JURNAL HUKUM NOVELTY
Volume 16, Issue 1, 2025, pp. 120-139
P-ISSN: 1412-6834
E-ISSN: 2550-0090

The legal effect of electronic bonds lacking an authenticated signature in Jordanian legislation

Ahmad Albnian[1*], Ali Al-Hammouri[2], Tareq Al-Billeh[2], Mohammed Al Makhmari[3], Roua Belghit[4], Mohammed Chakib Himmich[5]

[1] *Faculty of Law, Zarqa University, Jordan*
[2] *Faculty of Law, Applied Science Private University, Jordan*
[3] *Faculty of Law, Sohar University, Oman*
[4] *Faculty of Law, Larbi Tebesi University, Algeria*
[5] *Faculty of Law, University Ibn Tofail, Morocco*

*Corresponding Author: *aalbnian@zu.edu.jo*

Abstract

Introduction to the Problem: This study examines the Jordanian legislator's stance on the conditions for electronic signatures, as outlined in the Electronic Transactions Law and the Jordanian Evidence Law. It aims to assess the consistency between the two laws, particularly since the Electronic Transactions Law specifies requirements for electronic signatures, while the Evidence Law remains silent on such conditions.
Purpose/Objective Study: This study aims to examine how the recognition and enforceability of electronic bonds vary depending on the type of electronic signature used—specifically comparing authenticated and secured signatures versus unauthenticated yet secured signatures. The analysis will assess the impact of these signatures on the validity and legal standing of electronic bonds, similar to how handwritten signatures affect traditional bonds. Identifying gaps in this relationship will help address potential shortcomings in ensuring authenticity and legal compliance.
Design/Methodology/Approach: In this study, we follow two approaches: the descriptive approach in presenting electronic bonds, their types, protection, the validity of an authenticated and protected electronic signature in one hand, and the unauthenticated and unprotected electronic signature. The analytical approach was also relied on. The legal texts regulating the process of electronic bonds and electronic signatures will be reviewed, analyzed, and compared with other laws.
Findings: The study highlights how electronic authentication can streamline international trade by reducing documentation costs, provided legal frameworks ensure security and reliability. While Jordan's Electronic Transactions Law grants e-signatures legal validity, gaps remain in regulating authentication entities. Key recommendations include: (1) establishing an 'electronic examiner' to verify signatures, (2) clarifying certification providers' liability for data protection, and (3) formalizing government-contractor agreements for authentication services.

JURNAL HUKUM
NOVELTY
Volume 16, Issue 1, 2025, pp. 120-139

P-ISSN: 1412-6834
E-ISSN: 2550-0090

Strengthening judicial training on digital transactions is also advised to enhance enforcement.

Paper Type: Research Article
Keywords: Electronic Bond; Electronic Signature; Authenticated Symbols; Digital Transactions

Introduction

In an era characterized by technological advancements, particularly the swift advancement of electronic information technology, a multitude of electronic gadgets has been created for diverse application domains. This technologically-assisted equipment significantly impacts the lifestyle of all creatures, especially humans. Moreover, technology has facilitated the ability for individuals to write on electronic devices, as these gadgets produce electronic signature handwriting that is highly beneficial (Ruiz-Martínez et al., 2007). They can proficiently address the electronization of conventional handwritten signatures and alleviate the challenges associated with verifying the identity of the signatory of electronic papers when utilized alongside electronic documents. This approach is commonly employed in e-government, e-commerce, banking and insurance, healthcare, and various other sectors (Feng & Zhang, 2022).

Electronic bonds and signatures have emerged due to innovations in modern communication and the global shift toward digital transactions. The authenticity of electronic bonds and signatures has garnered close attention from lawmakers, especially regarding their legality and recognition in the legal protection of electronic transactions (Al-Bashkani, 2009). Many states have revised or amended existing legal frameworks governing judicial processes and legislation to keep abreast of digital-age developments and leverage contemporary communication methods (Hegazy, 2003).

For the purpose of associating electronic information with particular individuals or entities, ensuring the integrity of that information, and enabling individuals to verify their entitlement or authorization for access to particular services or information repositories, numerous methods have been developed as a result of the development of information and computer technology. Moreover, the term "authentication" is occasionally employed broadly to refer to any assurance of both authorship and integrity of material; however, certain legal systems may differentiate between these features. A brief summary of terminological and legal distinctions is essential to delineate the scope of this document (Al-Kilani, 2021).

Article History
Submitted 13 July 2024 - Revision Required 30 December 2024 - Accepted 30 April 2025

JURNAL HUKUM NOVELTY
Volume 16, Issue 1, 2025, pp. 120-139
P-ISSN: 1412-6834
E-ISSN: 2550-0090

Undoubtedly, several debates have been raised regarding electronic bonds and electronic signatures, for instance, their probative value or attempt to question the authenticity of the data or the signatures and whether the electronic signatures have the same authenticity as signatures in the provisions of the Evidence Law (Al-Arayshi, 2016).

