EUROSMART
The Voice of the Digital Security Industry

Quantum computers & identity documents

Which threats and which risks? How far are we from identity documents resistant to quantum computing and which mitigation strategy to set up as of now?

Executive summary

Research on quantum computers is very active. While there are still some technological challenges, quantum computers will very likely arise in the future. The advent of the **quantum computer is a major breakthrough that affects any system whose security relies on asymmetric cryptography.**

In that regard, the digital security of identity documents relying on secure hardware will also be affected. Quantum computers could be exploited to achieve fraud on identity, which entails major consequences (identity theft, liability…).

It is high time to reshuffle the digital security of identity documents - and in particular of eMRTDs[1] – so that it becomes resistant to the threat posed by quantum computers**. As the migration of quantum-safe eMRTD will take decades, it is urgent to start migrating as of today.**

Eurosmart calls on the eMRTD community to work on this topic as of today, as a major resilience disposition.

Section 1 focuses on quantum computers. It presents the new paradigm of quantum computers, how it could put at risk classical asymmetric cryptography, and provides insight into the current state of play of research in this field.

Section 2 focuses on the risks stemming from quantum computing and what it means for eMRTD which is the cornerstone of electronic identity documents.

Section 3 highlights the challenges to tackle to migrate eMRTDs towards quantum-safe implementation.

Section 4 provides an overview of the ongoing standardisation efforts required to accompany migration towards quantum-safe cryptography (QSC).

Section 5 proposes short-term actions to mitigate risks posed by quantum computers to the eMRTD.

In **Section 6** (conclusion), an action plan is proposed to organise the migration of eMRTDs towards quantum-safe implementation.

[1] electronic Machine-Readable Travel Document – refer to ICAO doc 9303.

I-The threat posed by quantum computers

Asymmetric cryptography is at the heart of IT security

Asymmetric cryptography relies on a pair of (cryptographic) keys. Each of them can only perform one single operation: one key can only transform a message, while the other one can only invert the latter transformation. The key which allows performing the sensitive operations (creating a signature for signature algorithm or decrypting a message for encryption algorithm) is called the private key, while the other one used to perform public operations (signature verification or encryption of a message) is called the public key. Indeed, these two keys are linked, as the signature computation or decryption performed with the private key can only be verified or encrypted using the public key, which implies that theoretically it is possible to revert back to the private key from the public key. Even though it is theoretically possible, asymmetric cryptography is designed in such a way that it is not achievable within a timeframe commensurate with human life. Asymmetric algorithms are designed so that reverting back to the private key from the public key implies solving a so-called "hard mathematical problem", namely a problem whose computational complexity cannot be handled by today's and tomorrow's conventional computers. This problem would take ages to be solved without quantum computers.

These two mathematical properties create a separation of roles by design between (1) entities entitled to perform sensitive operations – and owning private keys, and (2) the others only allowed to perform the public operations, and thus only having the public keys. Asymmetric cryptography is inescapable to support key use cases such as : (1) **authentication of entities** where only the holder of the private key can authenticate itself by generating an authentication token that anyone having the public key can verify, (2) **evidence of integrity and authenticity of message** to link it to its originator and demonstrate it has not been tampered with, and (3) **digital signature** ensuring non-repudiation of the consent given by the holder of the private key. Therefore, asymmetric cryptography (1) is the cornerstone of the PKI and authentication protocols over the Internet, and (2) is intrinsic to the digital signature concept, both being instrumental for IT security.

Besides, the threat to asymmetric cryptography posed by quantum computers may also indirectly weaken symmetric cryptography, despite quantum computers having a very limited impact on it. Most protocols used to establish a secure channel between two entities (such as TLS[2] or ICAO PACE) involve an asymmetric handshake to derive symmetric session keys in order to protect confidentiality (thanks to encryption), integrity, and authenticity (thanks to signature) of communications. A quantum computer could be used to disclose the private key from the public key of the handshake stage, and thus unveil the symmetric session keys, leading to the disclosure of the data that have been exchanged within the secure channel. Therefore, a quantum computer may also put at risk the strength of symmetric cryptography when the symmetric key has been generated using asymmetric cryptography.

The threat posed by quantum computers

Today's asymmetric algorithms rely on two types of hard mathematical problems: (1) factorisation in prime factors of a large number for RSA, or (2) computation of discrete logarithm for cryptography over elliptic curves, DSA and DH.

These mathematical problems have been studied for decades and are well known. In particular, the optimal algorithms solving these problems have been identified and analysed. It allows estimating the cost and time needed for solving any of these mathematical problems on today's conventional

[2] Transport Layer Security – standardised by the IETF.

computers and thus size the key length of an asymmetric algorithm to ensure the security of the private key over a defined timeframe.

Other types of optimal algorithms for solving these mathematical problems become achievable with quantum computing. Shor's algorithm is currently the best one known to solve the (1) factorisation in prime factors, or (2) computation of discrete logarithm, and may put at risk all asymmetric cryptography used as of today (RSA, ECC, DH, DSA).

> **Note**: Solving these mathematical problems on a conventional computer has a complexity which is sub-exponential (for finite field) or exponential (for elliptic curve) with N – the size of the finite field/group, (which makes it hard to solve), while Shor's algorithm has a much lower complexity (O((log N)^3) – in time - and O(log N) – in memory which therefore makes it possible to break them within a short timeframe.

