

Electronic Signature as a Mechanism for Enhancing Transparency and Combating Corruption under Law No. 26-02

التوقيع الإلكتروني كآلية لتعزيز الشفافية ومكافحة الفساد على ضوء القانون رقم 02-26

Bouziane Bouchra
PhD Candidate
University of Khenchela
bouziane.bouchra@univ-khenchela.dz

Boubaya Issam
University of M'sila
assam.boubaya@univ-msila.dz

Date of send: 17/04/2026	date of acceptance: 10/05/2026	date of publication: 10/06/2026
---------------------------------	---------------------------------------	--

abstract:

Electronic signature constitutes a vital legal and technological mechanism for ensuring integrity and transparency in digital transactions, through authenticating the identity of the parties, protecting data, and preventing manipulation or forgery. Law No. 26-02 establishes a comprehensive framework that defines the reliability conditions of electronic signatures and ensures their linkage to data in such a manner that any subsequent alteration can be detected. This enhances the role of electronic signatures in combating corruption and reinforcing legal trust in digital transactions.

Keywords: Electronic Signature; Transparency; Anti-Corruption; Law 26-02; Digital Transactions.

ملخص:

يعد التوقيع الإلكتروني أداة قانونية وتقنية حيوية لضمان النزاهة والشفافية في المعاملات الرقمية، من خلال توثيق هوية الأطراف وحماية البيانات ومنع التلاعب أو التزوير، ويوفر القانون رقم 02-26 إطاراً متكاملاً يحدد شروط موثوقية التوقيع الإلكتروني وكيفية ربطه بالبيانات بطريقة تكشف أي تعديل لاحق، مما يعزز دور التوقيع الإلكتروني في مكافحة الفساد وتعزيز الثقة القانونية في المعاملات الرقمية.

كلمات مفتاحية: التوقيع الإلكتروني، الشفافية، مكافحة الفساد، القانون 02-26، المعاملات الرقمية

***Bouziane Bouchra**

1. INTRODUCTION

In recent years, the electronic signature has emerged as a fundamental instrument for ensuring integrity and transparency in digital transactions, owing to its technological sophistication and its capacity to authenticate the identity of contracting parties, safeguard data confidentiality, and guarantee the reliability of exchanged information. It no longer merely serves to express the signatory's consent, but also provides robust legal assurances capable of limiting manipulation and forgery, thereby strengthening mutual trust and curbing manifestations of corruption.

Law No. 26-02 establishes a comprehensive legal framework governing electronic signatures and the associated trust services. It defines the requirements for their reliability, the mechanisms for their control, and the manner in which they are linked to electronic data so that any subsequent alteration becomes detectable. This significantly reinforces the protective function of electronic signatures in securing digital transactions.

In light of the growing reliance on electronic dealings, a crucial question arises as to the extent to which electronic signatures can provide sufficient guarantees to promote transparency and prevent corruption. Additionally, it is necessary to examine how Law No. 26-02 succeeds in striking a balance between facilitating digital processes and safeguarding the legal rights of the parties, particularly in view of rapid technological developments that may attempt to circumvent existing monitoring and authentication mechanisms.

2. Conceptual Framework of the Electronic Signature

The signature is an essential element for the completion of electronic transactions in general. Establishing trust between remotely contracting parties requires the existence of a legally protected interest. In order to ensure the validity and enforceability of such transactions, and to prevent breaches of data confidentiality, the presence of an electronic signature becomes indispensable, provided that it is issued by a duly authorized entity.

Accordingly, both Arab and European legislations have paid particular attention to regulating electronic signatures within their legal systems governing electronic transactions, including granting them criminal protection.

The ministerial decision dated November 17, 2013, which defines the content of the electronic portal for public procurement, explicitly provides that the portal shall include the electronic signing of documents ¹. It further stipulates that, in designing the information system for public procurement and ensuring the integrity of electronically exchanged documents, such documents must be signed using secure electronic methods in compliance with the applicable legislative and regulatory provisions ².

