

Protecting Electronic Signatures from Cyber Threats in Electronic Contracts

Protección de las firmas electrónicas frente a las amenazas cibernéticas en los contratos electrónicos

Bendjerad Abderrahmane (Ph.D)

University of Adrar, Algeria
bendjerad@univ-adrar.edu.dz

Received: 20.04.2026 Accepted: 07.09.2026 Publishing: 12.10.2026

Abstract

When electronic documents replaced traditional paper documents, electronic signatures took the place of traditional signatures. Consequently, electronic signatures required serious protection, especially since they are created through electronic means that are exposed to numerous cyber risks. Therefore, many mechanisms have been established to protect these signatures, including mechanisms related to their creation and others related to their verification.

Keywords: Electronic contracts, electronic documents, electronic signatures, cyber threats.

Resumen

Con la sustitución de los documentos tradicionales en papel por documentos electrónicos, las firmas electrónicas pasaron a ocupar el lugar de las firmas tradicionales. En consecuencia, se hizo necesario garantizar una protección rigurosa de las firmas electrónicas, especialmente porque se generan mediante medios electrónicos expuestos a numerosos riesgos cibernéticos. Por ello, se han establecido diversos mecanismos para protegerlas, tanto en su creación como en su verificación.

Palabras clave: Contratos electrónicos, documentos electrónicos, firmas electrónicas, amenazas cibernéticas.

Introduction

Today, humanity faces many challenges, particularly amid the rapid digital development. The greatest challenges of this progress lie in the widespread use of modern technologies across all fields, which are met with the absence of sufficient safeguards for these uses, leaving them vulnerable to numerous risks due to the growing phenomenon of cybercrime targeting personal data, as well as financial and reputational assets.

The widespread adoption of modern technologies in various sectors — notably in contracting processes — stems from the advantages and benefits they offer, such as saving time and effort. Contracting now takes place through electronic documents authenticated by electronic signatures. Additionally, communication between contracting parties is conducted remotely through electronic means, with the complete absence of physical presence, making these technologies increasingly attractive to all parties involved.

Cybercrimes have diversified, including crimes against electronic systems — such as stealing personal data stored within them, sabotaging these systems, or forging the information they contain — as well as crimes targeting financial assets and reputations. All these crimes cause significant harm to individuals and institutions alike.

The electronic signature is the mechanism that gives electronic documents their legal status and attributes them to their owners. Initially, there was considerable apprehension about electronic signatures, similar to the general fear people have toward any new technology. However, with the continuous advancement of information and communication technologies and the increasing issuance of legislation protecting such transactions, this fear has dissipated, and electronic signatures have even become more accepted than traditional signatures. According to the regulations of countries that recognize electronic transactions for concluding deals, any physical presence in the process of concluding public contracts is prohibited. Thus, the use of electronic signatures as a means of authenticating all documents exchanged between contracting parties is required. Nevertheless, this signature remains vulnerable to many breaches because it is transmitted via the internet, which is exposed to all kinds of cyber attacks. Therefore, what mechanisms have legislations put in place for creating and proving electronic signatures in the face of cyber threats and to instill trust among the contracting parties?

To instill confidence and security in such transactions, much legislation have sought to establish mechanisms for the creation of electronic signatures (First Section), as well as mechanisms for the verification of these signatures (Second Section).

First Section: Mechanisms for Creating Electronic Signatures

Many countries have resorted to adopting electronic contracts in their dealings, which necessitated the use of electronic signatures to authenticate these contracts.

To protect electronic signatures from tampering or infringement, these countries have required contracting parties to obtain an electronic certification certificate (First Requirement), and have adopted electronic encryption mechanisms to further enhance the protection of such signatures (Second Requirement).

First Requirement: *The Electronic Certification Certificate as a Mechanism for Protecting the Electronic Signature*

The electronic certification certificate has been established as an effective mechanism for granting legal validity to electronic signatures.

Article 7 of the UNCITRAL Model Law on Electronic Signatures states that any person, device, or authority designated by the enacting state—whether public or private—may be authorized to identify electronic signatures that comply with the provisions of Article 6 of this law.

