THE FUTURE OF EIDAS IN THE LIGHT OF POST-QUANTUM CRYPTOGRAPHY

AZ EIDAS JÖVŐJE A POSZT-KVANTUM KRIPTOGRÁFIA TÜKRÉBEN

NYÁRI Norbert[1]

Abstract

This paper examines the challenges and future of digital signatures, which are widespread today, and the electronic signatures based on them. Several electronic signature schemes have been defined worldwide; the European version is governed by the eIDAS Regulation. Electronic signatures based on public key cryptography currently in use will be compromised by high-performance quantum computers. In my article, the basic operation of electronic signatures is presented, and vulnerable points are identified. I shall furthermore cover the various recommendations to help the transition to the post-quantum era, NIST, ENISA, etc., which provide guidance on how to strengthen systems that are still operating in production environments against quantum attacks as long as standardized, quantum-safe public-key cryptographic primitives are on the way.

Keywords

digital signature, electronic signature, cryptography, post quantum cryptography, IT security

Absztrakt

Jelen cikk a manapság széleskörben elterjedt digitális aláírások, és az azokra épülő, joghatást is kiváltó elektronikus aláírások várható kihívásait és jövőjét vizsgálja. Világszerte több elektronikus aláírási sémát definiáltak, az Európai változatot az eIDAS rendelet szabályozza. A jelenleg alkalmazott nyilvános kulcsú rejtjelezésre épülő elektronikus aláírásokat kompromittálni fogják a nagyteljesítményű kvantumszámítógépek. Cikkemben bemutatásra kerül az elektronikus aláírások alapvető működése, azonosításra kerülnek a sebezhető pontok. Kitérek továbbá a különböző ajánlásokra, amelyek a poszt-kvantum érába való áttérést hivatottak segíteni, a NIST, ENISA stb, melyek irányt mutatnak, hogy hogyan erősíthetők meg a jelenleg is éles környezetben működő rendszerek a kvantum támadásokkal szemben addig, ameddig nem áll rendelkezésünkre szabványosított, kvantumbiztos nyílt kulcsú kriptográfiai primitív.

Kulcsszavak

digitális aláírás, elektronikus aláírás, kriptográfia, posztkvantum kriptográfia, informatikai biztonság

[1] nyari.norbert@uni-obuda.hu | ORCID: 0000-0003-0229-7584 | doctoral candidate, Óbuda University Doctoral School on Safety and Security Sciences | PhD hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola

INTRODUCTION

This paper examines the expected challenges of the now widespread public-key cryptographic technologies for digital signatures. The trust services and the various electronic signatures defined in the eIDAS framework adopted throughout the EU are based on the above-mentioned public-key cryptographic (PKC) primitives. Large-scale quantum computers with adequate computational capacity shall, over time, compromise all public-key cryptographic algorithms (RSA, DSA, Diffie-Hellman Key Exchange etc.) currently used in production environments.

The so-called quantum apocalypse shall have a great impact on eIDAS and thus the European trust services and electronic signatures as well. Not only that no more secure certificates can be issued, and no more documents can be signed in a secure manner but also already signed documents with today's technologies shall be easily tampered with seriously violating Confidentiality and Integrity IT security principles.

Fortunately, the future does not have to be that dark. Large companies researching quantum computing report new results every year (e.g., the IBM 127-qubit quantum computer November, 2021 [1]), but we still have time until universal quantum supremacy is achieved, notwithstanding, in my humble opinion the time available needs to be spent on conscious preparation and gradual migration. Thankfully, many guides and articles can be of help: security guides proposing methods and techniques for strengthening production systems (and PKI certificates).

Besides, in the meantime mathematicians, cryptographers and other scientists are trying to find new, secure, quantum-proof approaches in cryptography and in parallel, standardization institutes around the world working on new, quantum-safe standards for PKC and digital signatures.

Stressing the difference between "Electronic signature" and "digital signature" is vital. While digital signature is technical phrase including various encryption and hash algorithms, electronic signature is a legal concept, with many different interpretations and implementations. As for implementation, the most basic scenario is a simple name written on the end of an electronic document. An electronic signature can also be a legal application of digital signature technology, making electronic signature a special use case of digital signature. Let us get into the details of electronic signature.