Quantum computers would also affect the security of symmetric algorithms (such as AES) and hashing functions, but not to the same extent. It would only be necessary to double the key or hash size to maintain the same security level.

What is the state of play of quantum computers today?

Conventional computers manipulate bits that can only have an exclusive state: either 0 or 1. Quantum computers manipulate qubits, where the state of a qubit is a coherent superposition of both states |0> and |1>.

In 2001, IBM factorised number 15 with Shor's algorithm using a 7 qubits quantum computer. If this demonstration does not directly put conventional asymmetric cryptography at risk, it proves the concept. There are several challenges to increase qubit capacities of quantum computers. The main one, quantum coherence, is to maintain the stability over the time of computation of the quantum states underlying qubits, while they are disturbed by the computer's environment.

It is possible to simulate a quantum computer using a conventional computer, and such simulators are available on the market. They are very useful to get familiar with the specificities of quantum programming and learn how to design and exploit quantum algorithms. However, the number of qubits that can be simulated using a conventional computer is limited because of physical reasons that cannot be circumvented (memory, complexity of connection). This limit is around 50 qubits. Quantum supremacy will be reached once a quantum computer having at least this number of qubits will exist.

Some announcements were made regarding progress in the field of quantum computers. In October 2019, Google claimed to have reached quantum supremacy. In December 2020, a group of USTC Chinese University also claimed quantum supremacy with their photonic quantum computer Jiuzhang. However, these progresses are still to be confirmed.

In Europe, the Commission plans to build state-of-the-art quantum computers. This project is carried out by the European High-Performance Computing Joint Unit (EuroHPC JU). EuroHPC JU will develop exascale supercomputers that are capable of more than a billion operations per second. These capabilities will be ready by 2022/2024. In addition, EuroHPC JU will build hybrid machines that blend quantum and classical HPC technologies with the first state-of-the-art pilot quantum computers. This second objective should be completed by 2025.

Factorising an RSA 2048-bit private key requires thousands or millions of qubits (a study claims 8 hours with 20 million qubits). Predicting if or when it will happen is a hazardous exercise, as stated by NIST:

> *"The question of when a large-scale quantum computer will be built is a complicated one. While in the past it was less clear that large quantum computers are a physical possibility, many scientists now believe it to be merely a significant engineering challenge. Some engineers even predict that within the next twenty or*

> *so years sufficiently large quantum computers will be built to break essentially all public key schemes currently in use. Historically, it has taken almost two decades to deploy our modern public key cryptography infrastructure. Therefore, regardless of whether we can estimate the exact time of the arrival of the quantum computing era, we must begin now to prepare our information security systems to be able to resist quantum computing.*[3]*"*

In September 2021, researchers from the French CEA – Commissariat à l'Energie Atomique - demonstrated that this number could be reduced to 13 000 qubits thanks to an adapted design of the quantum processor[4]. The obverse is a much longer processing time (a few months compared to a few hours), yet it still remains of interest to break cryptography.

Research also makes a lot of progress to reduce the space and the power consumption needed for quantum computers. Researchers at the Institute for Experimental Physics of the University of Innsbruck (Austria) have built a prototype for a compact quantum computer. This device is the first of its kind in the world. The compact quantum computer can entangle 24 qubits. Researchers expect to increase this ability up to 50 qubits by next year. This achievement shows that quantum computers will soon be ready for installation in data centres alongside conventional computers.[5] This quantum computer also has a low power consumption, which stands at 1.5 kilowatts, the same amount of energy needed to power a kettle.[6]

As stated above, huge investments are made in quantum computers and new breakthroughs are highly likely in the future. It is now indisputable that the threat is serious enough to be addressed.

Considering the inertness required to introduce new asymmetric algorithms, it is urgent to anticipate as of today such risks and (1) to set up mitigation plans for today's IT systems, (2) to design quantum-safe asymmetric cryptography which is built on a new hard mathematical problem that cannot be easily solved by quantum computers, and finally (3) to migrate IT systems to quantum-safe asymmetric cryptography.

2-What would be the risks posed by quantum computers?

Overview of the risks

As described above, quantum computers would allow implementing and executing Shor's algorithm, and thus break any asymmetric algorithms used today such as RSA, ECC, DSA, or DH. More precisely, it would become possible to revert back to the private key from the public key. This would have substantial impacts as all the IT security relies on asymmetric cryptography. However, the nature and duration of the risks stemming from the possible advent of the quantum computer depend on the usage of asymmetric cryptography.

Risks on data pertaining to IT entities

Asymmetric cryptography is instrumental for the security of IT entities as it supports key features such as (1) distribution of rights, authorisations, and attributes in a manner ensuring their integrity and authenticity (thanks to PKI and certificates), and (2) authentication in a distributed environment where

[3] NIST, Computer Security Resource Centre, Projects, Post-Quantum Cryptography.

[4] *Factoring 2048-bit RSA Integers in 177 Days with 13 436 Qubits and a Multimode Memory*, Élie Gouzien and Nicolas Sangouard, Phys. Rev. Lett. 127, 140503 (2021), Published September 28, 2021.

[5] *Quantum computer compacted for data centres*, Engineering and Technology (E&T), Published June 18, 2021.

