Journal of Legal Studies and Researches
e-ISSN: 2676-1688 p-ISSN:2437-1084
Vol: 11 N°2, June 2026, p. 61–84

Legal Dimensions of Adopting Electronic Signatures in Digital Banking in Algeria

Sihamdi Narimane
Facuty of Law, University of Constantine 1, Algeria
narimane.sihamdi@doc.umc.edu.dz
https://orcid.org/0009-0004-6764-6874

Received:30/01/2026 | *Accepted:05/05/2026* | *Published*: *20/06/2026*

Abstract:
The financial services sector is among the main beneficiaries of recent developments in electronic identification and digital trust services, given the significant commercial opportunities these technologies offer and their tangible contribution to improving the quality of financial services. This study aims to analyze the legal framework governing electronic signatures in digital banks as a key instrument for enhancing trust and ensuring transaction security within the digital banking environment. The research is based on an analysis of comparative legislative texts and an examination of contemporary banking practices, with particular emphasis on their compliance with the requirements of legal certainty and evidentiary validity. The study concludes that the adoption of electronic signatures in digital banking constitutes an inevitable development for the banking sector, as they represent an effective legal tool that enhances trust in digital banking transactions by ensuring speed and efficiency while preserving full legal validity. The study further concludes that the Algerian legislator should take these modern uses into account by providing a legal framework regulating secure electronic identity verification mechanisms in order to support digital banking development and strengthen trust in electronic financial transactions.

Keywords: Digital Banking; Electronic Signature; Legal Validity; authentication; Banking Sector.

1. INTRODUCTION

The financial services sector constitutes one of the main areas benefiting from recent advancements in electronic identification and digital trust services, given the significant regulatory and commercial opportunities these technologies offer, as well as their substantial contribution to enhancing the quality and security of financial services, particularly those provided on a cross-border basis. The processes of customer identification, authentication, and transaction security within the financial sector have undergone an unprecedented level of digitalization, driven by the increasing reliance on online financial services and the necessity to comply with evolving regulatory frameworks relating to security, transparency, and anti-money laundering obligations.

Electronic signatures have introduced a fundamental shift in banking operations by providing a legally secure, efficient, and reliable alternative to traditional paper-based procedures. From a regulatory perspective, electronic signatures facilitate compliance with legal and supervisory requirements governing contractual formalism, record-keeping, and evidentiary standards. They enable financial institutions to remotely conclude legally binding contracts, open bank accounts, and offer savings and investment products, while ensuring the integrity, authenticity, and non-repudiation of electronic transactions.

Accordingly, the digital transformation of banking services increasingly depends on the adoption of robust technological solutions, with electronic signatures occupying a central role as a regulatory-compliant instrument that enhances operational efficiency, reduces administrative costs, and reinforces customer confidence in the digital financial ecosystem.

Despite these regulatory and operational advantages, the legal and supervisory treatment of electronic signatures remains fragmented and inconsistent across jurisdictions. While electronic signatures have emerged as a key mechanism for ensuring the validity and integrity of digital banking transactions, their regulatory treatment remains uneven across jurisdictions. In several legal systems, including emerging banking markets,

uncertainties persist regarding their evidentiary value, supervisory oversight, and compliance with banking regulatory requirements.

Against this backdrop, this study seeks to examine the following research question:

What are the legal implications of the implementation of electronic signatures within digital banking frameworks?

To address this question, the research will be structured as follows:

- Section One: The Legal Framework of Electronic Signatures in Digital Banking
- Section Two: Legal Considerations for the Digitization of Hand-Signed Documents.
- Section Three: Electronically Created and Signed Documents.

2. Regulatory Framework Governing Electronic Signatures in Digital Banking

Digital banks are regarded as financial technology (FinTech) institutions that provide financial services in ways that challenge traditional banking models, and they have increasingly become an inevitable necessity within contemporary financial systems.(1)At the same time, technological developments have expanded and progressed at such a rapid pace that existing legal frameworks have often proven incapable of keeping up with these transformations.

Technological advancement in the field of banking services and financial technology has led to the emergence of several legal gaps that required precise regulatory intervention. Over time, this situation has highlighted the need for a new and more refined regulatory framework governing the banking sector and all activities related thereto, including electronic signatures, particularly in light of the establishment of digital banks pursuant to Law N° 23-09 on Money and Banking (2023).(2)

In this context, the Algerian legislator had previously laid down a specific legal framework for electronic signatures through Law N° 15-04)3(on Electronic Signature and Electronic Certification (2015), which constitutes the principal legal basis governing the use of electronic signatures within digital banking transactions.