ELECTRONIC SIGNATURE AND DIGITAL SIGNATURE

The concept of electronic signature has a bit of a history: signatures transmitted by telegraph have existed and recognized by law since the mid-19th century. Faxed signatures have also been accepted since the 1980s. [2] In my personal experience I find that nowadays printed, hand-signed and then scanned or photographed electronic documents/filled forms sent in e-mail is accepted by many institutions. No wonder, as it is quite similar to the aforementioned and previously widely accepted fax signature. In my humble opinion this kind of electronic signature can be enough for everyday administration tasks of lesser importance.

In recent decades, various laws have been enacted around the world to create the legal basis for the use of electronic signatures in national and international trade, so there are many different definitions.

First of all, the United States has multiple federal and state laws regarding electronic signature. On one hand, in 2000, "Electronic Signatures in Global and National Commerce Act" (ESIGN Act) Sec 106 (US federal law) defined a quite basic electronic signature as follows "The term 'electronic signature' means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.", stating nothing on authentication, verifiability, or non-repudiation. [3]

On the other hand, in "Government Paperwork Elimination Act" (GPEA) Sec 1710 (US federal law) the term "electronic signature" means "a method of signing an electronic message that identifies and authenticates a particular person as the source of the electronic message; and indicates such person's approval of the information contained in the electronic message." [4]

In Canada "Personal Information Protection and Electronic Documents Act" (PIPEDA) regulates the use of electronic signatures. It distinguishes between two different types of electronic signatures: "electronic signature" and "secure electronic signature". An electronic signature is a "signature that consists of one or more letters, characters, numbers or other symbols in digital form incorporated in, attached to, or associated with an electronic document.". The other type, secure electronic signature is special kind of electronic signature, "that results from the application of a technology or process prescribed by regulations made" having a few restrictions: it has to be unique to the signatory, it has to provide mechanics for verifying the signature, and changes made to the signed document since the signature creation must be detectable. [5]

eIDAS ("electronic IDentification, Authentication, and trust Services") is the EU regulation "on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC", taken effect in 2016. One main goal of the regulation is supporting the Digital Single Market (DSM) for EU member states. [6]

The "Digital Single Market Strategy" is one of the European Commission's top ten priorities for creating an ecosystem that supports consumers and businesses in e-commerce across Europe using common solutions. [7]

The regulation thus also facilitates the transparent, secure, technology-neutral and trouble-free flow of commerce in the EU. eIDAS applies across borders as well as within individual member countries standardizing the use of electronic identification (eID), defining the "electronic trust services" (eTS), ensuring the legal validity of electronic signatures. As a result of consistent, Europe-wide regulations electronic trust services can be accessed through an internal market in the EU. [8] [6]

From now on I shall focus on the electronic signature model defined in eIDAS. Trust services are out of the scope of the current paper.

There are three kinds of electronic signatures defined by eIDAS: Electronic Signature (formerly known as Simple Electronic Signature), Advanced Electronic Signature (AES – not to be confused with Advanced Encryption Standard which a cryptographic algorithm), and Qualified Electronic Signature (QES). [6]

Electronic signature "means data in electronic form which is attached to or logically associated with other data in electronic form, and which is used by the signatory to sign". According to eIDAS the even most basic form of electronic signatures e.g., a simple name

typed as text at the end of an electronic document, can be accepted as valid, since "an electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures." [6]

An "Advanced Electronic Signature" in eIDAS has the same properties as the "secure electronic signature" in the Canadian PIPEDA, that is it must be one-to-one mapped to the signer. One must be able to identify the signer of a document based on the signature. Moreover, further changes on the signed document after the creation of the signature has to be detectable. [6]

"Qualified Electronic Signature" is a special type of "advanced electronic signature" having the same legal effect of a handwritten signature. It has to be created with a "qualified electronic signature creation device" using a qualified certificate for electronic signatures. [6]

A qualified certificate "means a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in" the Regulation. A few examples of the set of requirements defined: an indication that the certificate is a qualified certificate for electronic signature, data clearly identifying the issuer (including the Member State). In the case of a natural person, the data must include the name of the person and, in the case of a legal person, the registration number in addition to the name. [6]

eIDAS differentiates between advanced electronic signatures and advanced electronic stamps, the main difference is that the former is issued for a person, the latter is for a legal person. Technologically, at the end of the day, both are based on digital signature algorithms. [6]

Another important concept is electronic timestamp, according to the regulation it "means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time". There are two levels of timestamps, electronic timestamp, and qualified electronic timestamp. A qualified electronic time stamp is "an electronic time stamp which meets the requirements laid down in" the Regulation. [6]

