ETSI TR 104 005 V1.1.1 (2025-07)

TECHNICAL REPORT

Secure Element Technologies (SET); Technical Report on impacts of the post-quantum cryptography on ETSI TC SET specifications

Reference

DTR/SET-00104005

Keywords

post-quantum cryptography, SIM, UICC

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Secure Element Technologies (SET).

The contents of the present document are subject to continuing work within TC SET and may change following formal TC SET approval. If TC SET modifies the contents of the present document, it will then be republished by ETSI with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

0 early working draft;

1 presented to TC SET for information;

2 presented to TC SET for approval;

3 or greater indicates TC SET approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

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.

Executive summary

The present document is a technical report on impacts of post-quantum cryptography on the specifications managed by ETSI TC SET.

As quantum computing advances, existing cryptographic algorithms face potential vulnerabilities, necessitating a transition to Quantum-Safe technology.

The present document evaluates current ETSI TC SET specifications, including ETSI TS 102 224 [i.1], ETSI TS 102 225 [i.2], and ETSI TS 102 226 [i.3], and outlines necessary adaptations for a secure transition. It emphasizes the importance of initiating this transition despite the absence of finalized standards, e.g. from GlobalPlatform.

The present document concludes with recommendations for monitoring updates from GlobalPlatform and adapting ETSI TC SET specifications accordingly.

Introduction

Quantum computing realizations are evolving. To remain secure, systems using cryptography have to migrate to so-called "post-quantum algorithms", according to the recommendations published by the governmental security agencies.

As migration requires time to develop or update specifications and then, deploy equipment in the field, transition to post-quantum cryptography needs to be initiated without waiting for quantum computers, starting by inventorying cryptographic components.

The present document aims to assess the specifications under ETSI TC SET responsibility from the cryptography standpoint and provide recommendations for transitioning ETSI TC SET specifications to post-quantum cryptography.

1 Scope

The present document analyses the mechanisms that use cryptography in the specifications under ETSI TC SET responsibility. It describes the potential changes for a responsible industry transition to Quantum-Safe technology.

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.

- In the case of a reference to a TC SET document, a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

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 may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] ETSI TS 102 224: "Smart Cards; Security mechanisms for UICC based Applications - Functional requirements".

[i.2] ETSI TS 102 225: "Smart Cards; Secured packet structure for UICC based applications".

[i.3] ETSI TS 102 226: "Smart Cards; Remote APDU structure for UICC based applications".

[i.4] Peter W. Shor: "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer".

[i.5] Lov K. Grover: "A fast quantum mechanical algorithm for database search".

[i.6] ANSSI: "ANSSI views on the Post-Quantum Cryptography transition".

[i.7] BSI: "Quantum-safe cryptography – fundamentals, current developments and recommendations".

[i.8] NIST: "Post-Quantum Cryptography, Frequently Asked Questions".

[i.9] NSA statement: "Suite B Cryptography".

[i.10] GlobalPlatform: "GlobalPlatform Technology, Confidential Card Content Management Card Specification v2.3 - Amendment A", Version 1.2.

[i.11] GlobalPlatform: "Remote Application Management over HTTP, Card Specification v2.3 - Amendment B", Version 1.2.

[i.12] GlobalPlatform: "GlobalPlatform Card Technology, Secure Channel Protocol '03', Card Specification v2.3 - Amendment D", Version 1.2.

[i.13] GlobalPlatform: "GlobalPlatform Secure Channel Protocol '04' – Amendment K", Version 1.0.2.

[i.14] GlobalPlatform: "GlobalPlatform Card Specification v2.3.1".

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

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

AES	Advanced Encryption Standard
APDU	Application Protocol Data Unit
DAP	Data Authentication Pattern
ECC	Elliptic Curve Cryptography
KIc	Key and algorithm Identifier for ciphering
KID	Key and algorithm IDentifier for RC/CC/DS
PQC	Post-Quantum Cryptography
TLS	Transport Layer Security

4 General presentation

Cryptography has become part of our daily life, securing most of our electronic activities ranging from web browsing to mobile communications or payments. Although cryptography is a key component of digital security, it has never experienced the ever-faster cycle of attacks and patches that characterizes cybersecurity in general. Quite the contrary, cryptography has evolved quietly, without significant hitches, as epitomized by the omnipresence in current systems of 45-year-old protocols such as Diffie-Hellman key exchange or RSA signatures. Arguably, this stability is due to a good understanding of the mathematical foundations of cryptographic systems, which enables to precisely assess their concrete security level but also to identify in advance potential new threats.

Several decades ago, this approach led to identify vulnerabilities of those systems to quantum algorithms. The current public key cryptographic algorithms are proven to be compromised by the Shor's and Grover's algorithms (see note 1). The impacts on symmetric key cryptographic algorithms are still being analysed by security agencies and consensus for recommending an increase in key size has not been reached yet (see note 2).