In order to clarify the role of electronic signatures in ensuring the confidentiality of transactions and in proving electronic public procurement contracts, it is necessary first to define the concept and subsequently to identify its legal conditions.

2.1 Definition of the Electronic Signature

The concept of the electronic signature remains relatively recent and still evolving. Nevertheless, it represents a natural extension and development of the traditional signature, which constitutes the cornerstone of the law of evidence. The signature is a legally protected social phenomenon, serving as a distinctive mark that identifies its holder and expresses approval of the document's content.

It may refer either to the act of affixing a signature to a document containing specific information, or to the mark itself that distinguishes the signatory and enables identification. This is the meaning attributed to the signature within the framework of evidentiary law.

While this definition applies to the traditional signature, the electronic signature differs in that it relies on technological mechanisms.

The European Directive No. 99/93/EC on electronic signatures defines it, under Article 2(1), as: "data in electronic form which are attached to or logically associated with other electronic data (message or document), and which serve as a method of authentication".³

This directive grants electronic signatures the same evidentiary value as traditional signatures and adopts a broad definition encompassing all forms capable of identifying the signatory.

The French legislator defined the electronic signature under Article 1316-4 of Law No. 2000-230 dated March 13, 2000, amending the Civil Code, as follows: “The electronic signature identifies its author and ensures its link with the act to which it relates; it confirms the identity of its author and the authenticity of the act attributed to him unless proven otherwise”.⁴

This definition confers enhanced evidentiary value upon electronic signatures and affirms the validity of electronic transactions. It also clarifies that this provision applies not only to civil contracts but also to administrative contracts.

The Algerian legislator, although it enacted the law on electronic commerce only in 2018 under Law No. 18-05, had previously adopted Law No. 15-04 on electronic signature and certification, which was later repealed and replaced by Law No. 26-02 relating to trust services for electronic transactions and electronic identification.

Article 02(1) of Law No. 26-02 defines the electronic signature as: “data in electronic form, attached or logically associated with other electronic data, used by the signatory as a method of authentication”⁵

2.2 Conditions of the Electronic Signature

Article 2 of Directive 99/93/EC establishes the conditions that must be fulfilled by an electronic signature, namely:

- It must be uniquely linked to the signatory .The first technical-legal requirement is that the electronic signature must be uniquely linked to the signatory. Under Law 26-02, this is achieved through a distinct set of cryptographic data that serves as a digital fingerprint. This uniqueness ensures that the signature cannot be replicated or attributed to any other individual, creating a legal presumption that the signature belongs exclusively to the person who affixed it. This element is the cornerstone of authenticity in the digital environment
- It must enable the identification of the signatory A qualified electronic signature must be capable of identifying the signatory with absolute certainty. This identification is not merely symbolic but is facilitated through a 'Qualified Electronic Certificate' issued by a certified Trust

Service Provider. This certificate binds the technical signing keys to the physical and legal identity of the signatory (such as name, national ID, or professional status), thereby providing a verifiable bridge between the digital action and the real-world person

- It must be created using means that the signatory can maintain under his sole control. The signatory must be able to create the signature using electronic signature creation data that they can, with a high level of confidence, use under their sole control. In the context of the Algerian legal framework, this necessitates the use of a 'Qualified Electronic Signature Creation Device' (QSCD), such as encrypted smart cards or secure tokens. This condition ensures that the signing process remains under the exclusive custody of the signatory, preventing unauthorized third-party access and safeguarding the integrity of their legal consent
- It must be linked to the data in such a manner that any subsequent alteration is detectable. The electronic signature must be linked to the data signed in such a way that any subsequent change in the data is detectable. This creates a technical 'seal' over the document. If even a single character in the digital contract is altered after the signature has been applied, the cryptographic link is broken, and the signature becomes invalid. This feature provides a level of security against fraud and tampering that far exceeds traditional paper-based signatures, ensuring the immutability of legal transactions.⁶

The Algerian legislator adopted the same requirements under Article 04 of Law No. 26-02.⁷

