... ZAOULI N°14, Vol. 1, Juin 2026, pp. 505-529 ISSN : 2788-9343

Received: 05/01/2026 **Accepted:** 02/05/2026 **Published:** 27/06/2026

The Evidentiary Value of Electronic Signatures in Concluding Public Contracts: Between Legal Necessity and Technical Challenges

KECHEHA Messaoud
University Batna1 - Algeria
Email: messaoud.kecheha@univ-batna.dz

Abstract
The public procurement sector is undergoing a rapid digital transformation, creating the need to adopt the electronic signature as a legal and technical mechanism that ensures the conclusion of administrative transactions through secure digital means. This article aims to highlight the legal foundations that grant electronic signatures evidentiary value and to demonstrate their role in enhancing the speed and transparency of administrative contracting procedures. It also discusses the safeguards required to ensure the validity and reliability of electronic signatures, as they constitute the cornerstone for building trust in the digital environment. Conversely, the article examines the security and technical challenges that may affect their effectiveness, particularly in light of cybersecurity risks and the weakness of digital infrastructure. It concludes that the successful implementation of electronic signatures in public procurement depends on the integration of an adequate legislative framework with advanced technical measures capable of protecting electronic transactions and strengthening legal certainty.

Keywords: Public Procurement, Electronic Signature, Legal Validity, Evidence.

Résumé
Le secteur des marchés publics connaît actuellement une transformation numérique rapide, ce qui rend nécessaire l'adoption de la signature électronique en tant que mécanisme juridique et technique garantissant la conclusion de transactions administratives par des moyens numériques sécurisés. Le présent article vise à mettre en évidence les fondements juridiques qui confèrent une valeur probante aux signatures électroniques et à démontrer leur rôle dans l'amélioration de la rapidité et de la transparence des procédures de passation des marchés publics. Il aborde également les garanties requises pour assurer la validité et la fiabilité des signatures électroniques, celles-ci constituant la pierre angulaire de l'instauration de la confiance dans l'environnement numérique. À l'inverse, l'article examine les défis techniques et de sécurité susceptibles d'affecter leur efficacité, notamment au regard des risques liés à la cybersécurité et de la fragilité des infrastructures numériques. Il conclut que la mise en œuvre réussie des signatures électroniques dans les marchés publics dépend de l'intégration d'un cadre législatif adéquat à des mesures techniques avancées, capables de protéger les transactions électroniques et de renforcer la sécurité juridique.

Mots-clés : marchés publics, signature électronique, validité juridique, preuve.

Received: 05/01/2026 **Accepted:** 02/05/2026 **Published:** 27/06/2026

Introduction

In recent years, public administration has undergone a fundamental transformation toward the adoption of electronic means in carrying out its functions, within the framework of what is commonly referred to as e-government. This transformation aims to improve the quality of public services while promoting the principles of transparency and efficiency. Public procurement is among the sectors most affected by this transition, as the use of digital technologies, including electronic signatures, has become an essential requirement for keeping pace with technological advancements and accelerating the conclusion of administrative contracts.

However, the adoption of electronic signatures in the conclusion of public procurement contracts raises several legal issues, particularly regarding the extent to which they possess sufficient legal validity to prove the authenticity of contractual obligations, especially in light of potential technical risks such as cyberattacks, forgery, and the lack of trust in the digital environment.

Accordingly, this study seeks to address the following research question:

To what extent does the electronic signature possess sufficient legal validity to ensure the lawful conclusion of public procurement contracts?

To answer this question, the study is divided into two chapters. The first examines the legal framework governing electronic signatures, while the second analyzes the

evidentiary value of electronic signatures in the field of public procurement.

1. The Conceptual Framework of the Electronic Signature

The electronic signature represents one of the most significant legal mechanisms introduced by digital transformation to secure electronic transactions and enhance confidence in them. Its widespread use has required legislators to establish a legal framework regulating its application and defining the conditions for its validity. Therefore, it is necessary to examine the concept of the electronic signature and identify the legal requirements for its validity.

1.1. The Concept of the Electronic Signature

Defining the concept of the electronic signature is of paramount importance, as it constitutes the foundation upon which the legal rules governing its evidentiary value are based, particularly in the sensitive field of public procurement, which requires a high degree of legal certainty and security. This section examines the definition of the electronic signature, distinguishes it from the traditional handwritten signature, and explores its various forms.

