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

Important notice

Copyright Notification

Contents

Intellectual Property Rights 4
Foreword 4
Modal verbs terminology 4
1 Scope 5
2 References 5
2.1 Normative references 5
2.2 Informative references 5
3 Definition of terms, symbols and abbreviations 6
3.1 Terms 6
3.2 Symbols 6
3.3 Abbreviations 6
4 Staged approach to QSC migration 7
5 Stage 1 - Inventory compilation 7
5.1 Starting and end states of migration 7
5.2 Inventory compilation 8
5.3 Business process requirements for stage 1 10
6 Stage 2 - Preparation of the migration plan 11
6.1 Creation of the migration plan 11
6.2 Migration issues 13
6.3 Considerations for migration impact on hardware based security environment 13
6.4 Key management during migration 14
6.5 Trust management during migration 14
6.6 Isolation approaches during migration 14
6.7 Access to non-QSC protected resources after migration 14
6.8 Business process requirements for stage 2 15
7 Stage 3 - Migration execution 15
7.1 Migration management 15
7.2 Mitigation management 15
7.3 Business process requirements for stage 3 16
Annex A: Migration checklist 17
A.1 Inventory compilation and preparatory questions 17
A.1.1 Risk assessment 17
A.1.2 Data assessment 17
A.1.3 Cryptographic assessment 17
A.1.4 Infrastructure inventory 18
A.1.5 Supplier inventory 18
A.2 Preparation of the migration plan 18
A.2.1 Orderly transition planning 18
A.2.2 Disorderly transition planning 19
A.3 Migration execution 19
A.3.1 Migration management 19
A.3.2 Mitigation management 19
Annex B: Frequently Asked Questions 20
History 21

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].

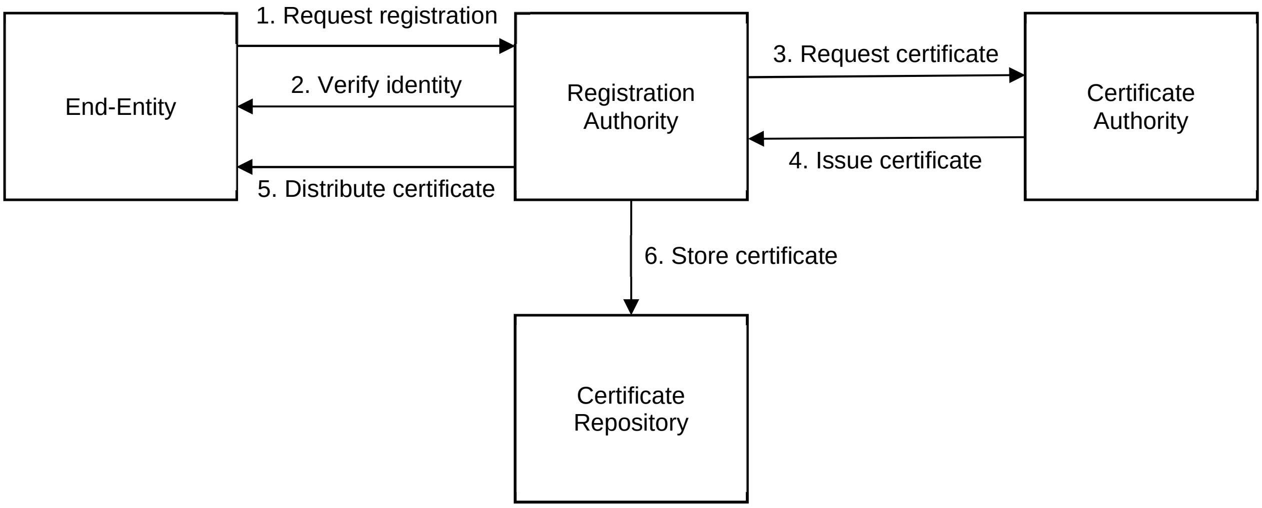
NOTE 2: The resources listed above are complimentary and can be used in combination.

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).