2.1.1 Identification of the Signatory

At first glance, the electronic signature may appear incapable of fulfilling the traditional function of identifying its author. However, from a technical standpoint, it consists of symbols, numbers, or codes uniquely assigned to each individual, allowing verification through certification authorities.⁸ This technical uniqueness creates a "digital fingerprint" that transcends the limitations of physical handwriting. While a manual signature can be imitated with relative ease, the electronic signature relies on complex cryptographic

algorithms and asymmetric encryption (Public and Private Keys). The role of "Certification Authorities" (CA) is crucial here; they act as a trusted third party that validates the link between the digital code and the real-world identity of the person. In the Algerian legislative context, this identification process is essential for establishing legal accountability, ensuring that every digital transaction in public procurement can be traced back to a specific authorized official or a legitimate economic operator.

2.1.2 Exclusive Control by the Signatory

The French legislator emphasized that the signature must be generated using a secure mechanism ensuring both the identification of the signatory and the linkage between the signature and the legal act ⁹. The concept of "Exclusive Control" implies that the means of creating the signature (such as a smart card, a USB token, or a biometric factor) must remain under the sole possession and authority of the signatory at the time of signing. This legal requirement is designed to prevent the unauthorized use of a person's digital identity. By ensuring a direct and unbreakable "linkage" between the signature and the legal act, the law guarantees that the content of the contract or the administrative decision has not been altered after the signature was applied. If the integrity of the document is compromised, the mathematical link is broken, rendering the signature void. This level of control provides a higher degree of security than traditional paper documents, where pages can be swapped or modified after signing.

2.1.3 Electronic Identity Certificate

Given the absence of physical presence, verifying the identity of contracting parties becomes a major issue. Therefore, electronic identity certificates serve as proof issued during the creation of the electronic signature, confirming the identity of the signatory. The Electronic Identity Certificate acts as a "Digital Passport" in the virtual world of public procurement. Since the parties do not meet face-to-face, the certificate provides the necessary legal certainty to proceed with high-value transactions. These certificates contain vital information, including the signatory's name, the public key, the expiration

date, and the digital signature of the issuing authority. In the fight against administrative corruption, these certificates prevent "identity fraud" and the creation of "ghost contractors." By mandating that all participants in a digital tender hold a valid, government-approved certificate, the legislator ensures that only verified and legitimate entities can interact with the public treasury, thereby strengthening the overall integrity of the electronic contracting system.¹⁰

3. Activating the Role of Electronic Signature in Combating Corruption and Preventing Document Manipulation

Electronic signature plays a pivotal role in promoting transparency and combating corruption within administrative transactions. It contributes to preserving document integrity, enhancing procedural transparency, reducing direct interaction, and strengthening both administrative and judicial oversight.

3.1 Preservation of the Electronic Signature

The electronic signature is characterized by confidentiality, as only its holder possesses knowledge of its components and is required to preserve them without disclosure.

Directive 99/93/EC provides that:

1. The signature must be created using means under the exclusive control of the signatory. This preservation duty stems from the "Principle of Personal Responsibility." The confidentiality of the signature's components (such as private keys or biometric data) is the legal basis for its evidentiary weight. According to Directive 99/93/EC and modern digital laws, this "Exclusive Control" ensures that the signatory is the only person capable of expressing legal will.
2. It must be linked to data in such a way that any modification can be detected. The technical "Linkage" to the data creates a digital "Seal" (Hash); if even a single character in the document is altered, the mathematical synchronization is broken, alerting the oversight bodies to a breach of integrity. This absolute fusion between the signature and the document is what makes electronic public procurement more secure than

traditional paper-based systems, where documents could be physically manipulated or pages replaced after signing.¹¹

Furthermore, the signature must be inseparably linked to the document, forming an integral whole, thereby ensuring the integrity of the content.¹²