1.1.1. Definition of the Electronic Signature

The electronic signature is one of the most prominent manifestations of digital transformation in the legal field, as it has become an effective alternative to the traditional handwritten signature in various transactions, including administrative contracts. According to one view in legal scholarship, it is defined as:

Received: 05/01/2026 **Accepted:** 02/05/2026 **Published:** 27/06/2026

> "A set of symbols, numbers, letters, signs, or sounds arranged in the form of electronic data and attached to an electronic document, intended to identify the signatory and provide assurance of his or her consent to the content of the message." [1]

Other scholars define it as an encrypted communication method used to authenticate transactions conducted via the Internet. [2]

At the international level, the UNCITRAL Model Law on Electronic Commerce defines the electronic signature in Article 2(a) 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 therein." [3]

As for the Algerian legislator, the electronic signature is defined in Article 2(1) of Law No. 15-04, which establishes the general rules relating to electronic signatures and electronic certification, as: "*Data in electronic form attached to or logically associated with other electronic data and used as a means of authentication*."

---

[1] Adel Ramadan Al-Abyouki, Electronic Signature in the Gulf Legislations: A Comparative Study, 1st ed., Modern University Office, Alexandria, 2009, p. 15.

[2] Mohamed Khaled Gamal Rostom, The Legal Regulation of Electronic Commerce and Electronic Evidence in the World, 1st ed., Al-Halabi Legal Publications, Lebanon, 2006, p. 39.

[3] UNCITRAL Model Law on Electronic Signatures, adopted on 12 December 2001, United Nations Publications, New York, 2002.

1.2. Distinguishing the Electronic Signature from the Traditional Signature

Both the traditional signature and the electronic signature share several common characteristics; however, they differ in a number of aspects that may be summarized as follows:[4]

1.2.1. In terms of the signing instrument:

The instrument used for a traditional signature is a pen of any type or a fingerprint. In contrast, the instrument used for an electronic signature consists of codes, symbols, signals, or one of the individual's biometric characteristics, in accordance with a specific technological process.

1.2.2. In terms of the signature medium:

The traditional signature is affixed to a paper document, whereas the electronic signature relies on an electronic medium, such as magnetic or optical storage devices and other digital media.

1.2.3. In terms of evidentiary value:

A traditional signature does not require any additional means to establish its authenticity. Conversely, an electronic signature acquires evidentiary value only after it has been authenticated by the competent certification authority.

1.2.4. In terms of stability and continuity:

If a traditional signature is forged or imitated by another person, the signer is not required to change the form of his or her signature upon discovering the forgery. In contrast, the

[4] Article 2, paragraphs (1), (2), and (3), Law No. 15-04 of 1 February 2015, establishing the general rules relating to electronic signatures and electronic certification, Official Gazette No. 06, issued on 10 February 2015.

Received: 05/01/2026 Accepted: 02/05/2026 Published: 27/06/2026

holder of an electronic signature must change it whenever it is discovered that an unauthorized person has gained access to the system used to generate it, by notifying the issuing authority.

1.3. Forms of Electronic Signatures

Electronic signatures vary according to the methods and technologies used to create them. The principal forms are as follows:

1.3.1. Digital Signature:

This type of signature is based on complex cryptographic algorithms using mathematical equations that convert characters into numerical values. These values cannot be restored to their original form except by the person possessing the original equation, commonly referred to as the key.[5] There are two types of keys: public keys and private keys. Public keys enable the recipient to read the message without allowing any modification. If the recipient approves the content of the message, he or she signs it using the private key. The signed message is then returned to the sender bearing the electronic signature.[6]

1.3.2. Biometric Signature:

This type of signature relies on the unique biological characteristics of each individual. It operates by capturing an

[5] Issa Ghassan Ridhi, Special Rules Governing Electronic Signatures, Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, 1st ed., 2009, p. 86 et seq.