NOTE 1: See Peter W. Shor: "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer" [i.4] and Lov K. Grover: "A fast quantum mechanical algorithm for database search" [i.5].

NOTE 2: Some security agencies (e.g. ANSSI) recommend to double the key size whereas some others (e.g. NIST, BSI) suggest that no increase is needed, see [i.6], [i.7] and [i.8].

For a long time, this quantum threat has remained elusive because of the lack of large-scale quantum computers required to run those quantum algorithms. This situation is expected to change because of the investment of many companies supported by important governmental fundings. This has led to significant advances in the design of quantum computers which would make the threat tangible from 2030 onwards (see BSI: "Quantum-safe cryptography – fundamentals, current developments and recommendations" [i.7]).

In 2015, NSA published a statement recommending to start planning the transition to quantum resistant cryptography, that is, cryptography immune to quantum algorithms (see NSA statement: "Suite B Cryptography" [i.9]). Since then, most of the security agencies worldwide have issued similar statements and recommendations to move to so-called "post-quantum algorithms". This led NIST to launch in 2017 a competition to select post-quantum standards for public key encryption and digital signatures. This competition ended in 2022 and the first standards have been published in 2024. In parallel, similar initiatives were launched by China and South Korea.

Post-quantum cryptography is the solution to the quantum threat. However, many security agencies and experts are reluctant to rely exclusively on those new algorithms because they have not been as scrutinized as classical ones. They therefore promote a phased transition where post-quantum algorithms will be used together with classical ones in a first stage so as not to weaken current security level. This "hybrid" approach is supported by most experts and agencies, with the notable exception of NSA and NIST (see [i.6] and [i.7]).

Although there is uncertainty surrounding the realization of large-scale quantum computers and the roadmaps mentioned above suggesting that it should not happen before 2030, migration process needs to start immediately. Indeed:

- Both ANSSI and BSI recommendations state that retroactive attacks cannot be ruled out. An example of retroactive attacks is the "store now decrypt later" attack, where data is gathered now for later decryption, when quantum computers are available.

NOTE: See BSI: "Quantum-safe cryptography – fundamentals, current developments and recommendations" [i.7] and ANSSI2: "ANSSI views on the Post-Quantum Cryptography transition" [i.6].

- Public key-based user authentication algorithms are not subject to retroactive attack. This means that classical algorithms could be still used, waiting for significant advances in the area of quantum computing before migrating to post-quantum ones. However, this assumes that the devices support migration features, which again calls for considering transition to post-quantum cryptography as soon as possible, at least for devices whose lifespan extends beyond 2030.

The quantum threat is likely to lead to a complete overhaul of cryptographic systems. Even if no post-quantum standards are currently available, transition to post-quantum cryptography can already be initiated by inventorying cryptographic components in standards along with the assets they protect.

5 Analysis of ETSI TC SET specifications

5.1 ETSI TS 102 224

ETSI TS 102 224 [i.1] describes the functional requirements of security mechanisms in conjunction with the Card Application Toolkit for the interface between a Network Entity and a UICC.

Regarding the cryptographic mechanisms, ETSI TS 102 224 [i.1], clause 6.2.2,contains only two high level requirements which are still valid in the context of post-quantum cryptography:

> *"When the security of a cryptographic algorithm from the technical specification is considered compromised, it may be deprecated.*
>
> *When a new cryptographic algorithm becomes state of the art, its addition to the implementation specification shall be considered."*

At the time of the publication, no particular changes are foreseen for transitioning ETSI TS 102 224 [i.1] to post-quantum cryptography. However, clause 6.2.3 of ETSI TS 102 224 [i.1] related to the recommended combinations of cryptographic mechanisms needs to be evaluated.

5.2 ETSI TS 102 225

ETSI TS 102 225 [i.2] specifies the structure of Secured Packets for different transport and security mechanisms.

The following impacts are seen, together with remediation proposals for transitioning ETSI TS 102 225 [i.2] to post-quantum cryptography.

Table 1

Impacts	Requirements to become Quantum-Safe
Coding of the KIc (clause 5.1.2) Based on symmetric encryption: • AES with length of 128, 194 or 256 bits.	AES key size security level is still under discussion by various cyber security agencies.
Coding of the KID (clause 5.1.3) Based on symmetric encryption: • AES with length of 128, 194 or 256 bits.	AES key size security level is still under discussion by various cyber security agencies.

5.3 ETSI TS 102 226

5.3.1 Introduction

ETSI TS 102 226 [i.3] defines the remote management of the UICC based on the secured packet structures specified in ETSI TS 102 225 [i.2], i.e.:

- SMS and CAT_TP based packet structures, also known as SCP80;
- HTTP-based using TLS cipher suites, also known as SCP81 and defined by GlobalPlatform in Amendment B to the GlobalPlatform Card Specification [i.11].

