Title: Electronic Writing and Signature as a Legal Mechanism for Protecting the Electronic Contractor in Algerian Legislation

Asma Keskes

Dr., Senior Lecturer A, Faculty of Law and Political Science, Mohamed Lamine Debaghine University – Setif 2, Email: a.keskes@univ-setif2.dz

Received: 09.02.2025 Accepted: 11.03.2025 Publishing: 15.05.2025 Doi: 10.56334/sei/8.4.52[1]

Abstract

Technological developments in the fields of communication and information technology have abolished geographical and political boundaries between states, transforming the world into a small village within a digital environment. This environment has witnessed numerous electronic commercial transactions that heavily rely on electronic contracts. These contracts present a legal and jurisprudential challenge due to their specific characteristics and virtual nature.

The issue of proving electronic contracts is among the most critical topics influencing the evolution and advancement of evidentiary rules. This shift corresponds with the scientific and technological progress in modern communication tools. In this context, the focus has been on examining the evidentiary value of electronic writing and electronic signatures to determine their legal standing as recognized forms of evidence—particularly in Algerian legislation and generally across legal systems. These mechanisms play a vital role in ensuring trust and security in digital transactions.

Keywords: electronic writing, electronic signature, legal mechanism, Algerian legislation.

Citation. Keskes A. (2025). Electronic Writing and Signature as a Legal Mechanism for Protecting the Electronic Contractor in Algerian Legislation. *Science, Education and Innovations in the Context of Modern Problems*, 8(4), 497-503; doi: 10.56352/sei/8.4.52. https://imcra-az.org/archive/362-science-education-and-innovations-in-the-context-of-modern-problems-issue-4-volviii-2025.html

Introduction

Proof is fundamental to the protection of rights and holds significant importance across legal systems, particularly concerning written evidence. Traditionally, such evidence required a physical, paper-based document bearing a seal and a signature. However, this concept of proof has transformed with the advent of electronic contracts, which rely on digital communication tools. These new forms and modes of transaction have replaced traditional paper-based agreements and handwritten signatures with digital formats and modern techniques.

Electronic transactions are now substantiated through electronic means—namely, electronic writing and electronic signatures—replacing conventional written methods that no longer align with the nature of electronic dealings. Writing remains one of the strongest forms of legal and judicial evidence for all types of transactions. Legislators have placed it at the forefront, especially in electronic commerce. The signature complements written proof by confirming the identity of the parties and their consent.

Thus, electronic writing and signatures have become essential mechanisms for validating electronic contracts. They have been legitimized through legislative amendments in contemporary legal systems.

This topic raises a central question:

To what extent are the provisions established by Algerian legislation regarding electronic writing and signatures sufficient as modern means of proof in electronic contracts?

In addressing this issue, this study employs both descriptive and analytical methodologies. It describes key aspects of the digital environment and analyzes relevant legal texts. Definitions and legal conditions for both electronic writing and electronic signatures are explored.

The study is structured into two main sections:

- The first section addresses electronic writing, providing its definition, conditions, and evidentiary value.
- The second section focuses on electronic signatures, including their definition, conditions, and evidentiary strength, concluding with a discussion on the certification of electronic signatures.

Section One: Electronic Writing (Electronic Document):

Written evidence is one of the most important forms of proof in legal proceedings due to its unique advantages over other forms, such as the ability to be prepared at the time of right creation, prior to any dispute. It also offers several guarantees, especially in recording the agreed-upon rights between parties, whether before or after a conflict arises.

The Algerian legislator addressed electronic writing as a form of evidence with the 2005 amendment to the Civil Code. Article 323 bis 1 of the Algerian Civil Code equates electronic writing with traditional paper-based writing, provided that the identity of the issuer can be verified and that the document is created under conditions that ensure its integrity. Consequently, electronic writing holds the same legal standing as written documents, whether formal or informal. This approach is inspired by the UNCITRAL Model Law on Electronic Commerce of 1996, particularly Article 6.

To better understand the concept of electronic writing, this section discusses its definition, the conditions under which it is admissible, and its evidentiary value:

1. Definition of Electronic Writing:

According to Article 323 bis of the Algerian Civil Code, the legislator has adapted to technological advancements by recognizing electronic writing. The article defines it as follows: "Proof by writing results from a sequence of letters, symbols, numbers, or any intelligible signs, regardless of the medium containing them or the method of their transmission."

This definition indicates that electronic writing comprises any symbols, letters, or numbers expressing thought or speech, stored on an electronic medium and transmitted in any manner, as long as it is retrievable. Therefore, electronic writing does not fundamentally differ from traditional writing, except in the nature of its medium—it is simply a form of writing expressed via digital means.