[6] Lazhar Ben Said, The Legal System of Electronic Commerce Contracts, Dar Houma, Algeria, 2012, p. 160.

image of a person's fingerprint, iris, or another biometric feature and storing it in a computer system for future verification. These data are encrypted to prevent unauthorized access, alteration, or tampering, since unencrypted information transmitted over the Internet is vulnerable to interception and modification.[7]

1.3.3. Electronic Pen Signature:

This form of signature is created when the signer writes his or her handwritten signature using a special electronic optical pen capable of writing on a computer screen. Dedicated software captures the signature and verifies its authenticity by analyzing the movement of the pen on the screen, the shapes it produces, the pressure applied during writing, and the distinctive characteristics of the signer's handwriting,[8] including its size, letter formation, curves, circles, lines, dots, and other identifying features, in addition to measuring the relative speed at which the signature is produced.[9]

1.3.4. PIN-Based (Code) Signature:

This type of signature is commonly associated with magnetic cards and other smart cards equipped with electronic memory. Electronic transactions are authenticated using a set of numbers, letters, or a combination of both, selected by the signer to identify his or her identity. This code

---

[7] Mounir Mohamed El-Geneihy & Mamdouh Mohamed El-Geneihy, The Legal Nature of the Electronic Contract, Dar Al-Fikr Al-Jami'i, Alexandria, n.d., p. 197.
[8] Fatima Al-Zahraa Mossaddaq, "Electronic Certification as a Means of Protecting the Electronic Signature," Journal of Legal Studies and Research, Vol. 5, No. 1, 2020, p. 36.
[9] Mamdouh Mohamed Ali Mabrouk, The Evidentiary Value of the Electronic Signature (A Comparative Study in Light of Islamic Jurisprudence), Dar Al-Nahda Al-Arabiya, Cairo, 2005, p. 14.

Received: 05/01/2026 Accepted: 02/05/2026 Published: 27/06/2026

is known only to the signer and to those authorized by him or her. It is commonly referred to by the English abbreviation PIN (Personal Identification Number). This is the most widely used form of electronic signature in electronic transactions, particularly in banking operations.[10] French courts recognized this method at an early stage, considering it to provide safeguards equivalent to those of a handwritten signature.[11]

1.4. Conditions for the Validity of the Electronic Signature

An electronic signature acquires legal validity only when a set of conditions ensuring its authenticity and integrity are fulfilled. These conditions are intended to establish trust in electronic transactions, particularly in the field of public procurement. They are discussed as follows.

Subsection One: Identification of the Signatory and the Signature's Link to Him

In legal doctrine, this condition means that the signature affixed to an electronic document must be attributable to a specific individual. For the electronic signature to perform its evidentiary function, it must clearly identify its owner and distinguish him or her from other persons.[12] The signature must therefore clearly and unequivocally indicate the identity

[10] Mahjouba Qassem, "Legal Protection of the Electronic Signature against the Crime of Forgery," Journal of Legal and Social Sciences, Vol. 6, No. 2, June 2021, p. 422.
[11] Ibid., p. 422.
[12] Alaa Ahmed Mohammed Al-Haj Ali, The Legal Regulation of Electronic Signature Certification Authorities, Master's Thesis, Faculty of Graduate Studies, An-Najah National University, Palestine, 2013, p. 49.

of its signatory.[13] The holder of an electronic signature possesses unique signature data and a private code that distinguish him or her from other signatories. Once signature-creation data are issued to a particular person, the same signature cannot be issued to another individual.[14]

With regard to legislation, Article 7(1) of the UNCITRAL Model Law on Electronic Commerce (1996) provides that:

"Where the law requires a signature of a person, that requirement is met in relation to a data message if: a method is used to identify that person and to indicate that person's approval of the information contained in the data message..."[15]

In Algerian legislation, Law No. 15-04 expressly provides for this condition, in addition to other requirements, under Article 7, which states:

"The electronic signature must be linked exclusively to the signatory."[16]

1.4.1. The Signatory's Exclusive Control over the Signature

One of the fundamental conditions for the validity of an electronic signature is that it must remain under the exclusive control of the signatory, both during its creation and its use. No person other than the signatory should be capable of

---

[13] El Yaqout Arar, "The Electronic Signature as a Mechanism for the Security and Integrity of Digital Performance," Journal of Legal and Political Sciences, Vol. 11, No. 3, December 2020, p. 497.

[14] Fatiha Hawas, "Electronic Signature: Characteristics and Applications," Journal of Comparative Legal Studies, Vol. 7, No. 1, 2021, p. 2997.

[15] UNCITRAL Model Law on Electronic Commerce, adopted on 16 December 1996, United Nations Publications, New York, 2000, p. 4. Available at: https://2u.pw/LdExo6

[16] Article 7 of Law No. 15-04, establishing the general rules relating to electronic signatures and electronic certification.