Electronic signatures differ from traditional handwritten signatures in several respects; however, the core distinction between them lies in the medium on which the signature is affixed. While a traditional signature is

inscribed on a paper-based medium, an electronic signature is created and recorded on an electronic medium through computer devices and via the Internet. This fundamental difference in the medium results in a corresponding divergence in the formal characteristics of each type of signature. A traditional signature is typically manifested in a specific and recognizable form, namely a handwritten signature, and in certain legal systems it may be supplemented by a seal, a fingerprint, or both. By contrast, an electronic signature may assume multiple forms, as it can consist of letters, numbers, symbols, or electronic signals generated, recorded, and transmitted through digital or optical electronic means.)4(

Electronic signature, also referred to as a digital signature, constitutes a secure mechanism that enables the execution of documents without recourse to paper-based media. Within the banking sector, electronic signatures currently enjoy the same legal validity as handwritten signatures, provided that they comply with specific regulatory requirements relating to authentication (identity verification), data integrity, and traceability. Consequently, banks make extensive use of electronic signatures across various banking operations, including account opening procedures, loan approvals, and investment management activities.

These shifts toward full digitalization enable the provision of remote banking services in a more seamless and user-friendly manner, while simultaneously reducing administrative and operational costs. One of the primary objectives of electronic signatures is to allow both natural and legal persons to rely on national electronic identification mechanisms when accessing digital banking services. The Algerian legislator defined the electronic signature under Law N° 15-04 of 2015 establishing the general rules relating to electronic signatures and electronic certification, whereby Article 2 provides that: *"An electronic signature consists of data in electronic form, attached to or logically associated with other electronic data, and used as a means of authentication."*

Furthermore, pursuant to Article 6 of the same law, the electronic signature is used to authenticate the identity of the signatory and to establish their consent to the content of the electronic document.

The legal validity of an electronic signature depends on several factors, including its conformity with the applicable legislation and the

security guarantees it provides. In general, for an electronic signature to acquire legal effect, it must comply with the legal and technical requirements established by the competent authorities. These requirements are primarily intended to ensure the following:(5)

- A verifiable and inseparable connection between the electronic signature and the signed document;
- Assurance of the document's integrity, guaranteeing that it is not modified post-signature;
- Reliable authentication of the identities of all parties participating in the transaction.

A qualified electronic signature refers to an electronic signature that fulfills the following criteria: (6)

- It is established on the basis of an electronic certification;
- It allows for the unequivocal identification of the signatory;
- It is generated through a secure mechanism specifically intended for the creation of the electronic signature ;
- It shall be created using mechanisms exclusively controlled by the signatory;
- It shall be logically associated with the signatory's data in a manner that enables the detection of any subsequent alterations to such data.

The intrinsic characteristics of electronically stored data render it inherently more vulnerable to tampering than traditional data formats. Accordingly, it is essential to implement detailed regulatory measures to safeguard data integrity and verify its authenticity throughout collection, storage, and transmission, thereby ensuring that electronic evidence remains unchanged from its creation onward.(7)

In this context, uniform standards for electronic trust services should be established, including qualified electronic certificates, electronic seals, time-stamping mechanisms, and secure electronic document delivery.

These objectives underscore the imperative of ensuring legal certainty in the deployment of electronic trust services, which must be both secure and readily usable. Such assurances are essential for fostering their adoption by individuals and entities in digital banking operations. Achieving this legal and regulatory certainty is pivotal to overcoming the prevailing lack of

trust—particularly the uncertainty regarding the legal validity of electronic transactions—which often deters consumers, businesses, and public authorities from conducting transactions with digital banks.(8)

2.1. Types of Electronic Signatures

The implementation of electronic signatures in the banking sector relies on advanced technologies that ensure the integrity, authenticity, and traceability of digital transactions. Law N° 15-04 does not explicitly classify types of electronic signatures; rather, Article 7 recognizes only the *qualified electronic signature* (advanced electronic signature) and, pursuant to Article 8, considers it legally equivalent to a handwritten signature, whether executed by a natural or legal person. This stands in contrast to the European eIDAS Regulation on electronic identification and trust services, which recognizes three types of electronic signatures: the simple electronic signature, the advanced electronic signature, and the qualified electronic signature.

While all these types are legally binding, their evidentiary value differs depending on the type of signature:

- **Simple Electronic Signature:** This signature type does not incorporate identifying information about the signatory, rendering its evidentiary value limited and difficult to establish before judicial authorities. While it is legally valid, it is generally unsuitable for most commercial transactions.
- **Advanced (Qualified) Electronic Signature:** The data embedded within this signature enables a reliable link to the actual signatory, making it widely used in e-commerce. It is easy to generate, legally secure, and possesses substantial probative value.
- **Qualified Electronic Signature:** This signature necessitates prior verification of the signatory's identity, a procedure that is more time-consuming. Consequently, it is typically employed for contracts that legally require a written form, i.e., contracts that must be signed either on paper or through a qualified electronic signature.