3.2 Electronic Signature Certificate

An electronic certificate is issued by an authorized certification authority and establishes the link between the signatory and the signature creation data. The electronic certificate serves as the "Digital Identity Card" that bridges the gap between the virtual signature and the physical person. It provides a technical and legal guarantee that the public key used to verify the signature actually belongs to the identified signatory. In the context of combating administrative corruption, this certificate is indispensable because it eliminates "anonymous" transactions. By establishing an unbreakable link between the signatory and the signature creation data, it ensures that every administrative approval or financial commitment in a public contract is attributable to a specific, verified individual, thereby facilitating legal accountability.¹³

3.2.1 Certification Authority

A trusted third party, known as a certification authority, is responsible for verifying identities and issuing certificates that confirm the authenticity of electronic signatures. The Certification Authority (CA) acts as the "Neutral Arbiter" in the digital ecosystem. Its role is fundamental to the "Circle of Trust" required for high-value public procurement. Before issuing a certificate, the CA must perform rigorous "Identity Proofing" to ensure that the applicant is indeed who they claim to be. By confirming the authenticity of signatures, the CA protects the public treasury from "Identity Theft" and "Fraudulent Bidding." This third-party verification adds an extra layer of oversight, as the administration does not verify itself; instead, it relies on an independent body to certify the credentials of its officials and the contractors it deals with.¹⁴

3.2.2 Trust Service Providers

Law No. 26-02 defines trust service providers as legal entities that provide trust services, including the issuance of certificates and other related services. Under Law No. 26-02, Trust Service Providers (TSPs) are recognized

as specialized entities that go beyond simple certificate issuance. They provide the "Legal Infrastructure" for the digital economy. These providers are subject to strict state regulations and technical audits to ensure they meet international security standards. By defining them as "Legal Entities," the legislator establishes a clear framework for their civil and criminal liability. Their presence is a prerequisite for "Procedural Transparency," as they provide the tools (such as digital seals and electronic time-stamps) that make the public procurement process auditable and resistant to administrative manipulation.¹⁵

3.2.3 Functions of Trust Service Providers

Their principal functions include:

1. Ensuring data confidentiality and security. The TSP is responsible for implementing high-level cryptographic protocols that ensure "End-to-End" confidentiality. In public procurement, the content of a bidder's offer must remain secret until the moment of the public opening of tenders. The TSP provides the encryption infrastructure that prevents anyone—including administrative officials. This function is a direct strike against collusion and information leaking, as it ensures that no competitor gains an unfair advantage through the premature disclosure of sensitive data.¹⁶
2. Verifying the identity of users. This is the "gatekeeping" function of the TSP. Before a digital certificate is issued to an official or a contractor, the TSP must conduct a rigorous verification process (Know Your Customer - KYC). They verify legal documents, commercial registers, and personal IDs to ensure that every signature belongs to a legitimate legal entity. In the context of anti-corruption, this prevents the use of "Front Companies" (الشركات الصورية) or unauthorized individuals from participating in tenders, ensuring that the state only deals with verified and accountable partners.¹⁷
3. Updating and revoking certificates when necessary. This function represents the "Dynamic Control" of digital identity. A certificate is not just issued once; it must be monitored throughout its lifecycle.

- **Revocation (الإلغاء):** If a public official is moved to a different department, loses their authority, or is under investigation for corruption, the TSP must immediately add their certificate to the Certificate Revocation List (CRL) or use the OCSP protocol.
 - **Importance:** This prevents "Unauthorized Authorization," ensuring that a person who no longer has the legal power to sign a contract or approve a payment cannot do so using an old digital key. It acts as a real-time security filter for administrative actions.¹⁸
4. Securing electronic transmission processes The TSP ensures the "Sanctity of the Digital Path." When an offer is sent from a contractor to the procurement portal, it travels through various networks. The TSP provides secure communication channels (such as SSL/TLS certificates) that protect the data from interception (الاعتراض) or Man-in-the-Middle attacks. By securing the transmission, the TSP guarantees that the "Digital Offer" received by the administration is identical to the one signed by the contractor, preventing any external or internal technical manipulation during the sensitive phase of data transit.¹⁹