Similarly to basic electronic signatures an electronic time stamp "shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic time stamp". In contrast a qualified electronic time stamp shall meet certain requirements: exact time must come from a reliable time source connected to UTC. Date and time data must be signed or sealed with an eIDAS conform advanced electronic signature or seal excluding the possibility of undetected modification. [6]

Although the main concepts are technology-independent, eIDAS stresses the need to create a pan-European public key infrastructure and mentions certificates several times, which means public key certificates (or in other words digital certificates). [6] This also shows that coming across close technical ties at implementation level is inevitable.

From a technical aspect a qualified electronic signature is nothing else than a digital signature created with a public key (digital) certificate. Let us take a closer look on how a digital signature is made.

The high-level requirements of digital signatures are the following according to Tannenbaum:

- authentication: the receiver must be able to check the alleged identity of the sender,
- non-repudiation: the sender cannot later repudiate the contents of the message,
- integrity: the receiver (or anybody else) cannot possibly counterfeit the message in the name of the original sender. [9]

Any public key cryptographic (PKC) primitive meets the above requirements, but the de facto standard is the RSA (Rivest-Shamir-Adleman) public key algorithm. A quick recap: in PKC every participant has a keypair, which consist of a private key and a public key. While the private key is prohibited from being disclosed to others and must only be used by the owner, the public key can be securely transmitted to anyone. [9]

If the public key of a keypair is used for encryption, only the private key can be used for decryption and vice versa. The use cases of the keys can be summarized as follows:

Key	Cryptographic operation	Usecase	Abridgment
Public	Encryption	Encrypt message	public-encrypt
Private	Decryption	Decrypt message	private-decrypt
Private	Encryption	Sign a message	private-encrypt
Public	Decryption	Verify a signature	public-decrypt

1. Table Usecases of keys of a keypair

Another vital cryptographic primitive is also used in the creation of digital signatures: a cryptographic hash function, which calculates a message digest (or hash) of fixed length for input data of any size. [9]

Historically in cryptographic examples the sender, the receiver, and the attacker are named respectively Alice, Bob, and Eve. I shall stick to this nomenclature in the following, where I present the basics of digital signature. [9]

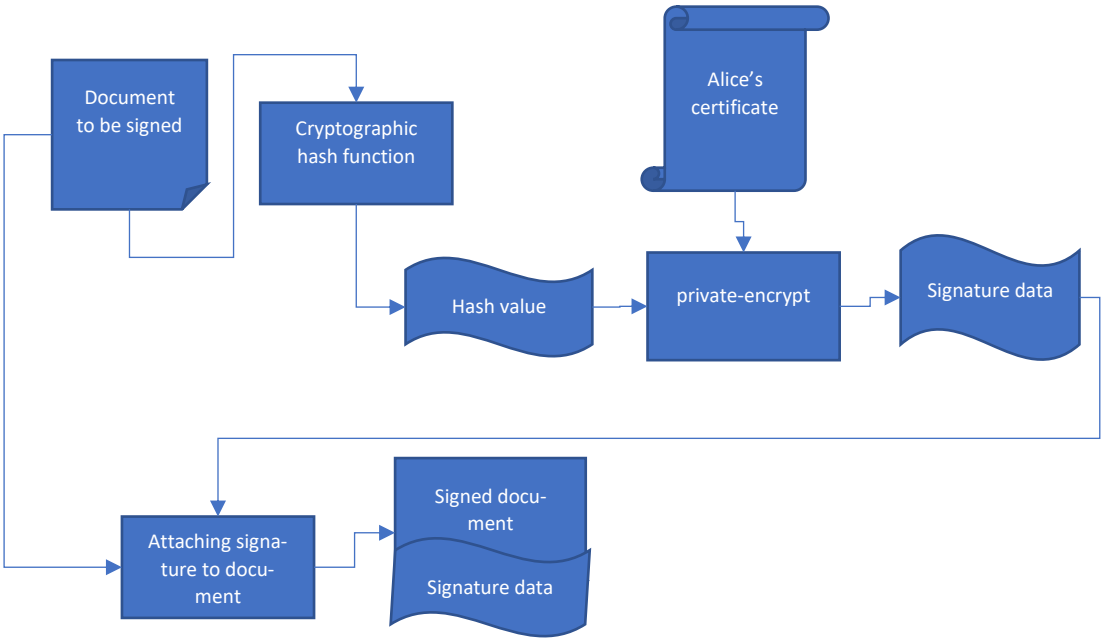
Consider a scenario where Alice wants to create and send a digitally signed document to Bob, with the above-mentioned requirements in place, making sure that Eve would not be able to alter the original document.