The prospective adoption of qualified electronic signatures in Algeria, coupled with potential amendments to Law N° 15-04, is anticipated to

enhance the development of electronic commerce and digital services. Such measures would secure online transactions and services, both within Algeria and across borders, and would have particular relevance for sectors such as digital banking.

The implementation of electronic signatures in digital banking necessitates reinforced authentication mechanisms, whereby security is ensured through strong, multi-factor authentication, combining[9]:(

- **Possession:** e.g a payment card or SMS code;
- **Knowledge:** e.g a password or PIN;
- **Certified digital identity**, recognized by the competent authorities.

These factors furnish robust evidentiary support in the event of any dispute, with signed documents maintained in secure electronic archiving systems designed in accordance with the highest regulatory and technical standards.

2.2. Mechanism and Verification Process of the Qualified Electronic Signature

In Algerian law, the legislator has established a framework governing the creation and verification of the advanced (qualified) electronic signature under Law N° 15-04 concerning Electronic Signatures and Certification.

Such a signature is produced using secure technological mechanisms that authenticate the identity of the signatory and ensure a verifiable link between the signature and the signed document, thereby preventing any post-execution modification from going undetected.

The authenticity of the qualified electronic signature must be confirmed through a secure electronic certificate issued by a certification authority accredited by the National Electronic Certification Authority. This confers upon the signature the same legal validity as a handwritten signature, rendering the qualified electronic signature a legally reliable instrument for establishing the identity of the signatory and their consent in banking transactions.[10]

3. Legal Considerations for the Digitization of Hand-Signed Documents

Law N° 15-04, regulating electronic signatures and certification, establishes the conditions under which electronic documents are granted legal recognition. The law emphasizes the need to ensure the security,

authenticity, and reliability of electronic documents through the use of electronic signatures and qualified certification. An electronic document is deemed to possess equal evidentiary value to its original paper counterpart, on the condition that:

- The digitization or generation of an electronic document shall be performed by duly authorized personnel, such as a delegate of the entity owning the document, or an individual authorized to provide electronic certification under the applicable certification laws;
- The equivalence of the electronic document to its original paper version must be confirmed through a qualified electronic signature or a qualified electronic seal issued by the authorized person or by a delegate to whom such authority has been lawfully transferred.

Pursuant to Article 323 bis 1 of the amended and supplemented Algerian Civil Code, writing in electronic form is acknowledged as a legally valid form of evidence, equivalent in effect to paper-based writing. The provision emphasizes the necessity of verifying the identity of the issuer of the electronic document to guarantee that it retains the same legal probative value as its handwritten counterpart.

3.1. Digitized Electronic Documents Derived from Original Non-Electronic Records

With respect to electronic documents derived from the digitization of original non-electronic documents, these constitute digital copies of original paper documents bearing handwritten signatures, which are scanned or otherwise digitally captured for storage in electronic form. The term refers to original paper-based documents that carry handwritten signatures and are subsequently scanned or digitally imaged to produce an electronic version suitable for storage or use in digital transactions. Such electronic documents are afforded the same legal probative value as the original paper documents, provided that the digitization is conducted in accordance with approved procedures and under proper supervisory control:(11)

- By a natural person, a person delegated by a natural person in their capacity as a registered entity, or by a person authorized by the legal entity to which the document belongs;

- By an individual authorized to certify signatures, manuscripts, or copies in accordance with the legislation regulating certification procedures;
- By individuals authorized under specific legislation to certify digital documents.

The conformity of the digital document with the original must be verified through a qualified electronic seal or a qualified electronic signature issued by one of the persons referred to in points (1) to (3) above, or by the individual to whom the authority for certifying the document has been delegated.(12)

Accordingly, digitized documents may enjoy the same legal force and evidentiary value as the original paper documents, provided that the digitization and qualified electronic certification procedures are respected, ensuring authenticity and reliability.

Algerian law does not explicitly address the digitization of paper documents and the conferment of the same legal value to the resulting electronic documents. It does not clearly stipulate that paper copies scanned digitally automatically possess the same evidentiary value as the original paper document, as an electronically reproduced copy. From a technical perspective, this process is referred to as digitization, which does not create a new document but rather produces an electronic version of the original paper document. Algerian legislation does not explicitly regulate the conversion of handwritten paper documents into digital copies.

From a legal perspective, the evidentiary value of such a digitized copy depends on the method of digitization and the authority performing it. If the digitization is carried out by an official person or entity (such as a notary or public officer) in a manner that ensures the integrity of the content and prevents alteration, the resulting copy may be recognized as a true replica and relied upon in judicial proceedings.