4. Role in Enhancing Transparency and Combating Administrative Corruption

Electronic signatures contribute significantly to:

- Preventing tampering with documents and offers. The electronic signature acts as a "digital seal" that guarantees the integrity of the data. Unlike paper documents, which are susceptible to physical alteration, page replacement, or forgery, an electronically signed document is cryptographically locked. Any attempt to modify the prices, technical specifications, or terms of a bid after the signature has been applied will result in an immediate mismatch in the digital hash, rendering the signature invalid. This technical barrier prevents the common corrupt practice of "bid-rigging" or the post-submission alteration of offers to favor a specific contractor.
- Ensuring traceability of all contractual procedures Traceability is the most potent enemy of administrative corruption. Every electronic

signature is accompanied by a digital audit trail that records the "who, when, and where" of every action taken during the procurement process. This creates an unbreakable chain of evidence from the initial announcement to the final award. This level of accountability ensures that administrative decisions are not made in a vacuum; every approval or rejection is signed and logged, making it impossible for officials to bypass legal procedures without leaving a permanent, discoverable record.

- Reducing direct contact between public officials and economic operators, thereby limiting bribery and favoritism. Corruption often thrives in the personal interaction between public officials and economic operators. Electronic signatures facilitate a "dematerialized" environment where the identity of the parties is verified through digital certificates rather than physical meetings. By shifting the contracting process to a remote, automated platform, the opportunities for "facilitation payments," personal lobbying, or the exercise of "favoritism" (Intercession) are drastically reduced. The system treats all participants as encrypted data points, ensuring that the process remains objective and rules-based.
- Strengthening administrative and judicial oversight through reliable digital evidence. The electronic signature provides both administrative and judicial oversight bodies (such as the Court of Auditors or the Judiciary) with "self-authenticating" evidence. In cases of suspected embezzlement or abuse of office, investigators can rely on the digital certificate to establish direct criminal liability. Since these signatures are issued by authorized certification bodies, they carry high evidentiary weight in court, making it much harder for perpetrators to deny their involvement or claim that documents were forged, thereby enhancing the overall effectiveness of the anti-corruption legal framework.
- Enhancing trust in public procurement systems and promoting fair competition. A transparent system secured by electronic signatures sends a strong signal of "legal certainty" to the market. When economic

operators are confident that their bids cannot be tampered with and that the selection process is monitored through digital logs, they are more likely to participate. This increased participation fosters a climate of fair competition, which not only prevents the monopolization of public contracts by a corrupt few but also ensures that the state achieves the best value for public money through a competitive and honest marketplace.

Thus, the electronic signature is not merely a technical tool but rather a modern legal mechanism that plays a decisive role in combating administrative corruption by promoting transparency, integrity, and accountability

5. CONCLUSION

The electronic signature, as rigorously regulated under Law No. 26-02, constitutes an indispensable legal and technological pillar for enhancing transparency and institutionalizing corruption prevention within digital transactions. Its significance transcends the mere digitization of traditional signatures; it establishes a new paradigm of "Technical Trust" that ensures the authentication of parties, protects data integrity, and provides an indisputable audit trail for the traceability of every modification. By replacing physical interaction with encrypted digital protocols, this mechanism effectively minimizes the human factor in administrative discretion, thereby limiting the opportunities for bribery, favoritism, and the misappropriation of public funds.

Furthermore, the implementation of electronic signatures strengthens both preventive and repressive oversight mechanisms. From a preventive perspective, it forces all participants in public procurement to operate within a transparent, logged framework. Repressively, it provides judicial and oversight bodies with "high-integrity digital evidence" that is difficult to forge or repudiate, ensuring that legal accountability is easily established in cases of administrative fraud. Consequently, the electronic signature represents not merely a technical instrument, but a comprehensive legal framework for promoting integrity, transparency, and public trust in the state's digital environment.