Firstly, the hash of the document is calculated with a cryptographic hash function. The hash value is encrypted with Alice's private key, which is stored in Alice's certificate. The singed document then created by attaching the signature data to the original document. [9]

The validity of the signature can be verified by anyone, who holds Alice's certificate (excluding the private key of course). The verification is basically the public-decryption of the signature data, after that the hash of the document is calculated with the same algorithm that of the signer used, and finally the two hashes (the one form the signature data, and the calculated one) are compared.

So, how does electronic signatures implement Confidentiality and Integrity? Should the two above hashes match, Bob can be certain that Alice signed the message (identification of the signatory). PKC guarantees that Alice's private key was used for encryption of the document hash if decryption of the signature data with Alice's public key results in the correct has (non-repudiation). The match of the two hashes guarantees that no modification was made on the original document (integrity).

This is however the most basic scenario with limitations. The signature can only be validated till the signer's certificate is valid (not expired, not revoked).



1. Figure Creation of a basic digital signature

The ETSI EN 319 102-1 V1.3.1 (2021-11) "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation" European Standard defines how the advanced electronic signature (AdES – AES is the legal concept, AdES is the technical implementation) is to be created and verified in accordance with the eIDAS regulation. AdES however heavily relies on PKC. [10]

Practically speaking ETSI EN 319 102-1 standard supports the eIDAS Regulation for creation of electronic signatures and seals implemented using digital signature technology. [10]

The standard defines four levels of electronic signatures, each level includes the level below itself signing the lower layers' unsigned attributes:

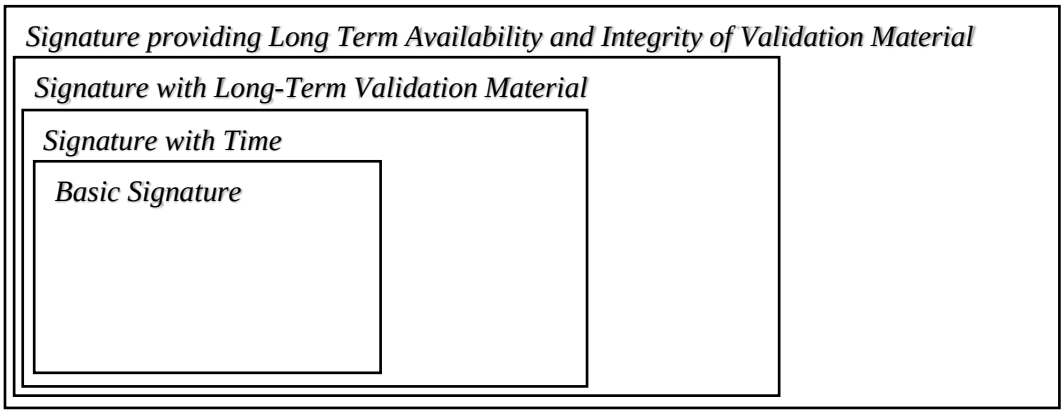
- *Basic Signature*: "is a signature that can be validated as long as the corresponding certificates are neither revoked nor expired."
- *Signature with Time*: "is a signature that proves that the signature already existed at a given point in time."
- *Signature with Long-Term Validation Material*: "is a signature that provides the long-term availability of the validation material by incorporating all the material or references to material required for validating the signature"

- *Signature providing Long Term Availability and Integrity of Validation Material*: "targets long term availability and integrity of the validation material of digital signatures over long term and can help to validate the signature beyond many events that limit its validity (for instance, the weakness of used cryptographic algorithms, or expiration of validation data)." [10]

The types of signatures above fundamentally differ in the number of attributes attached to the signature. The Basic Signature is very similar in essence to the procedure I have presented above. It consists of the signers document, the signing certificate and the signature value. [10]

Signature with Time encapsulates a Time Stamp Token (TST) as an unsigned attribute requested from a Time Stamping Authority (TSA), both defined in RFC 3161 "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)". This type can be validated as long as the required validation data is on-line available to the verifiers. It is intended to prove the existence of the signature at a given point in time. [10] [11] [12] TSP also relies on PKC being another potential subject to quantum attacks.