Electronic writing includes all electronic documents generated by modern communication tools, regardless of their format, medium, or transmission method. These writings occur on electronic media via electrical impulses and are converted into computer-readable formats. Examples include emails, electronic contracts, images, or any document stored and transmitted electronically—whether over the internet, through CDs, or even via fax or telex.

2. Conditions for Recognizing Electronic Writing:

For electronic writing to fulfill its legal evidentiary function and establish trust and security in contractual relationships, certain conditions must be met. These are primarily twofold:

- The ability to verify the identity of the person who issued the document.
- The requirement that the document is created and stored under conditions that ensure its integrity.

These conditions stem from the virtual nature of electronic environments, which are intangible and less secure by default. Further elaboration on these two conditions will follow in the subsequent analysis.

We elaborate on these two conditions as follows:

Condition 1 – The ability to verify the identity of the person who issued it:

Electronic contracting raises an important issue regarding the ability of one party to verify the identity of the other contracting party. This issue becomes particularly prominent in the event of a dispute concerning the probative value of such a contract. Specialists in this field have attempted to find technical solutions to this problem by using means of personal identification such as passwords or PIN codes, as well as encryption methods and biometric identification tools, such as retinal scans, voice recognition, or digitally or analogically transmitted fingerprints.

However, after experimenting with these tools, it has been confirmed that they are insufficient, as each has security vulnerabilities. Therefore, the idea of an intermediary party in the contractual relationship—known as "certification authorities"—was introduced. These are companies operating in the field of technical services, offering certificates that confirm whether a request or response was indeed issued by the concerned signer, and that specify the date of issuance. They do so using various personal identification techniques, from passwords to encryption technologies, to ensure the identity of the contracting party.

However, referring back to Algerian legislation, we find that although the legislator included this condition in Article 323 bis 1 of the Civil Code, it did not specify the mechanisms for verifying the identity of the person who issued the writing in the electronic document. This makes it difficult for judges to ascertain the identity of the issuer. Therefore, the creation of specialized entities for verifying the identity of contracting parties is considered the best solution to this issue. This is precisely what the French legislator did by establishing what is known as a certification service provider, and similarly, Tunisian law established what is called the National Agency for Electronic Certification.

Condition 2 – The electronic writing must be created and preserved under conditions ensuring its integrity:

The Algerian legislator stipulated the condition of preservation in Article 323 bis 1 of the Civil Code, mentioned earlier, emphasizing that the writing must be created and preserved under conditions ensuring its integrity (with the aim of making it accessible at a later time). However, it did not stipulate the recoverability of the writing when needed.

The issue of storing and retrieving writing is a purely technical matter. This is evident through the many programs, tools, and electronic media that ensure the protection and preservation of writings and facilitate easy access to them. This, in turn, reduces the risk of tampering, alteration, or manipulation of their content. The most important of these methods include:

- Preservation via a **PDF** program, which converts electronic writing from the editable **Word** format—which can easily be altered—into a format that cannot be tampered with.

- Storage on **magnetic media** and **email platforms**, as these means can store electronic writing and ensure its safe retrieval at any time.

- Storage by **electronic certification authorities**, which archive electronic data and information related to the certificates they issue for a duration corresponding to the statute of limitations of the legal act confirmed by the certification. This method confers a high level of security and long-term retention of the documented information.

3 – The probative value of electronic writing in evidence:

Writing holds great importance in proving legal acts and occupies the foremost rank among evidentiary means. It may be traditional—recorded on a physical medium such as paper—or electronic, recorded on a digital medium. The latter has emerged due to the rise of electronic transactions conducted remotely, which traditional means of evidence are no longer suited for.

Therefore, once electronic writing meets the conditions detailed above, it holds the same probative value as traditional writing. This is a principle adopted by most international and national legislations.

However, despite the recognition of electronic writing as having evidentiary value, a conflict may arise when a traditional written document concerning the same legal act is also presented. This raises the issue of conflict between different forms of written evidence and opens the door to judicial discretion in determining which evidence prevails. We elaborate on this evidentiary value by addressing two aspects: the principle of **functional equivalence** between electronic and traditional writing, and the **conflict between electronic and paper-based writing**.

A. The Principle of Functional Equivalence Between Electronic and Traditional Writing: This principle refers to the equal status of electronic and traditional writing in terms of evidentiary value and strength. This is inferred from Article 323 bis 1 of the Algerian Civil Code, previously cited, which establishes legal equality between electronic and handwritten writing as proof, provided that it indicates the author of the writing and is preserved according to technical standards that ensure its integrity.

