2026, Cilt 3, Sayı 4, 597-603

OPEN ACCESS
ISSN: 3062-262X

Akademik Eğitim ve Sosyal Bilimler Dergisi (AJESS Journal)

Electronic Signature in Algeria: Legal Framework and Evidentiary Value in the Context of Digital Transformation

Dr. Said Bouziane, Department of Law, Faculty of Law and Political Science , University of Mohamed Boudiaf University of M'Sila. bouzianesaid1974@gmail.com
Dr. Khelifa Boudaoud, Department of Law, Faculty of Law and Political Science , University: Mohamed Boudiaf University of M'Sila. khelifa.boudaoud@univ-msila.dz

Article History
Received: 31/07/2026; Accepted: 06/09/2026; Published: 15/09/2026

Abstract
As a genuine economic revolution, electronic commerce has facilitated commercial communication and interaction worldwide. It has also generated significant benefits in trade and contributed to economic development. Transactions conducted in this environment, however, require a form of signature suited to modern electronic dealings. The traditional concept of a handwritten signature does not readily fit this setting.
This development led most international and national legal systems, including Algeria, to regulate electronic signatures. Legislators defined the concept and established rules governing its use. Their aim was to provide a means of proving legal transactions concluded over the Internet without relying on conventional paper documents. This study therefore examines the evidentiary value of the electronic signature.

Keywords: electronic commerce; modern environment; traditional signature; electronic signature; proof of legal transactions.

Introduction

The widespread use of computers in all areas of life has introduced new methods of conducting transactions that do not fit the traditional concept of a signature. Public administrations, companies, and banks increasingly rely on electronic data processing. As a result, handwritten signatures have become difficult to integrate into modern administrative and accounting systems. This development encouraged the use of electronic signatures as an alternative to handwritten signatures.

Most international and national legal systems, including Algeria, consequently turned their attention to this technology. They defined electronic signatures and regulated their legal effects. The aim was to establish a means of proving legal acts carried out online without conventional paper documents. It was also necessary to determine the evidentiary value of this method.

The Algerian legislature recognised early the importance of regulating this technology. Law No. 15-04 of 1 February 2015, relating to the general rules governing electronic signatures and electronic certification, established a specific legal framework. It addressed electronic signatures, certification certificates, and the entities involved in the certification process.

However, the rapid development of digital transformation and the widening scope of electronic transactions required a reconsideration of this framework. This resulted in Law No. 26-02[i] of 17 February 2026, which lays down the general rules governing trust services for electronic transactions and electronic identification. The law expanded regulation beyond electronic signatures and electronic certification to a broader trust-services framework. It covers electronic signatures, electronic seals, electronic time stamps, electronic registered delivery services, and other mechanisms. It also repealed Law No. 15-04, while temporarily keeping its implementing texts in force until the implementing regulations of the new law are issued. Against this background, the present study examines the concept and legal framework of electronic signatures in Algeria. It then considers their evidentiary value and the main safeguards adopted by the legislature to ensure reliability. This leads to the following research question:

To what extent has the Algerian legislature established an adequate legal framework to ensure the evidentiary value and reliability of electronic signatures in the context of the digital transformation of transactions?

To address this question, the study is organised around the following main sections:

Section One. The Concept of Electronic Signature

Section Two. The Evidentiary Value of Electronic Signature

Section One: The Concept of Electronic Signature

This section is organised as follows:

Subsection One: Definition and Characteristics of Electronic Signature

This subsection first addresses the definition of electronic signature (Part A) and then its characteristics (Part B).

A. Definition of Electronic Signature

This part examines the statutory definition of electronic signature (1) and then its doctrinal definition (2).

1. Legal Definition of Electronic Signature

The 2001 UNCITRAL Model Law defines an electronic signature as "data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message." This definition clearly adopts a functional approach. It does not refer to any particular technical form of electronic signature. Instead, it focuses on the functions performed by the signature. Those functions determine whether a given method may be regarded as an electronic signature.

The European Union also defined electronic signatures by distinguishing between two types:

1. Electronic signature: "information in electronic form relating to other electronic information and closely associated with it, which is used as a means of authentication."