It also stipulates that any such designation must be consistent with internationally recognized standards, and that nothing in this article shall affect the validity of the rules of private international law. (Signatures, 2011)

Article 1 of the Egyptian Law No. 15 of 2004, concerning the regulation of electronic signatures and the establishment of the Information Technology Industry Development Authority, states that:

"An electronic certification certificate is the certificate issued by a licensed certification authority, proving the link between the signer and the data used to create the signature."(15/2004, 2004)

Similarly, Article 1 of the Iraqi Law No. 78 of 2012, concerning the Law on Electronic Signatures and Electronic Transactions, provides that:

"An electronic certification certificate is the document issued by a certification authority under the provisions of this law, and it is used to prove the attribution of the electronic signature to the signer."(78/2012, 2012)

The Algerian legislator used the term "electronic certification service provider" to refer to the entities that issue electronic certification certificates, defining it as:

"Any natural or legal person who grants specified electronic certificates, and who may also provide other services in the field of electronic certification, after obtaining a license granted by the economic authority(16-143, 2016) for electronic certification."(15-04, 2015)

The certificate holder, according to the definition in Law 15-04, is any natural or legal person who has obtained an electronic certification certificate from a certification service provider or a trusted third party. Thus, in the field of public procurement, the certificate holder is any public purchaser or economic operator who has been granted this certificate to sign electronically within the scope of electronic transactions in public procurement.

As for the trusted third party, according to the same law, it is defined as "a legal entity that issues qualified electronic certification certificates and may provide other services related to electronic certification for participants in the government sector." Therefore, the trusted third party is a legal entity entrusted by the governmental authority(**15-04, 2015**)with the task of granting electronic certification certificates on its behalf.

An electronic signature certificate is an electronic document intended to verify the identity of the signer (identity card), ensure the integrity of exchanged documents (protection against any alteration), and guarantee non-repudiation of the signature. It is usually provided on an external USB data storage device. The electronic signature certificate links the electronic signature data to a natural person.

Article 19 of Egyptian Law No. 15 of 2004 states that:

"It is not permitted to engage in the activity of issuing electronic certification certificates without a license from the Authority, in return for a fee determined by its Board of Directors, according to the procedures, rules, and guarantees set forth in the Executive Regulations of this Law, and without being bound by the provisions of Law No. 129 of 1947 concerning public utilities obligations.

It must be ensured that the licensee is selected through competition and transparency; the Board of Directors of the Authority shall determine the duration of the license, provided that it does not exceed ninety-nine years; and the means of technical and financial supervision and monitoring must be defined to ensure the regular and continuous operation of the service.(15/2004, 2004, p. Article 19)

Furthermore, it is not permitted to cease the licensed activity, merge with another entity, or transfer the license to a third party without obtaining prior written approval from the Authority."

Among all categories of electronic signature certificates marketed by specialized companies known as "electronic certification service providers," the minister responsible for state reform refers specifically to those that meet a cross-sectoral security reference framework by complying with minimum technical requirements.

As for public procurement, only RGS-type electronic signature certificates are accepted, and the electronic signature must comply with the EIDAS regulation.

It should also be noted that there are different formats for electronic signatures, such as (XAdES, CAdES, and PAdES).(910-2014, 2014).

EIDAS certificates for public procurement in European Union countries have been in effect since October 1, 2018. From that date onward, it became mandatory for public purchasers or economic operators wishing to engage in electronic contracting to have an advanced electronic signature (Advanced) compliant with the EIDAS regulation.(www.marche-public.fr, 2020)

It is important to note that there are three types of electronic signatures: simple, advanced, and qualified.

Several necessary steps must be followed to obtain an electronic signature certificate, which include: Having a valid email address and appropriate IT equipment; Requesting the electronic certificate from the certification authority and reviewing the required supporting documents; submitting the required supporting documents to the registration authority; personally collecting the certificate from the registration authority.(www.sallan.com, 2020)-

When an electronic signature is required for any document in electronic form for any public procurement contract, it must be signed in accordance with the provisions of the decree dated March 22, 2019, related to electronic signatures in public procurement contracts.

