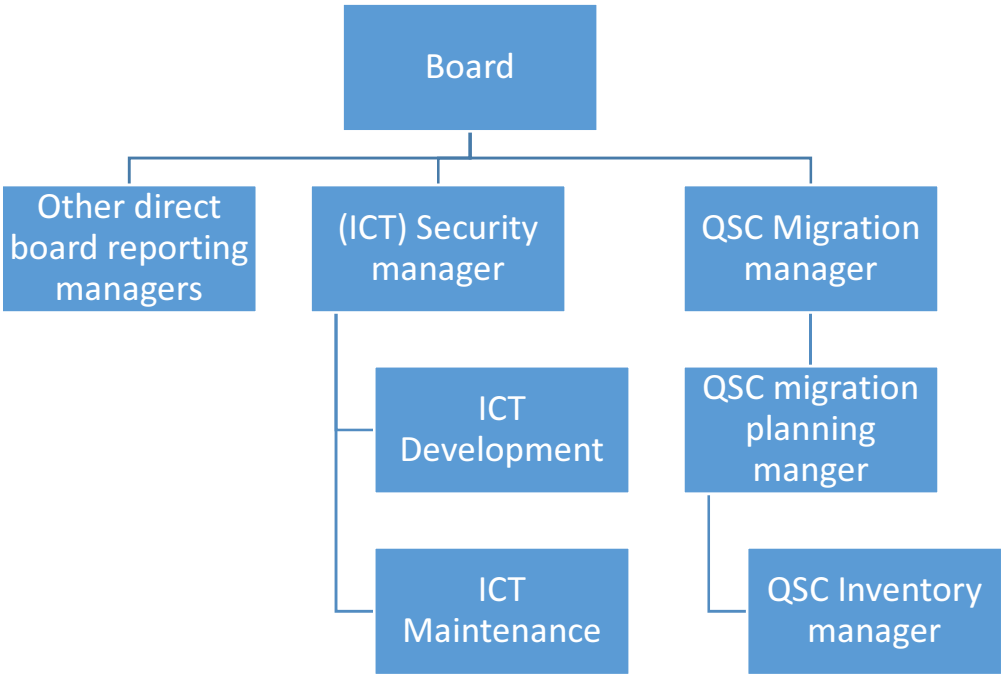


Figure 2: Example organization chart showing peer relationship of the ICT Security tree and QSC migration management tree

6 Stage 2 - Preparation of the migration plan

6.1 Creation of the migration plan

NOTE 1: It is assumed that migration will be like-for-like, that an asymmetric cryptographically protected asset will be protected in like manner after migration, and that symmetric cryptographically protected assets will likewise also be protected in like manner after migration.

NOTE 2: Whilst the focus of the present document is on migration from algorithms and other cryptographic protections that are vulnerable to attack by a quantum computer it is recognized that other quantum mechanical effects are used in the cryptographic domain, including Quantum Key Distribution and Quantum Random Number Generators. These mechanical effects are not addressed in the present document as they are not considered vulnerable to the forms of quantum computing attack that the migration described is intended to mitigate.

After completing stage 1 (Inventory compilation) as defined in clause 5, stage 2 can be started: preparation of the migration plan.

The set of questions contained in clause A.2 of the present document should be used to assist in the preparation of the migration plan.

The migration plan should include the following:

- A full inventory of assets as described in clause 5.
- For each asset:
  - Whether a given asset will be migrated.

NOTE 3: Not all assets will need to be migrated. Some assets can be retired, or made obsolete through redesign.

  - When a given asset will be migrated.
  - An orderly sequence of migration of inter-dependent assets.

NOTE 4: When, and in what order, assets are migrated depends on an understanding of their cryptographic relationship and any dependencies, which should have been identified in the inventory.

- The migration solution chosen for each given asset: replacement by full QS crypto or a hybrid solution.

- Testing including dependency testing.