2. Advanced electronic signature: "an electronic signature that must satisfy the following conditions:"

- It is uniquely linked to the signatory.
- It is capable of identifying the signatory.
- It is created using means over which the signatory can maintain complete confidentiality and control.
- It is linked to the information contained in the message in such a way that any alteration of that information can be detected.[ii]

French legislation also addressed the definition of electronic signature through Law No. 2000-230 of 13 March 2000.[iii] The law dealt with both traditional and electronic signatures. It focused on the recognised functions of a signature. Article 1316-4 of the French Civil Code, as amended, provided that a signature "identifies the person to whom it is attributed and expresses that person's acceptance of the content of the instrument to which it is attached and of the obligations stated therein."

French law adopted this as a general definition of signature. The second paragraph of the amendment defined an electronic signature as a signature resulting from the use of a reliable and acceptable method. That method must identify the signatory and guarantee the link between the signature and the act or document to which it relates.[iv]

The United States law issued on 30 June 2000 defined it as "a digital certificate issued by an independent authority that identifies each user and may be used to send any document, commercial contract, undertaking, or declaration."[v]

Among Arab legal systems, Jordanian legislation also defined electronic signature. Article 2 of the Electronic Transactions Law describes it as "data in the form of letters, numbers, symbols, signs, or other forms, incorporated electronically, digitally, optically, or by any similar means into an information message, or added to or associated with it, in a manner that identifies the person who signed it and distinguishes that person from others for the purpose of signing and approving its content."

The Algerian legislature first defined electronic signature in Executive Decree No. 07-162 of 30 March 2007 concerning the operating regime applicable to different types of networks, including radio-electric networks, and to various telecommunications services.[vi] Article 3(1) states that it is "data resulting from the use of a method that satisfies the conditions laid down in Articles 323 bis and 323 bis 1 of the Algerian Civil Code."[vii] Under those provisions, the legislature placed electronic writing and paper writing on an equal footing when certain conditions are met. These include the ability to verify the identity of the person from whom the writing originates, namely the signatory. They also require the electronic signature to be created within a system operating under conditions that ensure its integrity.

The Algerian legislature later enacted Law No. 15-04,[viii] dated 15 February 2015, which lays down the general rules governing electronic signatures and electronic certification. Article 2(1) defines an electronic signature as "data in electronic form attached to or logically associated with electronic data and used as a means of authentication." Article 6 further provides that "the electronic signature is used to authenticate the identity of the signatory and to establish the signatory's acceptance of the content of the writing in electronic form." This definition shows that the Algerian legislature adopted a functional approach. It focuses on the function of the signature rather than on the technical method by which it is created.

Approximately a decade later, in 2026, the continuing expansion of electronic transactions revealed the limitations of Law No. 15-04. The Algerian legislature therefore enacted Law No. 26-02 laying down the general rules governing trust services for electronic transactions and electronic identification. Article 115 repealed Law No. 15-04, which had governed electronic signatures and electronic certification. It provides: "The provisions of Law No. 15-04 of 11 Rabiʿ al-Thani 1436 AH, corresponding to 1 February 2015, laying down the general rules governing electronic signatures and electronic certification, are repealed ...".

Law No. 26-02 defines electronic signature in its General Provisions, specifically in Article 2: "For the purposes of this Law, the following shall mean: ... 2—Electronic signature: data in electronic form attached to or logically associated with other data in electronic form, used by the signatory to sign and serving as a means of authentication ...".

Under this definition, an electronic signature need not be a digital image of a traditional handwritten signature. It may take several technical forms, provided that it performs the function of authentication and attributes the electronic act to its author. The definition therefore reinforces trust in electronic transactions by emphasising the functions performed by the signature and by linking it to the electronic certification system. In this respect, the definition in Law No. 26-02 is more precise than the one in Law No. 15-04, which was confined to the forms of signature and certification recognised at the time, namely digital, biometric, and handwritten forms.

2. Doctrinal Definition of Electronic Signature

Academic definitions of electronic signature vary. Some adopt a technical criterion and emphasise the equations and symbols that enhance reliability. Others focus on the function of the signature, particularly the need to identify the signatory.