It is worth noting that since the reform of the French public procurement system in 2016, it is no longer necessary to sign requests and offers either manually or electronically. Instead, the public purchaser can impose a signature upon the submission of offers if stipulated in the procurement documents. However, the contract must be signed either manually or electronically after it is awarded, in accordance with the provisions set by the public purchaser.

Public purchasers, licensing authorities, and economic operators must use an electronic signature that complies with the requirements of the European Union's EIDAS system, in accordance with Regulation No. 910/2014 related to advanced electronic signatures based on a qualified certificate.(www.sallan.com, 2020)

As for the electronic signature under the concept of Article 1316-4, which was replaced by Article 1367 of the French Civil Code, it involves the use of a reliable identification process that ensures its connection to the act it is associated with. The reliability of this process is presumed unless proven otherwise, and it is achieved through the creation of the electronic signature, ensuring the signer's identity and the integrity of the guaranteed act, according to the conditions set by Council of State Decree No. 2001-272 of March 30, 2001, concerning the implementation of Article 1316-4 of the Civil Code related to electronic signatures.(2016-131, 2016)

Regarding the recognition of foreign electronic certificates and signatures, Article 12 of the UNCITRAL Model Law on Electronic Signatures states that:

When determining whether an electronic certificate or signature is legally valid or to what extent it is valid, no consideration shall be given to the geographic location where the certificate is issued or the electronic signature is created or used; the geographic location of the place of business of the issuer or signer. A certificate issued outside the enacting state shall have the same legal effect in the enacting state as a certificate issued within the enacting state if it provides an equivalent level of reliability. An electronic signature created or used outside the enacting state shall have the same legal effect in the enacting state as an electronic signature created or used within the enacting state if it provides an equivalent level of reliability.

When determining whether an electronic certificate or signature provide an equivalent level of reliability, consideration shall be given to internationally recognized standards and any other relevant factors."(Signatures, 2011, p. Article 12)

To provide the necessary protection for the electronic signature, the Algerian legislator has defined the responsibilities of the electronic certification service provider as well as the certificate holder. Thus, the electronic certification service provider who issues a qualified certification certificate is responsible for any damage caused to any entity or natural or legal person who relied on this electronic certificate in relation to:

The accuracy of all information contained in the qualified electronic certification certificate on the date it was issued and the presence of all the required data in the certificate; Ensuring that, when issuing the electronic certificate, the signer identified in the certificate possesses all the signature creation data corresponding to the verification data provided and specified in the certificate; ensuring that the signature creation data and verification data are usable in an integrated manner, unless the electronic certification service provider proves that no negligence was committed. (15-04, 2015, p. Article 53).

The electronic certification service provider who issued the qualified certification certificate shall also be responsible for any damage resulting from the failure to revoke the electronic certificate, which affects any entity or natural or legal person who relied on that certificate, unless the electronic certification service provider proves that no negligence was committed.(15-04, 2015, p. Article 54)

As for the holder of the electronic certification certificate, once the certificate is signed, they become solely responsible for the confidentiality of the signature creation data. In the event of doubt regarding the confidentiality of the signature creation data or if this data no longer corresponds to the information included in the electronic certification certificate, the certificate holder must request its revocation by the electronic certification service provider. Furthermore, upon the expiration or revocation of the electronic certification certificate, the certificate holder may not use the corresponding signature creation data to sign or certify the same data by another certification service provider. The holder of the qualified electronic certification certificate may not use the certificate for purposes other than those for which it was issued. (15-04, 2015, pp. Article 61,62)

Section Two: Electronic Encryption as a Mechanism for Protecting Electronic Signatures:

An electronic certificate is a digital identity that is personal, belonging to a member of a company or management agent. The electronic certificate consists of three inseparable elements. The first element includes information related to the identity of the owner (last name, first name, position, service, email, etc.), their organization (company, association, administration, etc.), the start and end date of the

certificate, the identity of the certifying authority that issued it, the functions authorized by the certificate, the address related to accessing the certification authority's issuance policy, and the address of the list of revoked certificates.

The second element is the private key, and the third element is the public key.