ETSI TS 102 226 [i.3] specifies the APDU format for remote management, as well as:

- A set of commands coded according to this APDU structure and used in the remote file management on the UICC;
- A set of commands coded according to this APDU structure and used in the remote application management on the UICC, based on the GlobalPlatform Card Specifications.

5.3.2 Analysis of the current content of ETSI TS 102 226

The following impacts are seen, together with remediation proposals for transitioning ETSI TS 102 226 [i.3] to post-quantum cryptography.

Table 2

Impacts	Requirements to become Quantum-Safe
Use of SCP81	According to GlobalPlatform PQC roadmap (see note), an update of Amendment B to the GlobalPlatform Card Specification [i.11] is not addressed yet but would rely on official cipher suites published by IETF in the future (RFC).
Remote Application Management (ETSI TS 102 226 [i.3], clause 8) Cryptographic computations, e.g. DAP, are based on AES with length of 128, 194 or 256 bits.	According to GlobalPlatform PQC roadmap (see note), an update of the GlobalPlatform Card Specification [i.14] introducing PQC is planned for beginning of 2026. AES key size security level is still under discussion by various cyber security agencies.
Confidential loading (ETSI TS 102 226 [i.3], clause 10.1) Cryptographic computations are based on AES with length of 128, 194 or 256 bits.	AES key size security level is still under discussion by various cyber security agencies.
Additional application provider security (ETSI TS 102 226 [i.3], clause 10.2) Based on SCP03 defined in GlobalPlatform Amendment D [i.12].	According to GlobalPlatform PQC roadmap (see note), SCP03 is based on a symmetric algorithm (AES), is widely used and is considered quantum-safe. Then, SCP03 will not be deprecated for now and no update of Amendment D to the GlobalPlatform Card Specification [i.12] is expected.

Impacts	Requirements to become Quantum-Safe
Confidential setup of Security Domains (ETSI TS 102 226 [i.3], clause 10.3) Refers scenarios defined in GlobalPlatform Amendment A [i.10]: • Scenario #2.B (Push Model), based on RSA; • Scenario #1 (Pull Model) using the public key scheme, based on RSA; • Scenario #3 using ECKA-EG.	According to GlobalPlatform PQC roadmap (see note), an update of Amendment A to the GlobalPlatform Card Specification [i.10] is planned in the middle of 2026. This update should introduce new PQC scenarios, should not deprecate ECC scenarios and might deprecate RSA scenarios or require a minimum key size (e.g. 3K).
NOTE: Based on the liaison statement exchange between ETSI TC SET and GlobalPlatform about PQC in spring 2025 (in document SET(25)000017).	

5.3.3 Other areas of improvement

5.3.3.1 Secure Channel Protocol '04' (SCP04)

Secure Channel Protocol '04' (SCP04), defined by GlobalPlatform in Amendment K to the GlobalPlatform Card Specification [i.13] is designed to be crypto agile, i.e. algorithms may be replaced with less effort by other algorithms when vulnerabilities are found, or more secure algorithms become available.

The current version of Amendment K to the GlobalPlatform Card Specification [i.13] includes algorithms SM3/SM4 in addition to AES.

With respect to clause 10.2 [i.3], Additional application provider security, the details of the encapsulation of SCP04 in SCP80, SCP81 and SCP82 would have to be defined in updates of GP UICC configuration and ETSI TS 102 226 [i.3].

6 Conclusion and way forward

The present document provides analysis regarding the mechanisms that use cryptography in the specifications under ETSI TC SET responsibility. Potential changes for a responsible transition to Quantum-Safe technology are described. However, the impact on performance which may be caused by the introduction of Quantum-Safe mechanisms is not considered. Such effects may require the adaptation of the current mechanisms, i.e. a one-to-one replacement may not be feasible in all cases.

For the mechanisms that use symmetric key cryptographic algorithms, the impacts are still being analysed by security agencies. ETSI TC SET needs to wait for their recommendations to make the appropriate changes to its own documents.

For the mechanisms that use asymmetric cryptographic algorithms, the specifications under ETSI TC SET responsibility rely on GlobalPlatform specifications. GlobalPlatform has planned updates of their specifications in 2026 (according to SET(25)000017: LS response to ETSI LS SET(24)000157r1 about PQC roadmap). ETSI TC SET needs to closely follow the publication of these updates and make the appropriate changes to its own documents.

Annex A: Bibliography

- ETSI GR QSC 001: "Quantum-Safe Cryptography (QSC); Quantum-safe algorithmic framework".
- ETSI GR QSC 003: "Quantum Safe Cryptography; Case Studies and Deployment Scenarios".
- ETSI GR QSC 004: "Quantum-Safe Cryptography; Quantum-Safe threat assessment".
- ETSI GR QSC 006: "Quantum-Safe Cryptography (QSC); Limits to Quantum Computing applied to symmetric key sizes".
- ETSI TR 103 619: "CYBER; Migration strategies and recommendations to Quantum Safe schemes".

History

Document history		
V1.1.1	July 2025	Publication