Any cryptographic entity requires that the credentials (e.g. keys) are managed. Organizations can have many such Security Credential Management Systems (SCMSs) for management of both symmetric and asymmetric cryptography. The most common form of an SCMS for asymmetric keys is a Public Key Infrastructure (PKI) and specific provisions should be made for such PKIs (and SCMSs in general). For any PKI in the inventory, and the Public Key Certificates (PKCs) that implement it, every entity in the PKI will need new PKCs that contain Quantum Safe public keys. If backwards compatibility is required during a phased migration, then the application will have to support both classical and Quantum Safe algorithms. This may be achieved using individual classical and Quantum Safe end-entity certificates, or by using hybrid certificates depending on the cryptographic agility of the existing application. The following should all be considered in developing the migration plan:

- The capabilities and limitations of the various entities in the PKI:

  - The planning should identify the ability of any PKI entity to handle certificates containing the larger Quantum Safe public keys and signatures. If any PKI entity cannot handle QSC primitives these entities should be marked for replacement.

NOTE 5: The ability to update (this includes the timing of the update) an existing CA can depend on the state of migration of individual participants in the supply chain.

NOTE 6: Recommendation ITU-T X.509 [i.4] specification for PKCs supports a number of modes that allows for staged migration including hybrid modes.

- A PKI that has been updated to use Quantum Safe cryptography will need new trust anchors and certificate chains that contain Quantum Safe signatures:

  - If backwards compatibility is required during a phased migration, then the PKI will have to support both classical and Quantum Safe signing algorithms, which can be handled either by using parallel classical and Quantum Safe certificate chains, or by using hybrid certificate chains depending on the cryptographic agility of the existing relying parties.

- Migration planning should take into account the interplay between upgrading the PKI and upgrading the various applications that depend on it. There may be an order of operations necessary in order to minimize cost or downtime in the process. In this case the analysis and inventory of cryptographic deployments should clearly identify dependencies that will allow the lead authority for migration to cater for such dependencies, i.e. if A depends on B, then B should be migrated before A.

- Provisions for cryptographic agility should be considered for any new or updated entities in the PKI:

  - If a vulnerability is found in the Quantum Safe algorithm, it may be necessary to switch to a different Quantum Safe algorithm entirely, although in some instances the specific vulnerability may be addressed by restricting modes or by revising the strength of individual parameters. Ensuring cryptographic agility will make this significantly easier.

As highlighted above migration requires detail planning based on knowledge of the inventory of cryptographic assets and their dependencies across the system supply chain. In any system the cost of implementing an intermediate step impacts the migration choices. For X.509 based PKI systems it is possible to migrate to the QSC end-state by hybridising the cryptographic modes, allowing classical and QSC modes to co-exist.

The migration plan should address the timing of migration and this implies understanding of cryptographic dependencies.

NOTE 7: Migration and initial deployment design will achieve the same end-point but migration differs only insofar as there is an existing (working) deployment that supports business functions that can be sensitive to disruption.

As stated in clause 5 above the inventory of assets should be clearly visible in any plan. The migration plan should stress the role of dependency testing.

Only when the migration plan is in place can migration be implemented.

6.2 Migration issues

Migration is the set of processes, procedures and technologies required to transition from non-QSC to QSC. The development of the migration path requires knowledge of the root or anchor of the security function of each asset. Every link in the chain of security with a QC vulnerability, or a dependence on an asset with a QC vulnerability, should be updated for migration to be considered a success.

EXAMPLE 1: Forms of roots or anchors of trust include the key manager for a cryptographic operation, and the Certificate Authority (CA) or Registration Authority (RA) for a certificate in a PKI.

EXAMPLE 2: If an asset creates an asymmetric key pair to be associated in a public key certificate to an attribute of the asset (normally its identity) a number of actions are taken in sequence for the distributable key to be usable that includes:

- The key generator has a source of entropy sufficient to ensure keys are suitably random (i.e. the entropy source for an RSA-3072 key is at least 128 bits (the relative security strength metric)).
- The signature used to prove the binding of attribute to the key pair needs has security strength at least equal to that of the key generator; and so on.

If an asset's primary state (i.e. its native state) is that no cryptographic operation has been applied, e.g. for speech transmission over an encrypted radio channel, the migration only impacts the key management system and the algorithm for encryption and not the content of the speech itself. If, however, the asset's primary state is that it has been cryptographically protected then the migration should maintain those protections during the transition from non-QSC to QSC. Where the base state is that all data is encrypted and also subjected to cryptographically assured file integrity the non-QSC encryption should not be removed (i.e. go clear) prior to imposing the QSC based encryption mode.

EXAMPLE 3: If prior to migration a file on disk is encrypted with a non-QSC key and algorithm, then it is migrated in such a way that its security state (i.e. encrypted) is maintained.