The certificate necessary for electronic transactions consists of a public key and its associated private key, which must remain confidential (this is called an asymmetric key certificate). It is usually in the form of an electronic physical medium, such as an encrypted USB key or a smart card.

The issuing authority for the certificate is a service provider that issues certificates for the benefit of users. When the service provider is a private company, it markets the produced certificates, while if the service provider is an administrative authority, it issues them to its agents.

The issuing authority signs the certificate (with its private key), thus ensuring the integrity of the certificate and the accuracy of the information contained in the certificates it issues. The issuing authority ensures the link between the user (the future signer) and the certificate it will issue to them, by verifying identity documents, meeting with the user face-to-face, or ensuring the accuracy of the information provided by the certificate applicant.

The certificate is valid for two to three years, and its annual cost depends on the services associated with it, ranging between 70 and 130 Euros.

Obtaining an electronic signature certificate practically takes between 15 days to 17 months, and sometimes even longer. Therefore, the company applying for the certificate must submit the request in advance. (www.marche-public.fr, 2020)

Encryption is a process that involves encoding, making the signature unreadable. It is done using a secret key generated by an encryption algorithm, and its purpose is to protect information and maintain its confidentiality.

Encryption can be either symmetric (using the same key for both encryption and decryption) or asymmetric (where the public key is used for encryption and the private key is used for decryption).(www.marche-public.fr, 2020)

Electronic responses can only be made under certain conditions. In the buyer's profile (Buyer Profile), the website ensures data transfers and allows entities, through a data encryption system, to be the only ones capable of revealing electronic offers and applications.

In fact, while the economic operator must sign their offers electronically with a unified electronic certificate, the public purchaser also uses a dual-key certificate to encrypt company offers. This means that on the platform for removing the physical form (the buyer's profile), the local authority records the public key of its electronic certificate on behalf of the contracting authority. When the electronic envelopes are opened, the platform will check for the corresponding private key on the computer performing the opening process, thus ensuring that the transmission is secure.

Also, the RGS certificates used in electronic signing do not have the technical capability to perform encryption and decryption of the offers from economic operators and the electronic treasury. (www.marchespublicsaffectes.com, 2020)

The signing software or "signing tool" allows for the electronic installation of the signature. Economic operators who do not have signing software can use the buyer's profile, but the public purchaser cannot mandate the use of the platform's tool.

It is also common to note that signing a compressed file is not sufficient if the documents related to the immaterial public procurement that it contains are not also signed.(www.sallan.com, 2020)

Many other legislations have addressed the encryption mechanism, similar to the Egyptian legislator, who confirmed in the executive regulations of the Electronic Signature Law No. 15 of 2004 that encryption is a technical computational system that uses special keys to process and transform electronically readable data and information in such a way that prevents the extraction of this data and information except through the use of a decryption key or keys. The public-key cryptography technique—also known as the public key system—is a system that allows any natural or legal person to have two separate keys: one public key that is electronically available, and one private key that is kept by the person and maintained with a high level of confidentiality. The root cryptographic key is an electronic tool generated through a specific computational process and is used by electronic certification authorities to issue electronic certification certificates and to generate electronic signature

data.(15/2004, 2004, p. Article one 01).

As for the Algerian legislator, they did not provide a definition of encryption, merely referring to it when discussing the verification data of the electronic signature, describing it as "codes or public encryption keys or any other data used to verify the electronic signature."(15-04, 2015, p. Article one 01).

Thus, all Arab legislations have not specifically allocated electronic signatures to public procurement; instead, they have enacted laws that address electronic signatures in general. This is in contrast to the European Union countries, which have distinguished between electronic signatures used in civil electronic transactions and those used in electronic transactions related to public procurement.