Received: 05/01/2026 Accepted: 02/05/2026 Published: 27/06/2026

reproducing its codes or signing on the signatory's behalf. Consequently, the electronic signature must be generated through means that remain entirely under the direct control of its owner.[17] This requirement ensures that the signatory alone has exclusive authority over the signature, whether at the time of signing or during any subsequent use, thereby preventing misuse by third parties, especially since an electronic signature produces legal effects for both the signatory and others.[18]

This requirement was also recognized by the UNCITRAL Model Law on Electronic Signatures (2001), particularly Article 6(3), which provides that:

"An electronic signature is considered reliable for the purpose of satisfying the requirement referred to in paragraph 1 if: ... the signature creation data were, at the time of signing, under the control of the signatory and of no other person ..."[19]

Similarly, Algerian legislation, through Law No. 15-04, incorporates this requirement in Article 7, which stipulates that the electronic signature must:

"be created by means of a secure mechanism or technical procedures that ensure effective control over it."

1.5. The Immutability of the Electronic Signature

The principle of immutability (Irreversibility) refers to the impossibility of altering the data contained in an electronic document except by destroying it or leaving a detectable

[17] Hanan Brahimi, The Crime of Forging Official Administrative Documents of an Information Technology Nature, Doctoral Dissertation, Faculty of Law, University of Biskra, 2015, p. 155.

[18] Said Si Kandil, Electronic Signature, University Publishing House, Beirut, Lebanon, 2004, p. 53.

[19] UNCITRAL Model Law on Electronic Signatures (2001), op. cit.

physical or technical trace. Consequently, any modification made to the document can be easily detected, whether through ordinary visual inspection or with the assistance of technical experts.[20]

This condition requires the integrity of the data associated with the electronic signature, so that any alteration affecting the data message or the electronic document after it has been signed can be detected. Any modification made to the electronic signature affixed to the electronic document inevitably alters the document's entire data, thereby rendering it invalid as evidence, since such modification undermines both the integrity of the document and the reliability of the electronic signature itself.[21]

This requirement is expressly provided for in the UNCITRAL Model Law on Electronic Signatures (2001), which states: "Any alteration to the electronic signature made after the time of signing is detectable."[22]

With regard to Algerian legislation, Law No. 15-04, previously mentioned, also incorporates this requirement by providing that the electronic signature must be linked to the information contained in the electronic document in such a way that any subsequent changes to that information can be detected.[23]

---

[20] Abed Fayed Abdel Fattah Fayed, Electronic Writing in Civil Law between Legal Development and Technical Security: A Study of the Legal Concept of Electronic Writing and Its Functions in Civil Law, Dar Al-Jami'a Al-Jadida, Alexandria, 2004, p. 65.

[21] Al-Yaqout Arar, op. cit., p. 498.

[22] Article 6 of the UNCITRAL Model Law on Electronic Signatures (2001).

[23] Article 7 of Law No. 15-04 laying down the general rules relating to electronic signatures and electronic certification.

Received: 05/01/2026 Accepted: 02/05/2026 Published: 27/06/2026

1.6. The Trust Element of the Electronic Signature (Certification Certificates)

In addition to satisfying the legal characteristics required of a qualified electronic signature in order to enjoy legal evidentiary value, Article 7(1) of Law No. 15-04 introduces an additional requirement, namely that a qualified electronic signature must be created on the basis of a qualified electronic certificate issued by an authorized certification service provider. Such a certificate establishes the link between the signatory and the signature creation data.

Indeed, an individual may unlawfully obtain a pair of public and private cryptographic keys and use them personally or transfer them to another person, or resort to other fraudulent methods. This makes it necessary to establish a mechanism enabling one contracting party to verify the identity of the other when concluding contracts or using electronic signatures. This mechanism is known as electronic signature authentication.

Accordingly, the concept of certifying digital signatures through neutral certification authorities emerged. These authorities play a fundamental role in ensuring the credibility of electronic signatures by issuing electronic certificates confirming the identity of the signatory and verifying that the signature was genuinely generated by that person.[24]

Accordingly, the fulfillment of these conditions constitutes an essential prerequisite for the legal recognition of an electronic signature and for granting it the same evidentiary value enjoyed by a traditional handwritten signature, particularly

[24] Al-Yaqout Arar, op. cit., pp. 498–499.

in the context of concluding sensitive administrative contracts such as public procurement contracts.