On the other hand, where digitization is performed by a private individual without official authentication, the legal validity of the electronic copy is limited. Such a copy is regarded solely for reference or informational purposes and does not carry the same evidentiary weight as the original document.

The essential distinction between a digitized copy of a manually signed document and a document signed with a qualified electronic signature is as follows:

- A manually signed document that is subsequently scanned does not contain a verifiable electronic signature, and its authenticity must be confirmed through the original paper document bearing the handwritten signature.
- Conversely, a document executed with a qualified electronic signature incorporates encrypted data that establishes both the signatory's identity and the integrity of the document. Such a document is recognized as a legally valid digital original and is admissible as evidence equivalent to a handwritten document in accordance with Article 323 bis 1 of the Algerian Civil Code.

The conditions for recognizing the equivalent legal validity of a digital document can be highly complex, and in some cases, they may create significant challenges for banks in judicial evidentiary procedures. In Serbia, between 2019 and 2022, banks faced substantial difficulties when clients initiated class-action lawsuits against them over what were perceived as unjustified loan processing fee deductions. During this period, it is estimated that more than 200,000 cases were filed in the courts regarding these disputes.(13)

Several factors contributed to the intensification of this issue. Chief among them is that annulment actions—initiated by clients to challenge specific contractual clauses regarding loan processing fees—are not subject to any statute of limitations or filing deadlines. Consequently, clients were able to bring claims concerning contracts entered into with banks dating back to 2003. (14)

Serbian legislation, under the Electronic Document Act, establishes that an electronic document produced by digitizing an original non-electronic document shall be deemed a copy of the original and enjoy the same legal probative value as the original document, provided certain conditions are fulfilled. These include oversight by an authorized entity

during the digitization process and authentication via a qualified electronic signature or a qualified electronic seal.(15)

In instances where a scanned copy of a document is submitted in lieu of the original as evidence before a court, and the opposing party (the client) raises an objection regarding the signature or the authenticity of the document, Serbian civil procedure law stipulates that, at the request of the objecting party, the court shall order the party presenting the evidence to produce the original document for inspection. A specific deadline is set for compliance, and the ruling on this matter is not subject to appeal (Article 100, paragraphs 3 and 4, Serbian Civil Procedure Code).

3.2. Legal Probative Value of Digitized Documents and the Obligation to Present the Original

According to Serbian law, when the opposing party (e.g a bank or client) challenges the authenticity or validity of a submitted document, the court may order the submitting party to produce the original document. While digital copies are acknowledged as valid evidentiary instruments, the opposing party retains the right to inspect the original in the event of a dispute concerning the document's validity or signature. The court establishes procedural rules to regulate this process, thereby ensuring transparency, legal clarity, and reliability in the treatment of electronic documents compared to their paper counterparts.

Accordingly, in any instance where the authenticity of a document is challenged by the opposing party, the court may order the bank to produce the original document. The bank may inevitably lose the dispute if it is proven that the original has been destroyed, whether due to the expiration of the statutory retention period or because it was digitized and subsequently destroyed without proper certification in compliance with Article 11 of the Serbian Electronic Document Act.

The obligation to produce the original document primarily serves the purpose of allowing technical examination, as handwriting analysis cannot be performed on a copy or digital reproduction but must be conducted on the original.

This procedure is grounded in the necessity of expert evaluation, such as signature verification, which can only be reliably performed on the

original document. From a technical standpoint, the validity of a signature can only be confirmed with the original document present. Should the original be lost or destroyed—whether due to the expiration of the statutory retention period or following digitization without proper certification in accordance with Article 11 of the Serbian Electronic Document Act—the bank is likely to lose the legal dispute due to its inability to establish the authenticity of the document.

This principle is reinforced by a ruling of the Serbian Supreme Court, which held that a handwriting expert examination could not be performed due to the absence of the original document, and that expert reports based on photographic copies are inadmissible, thus preventing the proof of signature forgery.

Consequently, Serbian law emphasizes the importance of preserving original documents and prohibits reliance solely on scanned or digital copies unless they are duly certified through a qualified legal process. The requirement to produce the original arises whenever the opposing party contests the document's authenticity, particularly for the purposes of expert verification. Such measures ensure the integrity of evidence and safeguard legal rights in disputes.