Section Two: Mechanisms for Proving Electronic Signatures

In order to strip contracts of their physical form and give them an electronic character in line with technological development, electronic documents were introduced to replace traditional paper-based ones. To ensure that these electronic documents are not deprived of their legal nature—or more precisely, their legal value—they must be signed using an electronic signature. This signature must carry full legal probative force, which we believe complements the overall evidentiary value of the document. This was addressed by the UNCITRAL Model Law on Electronic Signatures of 2001, which outlined the mechanism through which an electronic signature attains legal reliability and, consequently, legal recognition of its evidentiary validity.(Al-Dumyati, 2009)

In its review of the appeal against the ruling of the Administrative Court of Appeal in the city of Rennes, France, the French Council of State explicitly recognized the admissibility of signatures on electronic media. Thus, the Council upheld the appellant's request on the basis that the electronic document derives its evidentiary value from the signature placed on the form that was sent to the administration, as recorded and confirmed in the computer's memory.(Marcou, 2003)

With the emergence of the electronic signature, questions arose regarding the possibility of applying the conditions of a traditional signature to an electronic one, due to the unique nature of the electronic

signature, which is applied using electronic tools to an intangible electronic document, as opposed to the traditional signature, which is handwritten on a physical paper document.

The European Union Regulation No. 910 of 2014, concerning electronic identification and trust services for electronic transactions, addressed in many of its provisions both electronic identification and electronic authentication.(910-2014, 2014, p. Article one 01).

For the electronic signature to be valid in proving an electronic administrative contract, the identity of the signer must first be verified through the signature (First Requirement), followed by the need to preserve the electronic signature (Second Requirement).

First Requirement: Verifying the Signer's Identity

For the electronic signature to produce its legal effects, it must reflect the identity of its owner. This does not mean that the electronic signature replaces or serves as a personal identification card, nor does it imply that it replaces a pseudonym. Rather, what is meant by identifying the signer through the signature is that the electronic signature must be under the sole control of the signer. Moreover, the use of the electronic signature results in the issuance of a certificate by a competent authority, which serves as an electronic identification card for the signer.(Hejazi, 2003)

A secured electronic signature verifies the identity of the signer through a unique electronic code specific to the individual, which is processed electronically and reveals the person's identity, distinguishing them from others. In this context, a trusted electronic signature certification authority may also be relied upon to fully verify the identity of the person using the electronic signature.(Sareity, 2006)

Article 7 of the UNCITRAL Model Law on Electronic Commerce is based on recognizing the functions of signatures within a paper-based environment.

When drafting the Model Law, the functions of a signature were considered, including identifying the person, providing assurance of that person's involvement in the act of signing, and establishing a connection between the person and the content of the document. Additionally, it was noted that a signature can serve a variety of functions depending on the nature of the document it appears on. For example, a signature may attest to the intention of a party to be bound by the content of the signed contract, the intention of the person who authored the text, the commitment of a person to the content of a document written by someone else, or even confirm the presence of a person at a specific place and time.(Law, 1996)

To identify the signer through the electronic signature, it is necessary to ensure that the signer alone has control over the electronic signature tool (First Subsection), followed by the electronic issuance of a certificate or ID for the signer (Second Subsection).

First Subsection: The Signer's Exclusive Control over the Electronic Signature ToolFor an electronic signature to be admissible as evidence, it is required that the signer alone exercises control over the signature tool. This is affirmed by Article 2 of European Directive No. 93 of 1999 concerning electronic signatures, which states: "For an electronic signature to be admissible as evidence, it is required that the signer alone, to the exclusion of others, controls the electronic signature tool. The electronic signature must also be linked to the signer; allow for the identification of the signer; be created using means that enable the signer to retain and control it; and be associated with data in such a way as to allow the detection of any subsequent modifications to that data."(1999/93/CE, 1999)

Paragraph 4 of Article 1316 of the French Civil Code states that an electronic signature is created using a secure method to verify the identity of the signer, which must ensure a connection between the signer and the act to which the signature relates.(2000/230, 2000)

Article 18 of Law No. 15 of 2004 on Electronic Signatures in Egypt provides that electronic signatures, electronic writing, and electronic documents have legal probative value if the electronic signature is linked solely to the signer and no one else; if the signer alone controls the electronic medium; and if it is possible to detect any modification or alteration in the electronic document or the electronic signature.(15/2004, 2004, p. Article 18)

Furthermore, Article 9 of the Executive Regulations of Law No. 15 of 2004 on Electronic Signatures in Egypt requires that for the electronic signature to be exclusively linked to the signer, it must be based on a system for generating electronic signature creation data, as stipulated in Articles 2, 3, and 4 of these regulations.(109, 2005)

Article 10 of the same Executive Regulations clarifies that the signer's exclusive control over the electronic signature tool is achieved through the signer's possession of the device used to store the private cryptographic key, including a secured smart card and the associated PIN code.(109, 2005, p. Article 10)

Second Subsection: Electronic Issuance of a Certificate or ID for the Signer.