[6] *EU innovation moves one step closer to the world's first compact quantum computer*, European Commission, News Article, Published October 18, 2021.

it is not possible to share a common secret between two entities to establish trust (thanks to authentication protocols such as SSL/TLS).

Quantum computers would affect differently each of these features. The first one would face the risk of forgery of rights, authorisations (e.g. overriding of authorisations), and attributes, while the second one would face the risk of impersonation of IT entities. However, these risks could be overcome once for all by (1) simply revoking all the IT entities, and (2) replacing all regular asymmetric keys and algorithms they use with a cryptography resistant to quantum computers and the corresponding keys. While drastic, this measure would definitely curb any risks.

Here it is very important to note that the asymmetric cryptography is used to secure tokens related to IT entities only. Thus, these tokens cease to be meaningful as soon as the entities are revoked or replaced.

Risks on data pertaining to a natural or legal person

Asymmetric cryptography is also instrumental for the security of data pertaining to natural or legal persons, encompassing confidentiality of sensitive data but also the creation and verification of legally binding digital documents (contract…). Thereby it may be used for instance for (1) encryption of data which are considered as sensitive by the person, (2) digital signature representing the consent of a person to abide by the terms of a contract and that is legally binding, or (3) digital seal which is a proof of origin and ensures a document has not been modified since its creation and is legally recognised.

Quantum computers would affect differently each of these aspects. The two last ones would face the risk of forgery where an attacker would recover the private key and create forged or falsified legally binding documents on behalf of the rightful holder (e.g. forged contract or forged proof of origin). This risk will remain **invisible** as long as the existence of quantum computers able to break asymmetric cryptography is secret. Despite that exploitation of attacks may be complicated, the very existence of quantum computers breaking asymmetric cryptography will **annihilate the trust people had put into digital signatures and seals.** It will lead to **major legal consequences due to all digital legally binding documents immediately becoming void.** The confidentiality of data relying on asymmetric cryptography will be compromised.

However, unlike the former case, here it is very important to note that asymmetric cryptography is used to secure data pertaining to natural or legal persons, which remain sensitive well after its creation (several years, whole lifetime…). Furthermore, **these risks may exist as of today, as digital signature, digital seal or encrypted data may be captured and stored by attackers, with a view to exploiting them in a few decades when quantum computers are available while these data are still valuable.** For legally binding digital documents (relying on digital signature or seal), this risk may be mitigated by organising as of today their secure archiving to ensure that they have not been tampered since their creation. This approach would be very helpful to preserve the validity of legally binding digital documents (relying on digital signature or seal) created before the advent of the quantum computer and extend it well after this point. Regarding encrypted data, the issue is different, as the risk entails that they could be revealed in the future. The very nature of this risk will depend on whether data will still be meaningful and useful - and thus sensitive - at that moment. Therefore, the consequences of this risk have to be assessed in light of the sensitivity over time of data. **For data that remain sensitive for a short timeframe, the consequences are negligible. But when it comes to data whose sensitivity is long-lasting (e.g. medical data, biometric data) it has to be considered as of today.**

Impacts on eMRTD[7]

An electronic Machine-Readable Travel Document (eMRTD) is intended to provide secure identification of its holder by storing (1) its identification data, and (2) its biometric data (portrait and

[7] electronic Machine-Readable Travel Document.

optionally fingerprint) in order to bind the identification data to the holder of the eMRTD. An eMRTD is a secure embedded application relying on a secure hardware specified by ICAO doc 9303 and aiming at being incorporated within identity documents.

An eMRTD provides various security services such as (1) integrity and authenticity of identity data and biometric data it contains, (2) proof of authenticity to avoid cloning, (3) integrity, authenticity and confidentiality of the communication while reading the content of the eMRTD, and (4) access control over sensitive data such as fingerprints.

eMRTD is instrumental for nearly any identity document. It is used for electronic passports (ruled by ICAO), but also for seafarer identity documents (ruled by ILO). Besides, most identity cards issued by States also rely on eMRTD as they are usually accepted by some other States to enter their territory, and thus are travel documents. Within the EU, pursuant to Regulation 2019/1157[8], identity cards issued by Member States shall contain an eMRTD. The same analysis applies to resident permit, which is an identity card for foreigners. Within the EU, pursuant to Regulation 1030/2002[9], resident permits issued by Members States shall contain an eMRTD.

The possible advent of the quantum computer is also a threat to the eMRTD. The attack models made possible by quantum computers are manyfold:

- an attacker eavesdrops and intercepts communications with an eMRTD to exploit them – either in real-time or at a later stage (offline) - using a quantum computer;
- an attacker uses a quantum computer to work out private key(s) corresponding to the public key(s) contained in the certificate(s) processed by an eMRTD to authenticate an external entity (e.g., Inspection system) having special rights. This attack model requires (1) collection of certificates from the said entity and (2) live exchanges with the eMRTD;
- an attacker uses a quantum computer to work out private key(s) corresponding to the public key(s) stored in the eMRTD and clone an eMRTD. This attack model requires to collect public key(s) of eMRTD.
- an attacker uses a quantum computer to work out private key(s) corresponding to the Passive authentication certificates and forge an eMRTD or identity. This attack model requires to collect the certificate(s) of the issuing entity.

The table below summarises, for each security mechanism and asset, the possible risks and consequences.