2. The Evidentiary Value of the Electronic Signature in Public Procurement

The electronic signature constitutes one of the fundamental pillars of digital transformation in the field of public procurement. Its importance extends beyond facilitating administrative procedures to conferring legal evidentiary value upon electronically concluded legal acts and contracts. Since this evidentiary value is based on a set of legal and technical safeguards, it nevertheless remains subject to certain limitations and challenges that may affect its effectiveness. It is therefore necessary to examine its legal value as a means of proof and to identify the principal challenges that hinder its practical application.

2.1. The Legal Value of the Electronic Signature in Evidence

An electronic signature is considered a means of proving the contracting party's consent and commitment to the contents of the contract, just like a traditional handwritten signature, particularly when it is supported by an electronic certificate issued by a trusted certification authority. This recognition is of particular importance in the field of public procurement, where the signature constitutes an essential stage in concluding the administrative contract and giving it formal legal effect.

2.1.1. Its Equivalence to the Traditional Signature and Legislative Recognition

Legislators in numerous legal systems have acknowledged the legitimacy of the electronic signature and granted it legal

Received: 05/01/2026 Accepted: 02/05/2026 Published: 27/06/2026

evidentiary value, provided that it satisfies the required technical and legal conditions. This reflects a legislative trend toward establishing the principle of equality between the electronic signature and the traditional handwritten signature.

Since the difference between the electronic signature and the traditional signature lies in the means by which the signature is created rather than in the function it serves, the principal issue concerning the electronic signature is whether it fulfills the same legal functions as the traditional signature and provides the degree of reliability upon which legislators base its evidentiary value. Therefore, if the electronic signature fulfills the legal functions and reliability required by law, there is no reason to question its validity, and it becomes equivalent to the traditional signature in terms of legal effect.[25]

Although the electronic signature performs the same functions as the traditional signature, its legal recognition and acceptance as evidence were not easily established. This is primarily due to concerns regarding trust in this type of signature. Since many electronic signatures are generated automatically through electronic systems, they are generally protected against imitation and forgery. Nevertheless, doubts may still arise regarding their reliability unless they are accompanied by mechanisms that reinforce confidence in their authenticity.[26]

---

[25] Abbas Al-Aboudi, Challenges of Evidence by Electronic Documents and the Requirements of the Legal System to Overcome Them, 1st ed., Al-Halabi Legal Publications, Lebanon, 2010, p. 172.

[26] Hassina Cherroun & Sonia Mokri, "The Electronic Signature as a Mechanism for Authenticating Electronic Transactions," Journal of Judicial Ijtihad, Vol. 13, No. 2, October 2021, p. 609.

2.1.2. Its Role in the Formation of the Administrative Contract

The adoption of electronic signatures in this field contributes to accelerating public procurement procedures, reducing administrative delays, and enhancing transparency by minimizing direct human intervention. However, these advantages remain dependent upon the availability of certain conditions, particularly that the signature must be:

1. An Expression of the Signatory's Intention

This condition is intended to ensure that the signatory has freely consented to and accepted the legal obligations arising from the signed legal act. When the signatory affixes an electronic signature to an electronic document, such signature expresses his or her consent to be bound by the obligations contained therein.[27] This principle is reflected in Article 6 of Law No. 15-04, which provides that: "The electronic signature shall be used to authenticate the identity of the signatory and to prove his or her acceptance of the content of the electronic writing."[28]

Similarly, Article 7 of the UNCITRAL Model Law on Electronic Commerce (1996) states that: "The electronic signature is used to indicate the signatory's approval of the information contained in the data message."[29] Likewise, Article 2(1) of the UNCITRAL Model Law on Electronic Signatures (2001) provides that the electronic signature serves

---

[27] Habiba Abdeli & Wafaa Abdeli, "The Electronic Signature Between the Necessity of Legal Regulation and the Limitations of Practical Application," Journal of Judicial Ijtihad, Vol. 12, No. 2, October 2020, p. 624.

[28] Article 6 of Law No. 15-04 determining the general rules relating to electronic signatures and electronic certification.

[29] UNCITRAL Model Law on Electronic Commerce (1996).