Paragraph 1 of Article 1316 of the French Civil Code affirms that writing in electronic form is admissible as evidence, just like writing on paper, provided that the identity of the person from whom it originates can be established and that it is created and stored in a manner that guarantees its integrity.(2000/230, 2000, p. Paragraph 01)

Paragraph 4 of the same article emphasizes the necessity for the tool used in electronic signing to be reliable in order to ensure the connection between the signer and the signed act.

Accordingly, under the decree issued by the French Council of State on March 30, 2001, concerning electronic signatures, there are two types of electronic signature certification models:

1. The Simple Electronic Certificate:

This is an electronic document issued by the competent certification authority, in which it confirms the validity of the electronic signature data and its link to the signer. However, this model does not contain additional identifying information. (Salim, 2004)

2. The Qualified Electronic Certificate:

This model is more secure and must include several pieces of information as stipulated in Article 6 of the aforementioned decree by the French Council of State. These details provide greater security for the concerned party and include, among others: the name or pseudonym of the signature holder, their professional position, the duration of validity of the certificate, and the unique identification code of the electronic identity verification card.(Al-Mari, 1998)

In Iraq, the Iraqi legislator, in the Electronic Signature and Electronic Transactions Law No. 78 of 2012, emphasized that the certification certificate is what establishes the attribution of the electronic signature to its owner. (78/2012, 2012, p. Article 11)

It is well known that the process of certifying an electronic signature goes through several stages. It begins with the concerned party notifying the competent certification authority of the signer's public key. Based on the available information, the certification authority then verifies the identity and eligibility of the holder of the public key. Afterward, the authority prepares an electronic certificate to confirm the identity of the signer, in which it affirms the link between the public key and the signer. This certificate is then sent electronically to the requesting party after being electronically signed by the certification authority.

Second Requirement: The Necessity of Preserving the Electronic Signature

For electronic writing to enjoy the same probative value as paper-based writing, it must be preserved under conditions that ensure its integrity. The French legislator emphasized this in Article 1316 of the Civil Code, particularly in its first paragraph, which affirms that electronic writing has

evidentiary value equivalent to that of writing on a physical medium, provided it is created and stored in conditions that maintain and ensure its integrity.(2000/230, 2000, p. Paragraph 01)

The French legislator also stressed that a secured electronic signature must be: Linked to the signer, Capable of identifying the signer, created using means that allow the signer to retain and control it, and Associated with data in such a way that allows any subsequent modifications to those data to be detected.(2001-272, 2017)

This is the same definition provided by European Directive 1999/93 concerning electronic signatures.

To ensure the preservation of electronic signatures, Decree No. 692 of 2002 required public administrations to maintain the integrity of electronic documents and to secure the confidentiality of electronic signatures. Additionally, it placed the responsibility on candidates to bear the costs of accessing the website network and any appeals related to electronic signatures.(2006-975, 2006)

The sender of the electronic signature possesses a private key and can only alter their signature using a code they alone hold. The recipient, on the other hand, has access to a public key and can compare the sent message with the received one. If the signature is verified to be intact, the recipient may request its certification as valid.(2001-272, 2017)

It is worth noting that the preservation of the electronic signature must extend beyond the duration of the electronic administrative contract, whether it ends through termination or execution. This is to prevent any potential legal disputes between the contracting parties, allowing reference to the electronic documents and the signatures affixed to them. This preservation must last for the entire statutory period, and unless otherwise specified, the data should be stored on electronic media. This process also supports the verification of the order and timing of the administrative contract(Rahima Essaghir, 2007), a responsibility that lies with electronic certification authorities.