The UNCITRAL Model Law on Electronic Commerce confirmed the need for legislative regulation of electronic document evidence, rather than leaving the matter to judicial discretion. Article 9, paragraph 2, of the Model Law states:

"Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message."

Accordingly, the UNCITRAL Model Law on Electronic Commerce, adopted by the United Nations Commission on International Trade Law, recognizes the probative value of electronic documents as full legal evidence.

B. Conflict Between Electronic and Paper-Based Writing:

Under the traditional evidentiary system, the issue of conflict between written evidentiary means did not arise, as each had a legally determined evidentiary strength. Official documents held the highest rank, followed by private writings prepared for evidentiary purposes, and then private writings not prepared for such purposes.

However, under the new evidentiary rules recognizing different forms of writing regardless of medium or technique, a conflict may arise between these types. For example, a party might not be satisfied with expressing acceptance electronically and sends a paper letter to present an offer or to declare acceptance of an existing offer. If a discrepancy arises between the expressions of intent in the two writings, the judge must resolve this conflict based on objective standards.

From the above, it is clear that if both electronic and paper-based documents equally meet the conditions to be considered full written evidence, and a conflict arises between them with contradictory content, it becomes the judge's task to determine which document is more credible and preferable. The judge does this based on legal reasoning and evaluation, carefully examining and verifying the documents presented by both parties, and ultimately

favoring the one that his conscience deems most likely to reflect the truth.

Section Two: The Electronic Signature

The Algerian legislator recognized electronic signatures and certifications through Law 15/04, which established the general rules concerning them, thus marking a turning point in the field of electronic contracts. As a result, electronic contracts now possess evidentiary value comparable to traditional contracts, provided that the procedures for electronic signature and certification are respected.

Writing, whether in its traditional or electronic form, is not considered full evidence unless it is signed. The signature is a key element of written evidence prepared primarily for proof. It is an essential condition for the validity of a document, whether paper-based or electronic.

In the context of electronic transactions, there is no method by which one can confirm the identity of parties or prove the actions they undertake, except through the use of electronic signatures. These signatures determine the true identity of the parties. In addition, they can be used to preserve the integrity of data, thereby preventing any modification after signing. This is one of the foundations of the strength of electronic signatures and highlights their important role in proving legal actions in the event of a dispute between contract parties.

Thus, the electronic signature is a process that employs modern technology to confirm the identity of a person and document their intent in digital documents. It is an important tool in the world of business and modern communications, enabling individuals to conclude contracts online in an easy and secure manner. We will now define the electronic signature, identify its conditions, determine its probative value in evidence, and finally discuss the authorities responsible for certifying electronic signatures.

1. Definition of the Electronic Signature:

The Algerian legislator defined the electronic signature in Article 2 of Law 15/04 as: "data in electronic form attached to or logically associated with other electronic data and used as a means of authentication."

Thus, the legislator regarded the electronic signature as a means of authentication. However, it did not specify the method by which it is used, offering instead a general definition that allows for its broad application. Consequently, one function of the electronic signature is to identify the contracting party. It also serves as evidence of the intention to endorse the content. Therefore, the certification of this signature by accredited certification authorities will instill confidence in the contracting parties regarding identity verification, thereby ensuring security in electronic commercial transactions.

Electronic signatures take various forms to fulfill their functions, the most important being the biometric signature, which relies on physical and natural characteristics to identify the individual, given that each person has unique traits that distinguish them from others, such as fingerprints, retinal scans, voice recognition, hand geometry, and facial recognition.

For this reason, the mechanism of a certified electronic signature is considered an effective means of verifying the identity of contracting parties through the use of modern technologies that guarantee the confidentiality of their personal transactions.

It thus becomes clear that the electronic signature is a modern method of verifying the consent of the contracting party and their intent to be bound by the content they have signed. It is created via an electronic medium in response to transactions conducted electronically in the form of letters, numbers, symbols, and signals. This has rendered the concept of the traditional signature obsolete in this context.

2. Conditions of the Electronic Signature:

In order for the electronic signature to have the same evidentiary value as the traditional signature and to be trustworthy and admissible, it must meet several conditions. These include: the signature must be personal and unique to its owner; it must be readable, continuous, and direct; and it must be closely associated with the electronic document. We elaborate on these conditions as follows:

Condition 1 – The signature must be personal and unique to its owner:

The electronic signature must identify the signer; that is, it must indicate the personality of its owner. Since the environment is virtual and lacks the physical presence of the parties—making it impossible to identify the signer through their physical presence and their handwritten signature—linking the signature to its owner becomes a technical matter, requiring the deployment of appropriate technologies to secure the platforms and oversight from accredited entities capable of verifying the identity of signatories.