Security mechanisms /assets	Risks	Consequences
BAC	Already at risk as of today using a regular computer Can only get worse	-Compromising the confidentiality of data that have been exchanged under this secure messaging -Traceability of holder -Linkability of transactions

[8] Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement.

[9] Council Regulation (EC) No 1030/2002 of 13 June 2002 laying down a uniform format for residence permits for third-country nationals.

PACE	Offline attacks (log transaction & break)	-Compromising the confidentiality of data that have been exchanged under this secure messaging -Traceability of holder -Linkability of transactions
PACE-CAM	Compromising of the private key	Impersonation of a genuine eMRTD (clone)
Active Authentication	Compromising of the private key	Impersonation of a genuine eMRTD (clone)
Chip Authentication	Compromising of the private key → comprising of the secure messaging keys (past and future)	-Impersonation of a genuine eMRTD (clone) -Compromising the confidentiality of data that have been exchanged under this secure messaging
Passive Authentication	Compromising of private keys of the CAs (CSCA, DS)	-Hijack/impersonation of the CSCA or DS -Issuance of genuine counterfeited eMRTDs (forgery)
Portrait	Capture encrypted logs of genuine MRTD inspections, store and decrypt within a few decades	Access to portrait
For EU travel documents implementing TR 03110		
Terminal authentication	Compromising of private keys of the CAs (CVCA, DV, IS)	-Hijack/impersonation of the CVCA, DV or IS -Override of authorisations -Access to sensitive biometric data (fingerprint or iris)
Sensitive biometric data (fingerprint or iris)	Capture encrypted logs of genuine MRTD inspections, store and decrypt within a few decades	Access to sensitive biometric data (fingerprint or iris).

Unlike the portrait of the holder that changes over his lifetime, particular attention should be paid to the case of the sensitive static biometric data (fingerprint or iris that remain static over a lifetime). This biometric data - when transferred in the course of the inspection procedure in an encrypted manner (through secure messaging) - could be very easily captured and stored by an attacker, in order to be revealed when the quantum computer is available, as the encryption relies on asymmetric cryptography (generated in the course of Chip Authentication or PACE-CAM). Besides, because of their very nature, these sensitive biometric data usually remain sensitive for the whole lifetime of the holder, and thus may still be valuable at the time the quantum computer arises. Therefore, sensitive biometric data (fingerprint or iris) exchanged in an encrypted manner may already be at risk as of today, and this risk should be considered.

3-The migration towards quantum-safe eMRTD will take time

It will take decades before eMRTDs infrastructure is upgraded to be quantum-safe. First of all, because it is not possible to start it as of now, as standards and products are missing. Also, it is challenging to adapt the cryptographic protocols used within eMRTD to be quantum-safe, and finally, the deployment of quantum-safe eMRTD will stretch over time.

Lack of application standards

Cryptographic algorithms recognised as resistant to quantum computers are still being designed and defined through the NIST contest. However, while the NIST contest is still running, standards relying on asymmetric cryptography can already be updated in light of the new quantum-safe cryptographic algorithms. These standards are of two types:

- The **core standards** providing data structures and basic services to use quantum-safe cryptographic algorithms. The preparation of some of them has already started (e.g. work of AhG1 within the ISO SC17/WG4) or is even well ongoing. The update of these standards does not need to wait for the completion of the NIST contest;
- The **application standards** pertaining to applicative layers/applications making use of asymmetric cryptography. This is the case of eMRTD standards for instance. The preparation of these standards has not started yet, mainly because stakeholders are not aware of the need to anticipate migration to asymmetric cryptography resistant to quantum computers and thus to launch the upgrade of standards.

Lack of products

The lack of standards creates a fragmented market which hampers vendors to invest in the development of products supporting asymmetric cryptography resistant to quantum computers. The fragmentation of the market narrows down its ramp up, and thus fixed costs shall be amortised on a small number of products, increasing the unit cost, which limits their procurements. Besides, the lack of standards also affects procuring entities as they cannot benefit from competitive prices (resulting from a large market), and above all interoperability, be it between components or transnational (which is instrumental for eMRTDs in the context of inspection of national abroad). Moreover, they cannot benefit from a diversity of suppliers (to avoid vendor lock-in).

Therefore, the lack of standards hampers both the provision and the procurement of products supporting asymmetric cryptography resistant to quantum computers. Availability of standards is an essential prerequisite to foster their development and deployment.

Adaptation of cryptographic protocols used within eMRTD to be quantum-safe

eMRTD makes use of very specific cryptographic protocols that were designed to meet highly demanding privacy properties. These are PACE[10], PACE-CAM[11], and Chip Authentication. Their current versions rely on the Diffie Hellman Key Agreement. However, the scope of the NIST contest – and the

[10] Password Authenticated Connection Establishment.

[11] Password Authenticated Connection Establishment – Chip Authentication Mapping.

peer review performed by the cryptographic community – only includes signature and Key Encapsulation Mechanism (KEM). Though key encapsulation mechanism can be used for key establishment, they are not a pure analogy of classical key agreements. This somehow hampers the possibility to keep the existing cryptographic protocols and just replacing the Diffie Hellman Key Agreement primitive with a quantum-safe one. Furthermore, regarding PACE-CAM, the computation of the chip authentication token is tightly bound to the underlying mathematics, in the sense that it relies on specific properties of DH-related computations. Therefore, it will also have to be reshuffled when migrating to quantum-safe cryptography. This situation entails seriously considering designing brand-new cryptographic protocols to succeed PACE, PACE-CAM, and Chip Authentication -that are not just simple adaptations where cryptographic primitives are replaced by quantum-safe ones. It requires to rather focus on security and privacy properties that are sought, rather than on the design of the current cryptographic protocols. In that regard, a formal security proof – as provided for these cryptographic protocols in the past – should also be prepared to demonstrate the absence of any flaw, and ultimately to create trust amongst users. This task will take time but is absolutely necessary not to downgrade the overall security of privacy that has been achieved by eMRTD while trying to make it resistant to quantum computers.