French legal scholarship has defined it as "a set of numbers generated by an open computational process using a private secret code."[ix]

It has also been defined as "a signature based on a set of procedures and means that can be used through symbols and numbers. It is produced as an electronic message containing distinctive markers of the sender. The electronically transmitted message is encrypted using a key algorithm, one key being public and the other private to the sender."[x] Another definition describes it as "any signature made by a non-traditional method, namely electronically."[xi]

B. Characteristics of Electronic Signature

Electronic signatures have several distinctive characteristics. The most important may be summarised as follows:

1. An electronic signature consists of elements and features that are specific to the signatory. These may take the form of numbers, letters, signs, or other symbols that distinguish the signatory.
2. An electronic signature is created using electronic means and technologies, whether through computers and the Internet or through other electronic media. These tools allow contracting parties to communicate, examine the terms of the contract, negotiate its conditions and method of conclusion, draft it in electronic form, and complete the electronic signing process.
3. An electronic signature is associated with an electronic message. This means a set of information that is created, sent, delivered, or stored by electronic means.[xii]

C. Forms of Electronic Signature

Electronic transactions require an authentication method that gives contracting parties confidence in the transaction and in the integrity of the resulting effects. Electronic signatures have therefore developed in several practical forms. The most important are digital signatures, biometric signatures, electronic pen signatures, and signatures using a personal identification number. These forms are discussed below.[xiii]

1. Digital Signature

The digital signature is the most widespread form because it offers advanced levels of security and protection. It is created through encryption. The document and the signature are transformed from their ordinary form into a mathematical form using secret keys and complex computational methods known as algorithms.

The sender uses a private key to sign the document electronically in encrypted form. The recipient can verify the signature by using the public key. Digital signatures rely on two main forms of encryption:

1.1 Symmetric Encryption

This type of encryption relies on a secret code shared between the two parties and is used in a closed environment. A plastic card is one example. The secret number is known only to the cardholder and the device.

1.2 Asymmetric Encryption

This type uses a pair of asymmetric keys: a public key and a private key. The public key is available and known to others. The private key remains linked to its owner and is kept secret. This mechanism encrypts the message in a way that provides the necessary protection for its content.

2. Biometric Signature

A biometric signature relies on a characteristic that is distinctive to each person, whether physical or behavioural, in order to recognise and identify that person. It is therefore also described as a signature based on personal characteristics. Such characteristics make it easier to identify the signatory and verify identity. Common examples include fingerprints, voice patterns, the iris of the eye, and characteristics of the human hand.

When one of these characteristics is used, an image or template is first captured and stored in a computer for later comparison. The data are also encrypted to protect them from tampering or manipulation.

The Algerian legislature adopted this type of signature in response to requirements relating to international civil aviation. This was reflected in the decision of 19 July 2010 concerning the issuance of biometric passports and biometric identity cards.

3. Electronic Pen Signature

This form of electronic signature uses an electronic pen that allows a person to write on a computer screen through dedicated software. The software captures the customer's signature created with the electronic pen. It then verifies the signature and identifies its owner by comparing it with the original signature stored by the depositary. A handwritten

signature may also be transferred by scanning it and inserting the resulting image into the relevant file. This process allows the required evidentiary effect to be attached to the document.

4. Signature Using a Magnetic Card and a Personal Identification Number

A signature using a magnetic card together with a personal identification number is one of the oldest and most common forms of electronic signature, particularly in banking transactions. Its use is clearly illustrated when cash is withdrawn from an automated teller machine. The customer or cardholder inserts the card into the designated slot and then enters the personal identification number. If the number is correct, the machine allows the customer to select the amount to be withdrawn. The requested amount is then dispensed, and the card is returned through the same slot.

Section Two: The Evidentiary Value of Electronic Signature

An electronic signature acquires evidentiary value when it satisfies the conditions required for recognition as a complete signature and performs its legal function. In this respect, it is equivalent to a traditional signature, although the two operate in different environments. Electronic signatures are created in a digital environment that requires an adequate level of trust and security. These safeguards protect the rights of parties dealing through electronic media. National and international legal systems have therefore sought to recognise the electronic signature as the counterpart of the handwritten signature and to grant it equivalent evidentiary value. This section examines the conditions for electronic signatures (Subsection One), the positions of French and Algerian law on their evidentiary value (Subsection Two), and the role of trust services in reinforcing that value (Subsection Three).