According to these provisions, the requirement to preserve the electronic signature is essential for recognizing its validity as evidence—particularly given the risks that electronic messages face, such as alteration, unauthorized access, deletion, or addition, from the moment of sending to the moment of receipt.(Hejazi, 2003, p. p318)

Preserving the electronic signature means that it must remain exactly as it was when issued by its source until it reaches the recipient.

The decree issued on March 30, 2001, regulates the system for preserving the integrity of electronic signatures and electronic data in its Articles 1 and 5. It stipulates the necessity of issuing a certificate by a designated verification authority, which confirms the validity of the electronic signature and writing and certifies that the signature has been properly preserved from the time it was sent until it was certified.(2001-272, 2017, p. Article 01)

The long-term preservation of an electronic signature is closely tied to the statute of limitations. The stored information must remain intact for the full legal duration applicable to the preserved act. Therefore, the information and data must be stored on electronic media that protect them from damage, alteration, or destruction in any form.(Kandil, 2004)

For storage to take place at the electronic archive authority, the concerned party (one of the contracting parties) must compile the documents and data to be preserved, indicate the exact date and time of the contract's conclusion in these documents, and sign this bundle of electronic documents. This stage is referred to as "signing the signature" (Signer la signature). The bundle is then sent via email to the storage authority, which in turn stores the electronic documents, signs them, and includes the date and time of storage in a preservation certificate.(E-Caprioli, 2019) Ultimately, it is up to the judge to assess the integrity of the preserved data over time, as the judge is responsible for examining the documents and determining their validity.

Conclusion:

Through our study of the topic of electronic signatures and their protection against cyber threats, we reached several conclusions, including:

That the creation and validation of an electronic signature require several conditions, among them:

- The existence of an electronic certification certificate, which is issued by a licensed certification authority and confirms the link between the signer and the signature creation data.

- That no entity may engage in the activity of issuing electronic certification certificates without a license from the state, and this is in exchange for a fee determined by its board of directors in accordance with the procedures, rules, and guarantees established by laws and regulations.

- That there are several necessary steps to obtain an electronic certification certificate, including: Having a valid email address and appropriate technological equipment; Requesting the electronic certificate from the certifying authority and reviewing the supporting documents to be submitted; Sending the required supporting documents to the registration authority; Personally receiving the certificate from the registration authority.

- That in countries that rely on electronic transactions for the conclusion of contracts, it has become essential to sign contracts electronically under penalty of invalidity in terms of enforceability.

- The electronic certificate is a personal digital identity, and thus it personally belongs to a member of a company or a management agent. The electronic certificate consists of three inseparable elements:

- The first element includes information related to the identity of the owner (last name, first name, position, department, email address, etc.); their organization (company, association, administration, etc.); the certificate's start and end validity dates; the identity of the certifying authority that issued it; the functions granted by the certificate; the address to access the certifying authority's certificate issuance policy; and the address of the list of revoked certificates.

- The second element is the private key.

- The third element is the public key.

And that the electronic signature has mechanisms of proof, including:

- A secure electronic signature verifies the identity of the signer through a unique code assigned electronically, which reveals the individual's identity and distinguishes them from others. In this context, it is also possible to rely on an electronic signature certification authority for complete verification of the person using the electronic signature.

- The signer must have exclusive control over the electronic medium; and it must be possible to detect any modification or alteration in the content of the electronic document or the electronic signature.

In the course of our study on electronic signatures and methods of protecting them, we propose several recommendations, including:

- Continuing to enact various laws and regulations that provide sufficient guarantees for the use of electronic signatures, strengthen the authority of entities issuing electronic certification and those using such certificates, and impose stricter penalties on those who violate electronic systems and information.

- Establishing specialized regulatory bodies in the field of electronic system protection to detect and hold accountable any violations of these systems, whether by certificate-issuing authorities, certificate holders themselves, or individuals or entities that unlawfully attack electronic systems or information.