The Supreme Court of Cassation of Serbia confirmed this principle in one of its decisions, reasoning as follows:

"*During the proceedings, the plaintiff proposed a handwriting expert examination to substantiate the claim. However, the examination could not be carried out once it was established that the original will had been lost, and the expert declined to perform the analysis based on a reproduced copy. As the original document could not be located, the plaintiff was unable to conduct the necessary expert evaluation and therefore could not prove that the testator's signature on the will was forged*".)16(

Given that the banks in these disputes did not retain the original documents, as the legally mandated retention period had expired, they lost numerous cases for the following reason:

"*Where the authenticity of a document is contested, and neither the original nor a certified copy of the document is submitted, it is not possible to establish the facts based on such a document, especially when the*

existence and validity of the document are pivotal. Facts cannot be proven using other records or documents".(17)

Consequently, banks should refrain from destroying original documents containing the signatures of clients or agents when these documents are digitized, as doing so may jeopardize their position in future legal proceedings if the digitization is not accompanied by an official certification procedure verifying that the digital copy is faithful to the original.

This requirement does not extend to documents issued by the banks themselves, bearing only employee signatures or official seals. In such cases, courts may admit them as valid evidence, since they do not contain signatures or identifying information of external parties that could subsequently contest their authenticity in litigation.

Moreover, according to Serbian civil procedure law, where the court doubts the authenticity of a given document, it may require the issuing authority to provide a statement confirming its validity (Article 238, paragraph 4, Serbian Civil Procedure Code).

This provision illustrates that a declaration by the bank may be sufficient for the court to accept the document as valid, even in the absence of the original paper version, provided that only a digital copy exists. In such cases, the document contains no third-party signatures that could be contested, but solely the signature of an authorized bank employee or official representative.

Accordingly, it is expected that the certification of digitized paper documents will emerge as a critical legal issue in Algeria in the near future, as current practices are largely absent, the associated procedures are highly complex, and no legally authorized body currently exists to authenticate digital documents converted from paper originals.

4. Electronically Created and Signed Documents

Concerning documents that are electronically created and digitally signed in accordance with the methods established for electronic signatures, Article 25 of the eIDAS Regulation(18)stipulates that the legal effects of an electronic signature shall not be denied, nor may it be refused as evidence in legal proceedings merely because it is in electronic form or does not

satisfy the requirements of a qualified electronic signature. This provision strengthens the principle of legal equivalence between electronic and handwritten signatures.

Within this framework, attention will be given to examining the mechanisms for implementing electronic signatures in the banking sector, noting that two primary methods are commonly employed for electronically signing banking transactions, each varying in terms of security level and legal probative force.

4.1. Mechanisms for the Establishment of an Electronic Signature

for electronically capturing handwritten signatures. The device operates as an external input tool that digitizes a handwritten signature via a specialized sensor, analogous to a laptop touchpad, and is used with a dedicated electronic pen.(19)

Through this technology, the client signs by hand on a designated surface, with the device accurately recording all pen movements and pressure, producing a signature nearly identical in appearance to the handwritten original. Notably, the signature leaves no physical mark on paper; it is automatically converted into an electronic format, directly embedded in the document being signed, and permanently stored in the digital system.(20)

The security of this electronic signature method is ensured by the device's ability to record the time of signing and technical metadata; however, such data may remain within the internal system rather than being embedded directly in the document.

This signature method closely follows the conventional paper-based signing procedure, facilitating client acceptance, especially in banks transitioning gradually to digital operations or in fully digital banks. Its main advantage lies in its simplicity and speed, requiring no additional time beyond that of a traditional handwritten signature.

Furthermore, these devices can compare the newly captured signature with a previously stored signature (if the client has signed documents with the bank before) and can reject the signature or trigger further verification by a bank officer if it does not sufficiently match the stored original.

A particularly common use of this type of electronic signature concerns withdrawals or transfers from password-protected savings accounts, typically secured with a one- or two-word password.

The client enters the password via the digital signature pad, and the system then compares the newly captured signature with the previously stored version. Password recognition is performed using Optical Character Recognition technology, while handwriting analysis is conducted to assess correspondence with prior samples and determine the level of match.(21)

This type of electronic signature, implemented via a digital signature pen, is simple to execute and requires no more time than the client's conventional handwritten signature on paper. The devices provide the capability to compare the newly captured signature with a previously stored one; in cases of insufficient correspondence, the signature is either rejected or subjected to further verification by a bank officer.

It is noteworthy that for such accounts, a person other than the account holder may effectuate a withdrawal if the password is known. In these circumstances, entering the password through the digital signature pad records the handwriting of the individual, which subsequently allows, in the event of a legal dispute, the conduct of forensic handwriting analysis to establish the identity of the person who actually input the password.

A key legal question arises regarding the feasibility of performing forensic handwriting examination on this type of document if a client disputes the authenticity of their signature, conducted by technical experts officially accredited by Algerian courts. The handwriting expert is obliged to carry out the analysis, as the document was not first created on paper and subsequently digitized; rather, it was originally generated in digital format, including the signature itself, which was manually input via an electronic device and automatically converted into a digital format embedded within the document.