In conjunction with contemporary advancements, particularly in technology, notaries are required to perform their responsibilities more effectively and efficiently by leveraging available technology. It is recognized that in electronic transactions, electronic signatures (digital signatures) are increasingly substituting traditional signatures on paper. An electronic signature is essential for preserving the legitimacy of an electronic document. Nevertheless, during its development, numerous instances of signature forgery were identified, leading to financial losses for one party involved in the transaction (Sari et al., 2023).

Therefore, purpose of a signature is to identify the signatory and convey their intent, as it reflects the will of its owner. Consequently, it must be executed by an individual possessing full legal capacity. A document is not deemed complete evidence unless it bears a signature. The signature constitutes the second element of written evidence intended for verification. In the absence of a signature, written evidence forfeits its validity. The signature associates the document with the individual who signed it, regardless of whether it is inscribed in another's handwriting (Massad, 2022).

It is worth noting that the electronic signature may come in different forms: unauthenticated, protected and unauthenticated, or unauthenticated and unprotected (Al-Kilani, 2021). The strength of the electronic document varies depending on the forms of these signatures. In this study, we will discuss the previous concerns analytically (Al-Momani, 2003).

The electronic bond has a prominent role in legal transactions, and this is a fact that cannot be denied. Nevertheless, the legality of electronic bonds and electronic signatures has been a subject of debate. The debate often revolves around several issues, for example, its authenticity, whether it should be legally recognized as equivalent to its paper-based counterparts, and its probative value to prove (Rabadi, 2012). Laws and regulations in different jurisdictions have varied in their approach to this issue, with some fully recognizing electronic signatures while others have imposed restrictions. Hence, their validity must be examined, especially since legislation has varied in determining its forms, effect, and the extent of the authority of an unauthenticated electronic signature and resolving its ambiguity. This study attempts to highlight this issue in Jordanian legislation, hoping that lawmakers and scholars will benefit from the results of this study (Caprioli, 2014; Al-Billeh, 2024).

The authenticity, recognition, and scope of the applicability of electronic bonds vary according to the form of the electronic signature, whether it is authenticated and protected or unauthenticated and protected. This link mainly determines the extent

JURNAL HUKUM NOVELTY
Volume 16, Issue 1, 2025, pp. 120-139
P-ISSN: 1412-6834
E-ISSN: 2550-0090

of the authenticity of the electronic bond and its legal effect. Therefore, this link should be evaluated and solve its shortcomings (Casamento & Hatfield, 2014).

The preceding discussion illustrates that the concepts of signature and authentication are not consistently comprehended and that their purposes differ throughout legal systems. Notwithstanding these discrepancies, certain overarching commonalities may be identified. The concepts of "authentication" and "authenticity" in legal contexts pertain to the genuineness of a document or record, indicating that the document is the "original" source of the information it encompasses, in its recorded form and without any modifications (Tengku & Wan, 2019).

Methodology

In this study, we follow two approaches: the descriptive approach in presenting electronic bonds, their types, protection, the validity of an authenticated and protected electronic signature in one hand, and the unauthenticated and unprotected electronic signature. The analytical approach was also relied on. The legal texts regulating the process of electronic bonds and electronic signatures will be reviewed, analyzed, and compared with other laws.

An electronic signature can possess either a high level of security or a low level of security. If the document is not encrypted, there is a possibility that the signature has been altered (Krawczyk, 2014). An electronic signature is a method of adding authentication to an electronic document, whereas a digital signature is a particular type of electronic signature that uses encryption. A digital signature is a kind of data that is attached to or transformed via cryptography, and it enables the recipient of the data to verify both its source and integrity (Elsonbaty, 2014).

The determination of whether an individual allowed a specific transaction using a electronic signature will depend on the presentation of evidence (Elsonbaty, 2014; AL-Khalaileh et al., 2024). The electronic signature is distinct and frequently targeted for theft. In most instances, the act of affixing one's electronic signature is not typically the primary concern. Nevertheless, there exist some controversies about the act of withdrawing money from bank Automated Teller Machines (ATMs). When a bank provides a card with an embedded chip, the chip stores the private key used for a digital signature (Krawczyk, 2014).

Results and Discussion

Electronic Bonds

The facility modern technology has provided for contractual parties via the Internet, such as extracting electronic bonds easily and faster, has encouraged parties to contract to use this method widely; therefore, the conditions under concluding this type of contract and its legality should be examined (Mason, 2014).