Signatures created with Long-Term Validation Material, in contrast, includes the validation data that is necessary for verification beyond the end of the validity of the signing certificate. The "necessary data" is attached as unsigned properties containing the complete certificate (chain of trust) and revocation data. [10] [12]



2. Figure Embedding of different signature types

Signature providing Long Term Availability and Integrity of Validation Material, as its name suggests, targets creating signatures that can be validated long after creation. Built from the previous level, a time stamp token is added on the validation data from the previous level, proving that the validation data existed at a given point of time. [12]

Used in conjunction with appropriate additional measures this kind of signature can be verified long after creation even if the applied cryptographic algorithms were compromised in the meantime. This can be achieved utilizing periodical timestamping which is practically the re-signing of validation data with up-to-date cryptographic primitives. [12] [10]

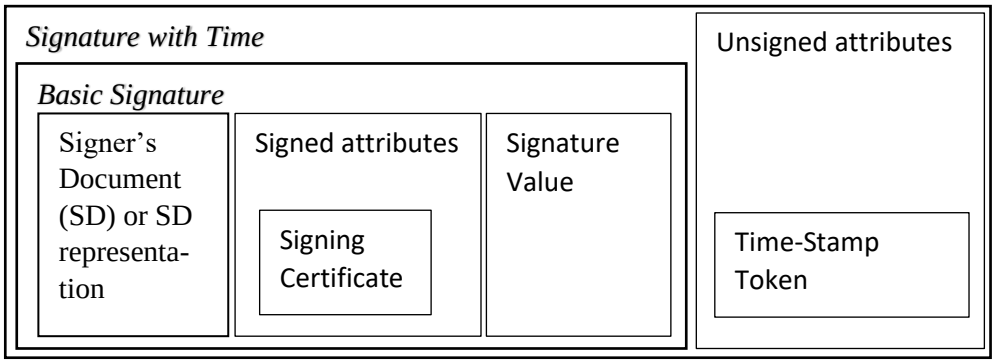
However, in order to make my point in this paper the 'Signature with Time' type of electronic signatures is sufficient to know in detail.

The Signature with Time utilizes the aforementioned Time-Stamp Protocol. With a signed time-stamp token attached to a Basic Signature shortly after signing, this level provides evidence of the existence of the signature at a given point in time. [10]

The Time-Stamp Token is provided by a Trust Service Provider, with the responsibility of proving the validity of the time-stamp when required to do so. [10] Requesting a time-stamp is done in the following way: the requesting entity sends a request (TimeStampReq) to the Time Stamping Authority, which responds with a Time stamp response (TimeStampResp) including a TimeStampToken (TST). Each TST is signed by the TSA with a certificate generated exclusively for this purpose. The validity of a time-stamp can be verified with the public key certificate of the TSA. [11]

A time-stamp token should ideally be created and attached to the signature right away. The sooner the timestamp is attached to the signed document, the lower the risk of repudiation of the signature creation. In certain cases, it is advisable for the verifier to create a Signature with Time on a newly received document: the signer does not provide a Time-stamp token, or the verifier does not trust the provided Time-stamp token. [10]

The logical structure of the signature type is shown in the figure below.



3. Figure Signature with Time

Signature with time consists of a Basic signature and a timestamp signed by a TSA. Let us move on to the threats and challenges regarding to digital signatures.

THREATS FROM QUANTUM COMPUTING

This section is a brief review of what has been discussed in detail regarding the threats posed to today's cryptography by quantum computing in my previous article on the topic, "The Impact of Quantum Computing on IT Security".

Today's PKC is based on mathematical problems that cannot be solved in normal time, such as the factorization problem of integers, the discrete logarithm problem or the elliptic-curve discrete logarithm problem. These problems however can be solved in feasible time on a quantum computer capable of running Shor's prime factor finding algorithm. Increasing the key size in this case shall unfortunately be of no help, new, quantum-safe public-key algorithms must be found and utilized. [13]

Quantum searching algorithms give a quadratic speed up to Known Plaintext Attacks (KPA) against Symmetric Key Cryptographic (SKC) algorithms. Quantum-safeness

can be provided increasing the key size, as a rule of thumb doubling the key size would be enough. [14]

Quantum attacks can potentially accelerate the breaking of cryptographic hash functions. The resistance to such attacks can be increased in a similar way as in the case of SKC, the output length of hash functions needs to be increased. [14]

Practically speaking large-scale quantum computers shall compromise today's PKC and halve the security of SKC and hash functions.

eIDAS qualified electronic signatures are built around public key cryptography, large scale quantum computers shall probably cause many problems in the application of electronic signatures. As stated, before an electronic signature is used to ensure the integrity and non-repudiation of signed documents.