On the other hand, Active Authentication, Passive Authentication, or Terminal Authentication are eMRTD protocols that seem much easier to convert into a version resistant to quantum computers by just replacing the signature primitive with a quantum-safe one. However, the drawbacks of quantum-safe signature (size, performance…) may imply revisiting the design of these authentication protocols to shift from a quantum-safe signature primitive to a key encapsulation mechanism.

Quantum safe algorithms are currently being designed, reviewed, and analysed in the course of the NIST contest that should be completed around 2024. This process involves many searchers and academia worldwide. However, some national security agencies may likely require hindsight of several years before fully trusting this new generation of cryptography. In that respect, two approaches may be adopted. The first one is the hybrid approach, mixing a conventional algorithm with a quantum-safe one. This could be a good way to reconcile (1) the need to start as soon as possible the migration towards quantum-safe eMRTD, and (2) reluctance from some national security agencies to have eMRTD security fully relying on quantum-safe algorithms that have not been experienced enough. For instance, keys derived by a hybrid key-establishment scheme remain secure if at least one of the underlying schemes is secure. NIST plans to incorporate a hybrid key establishment construction in a future revision of SP 800-56. An alternative approach is crypto agility whereby security services could be achieved using multiple algorithms based on different mathematical problems. At any time only a single one is used for a given security service, but should one cryptographic algorithm be threatened, another one can be added (if needed) and instantaneously be used instead.

Above all, quantum-safe cryptographic algorithms to be employed shall be suitable to be executed on secure elements/chips used for eMRTD. More precisely their limited capacity in terms of processing and memory shall be taken into consideration when identifying the most suitable quantum-safe cryptographic algorithm(s) to use. The executable code of the cryptographic algorithm, as well as the necessary keys, shall fit within the available memory, and also its execution shall be very quick, not to affect the user experience or the fluidity of the control. This limited capacity of eMRTD hardware adds complexity and will require studies to make sure that the proposed protocol will be suitable. New hardware developments may be required with a dedicated coprocessor or resource to reach reasonable performances. Yet another reason to start the work as soon as possible.

The migration to quantum-safe cryptography of eMRTD will also need actions from certification authorities and security assessment laboratories (ITSEF) in order to evaluate the strength of implementation of these algorithms. In particular, the new possibilities offered by quantum computers should be studied to identify the right test methodologies.

Deployment of quantum safe eMRTD

eMRTD is instrumental to prove one's identity when travelling and crossing borders. Despite the numerous initiatives launched to digitalise travel documents, such as the DTC (Digital Travel Credential), it is highly likely that physical eMRTD, i.e. physical travel document (e.g. passport booklet with a secure chip) will stay in use for many decades and will not disappear in a predictable future. Unlike digital travel documents, a physical travel document does not need any connection to a network, or battery, or energy supply to be available, so much so that it can be used at any moment, anywhere to prove one's identity. Besides, getting or using digital travel documents requires digital skills as well as supplemental items (smartphone, internet access…), which may be an obstacle for some types of population, either because of digital illiteracy or because they cannot afford it. As such, the physical travel document is a key enabler for social inclusion. Moreover, people have been used to passports in the form of a booklet for a century. Definitely, changing this habit will not happen overnight. Last but not least, security and availability considerations command to organise the resilience of means to prove one's identity. It shall remain possible to prove one's identity, should mobile phone or internet/cloud be hacked, compromised, or not available.

For all these reasons, physical travel documents for sure will remain in use at a very large scale for many decades. Therefore, the strategy for deployment of quantum-safe eMRTD cannot rely on a replacement of the latter by purely digital eMRTD, offering higher agility and versatility. Physical eMRTDs – as well as digital ones - will have to be upgraded to quantum-safe. This situation will have a direct impact on the migration scenario.

The best scenario for the deployment of quantum-safe eMRTDs is to achieve it through the regular renewal of eMRTDs. It entails that the deployment will span over a long period of time, which matches the validity duration of eMRTD, usually 10 years for a passport. Moreover, this approach allows upgrading in parallel the IT part of the eMRTD, namely PKI and inspection systems.

An alternate scenario where eMRTDs on the field would be replaced overnight by quantum-safe eMRTDs is not realistic. It would lead to substantial bottlenecks on the production capacity and enrolment facilities, but also would put at risk the capacity to control eMRTDs, and thus verify the identity of individuals (infrastructure would also have to be upgraded overnight). However, if the threats posed by quantum computers are not anticipated as of now, we may be in a situation in the future where there may not be time enough to perform the deployment of quantum-safe eMRTDs through natural renewal before quantum computer arises. It is important to avoid this scenario that would be very problematic and costly. Therefore, it is important and urgent to address the threats posed by quantum computers as of now.