Accordingly, the expert may compare this electronic signature with the client's prior handwritten signatures by examining features such as letter size, character formation, inter-word spacing, and pen pressure during signing, all of which are technical parameters captured by the device.

Nevertheless, the examination should not be conducted solely by a handwriting expert; it must also involve an information technology specialist.

While the handwriting expert can identify forgeries arising from manual or mechanical manipulation, they cannot detect alterations made digitally through software or computational means. Hence, the forensic analysis must be dual—technical and handwriting-based—to guarantee both the accuracy of the verification and the legal probative value of the electronic signature.

It may be observed that establishing the authenticity of a digital element does not depend on the presence of a "material original," as is the case with paper documents. Instead, it hinges on the reliability of the technical evidence provided. The legal focus is not on demonstrating the physical existence of an original, but on furnishing sufficient evidence to satisfy the court that the digital copy accurately reflects the content of the original or the version genuinely utilized by the signatory.

4.2. Electronic Signature in the Banking Sector

The procedure is structured around three simple yet highly secure steps:(22)

- **Document creation and transmission:** A digital document is generated via a secure platform and delivered to the client electronically, typically by email.
- **Signature and authentication:** The client executes the signature after verifying their identity. Authentication may be conducted through SMS codes, payment cards, identity cards, or a certified digital identity.
- **Secure archiving:** Following the signature, the document is preserved in an electronic archiving system hosted on a server that complies with established information security standards.
- **Additional channels:** Clients may alternatively provide their electronic signatures via mobile banking (m-banking) or online banking (e-banking) platforms.

In the context of the banking sector, this type of electronic signature mentioned above has several practical and legal limitations that should be noted:

- **Restricted use within bank branches:** Digital pen pad devices can only be used on-site within bank branches, as each device is directly linked to the bank's computer system and contains identifying data that can later be used to determine the device through which the signature was made. This data may serve as legal evidence in court. Consequently, clients cannot sign remotely using this type of device.(23)
- **Time-consuming for clients:** The system requires the client to be physically present at the bank branch to sign the document, which conflicts with the speed and flexibility objectives pursued by digital banking services.
- **Not a qualified electronic signature:** This type of signature does not qualify as a Qualified Electronic Signature, because the device is not issued by a certified trust service provider, nor does it provide biometric verification (such as fingerprint or facial recognition) prior to permitting the signature. While bank staff do verify the client's identity using official documents, this does not replace the legally recognized technical verification required for a qualified electronic signature, which ensures strong authentication of the signer's identity.

Another legal issue arises regarding the fulfillment of the "writing" requirement in contracts, as the declaration or contractual text does not appear on the digital signature pad but on the computer screen. Consequently, the signature is not placed directly beneath the legal text as it would be in paper documents. Therefore, laws concerning the bank's duty to inform the client and third parties should be adapted to this type of signature. Nevertheless, the prevailing opinion is that this type of signature satisfies the requirements of the written form, since the signatory's intent is clearly expressed by executing the signature on the electronic document within the banking system.(24)

It is thus crucial in banking applications and digital banks to separate the stages of reviewing the document's content and signing it. If the

processes of authentication, review, and signature are combined into a single procedure, the client could later claim that the signature was made inadvertently during the review, attempting to argue a lack of genuine consent in concluding the contract.

It is likely that this type of signature will be classified as a qualified electronic signature in the future upon the establishment of digital banks. However, the Algerian banking sector must address the current technical and regulatory shortcomings, particularly regarding biometric verification and the digital authentication of the user's identity.

4.3. Legal and Operational Characteristics of Electronic Signatures in the Banking Sector

Thanks to the effective implementation of electronic signatures within banking systems, clients are now able to sign and validate various types of documents and transactions easily, at any time of the day, without the need to physically visit the bank.(25)

The validity of an electronic signature relies on the verification of the accompanying qualified electronic certification. A signature is considered valid as long as the certificate is qualified and issued by a trusted third party or an accredited electronic certification service provider, in accordance with the approved electronic certification policy, and is granted exclusively to the signer. The certificate must particularly include:

a. An indication that the certificate has been issued as a qualified electronic certification**;**
b. Identification of the trusted third party or licensed electronic certification service provider that issued the certificate, including the country of their residence;
c. The name of the signer or an alias allowing their identification;
d. The possibility of including a special attribute for the signer, if applicable, depending on the purpose of using the electronic certification;
e. Data related to the verification of the electronic signature, consistent with the signature creation data;

f. Reference to the start and end dates of the electronic certification's validity;
g. The unique identification code of the electronic certification;
h. The qualified electronic signature of the certification service provider or the trusted third party issuing the electronic certification;
i. The limits on the use of the electronic certification;
j. The limits on the value of transactions for which the electronic certification may be used, where applicable;
k. Reference to the document evidencing representation of a natural or legal person, where applicable.(26)