Received: 05/01/2026 Accepted: 02/05/2026 Published: 27/06/2026

"to indicate the signatory's approval of the information contained in the data message."[30]

Accordingly, when a person signs a document, the signature expresses the signatory's intention to be legally bound by the contents of the document and constitutes an acknowledgment of its authenticity. In the case of a handwritten signature (i.e., signing one's personal name), the name functions as an instrument placed at the disposal of the individual to express his or her intention with respect to a particular document and to assume responsibility for its contents, thereby transforming the written document into a legally binding act.[31]

2. Ensuring the Integrity of the Electronic Document

This function consists of preserving the content and integrity of the contract and ensuring that it is not altered. In a traditional paper environment, this function is fulfilled by the physical paper medium, which facilitates the detection of fraud, erasures, or unauthorized additions to the document, thereby preserving the contract in its original form without any modification or alteration.[1] This is reflected in Article 4 of Algerian Law No. 15-04 concerning electronic signatures and electronic certification, which provides:

"The electronically signed document shall be preserved in its original form, and the procedures relating to the preservation of electronically signed documents shall be determined by regulation."

[30] UNCITRAL Model Law on Electronic Signatures (2001).

[31] Tharwat Abdel Hamid, The Electronic Signature: Its Nature, Risks, Means of Protection, and Its Evidentiary Value, Dar Al-Jami'a Al-Jadida, Alexandria, 2007, p. 37.

While paper documents are characterized by permanence and stability, allowing them to be preserved for long periods under appropriate storage conditions while protecting the signed document from alteration, the situation differs in the electronic environment, where the storage medium is intangible. In this context, it is necessary to ensure the security of the content of documents exchanged over electronic networks due to the inherent vulnerabilities of such networks. A digital signature based on asymmetric encryption guarantees the integrity of the document through a mathematical process known as a hash function, which generates a compressed representation of the electronic document, referred to as the electronic fingerprint (digital hash) of the document. This fingerprint cannot be interpreted or reconstructed except through the appropriate cryptographic key.[32]

Section Two: Limits of the Evidentiary Value of the Electronic Signature

Despite the increasing legal recognition of the evidentiary value of electronic signatures, such value is not absolute. Rather, it remains subject to several limitations and challenges that may affect the degree of trust placed in it, particularly in the field of public procurement.

First Branch: Security Risks (Hacking and Forgery)

Among the most significant challenges affecting the evidentiary value of electronic signatures are technical security risks, including hacking, forgery, and the

[32] Amina Qahwaji, The Conceptual and Legal Framework of Electronic Signature and Electronic Certification in Algeria, Al-Mishkat Journal of Economics, Development and Law, Faculty of Economic, Commercial and Management Sciences, University of Boumerdes, Vol. 4, No. 8, 2018, p. 24.

Received: 05/01/2026 Accepted: 02/05/2026 Published: 27/06/2026

unauthorized use of signature tools. These risks raise serious concerns regarding the authenticity of contractual consent. In the field of information systems, forgery is defined as: "the manipulation of information stored in networked computer systems or the interception of information with the intention of altering and falsifying it."[33]

One of the most common methods of forging an electronic signature is the use of specialized computer programs or information systems specifically designed to imitate legitimate software and systems. Another method involves breaking encryption codes to gain access to the confidential digital signature data, copying it, and subsequently reusing it.[34] Consequently, electronic signatures are vulnerable to forgery by individuals possessing advanced computer expertise and technical knowledge of software systems. Such individuals may infiltrate electronic signature systems using specialized software, deceive these systems, decrypt electronic signatures, and exploit them for fraudulent purposes by copying or falsifying them and attaching them to forged electronic documents.[35]

Although the Algerian legislator introduced legal provisions criminalizing attacks against automated data processing systems—including acts such as modification, deletion, and unauthorized insertion of data—it did not

[33] Habib Belqneishi, Proof of Contracting via the Internet and Video Mail: A Comparative Study, Ph.D. Dissertation in Private Law, Faculty of Law, University of Oran, Department of Private Law, Es Sénia, 2010–2011, p. 132.
[34] Hossam Mohamed Nabil Al-Sharraqi, Cybercrimes: A Comparative Applied Study of Crimes Against Electronic Signatures, Dar Al-Kutub Al-Qanuniyyah, Egypt, 2013, p. 253.
[35] Saleh Shnin, Criminal Protection of Electronic Commerce: A Comparative Study, Ph.D. Dissertation, University of Tlemcen, 2013, p. 360.

explicitly address forgery committed within the field of information technology.[36] However, Algeria's ratification of the Arab Convention on Combating Information Technology Offences, pursuant to Presidential Decree No. 14-252 of 8 September 2014, resolved this issue. Article 10 of the Convention defines the offence as:

"The use of information technology means to alter the truth of data in a manner likely to cause harm, with the intention of using such data as if it were authentic."