6.3 Considerations for migration impact on hardware based security environment

The Quantum Computing risk to the Hardware Based Security Environment (HBSE) is that the implementation of each may not be optimized for Quantum Safe Cryptography.

Current (mid-2020) HBSEs have not been optimized for the kind of algorithms that are considered as Quantum Safe for asymmetric application. The degree to which this is an urgent concern depends on the level of cryptographic agility defined for the HSM/TPM. The current version of ISO/IEC 11889-1 [i.8], the 2015 edition, supports only RSA and ECC using prime curves, thus the current version of ISO/IEC 11889-1 [i.8] is not classifiable as Quantum Safe. Any implementation using a TPM/TSS that complies with ISO/IEC 11889-1 [i.8] will need to be migrated to a future QS variant.

The more general case of HSM (as distinct from the TPM/TSS examples in ISO/IEC 11889-1 [i.8]) is that they could already be able to support QSC, although some fielded examples of HSM can have already been in service for 10 years or more and predate the evolution of QS characteristics.

NOTE: GlobalPlatform® has started to investigate the evolution needed for secure components management (including SE and TEE) in terms of algorithms and key sizes for a use in in a QSC environment, and is more generally looking for cryptographic agility with a new Smart Card Platform (SCP) under construction.

If any asset to be migrated is dependent on an HBSE, then that HBSE should be migrated to ensure it supports the algorithm and cryptographic key requirements of the migrated asset before the depending asset is migrated.

6.4 Key management during migration

Key management is a critical element of any cryptographic application. In any one organization it is highly likely that many Key Management Systems (KMS) are deployed with a number of different formats. For further discussion of the key management topic the use of X.509 is assumed. If alternative certificate formats are used the overall structure and guidance of this clause still applies subject to the capability of the alternative format.

NOTE 1: Unless otherwise stated certificates in the present clause refer to certificates containing a single signature, where more than one signature is required, e.g. for hybrid modes, this is explicitly stated.

It is straightforward to include a Quantum Safe public key in the Subject Key Info field of an X.509 [i.4] end-entity certificate provided that the Quantum Safe algorithm has a corresponding algorithm ID and the CA knows how to encode the public key. Although Quantum Safe algorithms generally have much larger public keys than classical algorithms, experiments [i.5] have shown that many existing cryptographic libraries are able to handle large certificates. However, the ease of use of end-entity certificates containing Quantum Safe public keys depends on whether the application allows the negotiation of cryptographic algorithms; for example, via the Signature Algorithms extension in TLS 1.3 (IETF RFC 8446 [i.6]). This capability of X.509 suggests that migration using X.509 is possible now.

NOTE 2: Any certificate that has been signed using a classical algorithm, and all certificates below it in the chain, can potentially be replaced with a certificate forged by a quantum attacker.

NOTE 3: A certificate chain that relies on a classical trust anchor cannot be considered Quantum Safe.

6.5 Trust management during migration

As identified in clause 5 the inventory will have identified the trust infrastructures. As stated in clause 5 whilst the roles and relationships in the trust infrastructures and the associated key management infrastructures remain constant the means by which they perform the technical tasks may change.

EXAMPLE: A Root Authority can require that verification of CA keys is done in a face-to-face signing ceremony and thus the scheduling of such ceremonies as well as the distribution of new keys and certificates throughout the infrastructure will need to be considered in the planning of migration.

Many security primitives require a trust management framework. Multiple models have been proposed for cryptographically assured trust management that extend the models for key management in clauses 5 and 6 for the trust application or service.

A number of functions can be reliant on specific roots of trust and the transfer of each root of trust to a Quantum Safe model is a key element that is present in the migration plan.

6.6 Isolation approaches during migration

Not all systems will be updated at the same time. As a part of a migration strategy sub-systems should be isolated as far as is possible to discrete security domains. Security domains that need to be interconnected may then be interconnected by Quantum Safe pathways, such as Quantum Safe VPNs as defined in ETSI TR 103 617 [i.7].