I think that should the quantum apocalypse occur, soon after that quantum cryptographic algorithms shall probably be developed and implemented running on quantum computers. So, the problem of the signature creation shall be solved soon after the quantum apocalypse.

The main problem however arises with previously signed documents: in theory, an attacker using a large-scale quantum computer can easily tamper with the signature data, timestamps and validation material of any signature created with today's technology. So, basically any electronically signed document can be counterfeited.

The above detailed Signature with Time scheme (and so the other schemes as well) could be compromised in many ways. Suppose the attacker has a large-scale, universal quantum computer, being able to counterfeit the signature data, in violation of the Confidentiality and Integrity of the original document. The attacker could create a new version of the document that was apparently signed by the original signer at the original point in time, but with a different content.

In my opinion, because of the technology dependencies of electronic signatures on public-key cryptography, the review and revision of the cryptographic requirements of the regulation should also start in time to ensure a smooth transition into the post-quantum era.

WHAT CAN BE DONE IN THE MEANTIME?

There are several guides in the topic issued by many nations' IT security or standardization organizations. Firstly, the NIST National Cybersecurity Center of Excellence (NCCoE) started a program to develop methods and best practices regarding migration from today's PKC to quantum-safe replacement algorithms, complementing the NIST PQC project. [15] [13]

The paper aims to provide help in discovering quantum-vulnerable cryptographic modules (hardware or software) in cryptosystems, demonstrating through five scenarios listed in the table below. [15]

#	**Title**
Scenario 1	"FIPS-140 validated hardware and software modules that employ quantum-vulnerable public-key cryptography"
Scenario 2	"Cryptographic libraries that include quantum-vulnerable public-key cryptograpy"
Scenario 3	"Cryptographic applications and cryptographic support applications that include or are focused on quantum-vulnerable public-key cryptography"
Scenario 4	"Embedded quantum-vulnerable cryptographic code in computing platforms"

Scenario 5	"Communication protocols widely deployed in different industry sectors that leverage quantum-vulnerable cryptographic algorithms"

2. Table Migration to Post-Quantum Cryptography Scenarios

Basically, the possibly quantum-vulnerable components of production cryptosystems should be identified and replaced with quantum-safe alternatives. Replacing them however is not always so straightforward, because the classical primitives are not interchangeable as is with new primitives due to differences in key size, signature size, performance etc. [15]

The first paper in the project, Getting Ready for Post-Quantum Cryptography was originally released on May 26th, 2020, the latest version is dated April 28th, 2021. Not only it describes the possible impact of quantum computing on today's cryptography especially public-key cryptography but introduces the expected challenges of migration to post-quantum cryptography, and post-quantum cryptography itself. [15]

The paper emphasizes the very important concept of "crypto agility", stating that unfortunately many cryptosystems lack this feature. Practically speaking "crypto agility" is the openness of cryptographic systems to rapid replacement of cryptographic primitives. [16]

My understanding is that crypto agility is a vital concept and should be treated as a design pattern in the design of cryptosystems, that is, the possibility that the embedded cryptographic primitives shall become compromised in time making it necessary to replace them, should be considered.

We will have to wait for the end of NIST PQC standardization process for concrete recommendations regarding public key cryptography.

The German Federal Cyber Security Authority (BSI - Bundesamt für Sicherheit in der Infromationstechnik) developed and released a set of recommendations in 2020 written in German. The paper "Migration zu Post-Quanten-Kryptografie" introduces the technological backround of the matter and describes the possible effects of quantum computing getting large-scale. The recommendations are focused around seven points including crypto agility, key sizes for symmetric cryptography, hybrid solutions, quantum-safe key encapsulation mechanisms (KEMs). [17]

The article also stresses out the importance of crypto agility like the above mentioned NIST guide. Furthermore it suggests that some caution should be exercised when applying quantum-safe algorithms, as these are relatively new solutions and their application has not yet had enough time to expose their shortcomings, so it is vital to apply them in combination with classic algorithms, that is hybrid solutions should be used. [17]