4-Quantum-safe cryptography standardisation is already ongoing

There are ongoing standardisation efforts that organisations started before the NIST challenge completion. This work can also be used to define new standards for eMRTDs relying on post-quantum cryptography (PQC).

This section is an overview of some of the ongoing standardisation activities which can serve eMRTD[12].

The NIST contest

The US National Institute of Science and Technology (NIST) is in a several-year process to solicit, evaluate, and standardise one or more quantum-resistant public-key cryptographic algorithms.

[12] This overview is valid at the time this White Paper is published. Progress is expected in the future.

NIST selection targets two different use cases: (1) key encapsulation mechanisms and (2) digital signature algorithms.

In July 2020, NIST announced finalists of the third-round selection.[13] This list comprises 3 finalists (Crystals-Dilithium, Falcon, Rainbow) and 3 alternates (GeMSS, Picnic, Sphincs+) candidates for a signature algorithm, 4 finalists (Crystals-Kyber, NTRU, SABER, Classic McEliece), and 5 alternates (Bike, FrodoKEM, HQC, NTRUprime, SIKE) candidates for a key encapsulation mechanism.

In mid-2021, NIST announced it would select at most one between Crystals-Kyber, NTRU, and Saber for a key encapsulation mechanism, and one among Crystals-Dilithium and Falcon (all based on structured lattices) for a signature algorithm.

NIST plans to release for public comment a draft technical specification standardising the selected algorithms in 2022-2023. NIST does not exclude releasing another one later standardising supplemental algorithms. Moreover, NIST is also considering organising a fourth round of the contest with a new call for proposals for signature algorithms.

Now is the latest opportunity to evaluate selected algorithms and to make sure that candidates are compliant with small chip capabilities and to comment to NIST.

It shall also be noted that China organised a similar contest in 2018, which was concluded at the end of 2019.

International Standardisation Organisation (ISO)

ISO/IEC JTC1/SC17 WG4 initiated in July 2020 an ad hoc group (AhG1) instructed to determine the necessary enhancement of ICC[14] main existing standards (i.e. ISO/IEC 7816 series) to allow for quantum-safe cryptography interoperability for interchange at card edge. On the ground of the NIST contest outcome and conclusions, and with regard that the final standard will be released by NIST as a draft for public comment in 2022-2023, and finalized by 2024, this ad hoc group took a decision: to specify in the most generic way the new interoperability features so that to cater to a variety of quantum-safe cryptography algorithm likely to result from the NIST selection.

Concerned by ICC constraints, the ad hoc group defined its most appropriate functionality to allow for its implementation on ICC, but without ignoring that ICC can be embedded (eSE) on devices with less stringent resources. The following features were designed and are on their way to figure in the upcoming revision of ISO/IEC 7816-8 (*Identification cards — Integrated circuit cards — Part 8: Commands and mechanisms for security operations*):

- new ordered templates for quantum-safe cryptography private/public keys and/or shared parameters
- new algorithm identifier for referencing of quantum-safe cryptography interchange within security commands
- new quantum-safe cryptography key type coding
- optimisation of quantum-safe cryptography signature flow of APDU instructions
- enhancement of existing security command i.e., for security context establishment
- new hybrid certificate options for transition phase
- recommendation for quantum-safe cryptography encryption/decryption flow of APDU instructions

[13] NIST, Computer Security Resource Centre, Projects, Post-Quantum Cryptography, Round 3 Submissions.

[14] Integrated Circuit Card.

Besides the material described above and stacked up for a revision of ISO/IEC 7816-8, the ad hoc group submitted a series of questions to NIST and considered with attention NIST recommendation and rationale regarding key agreement protocols.

The ad hoc group decided to dedicate an Amendment of ISO/IEC 7816-8 especially bearing on example(s) of interchange with quantum-safe cryptography key agreement protocol i.e. by reusing the new functionality and extensions of the first Amendment. Accordingly, a new informative annex could be appended to ISO/IEC 7816-8 to describe how key agreement protocol can be rolled out while using extended instructions, new key templates, new certificate format, etc.

Internet Engineering Task Force (IETF)

The Internet Engineering Task Force (IETF) organisation publishes RFCs which become *de facto* standard for the protocols used on the Internet.

In June 2021, IETF has released version 1.0 of "RFC Quantum-Safe Key Identification and Serialization"[15] based on NIST Round 3 finalists. This RFC is a standardisation brick that completes the NIST process. While the latter focuses on defining quantum-safe algorithms, this RFC defines Object Identifier (OIDs), and the formatting of private and public keys. It covers the key encapsulation mechanisms and signature algorithms selected as finalists and alternates on the third round of the NIST contest (Classic McEliece, Crystals-Kyber, NTRU, SABER, Crystals-Dilithium, FALCON, Rainbow). This RFC is instrumental as it will foster usage of quantum-safe cryptography by providing (1) unambiguous identification of algorithms (through OID), and (2) interchange of the formatting of keys. Amongst others, it will support deploying (1) PKCS#8 key files or (2) X.509 certificates relying on quantum-safe signature algorithms. It shall be noted that the latter is of direct relevance for eMRTD, as the PKI used for the Passive Authentication makes extensive use of X509 certificates.