Subsection One: Conditions for Electronic Signature

To produce legal effects and enjoy evidentiary value, an electronic signature must satisfy the following conditions:

A. The Signature Must Be Unique to the Signatory

The signature must belong exclusively to the signatory and must not be confused with another person's signature. This allows the signed document to be attributed solely to that person.[xiv]

This condition is met when the electronic signature distinguishes the signatory from others and is linked to that person. The link must make it possible to identify the signatory through the electronic medium and the certification authorities, in the same way that a handwritten signature identifies its author.[xv]

B. The Signature Must Be Preserved Under Conditions That Ensure Its Integrity and the Accuracy of Its Content

This condition follows from Article 323 bis 1 of the Algerian Civil Code. The provision requires the electronic signature to be preserved under conditions that ensure its integrity. This is achieved only when the signatory retains control of the signature method or of the electronic medium used to sign. If that method or medium is stolen or leaves the signatory's control, the signature has no legal effect.[xvi]

C. Any Alteration to the Electronic Signature Data Must Be Detectable

Security and trust require the electronic record and its signature to be created using systems and methods that preserve the accuracy and integrity of the signed electronic record. Those systems must also make it possible to detect any alteration to the data after signature. This can be achieved through public- and private-key encryption, by comparing the electronic certification certificate and the signature-creation data with the original certificate and data, or by any similar method.[xvii]

Subsection Two: The Positions of French and Algerian Legislation on the Evidentiary Value of Electronic Signature

The following discussion first considers the position of the French legislature (Part A) and then the position of the Algerian legislature (Part B).

A. The Position of the French Legislature

The French legislature implemented the provisions of European Directive 1999/93 concerning electronic signatures, particularly Article 5(2).[xviii] That provision requires Member States of the European Union to recognise the legal effectiveness of electronic signatures and their evidentiary value. It also reflects the principle that an electronic signature should not be denied the legal status enjoyed by a handwritten signature merely because of its electronic form.

Decree No. 2001-272 of 30 March 2001, concerning the protection and security of electronic signature data,[xix] amended Article 1316-4 of the French Civil Code. The provision states: "Where the signature is electronic, a reliable method must be used to identify its author and to demonstrate the intention to be bound by the legal act to which it is attached. The method used is presumed to be reliable until the contrary is proved."[xx]

In implementing the European rules on electronic signatures, the French legislature distinguished between two types. The first is the reliable or secure electronic signature.[xxi] It is created through a certification service provider and is recorded in a certificate approved by that provider. This form benefits from the presumption in Article 1316-4 that the method used to identify the signatory and establish the intention to be bound is reliable. The legal act is therefore presumed to be attributable to the person named in the certificate. Trust is a fundamental element of the electronic-signature system.

The second type is the simple electronic signature.[xxii] It does not satisfy the conditions required for a secure signature. A party relying on this type of signature therefore does not benefit from the presumption of reliability. That party must prove that the method used to sign was reliable.

B. The Position of the Algerian Legislature

The Algerian legislature recognised electronic signatures subject to specific conditions. Article 327 of the Civil Code, as amended by Law No. 05-10, and in particular Article 323 bis 1, places the electronic signature on the same footing as the handwritten signature. This equivalence applies when the identity of the signatory can be verified and the signature is created and preserved under conditions that ensure its integrity. Law No. 15-04 on electronic signatures and electronic certification confirmed this approach. It distinguished between a simple electronic signature and a qualified electronic

signature, in line with French legislation and the European Directive. The law granted electronic signatures evidentiary value equivalent to that of written signatures.[xxiii] It also required the creation mechanism for a qualified electronic signature to be secured by specific conditions.[xxiv] Article 12 further required a reliable mechanism for verifying a qualified electronic signature by imposing a number of requirements.[xxv]

Law No. 26-02 also confirms this evidentiary value. Article 7 provides that "only an accredited electronic signature shall be equivalent to a written signature." Article 16 further states that "an electronic signature or electronic time stamp may not be deprived of legal effect and may not be rejected before a court solely because it is in electronic form or because it does not satisfy the requirements of this Law." Article 57 also confirms the validity of contracts concluded by electronic means. Such contracts enjoy full evidentiary value under that provision.[xxvi] The same law also confirms the evidentiary value of electronic records before the courts in Article 61.[xxvii]

This development represents a significant legislative shift in the Algerian approach to the evidentiary value of electronic signatures. Law No. 26-02 of 17 February 2026 moved beyond the narrow regulation of electronic signatures and electronic certification under Law No. 15-04. It established an integrated framework for "trust services for electronic transactions and electronic identification," in line with the requirements of contemporary digital transformation.