As for symmetric-algorithm key sizes it recommends the already mentioned doubling of key sizes with reference to the Grover search algorithm. The size of the keys for symmetric algorithms is even more important when the goal is to provide long-time security for encrypted data. [17]

The ENISA paper "Post-Quantum Cryptography: Current state and quantum mitigation", published on May 3rd, 2021, firstly gives a good technical background on post-quantum cryptography including the description of five main families of algorithms, reviews the NIST PQC project and the Round 3 finalists, and finally comes with two recommendations in the Quantum Mitigation section, in order to improve security against quantum attacks. [18]

One of the two proposals is, similarly to the German paper "Migration zu Post-Quanten-Kryptografie", is the usage of hybrid schemes of pre-quantum and post-quantum cryptographic primitives. The basic idea is to combine a traditional PKC algorithm like RSA with a post-quantum one, at least one of them being secure ensures the security of the cryptosystem. [18]

This scheme can be applied to either in the context of TLS (Transport Layer Security) or that of electronic signatures. The paper cites the article "Transitioning to a Quantum-Resistant Public Key Infrastructure". [18] The article states that X.509 certificates could be used in a hybrid manner in two different ways: Dual certificates, Second certificate in extension [19]

Dual certificates means that there would be two certificates created, since there is no option in X.509 for including more than one keys in a certificate, one for the classical public key algorithm and another one for the post-quantum one, implying that two signatures have to be created for every document, one for each algorithm. [19]

The other approach is the extension of X.509 standard with the possibility of including more keys in a certificate. However, problems arise as a result of the key sizes of the PQC algorithms. [19]

There was an attempt in standardizing the above concept of multiple key certificates in 2018, the IETF draft "Multiple Public-Key Algorithm X.509 Certificates draft -truskovsky-lamps-pq-hybrid-x509-01" proposed ways to embed alternate cryptographic materials in certificates in order to use multiple algorithms with one certificate. But unfortunately, the draft expired on March 2, 2019. [20] To the best of my knowledge, there is no standardized solution for this approach, but many organizations offer non-standard solutions for multiple-key X.509 certificates e.g., the Open Quantum Safe project or ISARA Corporation. [21] [22]

SUMMARY

Universal quantum supremacy is apparently on its way, and it is very difficult to estimate when it shall occur, but should it happen, it shall cause serious problems in cryptography. Companies operating IT systems and IT security professionals need to prepare for the occurrence of the so-called quantum apocalypse. Fortunately, the cryptographic community is working hard to replace quantum vulnerable cryptographic primitives.

In my humble opinion is vital to keep track of the development of quantum computing and post-quantum cryptography so that the necessary steps can be taken in time to maintain and enhance IT security.

In my opinion, the review of eIDAS regulation and the ETSI EN 319 102-1 V1.3.1 (2021-11) "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation" European standard from a post-quantum point of view is vital and should be done in time to ensure a smooth transition into the post-quantum era.

My understanding is that crypto agility is a vital concept, practitioners should design cryptosystems keeping in mind that the used primitives may become compromised in time making it necessary to replace them.

Transition to post-quantum cryptography is crucial but so as proceeding with caution. The use of hybrid schemes of pre-quantum and post-quantum cryptographic primitives

ensures that we do not fall victim to possible, yet unknown vulnerabilities of post-quantum primitives during the transition period.

RESOURCES

[1] P. Rincon, "IBM claims advance in quantum computing," 17 11 2021. [Online]. Available: https://www.bbc.com/news/science-environment-59320073. [Accessed 20 12 2021].

[2] Turner, Dawn. "What is a Digital Signature - What It Does, How It Works". Cryptomathic. https://www.cryptomathic.com/news-events/blog/what-is-a-digital-signature-what-it-does-how-it-works [Accessed 05 11 2021].

[3] "Electronic Signatures in Global and National Commerce Act," 30 06 2000. [Online]. Available: https://www.govinfo.gov/content/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf. [Accessed 05 11 2021].

[4] "GOVERNMENT PAPERWORK ELIMINATION ACT," 21 10 1998. [Online]. Available: https://www.govinfo.gov/content/pkg/PLAW-105publ277/pdf/PLAW-105publ277.pdf. [Accessed 05 11 2021].