Accordingly, electronic forgery committed through modern technological means, including the forgery of electronic signatures, is recognized, and the penalties prescribed under the general rules of criminal law are applicable.[37]

Second Branch: Technical Risks (Weak Digital Infrastructure)

In addition to the risks of hacking and forgery, the effectiveness of electronic signatures may also be undermined by weaknesses in the digital infrastructure of certain public administrations and by the shortage of qualified personnel capable of operating electronic systems efficiently. These factors may significantly limit the practical effectiveness of electronic signatures.

Electronic administration also faces the critical challenge of ensuring information security in a manner that preserves the credibility and reliability of public institutions. This requires integrating information security as a fundamental component

[36]Hanan Brahimi, op. cit., p. 248.

[37]Mostafa Youssef Kafi, Crimes of Corruption, Money Laundering, Tourism, Cyber Terrorism, and Information Technology, 1st ed., Arab Society Library for Publishing and Distribution, Amman, 2014, p. 91.

Received: 05/01/2026 Accepted: 02/05/2026 Published: 27/06/2026

of the technological infrastructure. Effective information system security should be achieved through the implementation of internal control mechanisms that guarantee the protection of electronic transactions and stored documents, as well as the secure electronic processing and transmission of data required for institutional operations. Weak information security inevitably undermines confidence in electronic services, making it essential to ensure adequate protection of electronic systems, their users, and the surrounding digital environment.[38]

Conclusion

The electronic signature is one of the most significant outcomes of digital transformation, as it has brought about a qualitative shift in the methods of concluding and proving contracts, particularly in the field of public procurement, which requires speed, transparency, and reliability. This study has examined the concept of the electronic signature, its various forms, and the conditions for its validity, while highlighting the characteristics that confer legal evidentiary value upon it and render it equivalent to the traditional handwritten signature whenever the required legal and technical conditions are fulfilled.

The study also demonstrates that the adoption of electronic signatures in public procurement enhances the efficiency of e-government and contributes to simplifying administrative procedures. Nevertheless, the evidentiary value of electronic

[38] Abbas Hafsi, Electronic Forgery Crimes: A Comparative Study, Ph.D. Dissertation, Ahmed Ben Bella University of Oran 1, 2015, p. 97.

signatures remains dependent upon the availability of a secure digital environment, an advanced technological infrastructure, and effective electronic certification systems capable of addressing security and technical risks. Accordingly, strengthening the legislative and technical framework governing electronic signatures is essential to ensuring trust in electronic transactions and achieving the objectives of the digitalization of public procurement.

References

Legislation

1. UNCITRAL Model Law on Electronic Commerce, adopted on 16 December 1996, United Nations Publications, New York, 2000, p. 4. Available at: https://2u.pw/LdExo6.
2. UNCITRAL Model Law on Electronic Signatures, adopted on 12 December 2001, United Nations Publications, New York, 2002. Available at: https://2u.pw/3i3UQv.
3. Law No. 15-04 of 1 February 2015, establishing the general rules relating to electronic signatures and electronic certification, Official Gazette No. 06, issued on 10 February 2015.

Books

1. Tharwat Abdel Hamid, Electronic Signature: Its Nature, Risks, Means of Protection, and Its Evidentiary Value, Dar Al-Jami'ah Al-Jadidah, Al-Azareeta, 2007.
2. Hossam Mohamed Nabil Al-Sharqi, Cybercrimes: A Comparative Applied Study on Crimes Involving