Regarding the introduction of quantum-safe cryptography, IETF intends to streamline the migration to quantum-safe cryptography. By preparing as soon as possible technical standards that can be started without waiting for the completion of the NIST contest, it helps the industry propose products and solutions as early as possible, as stated by IETF:

> *"By addressing these problems now rather than after waiting for the NIST standards process to complete, it should reduce the time it will take for the industry to adopt a new generation of quantum-safe cryptography."*

European Telecommunications Standards Institute (ETSI)

ETSI's Technical Committee on Cyber Security (TC CYBER) has launched a working group dedicated to quantum-safe cryptography: the Quantum-Safe Cryptography Working Group.

This working group aims to assess and make recommendations for quantum-safe cryptographic primitives' protocols and implementation considerations, taking into consideration both the current state of academic cryptography research and quantum algorithm research, as well as industrial requirements for real-world deployment. The focus is on the practical implementation of quantum-safe primitives, including performance considerations, implementation capabilities, protocols, benchmarking, and practical architectural considerations for specific applications. However, the objective of the group does not include the development of cryptographic primitives, which remain in the NIST remit.

[15] IETF, "RFC Quantum Safe Key Identification and Serialisation V1".

This working group considers the security properties of the proposed algorithms and protocols along with practical considerations, such as extensible security architectures and technology switching costs, which will allow these recommendations to support a variety of industrial use cases. The working group makes pragmatic comparisons and concrete characterisations and recommendations to assist the global technology community to select and deploy the best available quantum-safe alternatives.

This working group has released several publications such as:

- TR 103 619 (2020) defining migration strategies and recommendations for quantum-safe schemes, and enhancing cryptography awareness across all business sectors;
- TS 103 744 (2020) on quantum-safe hybrid key exchange protocols.

The TS 103 744 “Quantum-safe Hybrid Key Exchanges” investigates quantum-safe hybrid key exchanges mechanisms in the running course of the NIST contest rounds and selection of a quantum-safe key encapsulation mechanism. The key encapsulation mechanism is itself constructed from PKE (Public Key Encryption) with variants introducing further resistance to PQ attacks. Quantum-safe hybrid key exchange mechanisms combine a classic key exchange method like ECDH and a quantum-safe key encapsulation mechanism. The hybrid exchange mechanisms specified by the TS 103 744 use two or more shared secrets to derive cryptographic key material using a key derivation function such as the derived key is at least as secure as the maximum security of the key exchange method. Accordingly, the resulting hybrid scheme is considered secure if one of the key exchange methods remains secure. The key encapsulation mechanism properties are defined as comprising a public/private key generation, an encapsulation and a de-capsulation algorithm with the purpose of establishing a shared secret between two entities using quantum mechanics.

The TS 103 744 considered a list of variants of post-quantum key encapsulation mechanisms e.g. BIKE, Classic McEliece, CRYSTALS-Kyber, FrodoKEM, NTRU, SABER, amongst which BIKE, FrodoKEM, and NTRU were quoted as alternates whereas the remaining ones were finalists.[16]

One benefit of the TS 103 744 is that it provides test vectors that were generated by the C reference implementation for Quantum-safe Hybrid Key Exchanges.[17]

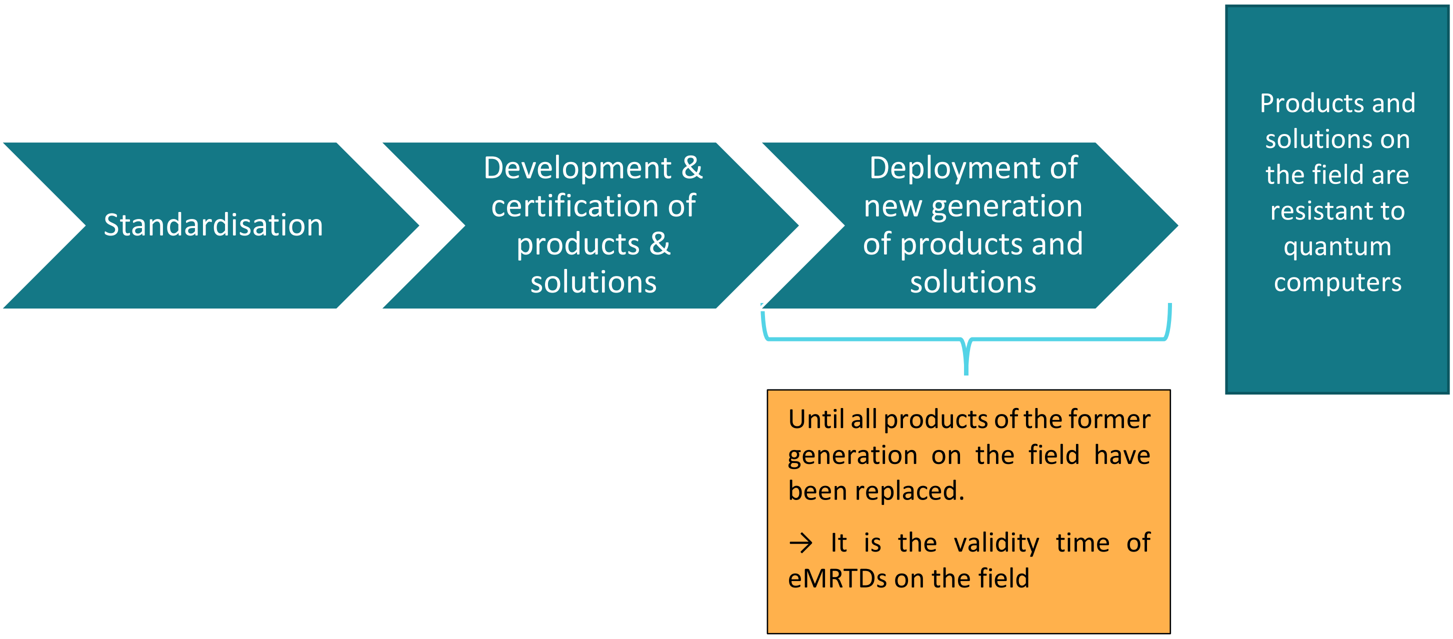
5-Which mitigation strategy for eMRTDs to start with as of today?