Therefore, the certificate meeting all these requirements must be valid at the time of signing, and the verification data must correspond to the data provided to the counterparty. Additionally, a set of unique data representing the signer, as specified in the electronic certificate, must be present. The integrity of the signed data remains guaranteed as long as the qualified signature creation device is actually used and all requirements of the qualified electronic signature are fulfilled, thereby preventing any manipulation or breach.(27)

Therefore, for a signature executed via a mobile banking application (m-banking), a digital bank platform, or an online banking service (e-banking) to have legal effect equivalent to a qualified electronic signature, these platforms must incorporate a qualified remote signature creation tool and be equipped with a qualified electronic certificate issued by authorized bodies as provided for under Law N° 15-04.

Since banks are not authorized to provide trust services themselves, it becomes essential that, when developing mobile banking (m-banking) applications, online banking platforms, or digital banks (e-banking), qualified trust service providers participate in the development of these applications or platforms and assist digital banks, in accordance with the provisions set by the Algerian legislator. In this manner, banks are able to implement a qualified electronic signature based on a smart card, USB token, or cloud service. Considering that banks continually seek efficiency

and speed in executing electronic signatures, the most common method for implementing a qualified signature is through cloud-based solutions.(28)

In this system, the entire electronic file is stored on a secure cloud server, thereby mitigating the risk of losing the private encryption key when it is in the form of a smart card or USB token.

The client receives the document to be signed through the mobile or digital banking application, where they can fully review its content. At the moment of signing, the client's identity is verified through multiple authentication methods, such as:

- Entering an additional code sent to the client via SMS or email, as part of a Two-Factor Authentication system;
- Biometric authentication, such as facial recognition or fingerprint scanning;
- In combination with the application PIN or the user's platform-specific password.

This approach ensures a high level of security and reliability in the creation of a qualified electronic signature, safeguarding the client's digital identity and reinforcing the legal probative value of the signature.(29)

Another method for verifying the client's identity is through a live video call conducted between the client and a bank employee when opening a new bank account. During this session, the client is required to present their identity card to the camera and perform certain head movements or hand gestures, enabling the bank employee to ensure that the interaction occurs in real-time rather than via a pre-recorded video.

At the same time, it is important to note the increasing use of artificial intelligence technologies, which could potentially be misused in such identity verification procedures, thereby posing risks to the reliability and credibility of electronic identification processes.(30)

Given the dual nature of artificial intelligence, encompassing both its immense capabilities and the potential risks it entails, it is entirely reasonable to anticipate the enactment of new legislation or amendments to existing laws in the near future. These legal developments are expected to aim at a more precise and stringent regulation of electronic signature mechanisms and personal identity verification procedures, ensuring a

balanced approach that safeguards technological innovation, data protection, and legal security.

The benefits of electronic signatures for digital banks include:

- **Enhanced customer experience**: Electronic signatures allow clients to sign their documents anytime and anywhere, whether via smart phone, tablet, or computer, eliminating the need to visit a branch or wait for procedures to be completed.
- **Significant cost savings**: The elimination of printing, postal delivery, and paper archiving substantially reduces operational costs. Moreover, digitization saves valuable time for internal teams.
- **Increased employee productivity**: Electronic signatures enhance productivity through automated processes, enabling employees to free their time from repetitive administrative tasks and focus on providing advisory services and strengthening customer relationships.
- **Reduced environmental impact**: The use of digital documents and the elimination of paper support corporate social responsibility policies for banks and help reduce their environmental footprint.

5. CONCLUSION

In light of the foregoing, it is evident that the electronic signature has evolved beyond being a mere technical tool for reducing paper usage; it has become a pivotal element in building digital trust within the modern banking environment. It simultaneously fulfills legal compliance and transparency requirements, while enhancing speed, efficiency, and customer experience. With the rapid shift toward digital banking services, the adoption of electronic signatures has become a strategic necessity, indispensable for both traditional banks seeking modernization and digital banks that base their identity on innovation and full reliance on digital solutions.

This study has reached the following conclusions:

- Electronic signatures in digital banking represent an inevitable evolution for the banking sector, serving as an effective legal tool that reinforces trust in digital banking transactions and forms a fundamental component in the transition toward digital banking.