The signer must also exercise control over the electronic signature to ensure exclusivity, both at the time of signing and when it is used. This technical control is achieved when only the signer can operate the electronic medium used to apply the signature, typically through possession of the encryption key storage tool, such as a secure smart card and its associated PIN, for example.

Condition 2 – The signature must be readable, continuous, and direct:

Since the signature is a form of writing, it is subject to the same conditions as writing in terms of being visible and readable, either directly or using specific tools such as a computer. It must be generated in a way that allows it to be retrieved within a certain period. This condition is fulfilled when the electronic signature contains data that can be read by feeding the information into a computer equipped with software capable of translating binary machine language into a human-readable format.

As for continuity, this is achieved when the data associated with the electronic signature can be retained for an extended period. This requires the use of devices and media with high storage capacity to protect the data from loss due to potential damage to magnetic chips or storage discs, such as from a power outage.

Condition 3 – The signature must be closely associated with the electronic document:

For the electronic signature to perform its function of evidencing the signer's acknowledgment of the document's content, it must be connected to the document in a way that cannot be separated from it. This connection must be continuous, storable, and retrievable. In traditional writing, the physical and chemical connection between the ink and the paper ensures this inseparability—one cannot be removed without damaging the other or altering the chemical structure.

In the case of electronic signatures, their tight connection to the electronic document is primarily dependent on the efficiency of the technologies used to secure the document's content. Only the individual possessing the correct decryption key can access the content. Thus, the document and the signature are connected in a way that prevents separation, and no one else can alter the content without the owner's authorization.

3. The Probative Value of the Electronic Signature in Evidence:

The legislator stipulated in Article 327, paragraph 2, that: "The electronic signature shall be recognized in accordance with the conditions mentioned in Article 323 bis 1." Here, it is evident that the legislator equated the evidentiary value of the electronic signature with that of the traditional signature. This is referred to as the **functional equivalence** between the two, as the electronic signature can perform the same functions as the handwritten signature in terms of identifying the signer and confirming their acknowledgment of the content of the transaction executed using that signature.

At the same time, the legislator referred to the conditions set forth in Article 323 bis 1 of the Civil Code for the recognition of the signature, which are: the possibility of verifying the identity of the person who issued it, and that it is prepared and stored in conditions that ensure its integrity.

Thus, it becomes clear that the Algerian legislator has established equality between electronic and traditional writing, i.e., it equated them in terms of evidentiary value if the aforementioned conditions are met—specifically, that the writing is prepared and stored under conditions that ensure its integrity.

This has been further reinforced by the issuance of **Electronic Signature Law No. 15/04**, which recognized the evidentiary value of electronic

signatures by affirming the use of the electronic signature to verify the identity of the signer, and to prove their acceptance of the content of the writing in its electronic form.

Hence, when the legally required conditions are met, the electronic signature has **legal evidentiary force**, being equal in value to the traditional signature, as it performs the same functions—identifying the signer and confirming their acknowledgment of the signed transaction. However, this is only achieved with the presence of an intermediary that ensures both the issuance and certification of the electronic signature, in accordance with what is called the **electronic signature service**.

4. Certification of the Electronic Signature

Electronic transactions have raised several legal issues regarding their adoption. As a result, there emerged a need to ensure that the electronic transaction originates from the person to whom it is attributed, without alteration or tampering. This task is currently performed by specialized and licensed entities known as **electronic certification authorities**, which issue **electronic certification certificates**. These certificates confirm the connection between the signer and the data used to create the electronic signature. The certificate is an electronic record issued by an accredited certification authority containing personal information about the holder, the issuing authority, and the certificate's validity date. It serves as an identity document issued by a neutral party to identify the holder and certify their electronic signature during a specific period, as well as the transactions they carry out via the internet.

To use the electronic signature in a secure and reliable manner, the intervention of a certification authority is necessary to grant it full effectiveness and credibility as evidence. This, in turn, imparts trust, security, and confidentiality to individuals' messages and electronic signatures, encouraging third parties to contract with them after verifying their identity and genuine intention to enter into a contract.

As for the **electronic certification service provider**, Article 2, paragraph 12 of Law 15/04 defined it as: "Any natural or legal person who provides described electronic certification certificates and offers other services in the field of electronic certification."