Subsection Three: The Role of Trust Services in Reinforcing the Evidentiary Value of Electronic Signature

Electronic signature cannot be studied separately from the trust-services framework. The level of confidence in a signature depends on the existence of technical and legal bodies and mechanisms that can verify the signature, the signature certificate, and the identity of its holder.

Law No. 26-02 made the National Electronic Certification Authority a central body in the organisation of the trust-services system. Its responsibilities include issuing licences to trust service providers, preparing, updating, and publishing the trust list, preserving expired electronic certificates and the data associated with them, and taking the measures required to ensure continuity of service and protect subscribers' interests.

The new framework also extends beyond electronic signatures. It includes electronic seals, which may be associated with legal persons, and electronic time stamps, which link data to a specific time in order to prove their existence at that time. It also includes electronic registered delivery services. This reflects a shift from regulating a single electronic authentication method to building an integrated system of digital trust.

Conclusion

In conclusion, the growing use of electronic signatures in different areas of life and their adoption as a means of authenticating electronic transactions have reduced reliance on signatures in their traditional form. Comparative legal systems have therefore tended to place electronic signatures on an equal footing with handwritten signatures and to grant them the same evidentiary value. This value, however, is neither automatic nor unlimited. Full evidentiary effect depends on specific requirements and conditions that the electronic signature must satisfy.

Through Law No. 26-02, the Algerian legislature granted electronic signatures and digital records clear and reliable legal force and evidentiary value equivalent to that of traditional handwritten signatures. The focus is no longer limited to the signature itself. It also extends to modern digital mechanisms, including accredited electronic seals and accredited electronic delivery services.

Nevertheless, the effectiveness of this legal framework does not depend on legislation alone. It also requires the completion of the relevant regulatory and technical texts, the development of digital infrastructure, wider use of electronic signatures, stronger information-system security, and greater awareness among economic operators, public administrations, and individuals.

The current challenge for the Algerian legislature is therefore not limited to the legal recognition of electronic signatures. It also lies in ensuring their practical effectiveness and broad adoption. Achieving this objective would strengthen the legal and technical security of electronic transactions and increase confidence in Algeria's digital economy.

Sources and References

---

[i] Law No. 26-02, dated 29 Shaʿban 1447 AH, corresponding to 17 February 2026, laying down the general rules relating to trust services for transactions, Official Gazette No. 14, 2026.

[ii] Alaa Mohammed Nusairat, The Evidentiary Value of Electronic Signatures: A Comparative Study, Dar Al-Thaqafa for Publishing and Distribution, 1st ed., 2005, p. 24.

[iii] Mohammed Ouziane, "The Extent to Which the Rules of Evidence in the Dahir of Obligations and Contracts Can Accommodate Electronic Signatures," Al-Qada' wa Al-Qanun [Judiciary and Law], no. 155.

[iv] Alaa Mohammed Nusairat, op. cit., p. 24.

[v] Abdel Fattah Bayoumi Hegazy, Electronic Signature in Comparative Legal Systems, Book One, Dar Al-Fikr Al-Jamiʿi, Cairo, Egypt, 2005, p. 186.

[vi] Executive Decree No. 07-162, dated 30 May 2007, amending and supplementing Executive Decree No. 01-123 of 9 May 2001, concerning the operating regime applicable to all types of networks, including radio-electric networks, and to various wired and wireless telecommunications services, Official Gazette No. 37, 7 June 2007.

[vii] Ordinance No. 75-58 of 20 Ramadan 1395 AH, corresponding to 26 September 1975, containing the Civil Code, as amended and supplemented.

[viii] Law No. 15-04, dated 15 February 2015, laying down the general rules governing electronic signatures and electronic certification, Official Gazette No. 06, 10 February 2015.