Looking ahead, the effectiveness of this legal framework remains contingent upon the continuous development of its supporting infrastructure. To fully realize the potential of electronic signatures in combating corruption, it is essential to:

- Keep pace with technological advancements, such as integrating blockchain or biometric factors to stay ahead of sophisticated cyber-attacks.
- Strengthen the role of Trust Service Providers by ensuring regular technical audits and strict compliance with international security standards.
- Bridge the gap between legislation and implementation by promoting a "Digital Culture" among public officials and economic operators, ensuring that the law is not just a text, but a living administrative practice.

Ultimately, while Law No. 26-02 provides the necessary legal armor, the true success of electronic signatures lies in their ability to foster a resilient and transparent digital ecosystem capable of defending public interests against emerging cybersecurity challenges and evolving forms of administrative corruption.

6. Margins:

¹ -Hiba Hussein Mohamed Zayed, *Criminal Protection of Electronic Transactions*, Dar Al-Jami'a Al-Jadida, Alexandria, Egypt, 2011, pp. 34–35

² -Article 4, paragraph 11 of the Ministerial Decision defining the content of the electronic portal for public procurement provides that:
“The electronic portal shall include:

- Electronic signature of documents

³ -Article 1/7, paragraph 2 of the Ministerial Decision defining the content of the electronic portal for public procurement provides that: “The information system for public procurement must be designed in compliance with the principle of integrity of documents exchanged electronically:

- Documents must be signed using secure electronic methods in accordance with the applicable legislative and regulatory provisions.”

⁴ -Ayman Hussein Al-Houthi, *Electronic Signature between Theory and Practice: A Comparative Study*, Dar Al-Fikr Al-Jami'i, Alexandria, Egypt, 1st edition, 2011, pp. 12–13

⁵ -Article 2 of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a community framework for electronic signatures

⁶ -L'article 1316-4 :« Lorsqu'elle électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée jusqu'à preuve contraire, lorsque la signature est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie ». (JO N° 62 du 14-03-2000)

⁷ - L'alinéa 2 de l'article 1316-4 du Code civil, désormais abrogé, disposait que : « Lorsqu'elle est électronique, [la signature] consiste en l'utilisation d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache

⁸ - Rahima Al-Saghir Saad Namdili, *The Electronic Administrative Contract (An Analytical Comparative Study)*, Dar Al-Jami'a Al-Jadida, Alexandria, Egypt, 2010, p. 82

⁹ - Law No. 18-05 of May 10, 2018 relating to electronic commerce, Official Gazette No. 28, issued on May 16, 2018

¹⁰ - Law No. 15-04 of February 1, 2015 defining the general rules relating to electronic signature and certification, Official Gazette No. 06, issued on February 1, 2015

¹¹ - Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, JO n°L 013 du 19/01/2000

¹² - Ayman Hussein Al-Houthi, *op. cit.*, p. 35.

¹³ - Amin Faraj Youssef, *Electronic Signature*, Dar Al-Matbou'at Al-Jami'iya, Alexandria, Egypt, 2007, p. 338

¹⁴ - L'article 1316-4 cité : « La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose, elle manifeste le consentement des parties aux obligations qui découlent de cet acte; quand elle est opposée par un officier public, elle confère l'authenticité de l'acte

¹⁵ - Amin Faraj Youssef, *op. cit.*, p. 184

¹⁶ - Hamdi Suleiman Al-Qubailat, "The Legal System for Concluding Electronic Administrative Contracts," *Journal of Sharia and Law Sciences Studies*, Vol. 34, 2007, p. 221.

¹⁷ - Rahima Al-Saghir Saad Namdili, *op. cit.*, p. 36.

¹⁸ - Ayman Ali Hassan Al-Houthi, *op. cit.*, p. 24.

¹⁹ - Mohamed Ali Souilem, *Criminal Protection of Electronic Transactions: Cyber and Electronic Crimes between Procedural and Substantive Aspects*, 1st ed., Dar Al-Matbou'at Al-Jami'iya, Alexandria, Egypt, 2018, p. 53; same definition also appears at p. 58. See also: Amin Faraj Youssef, *op. cit.*, p. 52