- Electronic signatures combine performance, security, and compliance, making them an essential instrument for digital banks, enabling them to consistently meet customer expectations while adhering to the highest standards.
- The implementation of qualified electronic signatures in the banking sector depends on partnerships with trusted third parties or certified electronic trust service providers, which are authorized to issue electronic certification to ensure the legal and technical security of electronic signatures.
- The Algerian legislator must consider these modern applications by providing a regulatory framework for secure electronic identity verification, as this raises challenges regarding the need to update legislative frameworks to keep pace with technological developments and to anticipate emerging technical and legal challenges posed by the use of artificial intelligence as a means of identity verification or as a potential tool for fraud.

6. Endnotes

[1]- Mabrouk Belazzem, Financial Inclusion in Monetary and Banking Law, Journal of Legal Studies and Researches, Vol. 9 No. 2, 2024, p 101.

[2]-Law n° 23-09 of 21 June 2023 Relating to Money and Banking Law, Official Journal of the Algerian Republic. N° 43 is dated 27 June 2023, P04.

[3]-Law n° 15-04 of 01 November 2015 Relating on Electronic Signature and Electronic Certification, Official Journal of the Algerian Republic. N° 06 is dated 10 November 2023, P04.

[4] -Fatima-zohra Messedek.(2020), Electronic Authentication as a Means of Protecting electronic signature, Journal of Legal Studies and Researches, Vol. 5, No. 1, p 33.

[5] -Quelle est la valeur juridique d'une signature électronique?,(2024), https://www.docaposte.com/blog/article/valeur-juridique-signature-electronique, (Consulted on 11/03/2025).

[6]-Article 15 of Law No. 15-04.

[7]-Maria Angela Biasiotti, (2017). A proposed electronic evidence exchange across the European Union, Digital Evidence and Electronic Signature Law Review (14), p 03.

[8] -Thomas J., Smedinghoff; Ruth Hill, Bro (1999), Moving with Change: Electronic Signature Legislation as a Vehicle for Advancing E-Commerce. UIC John Marshall Journal of Information Technology & Privacy Law, Vol. 17, No. 03, p 728.

[9]-Lea Vaquero, (2025),Pourquoi la signature électronique est essentielle pour le secteur bancaire?,https://www.oodrive.com/fr/blog/signatureelectronique/secteurs-metiers/signature-electronique-banque/ ,(Consulted on 11/04/2025)

[10]-Articles 10 and 11, Law No. 15-04.

[11] -Sead Kadrić, Imran Rašljanin, (2024), LEGAL ASPECTS OF IMPLEMENTING DIGITAL SIGNATURES IN PAPERLESS BANKING, Facta Universitatis, Law and Politics , Vol. 22, No. 01, p 60.

[12]- Ibid.

[13]- Daniela Ilić Krasić, (2022), The Banking Association: Thousands of Review Proceedings before the Supreme Court, https://n1info.rs/biznis/udruzenje-banaka-pred-vrhovnim-sudom-nekoliko-hiljada-postupaka-revizije/, (Consulted on le 11/04/2025).

[14]- Ibid.

[15]- Ibid.

[16]-Judgment of Supreme Court of Cassation, (2021), Rev 4898/2020, Serbia.

[17]- Judgment of Higher Court. (2022). Court of Appeal of Novi Pazar, Case No Gž 504/22, Serbia.

[18]- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, repealing Directive 1999/93/EC (eIDAS).

[19]- Sead Kadrić, Imran Rašljanin, op.cit, p 62.

[20]- Sead Kadrić, Imran Rašljanin, op.cit, p 62.

[21]-Ibid, p 64.

[22]- Lea Vaquero, op.cit.

[23]-Ibid.

[24]- Sead Kadrić, Imran Rašljanin, op.cit, p 66.

[25] -Danica Lecic-Cvetkovic, Jasmina Omerbegovic-Bijelovic, Sanja Zaric; Radmila Janicic (2015), E-banking application in business companies – A case study of Serbia. Information Development, Vol. 32, No. 04, p 765.

[26]- Article 15, Law N° 15-04.

[27]-Vukotić, J. (2021). Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation), adopted by the European Parliament and the Council. , Vol. 20, No. 75, p153.

[28]- Sead Kadrić, Imran Rašljanin, op.cit, p 64.

[29]-Đurić, D, (2021). Elektronski potpis i zašto ga (ne) primjenjujemo (Electronic Signature and why do we (do not). Godišnjak Pravnog fakulteta u Banjaluci , Vol. 43, No. 43, p 90.

[30]-Boljanović, V. (2019), Elektronski potpis u Srbiji i harmonizacija sa pravom Evropske unije: mogućnosti i izazovi (Electronic Signature in Serbia and Harmonization with EU Law: Possibilities and Challenges),University of Belgrade, Serbia, p 31.