6.7 Access to non-QSC protected resources after migration

In determining the risk to business of re-encrypting previously encrypted assets, held in an archive for example, the risk calculation can determine that it is economically infeasible to migrate all encrypted assets to a quantum safe state. In such an eventuality steps to quarantine any non-QSC resources (i.e. both physical and logical quarantine) from any external attack are included in the migration plan. In this case all non-QSC protected assets that will not be migrated are physically moved to explicitly identified quarantine zones and risk managed inside the quarantine zone. If any form of PKI and associated PKCs have been used to maintain any non-migrated assets then a reasonable facsimile of the PKI will be maintained in the quarantined zone. There is a strong likelihood that certificates and associated public keys used in protecting such assets will expire whilst in the quarantine zone and processes should be put in place to allow the cryptographic operations to continue even if normal protocols and policies fail.

EXAMPLE: Normal security policy can be to refuse to process any asset protected by an expired key, whereas for quarantined assets the key can be expected to expire whilst in quarantine and thus if access is to be enabled to the asset whilst quarantined the policy is updated to allow for recognition of the quarantined state.

However, given the nature of the QC threat, resources that have to be maintained in a secured state (e.g. encrypted, cryptographically enabled access restriction) over multiple generations of cryptography (i.e. keys or algorithms) should always be migrated to the latest generation. Assets that can be covered by such multi-generation concerns include patient health records, and some critical infrastructure assets.

6.8 Business process requirements for stage 2

As a business process, migration requires a number of requirements to be met in order to enable the migration to be executed. These business processes need to be planned, and often in place, before execution of the plan (defined in stage 3):

1) Appointment of a migration manager:

   - A single manager should be appointed with responsibility for executing the migration. The migration manager should have knowledge of the overall business/organization and should have access to all parts of the organization to ensure that each stakeholder in the migration is aware and briefed on their role.

2) Allocation of budget for migration:

   - In the task of analysing the inventory to identify which assets are to be migrated, which to be retired and which need redesign it is essential to be able to assure that budget (time, finance, facilities) are available to ensure that stage 3 can be completed.

   - It is also essential that stages 1 and 2 are sufficiently budgeted. For stage 1 this is considered in clause 5.3.

3) Management of "down time":

   - In working to develop the plan it may be necessary to close or pause parts of the organization. Ensuring this is possible and approved before entering stage 3 is essential.

7 Stage 3 - Migration execution

7.1 Migration management

After completing stage 1 (Inventory compilation) as defined in clause 5 and completing stage 2 (Preparation of the migration plan) as defined in clause 6, stage 3 can be started: migration execution.

Whilst stages 1 and 2 address, respectively, the compilation of an inventory of all crypto assets, and the preparation of a migration plan, the role of stage 3 is to implement the plan from stage 2 against the inventory from stage 1. The elements of management required for QSC migration are similar to the provisions for effective management of any other activity.

7.2 Mitigation management

Management checkpoints, added to the migration plan as stated in clause 6.1, are metrics to track progress. Where management checkpoints are missed, mitigations as detailed in the plan should be followed.

A key element of mitigation management, in the overall context of migration management, is conducting exercises to simulate and test the migration, with the aim to determine the viability of the plan. Whilst this is not, conceptually at least, different from any other migration or large project plan, there is significant value in such exercises as they can uncover missing inventory elements (it is highly probable that the inventory will be incomplete, or that the supply chain has breaks that need to be found and mitigations designed into the plan).

NOTE: The planning of mitigations as above falls in both steps 2 and 3 and as such there will be overlap in project management if and when mitigations are triggered (i.e. during execution a mitigation may need to be invoked, or an unforeseen mitigation developed).

Mitigations to unexpected events will place strain on any previously agreed budget and thus the exercises and pre-planning tests will be essential in being able to give an accurate estimate of the budget and other costs of such mitigations.

7.3 Business process requirements for stage 3

The elements of management required for a QSC migration to a FQSCS are similar to the provisions for effective management of any other business activity. To allow successful management:

1) the migration manager (see clause 6.7) should be given lead and responsibility for the process; and

2) the migration manager should be given financial and organizational backing; and

3) the migration manager should not stop partway through a phase of the migration plan.

Annex A:
Migration checklist

A.1 Inventory compilation and preparatory questions

A.1.1 Risk assessment

Quantifying the level of risk is the first step of inventory compilation. The questions relate to the threat of QC in its own right on the wider organization and its supply chain.