[5] "Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5)," 20 10 2021. [Online]. Available: https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/index.html. [Accessed 05 11 2021].

[6] The European Parliament and The Council of The Euroepean Union, "REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL," Official Journal of the European Union, 23 07 2014.

[7] European Economic and Social Committee, "The digital single market - trends and opportunities for SMEs (own-initiative opinion)," 18 09 2020. [Online]. Available: https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/digital-single-market-trends-and-opportunities-smes-own-initiative-opinion. [Accessed 05 11 2021].

[8] scrive, "eIDAS and the Digital Single Market," [Online]. Available: https://www.scrive.com/trust-center/eidas-summary/. [Accessed 05 11 2021].

[9] A. S. Tannenbaum, Computer Networks, New Jersey: Pearson Education, 2003.

[10] ETSI, "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation," 11 2021. [Online]. Available: https://www.etsi.org/deliver/etsi_en/319100_319199/31910201/01.03.01_60/en_31910201v010301p.pdf. [Accessed 11 11 2021].

[11] Adams, et al., "RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)," 08 2001. [Online]. Available: https://www.ietf.org/rfc/rfc3161.txt. [Accessed 11 11 2021].

[12] W. Vercruysse, "What are the B-T-LT and LTA levels of an electronic signature," 18 12 2019. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/ESIGKB/What+are+the+B-T-LT+and+LTA+levels+of+an+electronic+signature. [Accessed 11 11 2021].

[13] N. Nyári, "The Impact of Quantum Computing on IT Security," Safety and Security Sciences Review, vol. 3, no. 4, pp. 25-37, 2021.

[14] S. Vogt and H. Funke, "How Quantum Computers threat security of PKIs and thus eIDs," 02 06 2021. [Online]. Available: https://dl.gi.de/bitstream/handle/20.500.12116/36504/proceedings-07.pdf?sequence=1&isAllowed=y. [Accessed 21 11 2021].
[15] NIST NCCoE, "Migration to Post-Quantum Cryptography," 08 2021. [Online]. Available: https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms. [Accessed 21 11 2021].
[16] NIST, "Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms," 28 04 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf. [Accessed 07 12 2021].
[17] Bundesamt für Sicherheit in der Informationstechnik, "Migration zu Post-Quanten-Kryptografie," 24 08 2020. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-Kryptografie.pdf. [Accessed 21 11 2021].
[18] ENISA, "Post-Quantum Cryptography: Current state and quantum mitigation," 03 05 2021. [Online]. Available: https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation. [Accessed 24 10 2021].
[19] Nina Bindel and Udyani Herath and Matthew McKague and Douglas Stebila, "Transitioning to a Quantum-Resistant Public Key Infrastructure," 24 05 2017. [Online]. Available: https://eprint.iacr.org/2017/460. [Accessed 07 12 2021].
[20] A. Truskovsky, D. Van Geest, S. Fluhrer,P. Kampanakis, M. Ounsworth, S. Mister, "Multiple Public-Key Algorithm X.509 Certificates draft-truskovsky-lamps-pq-hybrid-x509-01," 29 08 2018. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-truskovsky-lamps-pq-hybrid-x509-01. [Accessed 07 12 2021].
[21] Open Quantum Safe, "X.509," [Online]. Available: https://openquantumsafe.org/applications/x509.html. [Accessed 07 12 2021].
[22] ISARA Corporation, "ISARA Radiate OpenSSL Connector 1.4 QS Multiple Public Key Algorithm Certificate Tutorial," 26 03 2018. [Online]. Available: https://www.isara.com/openssl/1.4/OpenSSL-Connector-MPKAC-Tutorial.html#ProgrammersGuidetoMPKAC. [Accessed 07 12 2021].
[23] eIDAS eID Technical Subgroup, "eIDAS Cryptographic Requirements for the Interoperability Framework," 31 08 2019. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20Interoperability%20Architecture%20v.1.2%20Final.pdf. [Accessed 05 11 2021].
[24] D. J. Bernstein, "Grover vs. McEliece," Sendrier N. (eds) Post-Quantum Cryptography. PQCrypto 2010. Lecture Notes in Computer Science, vol. 6061, 2010.
[25] L. K. Grover, "A fast quantum mechanical algorithm for database search," in Proceedings of the twenty-eighth annual ACM symposium on the, Philadelphia, Association for Computer Machinery, 1996, pp. 212-219.