As explained above, the migration towards quantum-safe eMRTD will take time and will primarily impact physical eMRTD that will remain for many decades. Yet, it also appears urgent to have completed this migration as soon as possible not to be exposed to the risks stemming from quantum computers, in particular the compromising of sensitive biometric data (fingerprint or iris) of holders.

The timeframe required to prepare the necessary standards is hard to estimate and difficult to reduce. However, the deployment period where quantum-safe eMRTDs will be introduced to progressively replace old ones thanks to natural renewal could be reduced. Usually, this period will span over 10 years, which is the usual validity period of an eMRTD (passport). It could easily be divided by two by reducing the validity period of eMRTD to 5 years as of now (instead of 10) in order to speed up the deployment to come in the future of quantum-safe eMRTDs. Indeed, once the complete deployment would be achieved, it would be possible to revert to 10 years validity period for eMRTD.

[16] NIST, Computer Security Resource Centre, Projects, Post-Quantum Cryptography, Round 3 Submissions.
[17]ETSI, Informative reference implementation as reported in Annex C of ETSI TS 103 744, "CYBER; Quantum-safe Hybrid Key Exchanges”.

Overview of migration planning



Standardisation

Development & certification of products & solutions

Deployment of new generation of products and solutions

Products and solutions on the field are resistant to quantum computers

Until all products of the former generation on the field have been replaced.

→ It is the validity time of eMRTDs on the field

6-Conclusion

The threats posed by the quantum computer should seriously be considered. Even though its advent may seem (very) far, the risks exist as of today and require taking immediate actions.

We call the EU and the ICAO New Technology Working Group (NTWG) to prepare as soon as possible the migration to quantum-safe eMRTD. This task is substantial and requires to:

- Perform a comprehensive risk analysis of today's eMRTD in light of quantum computers;
- Design of a new generation of eMRTD which is quantum-safe;
- Identify and propose strategies to migrate from today's eMRTD to quantum-safe eMRTD;
- Propose migration planning taking into account (1) completion of key standards on which eMRTD shall rely, and (2) availability of products on the market.

In that regard, we call the EU and the ICAO NTWG to leverage the expertise and in-depth knowledge gained by the ISO SC17/WG4/AhG1 on this topic, which has started its activities in July 2020. We advise the EU and the ICAO NTWG to mandate the AhG1 to assist them in the completion of all these four tasks.

In addition, we invite eMRTDs issuing authorities to consider reviewing the validity period of physical eMRTD to set it to 5 years as of now to reduce the deployment period of quantum-safe eMRTD, once this one is ready.

About us

Eurosmart, the Voice of the Digital Security Industry, is a **European non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

Our members

Members are designers or manufacturers of secure elements, semiconductors, smart cards, systems on chip, High Security Hardware and terminals, biometric technology providers, system integrators, secure software and application developers and issuers. Members are also involved in security evaluation as laboratories, consulting companies, research organisations, and associations.

Eurosmart members are companies (**BCA, Bureau Veritas, CYSEC**, **Fingerprint Cards**, **G+D Mobile Security**, **IDEMIA**, **IN GROUPE**, **Infineon Technologies**, **NXP Semiconductors**, **PayCert**, **Prove & Run**, **Qualcomm**, **Real Casa de la Moneda**, **Samsung**, **Sarapis**, **SGS**, **STMicroelectronics**, **Synopsys, Thales**, **Tiempo Secure, Trusted Objects, TrustCB, WISekey**, **Winbond, Xilinx**), laboratories (**Brightsight**, **Cabinet Louis Reynaud, CCLab, CEA-Leti, Jtsec, Keolabs**, **Red Alert Labs**, **Serma**), consulting companies (**Internet of Trust**), research organisations (**Fraunhofer AISEC, Institut Mines-Telecom - IMT, ISEN - Institut Supérieur de l'Électronique et du Numérique Toulon**), associations (**SCS Innovation cluster**, **Smart Payment Association**, **SPAC, Mobismart**, **Danish Biometrics**).

Eurosmart is a member of several European Commission's groups of experts: Radio Equipment Directive, eCall, Multistakeholder platform for ICT standardisation, and Product Liability.

Eurosmart and its members are also active in many other security initiatives and umbrella organisations at the EU level, like CEN-CENELEC, ECIL, ETSI, ECSO, ESIA, GlobalPlatform, ISO, SIA, TCG, Trusted Connectivity Alliance and others.

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com

@Eurosmart_EU

@Eurosmart

Square de Meeûs 35 | 1000 Brussels | Belgium
Tel +32 2 895 36 56 | mail Contact@eurosmart.com