Article 34 of the same law stipulated a set of conditions that must be met by the provider of the electronic certification service, namely:

1. Being subject to Algerian law if a legal person, or holding Algerian nationality if a natural person.

2. Possessing sufficient financial capability.

3. Possessing established qualifications and expertise in the field of information and communication technologies.

4. Having no prior conviction for a felony or misdemeanor incompatible with the activity of providing electronic certification services.

As for the **tasks of the electronic certification service provider**, they include: registering, issuing, granting, canceling, and storing electronic certification certificates. The provider is also responsible for safeguarding the data and information related to the issued certificates, which it collects only after obtaining the explicit consent of the concerned individual. This data must be limited to the personal information necessary for issuing and storing the certificate and cannot be used for other purposes.

The certification service provider also verifies the integrity of the signature creation data in relation to the signature verification data, as well as the identity of the certificate applicant—and their attributes, when necessary. If the applicant is a legal person, a record is kept that details the identity and legal capacity of its legal representative, such that the identity of the natural person using the electronic signature can be determined in every instance of use.

The Algerian legislator established the **liability of electronic certification service providers** in Articles 53 to 60 of Law 15/04. Based on this, the provider who issued the described certification certificate is liable for any harm caused to any entity or individual—natural or legal—who relied on the certificate, with regard to the accuracy of all the information it contains. The provider is also liable for damage resulting from **failure to cancel** the electronic certification certificate, which causes harm to any entity or

individual who relied on it—unless the provider can prove that no negligence was committed.

Conclusion:

Through the study of this topic, we conclude that the Algerian legislator has equated traditional writing and electronic writing in proving electronic contracts, regardless of their impact on the legal act, by granting them the same evidentiary value as traditional writing—provided that it is possible to verify the identity of the person who issued it.

As for the **electronic signature**, it appears to be a **necessary tool in electronic commerce**, which requires the Algerian legislator to keep pace with this development by enacting a sufficient set of legal provisions related to electronic signature technology, given the rapid conclusion of electronic contracts and the complexity of certain aspects imposed by the electronic environment. In addition, the electronic signature suffers from functional shortcomings in proving legal acts, particularly in terms of security. Therefore, the highest level of **protection and privacy** must be provided in the medium used to create it, using technologies that safeguard both the signature and the data message exchanged between the parties to the electronic contract.

Furthermore, the **legal system related to electronic notarization** must be developed, with the potential for the establishment of a future **electronic notary** tasked with eliminating fraud and deception in this electronic environment, particularly in light of the absence of **specialized bodies** that monitor and regulate the electronic market—a market in which the **electronic consumer** has become the primary victim.

References

- Algerian Civil Code. (2005, June 26). *Ordinance No. 05/10 of June 20, 2005, amending and supplementing the Algerian Civil Code*. Official Gazette No. 14.
- Law No. 15/04. (2015, February 10). *Law of February 1, 2015, establishing the general rules related to electronic signatures and certification*. Official Gazette No. 06.
- Bouaïs, Y., & Ben Ahmed El-Hadj. (2018). *The legal framework of the electronic contract. Journal of Legal and Political Research*, (10), June.
- Abdel Hamid, T. (2007). *Electronic signature*. Alexandria, Egypt: New University House.
- Zarouk, Y. (2012). *The position of electronic writing in evidence: A comparative study. Al-Mi'yar Journal*, University Center of Tissemsilt, (6), December.
- Jum'ah, S. F. (2013). *Disputes of electronic commercial contracts between judiciary and arbitration: Mechanisms of dispute resolution*. Alexandria, Egypt: New University House.
- Higazy, A. B. (2002). *The legal system for the protection of electronic commerce* (Vols. 1–2). Alexandria, Egypt: University Thought House.
- Nuseirat, A. M. E. (2005). *The evidentiary value of the electronic signature* (1st ed.). Amman, Jordan: Dar Al Thaqafa for Publishing and Distribution.
- Lazaar, W. (2019). *Consent in electronic contracts* (Doctoral dissertation, Private Law, University of Larbi Ben M'hidi, Faculty of Law and Political Science, Oum El Bouaghi, 2018–2019).
- Mansour, M. H. (2009). *Electronic liability*. Alexandria, Egypt: New University House.
- Moussa, N. (2014). *The electronic contract in Algerian legislation. Algerian Journal of Legal, Economic, and Political Sciences*, University of Algiers 1, Faculty of Law, (2), July.
- Arab, Y. (n.d.). *Evidentiary value of electronic extracts in banking cases: Part I—Issues and challenges of electronic evidence in civil, commercial, and banking matters*. Retrieved from http://www.arablaw.org/download/E-Evidence%20Article.doc