Magnitude	What risks will information disclosure create? Classifications of where risk lies include: Monetary loss (i.e. direct financial impact), Compliance (i.e. will existing compliance procedures be maintained?), Legal (e.g. will existing legal safeguards apply?), Reputation (e.g. how will readiness or failure be ready to impact the reputation of the organization either in absolute terms or by comparison to peer and competitor organizations?)
Duration	How long has confidentiality to be maintained for each asset or class of assets?
Scope	Are keys or certificates issued by the affected organization to third parties? Under what CPSs or SLAs?
Duration	Can damage due to degradation or interruption of each services that uses crypto be quantified?
Response	Is there a plan to protect encrypted assets in case of a crypto failure?

A.1.2 Data assessment

Many organizations group data into classes, and have policies relating to the treatment of each data class. These questions relate to capturing how such data policies will impact the inventory.

Type	What classes of data are subject to encryption? (PII, Trade Secret, Custodial Secret, Government Classified, etc.)?
Protection duration	How long does confidentiality need to be maintained for each data class?
Retention	Is encrypted data deleted according to a regular schedule?
Disclosure impact	What are the consequences of disclosure of each data class?
Exposure	Is encrypted data normally exposed to potential attackers? (e.g. in transit or public cloud)?

A.1.3 Cryptographic assessment

These questions relate to capturing cryptographic properties of keys for the inventory.

Type	For each key, what is the strength, the algorithm binding, and the usage (signature or encryption, application specific security, etc.)?
Strength	What is the effective strength of each key in view of classical and quantum attacks?
Lifetime	What are the issuance and expiration dates for each key?
Management	Are all keys inventoried and locatable? Are keys easy to revoke and reissue?

A.1.4 Infrastructure inventory

These questions relate to the core of the inventory where an asset in the inventory can have many uses.

Crypto software inventory	What crypto libraries are in use? What protocol libraries are in use?
Key inventory	What keys are in use, by what applications?
Admin inventory	Who (or what role) is authorized to manage which keys and which crypto modules and devices?
Certificate inventory	What certificates are issued to the organization? Who issued them?
Crypto hardware inventory	What crypto hardware is in use? What attributes does each certificate have?
Application inventory	Which applications use which libraries, which keys, and which protocols?

A.1.5 Supplier inventory

These questions relate to capturing assets related to the supply chain and their role.

Certificate Authorities (CAs)	Do the organization's CA agreements hold the CA to an SLA for timely reissuance? Does the organization backup CA under contract?
Code signatures	Can and will application vendors in the supply chain re-sign applications in a timely way?
Service Level Agreements (SLAs) with the CA	Do revocation and reissuance requests get priority vs. other firms in emergencies?
SLAs with the data custodian	What obligations do the custodians of data have in case of algorithm breach?
CSRs	Does the organization retain CSRs in order that the organization can request reissuance of certs with the correct attributes?
SLAs with software vendors	Are vendors in the supply chain obligated to timely upgrades to fix crypto breaches? (see note)
NOTE: This is likely to be a specific requirement if the vendor is subject to the constraints of the EU Cyber Security Act.	

A.2 Preparation of the migration plan

A.2.1 Orderly transition planning

These questions relate to engaging stakeholders in creating a plan for orderly migration.

Supplier readiness plans	Do all the suppliers in the supply chain have quantum readiness plans? Are their obligations placed on participants in the supply chain to have them?
Standards participation	Is the organization and its key partners in the supply chain participating in standards groups preparing for QSC?
Product testing	Is the organization and its key partners in the supply chain testing and certifying QSC algorithms and QSC-enabled products in advance?
Hybrid crypto	Is the organization and its key partners in the supply chain investigating or implementing hybrid classical/PQC modes of operation?
Crypto agility	Will the organizations' infrastructure support rapid replacement of crypto algorithms and protocols?
Regulatory engagement	Is the organization and its key partners in the supply chain engaging with regulators on use of PQC?

A.2.2 Disorderly transition planning

These questions relate to engaging stakeholders in creating a plan for orderly migration.