Bibliographie

- 109, D. (2005, 05 25). The issuance of the Executive regulations of the Electronic Signature Law and the Establishment of the Information Technology Industry Development Agency. 115. Egypt: Official Gazette of Egypt.
- 15/2004. (2004, April 22). Regulation of Electronic Signatures and establishment of the Information Technology Industry Development Authority. *Egyptian Law*, 17, Article One 01. Egypt: Official Gazette.
- 15-04. (2015, February 01). Algerian Law. (06), Article 06. Algeria: Official Gazette.
- 16-143. (2016, April 25). Algerian Law. *Organization, operation, and functions of the technical and administrative departments of the National Electronic Certification Authority*. Algeria.
- 1999/93/CE. (1999, 12 13). The European Parliament and of the Council. L13/12. CE: Official Journal.
- 2000/230. (2000, 03 13). (14 March 2000). France: JORF.
- 2001-272. (2017, September 28). taken for the application of article 1316-4 of the civil code and relating to electronic signature. *Abrogate by decree n 2017-1416 of 28 September 2017*. France: JORF.
- 2006-975. (2006, August 01). relating to the public procurement code. Article 07. France: JORF.
- 2016-131. (2016, february 10). Ordinance. *the reform of contract law, the general regime and proof of obligations*, Article 03. France.
- 78/2012. (2012, november 05). Iraqi Law. *Electronic Signatures and Electronic Transactions*, Article One 01. Iraq.
- 910-2014. (2014, July 23). CE. *electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, L257/73*. CE: Official Journal of the European Union.
- Al-Dumyati, T. M. (2009). *Proof of Electronic Contracting via the Internet A Comparative Study First Edition*. Alexandria Egypt: Mashat AL-mAAREF.
- Al-Mari, A. R. (1998). The Proprietary Value of Technological Media in Establishing Commercial Contracts. *Ph.D Thesis in Law*, 39.
- E-Caprioli. (2019). *Administrative Law and Electronic Evidence*. France. Récupéré sur <https://www.caprioli-avocats.com>
- Hejazi, A.-F. B. (2003). *Introduction to Arab E-Commerce, the Legal System of E-Commerce in the United Arab Emirates, Book Two*. Alexandria Egypt: Dar Al-Fikr Al-Jamii.
- Kandil, S. E.-S. (2004). *Electronic Signature*. Alexandria: Dar Al-Gamaa Al-JADIDA.
- Law, U. (1996). Model Law on Electronic Commerce of 1996. 36. New York, UNITED NATIONS.

Marcou, G. (2003). *The Regime of the Administrative Act in the Face of Electronics, Conference on Electronic Administration in the Service of citizens*. Paris France, University of Paris Sorbonne: Brylant Paris.

Rahima Essaghir, S. (2007). *The Electronic Administrative Contract*. Alexandria: Dar Al-Jamiaa Al-Jadida.

Salim, A. S. (2004). *Electronic Signature Comparative Study*. Cairo: Dar Al-Nahda Al-Arabia.

Sareity, M. A. (2006). *The Impact of E-Commerce on Market Structures with Reference to Developing Country*. Alexandria Egypt, University of Alexandria: Journal of Law.

Signatures, U. M. (2011). Article 07. *Electronic Signatures, Article 07*. New York USA, United Nations Publications.

www.marche-public.fr. (2020, 04 06). Consulté le 04 06, 2020, sur French public procurement website: www.marche-public.fr/Certificat-signature.htm

www.marchespublicsaffiches.com. (2020, 04 16). *marchespublicsaffiches*. Récupéré sur www.marchespublicsaffiches.com/certificats-electroniques/

www.sallan.com. (2020, 04 16). Consulté le 04 16, 2020, sur Sallan website: www.sallan-news-item/dematérialisation-des-marches-publics-5-cles-comprendre-lusage-de-la-signature-electronique.com

Declaraciones

Conflictos de interés: La autora declara no tener conflictos de interés relacionados con este estudio.

Financiación: La autora declara que este estudio no recibió financiación específica.

Responsabilidad autoral: La autora asume la responsabilidad del contenido del artículo.

Licencia

Este artículo se publica bajo la licencia Creative Commons Atribución 4.0 Internacional (CC BY 4.0), que permite su uso, distribución, reproducción y adaptación en cualquier medio, siempre que se cite adecuadamente a la autora y la fuente, se incluya un enlace a la licencia y se indiquen los cambios realizados.

<https://creativecommons.org/licenses/by/4.0/>