Received: 05/01/2026 **Accepted:** 02/05/2026 **Published:** 27/06/2026

Electronic Signature Infringement, Dar Al-Kutub Al-Qanuniyyah, Egypt, 2013.
3. Lazhar Ben Said, The Legal Regime of Electronic Commerce Contracts, Dar Houma, Algeria, 2012.
4. Mohamed Khaled Gamal Rostom, The Legal Regulation of Electronic Commerce and Electronic Evidence in the World, 1st ed., Halabi Legal Publications, Lebanon, 2006.
5. Mamdouh Mohamed Ali Mabrouk, The Evidentiary Value of the Electronic Signature: A Comparative Study in Light of Islamic Jurisprudence, Dar Al-Nahda Al-Arabia, Cairo, 2005.
6. Mounir Mohamed Al-Jeneihi and Mamdouh Mohamed Al-Jeneihi, The Legal Nature of the Electronic Contract, Dar Al-Fikr Al-Jami'i, Alexandria, n.d.
7. Mustafa Youssef Kafi, Crimes of Corruption, Money Laundering, Tourism, Cyber Terrorism, and Information Technology, 1st ed., Arab Society Library for Publishing and Distribution, Amman, 2014.
8. Saddam Mohamed Talib Al-Khamayseh, Smart Government: Beyond E-Government, 1st ed., Qindeel Printing, Publishing and Distribution, Dubai, United Arab Emirates, 2017.
9. Abed Fayed Abdel Fattah Fayed, Electronic Writing in Civil Law between Legal Development and Technical Security: A Study of the Legal Concept and Functions of Electronic Writing in Civil Law, Dar Al-Jami'ah Al-Jadidah, Alexandria, 2004.
10. Adel Ramadan Al-Abiouki, Electronic Signature in Gulf Legislations: A Comparative Study, 1st ed., Modern University Office, Alexandria, 2009.

11. Abbas Al-Aboudi, Challenges of Proof by Electronic Documents and the Requirements of the Legal System to Overcome Them, 1st ed., Halabi Legal Publications, Lebanon, 2010.
12. Issa Ghassan Ridhi, Special Rules Governing Electronic Signatures, 1st ed., Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, 2009.
13. Saeed Si Qandil, Electronic Signature, University Publishing House, Beirut, Lebanon, 2004.

Journal Articles

1. El Yaqout Ar'ar, "Electronic Signature as a Mechanism for the Security and Integrity of Digital Payment," Journal of Legal and Political Sciences, Vol. 11, No. 3, December 2020.
2. Amina Qahwaji, "The Conceptual and Legal Framework of Electronic Signature and Electronic Certification in Algeria," Al-Mishkat Journal of Economics, Development and Law, Faculty of Economic, Commercial and Management Sciences, University of Boumerdes, Vol. 4, No. 8, 2018.
3. Boualem Bouzidi, "On the Electronic Signature," Al-Badr Journal, University of Bechar, No. 5, May 2012.
4. Habiba Abdeli and Wafaa Abdeli, "Electronic Signature between the Necessity of Legal Texts and the Limitations of Practical Application," Journal of Judicial Ijtihad, Vol. 12, No. 2, October 2020.
5. Hassina Cherroun and Sonia Makri, "Electronic Signature as a Mechanism for Authenticating Electronic Transactions," Journal of Judicial Ijtihad, Vol. 13, No. 2, October 2021.

Received: 05/01/2026 Accepted: 02/05/2026 Published: 27/06/2026

6. Mahjouba Kacem, "Legal Protection of the Electronic Signature against the Crime of Forgery," Journal of Legal and Social Sciences, Vol. 6, No. 2, June 2021.
7. Fatiha Hawas, "Electronic Signature: Characteristics and Applications," Journal of Comparative Legal Studies, Vol. 7, No. 1, 2021.
8. Fatima Al-Zahra Mossaddaq, "Electronic Certification as a Means of Protecting the Electronic Signature," Journal of Legal Studies and Research, Vol. 5, No. 1, 2020.

Theses and Dissertations

1. Alaa Ahmed Mohamed Al-Haj Ali, The Legal Regulation of Electronic Signature Certification Authorities, Master's Thesis, Faculty of Graduate Studies, An-Najah National University, Palestine, 2013.
2. Habib Belkneichi, Proof of Contracting via the Internet and Visual Mail: A Comparative Study, Ph.D. Dissertation in Private Law, Faculty of Law, University of Oran, Department of Private Law, 2010/2011.
3. Hanan Brahimi, The Crime of Forging Official Administrative Documents of an Information Technology Nature, Ph.D. Dissertation, Faculty of Law, University of Biskra, 2015.
4. Saleh Shnin, Criminal Protection of Electronic Commerce: A Comparative Study, Ph.D. Dissertation, University of Tlemcen, 2013.
5. Abbas Hafsi, Electronic Forgery Crimes: A Comparative Study, Ph.D. Dissertation, Ahmed Ben Bella University, Oran 1, 2015.