Exercises	Is the organization and its key partners in the supply chain planning and executing table top and simulation exercises for crypto algorithm failure response?
Supplier agreements	Is the organization and its key partners in the supply chain updating supplier and partner agreements to cover algorithm failure?
Saved CSRs	Is the organization and its key partners in the supply chain retaining your Certificate Signing Requests to support emergency centre issuance?
CA agreements	Is the organization and its key partners in the supply chain updating your CA agreements to cover algorithm failure?
Emergency software distribution	Is the organization and its key partners in the supply chain making arrangements to securely receive and deploy patches and updated software versions while network protocol and code signing cryptography is insecure?
E-risk coverage	Is the organization and its key partners in the supply chain investigating Cyber Insurance for cryptographic algorithm failures?

A.3 Migration execution

A.3.1 Migration management

These questions relate to business management of the migration execution phase.

Responsibility	What executive is responsible for Quantum Safety?
Project management	Is there a detailed plan for Quantum Safety? What is its priority?
Budget	Is there a budget for Quantum Safety projects?
Metrics and tracking	Are there metrics for Quantum Safety? To whom are they reported?

A.3.2 Mitigation management

These questions relate to mitigation measures if the migration execution encounters issues.

Stakeholder engagement	Are Legal, Compliance, and Corporate Communications involved in planning?
Exercises	Is the organization and its key partners in the supply chain planning and executing table top and simulation exercises for crypto algorithm failure response?
Budget	Is there a budget for mitigation of crypto algorithm failures?
Playbooks	Have exercises been used to create playbooks for mitigation?

Annex B:
Frequently Asked Questions

Question	Guidance or answer
What is impacted by a Quantum Computer?	Known attacks on the mathematical properties of some cryptographic algorithms make vulnerable algorithms null and void in terms of the security they offer. This particularly impacts popular asymmetric (public key) systems such as RSA and ECC in which all material protected by vulnerable algorithms has their protection voided. For symmetric algorithms the impact is less severe but the effective key length is at most halved (due to inherent overhead in running Grover's algorithm on realistic quantum architectures [i.14] (e.g. a 128-bit key will only offer the equivalent security of at least 64-bits)).
Can existing hardware cope with hybrid systems, in terms of memory, processing power, crypto agility?	Not always. For symmetric key systems to cope with increased key size, in the same time, the required combination of memory, i/o and processor, bandwidth may not be available. Hardcoded systems with no crypto-agility may not be able to cope at all. For many systems whilst the QSC and hybrid algorithms can be substantially different the building blocks can be the same (e.g. hash processing), however unless the base pre-QSC system has some crypto agility it can be very difficult to re-use these capabilities.
How long will migration take?	There is no simple answer as this depends on the number of cryptographic assets to be migrated. The more complex answer is in part given in ETSI GR QSC 004 [i.1] as 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. An organization is in the position to determine X and Y. Industry at large will be able to give guidance on T and Z. The migration time is a combination of Y and T with the controllable element being Y, with some risk if Y is initiated before T is complete (i.e. starting migration before trusted algorithms are available). As with all major changes in an organization migration should be practiced and tested well in advance of the necessary changeover date.
Is migration a QSC only issue?	No. All of the steps and mechanisms given in the present document apply to any migration of any technology to a new technology. The peculiarities of QSC migration are only that assets which make a claim of security that is challenged by the existence of a quantum computer (i.e. asymmetric cryptography based on discrete logarithms or on factorization) are made immediately null and void (as the trust in the mathematics that surrounds their security claim no longer holds true).
Are Distributed Ledger Technologies (DLTs) impacted by QSC developments?	A complete answer depends on the nature of the ledger and the transactions it contains. However the nature of DLTs is that the integrity of each entry (the entry can be simply the hash of an externally held transaction) and each page is verified by a hash and each page is verified by finding a hash of the set of transactions and a random sealing value that results in a hash of a particular pattern, with the hash of the "sealed" page being the first entry in the next page of the ledger (hence linking all pages in the ledger together). If hashing is the only cryptographic function taking place the impact of a quantum computing attack is low. However in practice transactions can also be signed and in some instances encrypted which significantly alters the risk assessment.
Are all cryptographic operations impacted by a quantum computer?	Yes, but to a different degree in each case. The default position prior to migration should be that asymmetric cryptographic operations are nullified, and that the cryptographic strength of all other operations are severely cut.
Are hybrid solutions Quantum Safe?	Hybrid solutions are a way-point on the path to QSC and do not represent the end state (thus a system with hybrid solutions has not achieved FQSCS). Hybrid solutions have themselves to be migrated to the end state.

History

Document history		
V1.1.1	July 2020	Publication