[ix] Cited in Abdullah Misfer Al-Hayyan and Hassan Abdullah Abbas, "Electronic Signature: A Critical Study of the Kuwaiti Ministry of Commerce and Industry Draft," Journal of Economic and Administrative Sciences, vol. 19, no. 1, June 2003, p. 14.

[x] Mohammad Fawaz Al-Matalqa, A Concise Guide to Electronic Commerce Contracts, Dar Al-Thaqafa for Publishing and Distribution, 1st ed., Amman, Jordan, 2008, p. 173.

[xi] Souhila Tamine, Formality in Electronic Commerce Contracts, Master's thesis in Law, Public International Law, Faculty of Law and Political Science, Doctoral School of Fundamental Law and Political Science, Mouloud Mammeri University, Tizi Ouzou, Algeria, 2011, p. 49.

[xii] Amina Kahouadji and Leila Matali, "The Conceptual and Legal Framework of Electronic Signature and Certification in Algeria," Al-Mishkat Journal of Economics, Development and Law, vol. 4, no. 8, 2018, p. 21.

[xiii] Hassiba Khechna and Ghania Batli, "The Evidentiary Value of Electronic Signatures in Algerian Legislation in Light of Law No. 26-02," Dafater Al-Siyasa wa Al-Qanun [Notebooks of Politics and Law], vol. 18, no. 2, 2026, pp. 39–40.

[xiv] Ibrahim Ubaid Ali Al Ali, The Electronic Contract, doctoral thesis in Law, Helwan University, Egypt, 2010, p. 331.

[xv] Osama bin Ghanem Al-Obaidi, "The Evidentiary Value of Electronic Signatures," Arab Journal for Security Studies and Training, vol. 28, no. 56, p. 164.

[xvi] Souria Bourbaba, Proof by Writing in Electronic Form, Dar Ibn Battuta for Publishing and Distribution, Amman, Jordan, 2014, p. 43.

[xvii] See Article 2 of Law No. 15-04 of 1 February 2015 concerning electronic signatures and electronic certification in Algeria.

[xviii] Art. 5.2 du (Directive 1999/93/CE du parlement européen et du conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques): « Les Etats membres veillent ce que l'efficacité juridique comme preuve en justice ne soient pas refusées à une signature électronique au seul motif que: -La signature se présente forme électronique, Où -qu'elle ne repose pas sur un certificat qualifié, Où -qu'elle ne repose pas sur un certificat qualifié délivré par un prestataire accrédité ou service de certification, où -qu'elle n'est pas été créé par un dispositif de création de signature ».

[xix] Décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316/4 du code civil et relatif à la signature électronique, J.O.R.F n° 0077 du 31 mars 2001, page 5070, texte n° 19.

[xx] Art. 1316/4 du code civil et relatif à la signature électronique: « lorsqu'elle est électronique, elle, consiste eu l'usage d'un procédé fiable d'identification son lien avec l'acte auquel elle s'attache. La

fiabilité de procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signature assurée et l'intégrité de l'acte garantie, dans les conditions fixées par décret eu conseil d'états ».

[xxi] Art. 1 (décret 2001-272) du 30 mars 2001: « 2- signature électronique sécurisée: une signature électronique qui satisfait, en outre, aux exigences suivantes: -être propre au signataire; -être créée par les moyens que le signataire puisse garder sous son contrôle exclusif; -garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable ».

[xxii] Art. 1 (décret 2001-272) du 30 mars 2001: « Au sens du présent décret on entend par: 1. signature électronique: une donnée qui résulte de l'usage d'un procédé répondant aux conditions définis à la première phrase du second alinéa de l'article 1314-4 du code civil… ».

[xxiii] See Article 8 of Law No. 15-04 on electronic signatures and electronic certification, cited above.

[xxiv] See Article 11 of Law No. 15-04 on electronic signatures and electronic certification, cited above.

[xxv] See Article 12 of Law No. 15-04 on electronic signatures and electronic certification, cited above.

[xxvi] See Article 57 of Law No. 26-02 laying down the general rules relating to trust services for electronic transactions and electronic identification, cited above.

[xxvii] See Article 61 of Law No. 26-02 laying down the general rules relating to trust services for electronic transactions and electronic identification, cited above.