Article History
Submitted 13 July 2024 - Revision Required 30 December 2024 - Accepted 30 April 2025

JURNAL HUKUM NOVELTY
Volume 16, Issue 1, 2025, pp. 120-139
P-ISSN: 1412-6834
E-ISSN: 2550-0090

Currently, electronic signatures are extensively utilized throughout multiple industries, notably in banking, finance, insurance, and other sectors. Electronic signatures differ from digital signatures, the latter being a cryptographic method commonly employed to facilitate electronic signatures. Although an electronic signature may merely consist of a name in a digital document, digital signatures are progressively employed in e-commerce and regulatory submissions to facilitate electronic signatures in a cryptographically secure fashion. An electronic signature, or e-signature, is data that is logically associated with other data and employed by the signatory to authenticate the linked data. This type of signature holds equivalent legal validity to a handwritten signature, provided it adheres to the stipulations of the relevant rule under which it was created. Given its extensive application, several individuals have started to inquire about the distinctions between electronic signature tracks and conventional signature tracks, aiming to mitigate any adverse effects stemming from significant disparities between the two (Lubis, 2021).

Defining the Electronic Bond

Defining the electronic bond requires recognizing the concept of an electronic record that contains the electronic bond. In the following subsections, we will define the electronic bond and record from this standpoint (Martin & Pascarelli, 2014).

In jurisprudence, an electronic bond is defined as a bond created electronically. It represents the obligation of its initiator towards the other party in such a way that this bond is transferable. Or it is electronic information sent or received by electronic means, regardless of the means of obtaining it in the place of receipt. It is every electronic means used in electronic transactions that can be invoked or resorted to for purposes of proof, including electronic messages, electronic records, contracts, and bonds (Linh, 2014). Based on the definition, we can hold that it is traded electronically, and its data is a kind of information message created using electrical, magnetic, optical, electromagnetic, or any similar means (Al-Billeh, 2022; Tengku & Wan, 2019).

An electronic bond is defined by the Jordanian Electronic Transactions Law No. 15 of 2015 and its amendments as "A bond that is created, signed, and dealt with electronically." In the UNCITRAL Law on Electronic Commerce 2001, Article 2, an electronic bond is referred to as a "Data message". Which is described as "information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy." However, under Article 1, in the Egyptian Law No. 15 of 2004, Regulating Electronic Signature, it is termed "Electronic Document." It is though defined as "A data message comprising information originated, merged, stored, sent or received, wholly or partially, by an electronic, digital, or light method, or any other similar means."

JURNAL HUKUM NOVELTY
Volume 16, Issue 1, 2025, pp. 120-139
P-ISSN: 1412-6834
E-ISSN: 2550-0090

Article 9 in the Jordanian Electronic Transactions Law No. 15 of 2015 stipulates, "the information message shall be deemed as a means of expressing the will legally admissible to convey offer or acceptance for establishing a contractual intent." Accordingly, this text conveys that if the information message satisfies the legal obligations for an offer and acceptance, it shall be regarded as an electronic bond, leading to a legally binding obligation.

Electronic records are a record or a register created, sent, stored, or received via electronic means or other similar means. This record is comparable to the paper record that the vendor uses in daily transactions and is saved on the computer instead of paper records. Electronic bonds are kept within what is called the electronic register (Casamento & Hatfield, 2014). This implies that the electronic bond is integral to the electronic record. For more explanation, let's examine Article 8 of the Jordanian Electronic Transactions Law, which states that: "If the law stipulates the retention of a [written] document for any reason, its retention in the form of an electronic record shall have the same legal consequences, provided that the electronic record fulfills the conditions stipulated in Article 7 of this law."

Conditions in Article 7(a) of the same law indicate the following:

> "If any legislation requires the submission of the original copy of the register, contract, document, or certificate, the electronic record shall have the strength of the original if it fulfills the following: 1. Retained in the form it had been generated, sent, or received and in a way that does not allow making any modification or change on its content; 2. Retained in an accessible form to enable easy access to the information contained therein and to use such information and refer to it at any time; 3. Enable recognizing the initiator, addressee, and the date and time when the record was initiated, sent, or received."

Article 7(b) of the same law specify that: "The conditions stipulated in paragraph (a) of this Article shall not apply to the information attached to the electronic record if the purpose of such information is to facilitate the sending and receiving of the electronic record". Then Article 7(c) stated: "The initiator or addressee may prove the conditions stipulated in paragraph (a) of this Article through any types of proofs with due regard to the principles stipulated in the relevant laws."

It is important to highlight that in reference to Article 6 of the Electronic Transactions Law, the Jordanian legislator deemed electronic documents, contracts, and bonds within electronic records to have legal consequences as in written contracts and documents, as explicitly outlined therein. Article 6 specifies that:

> "With regard to the provisions of paragraph (b) of Article (3) of this law if any legislation requires the submission of any register, contract, document, or certificate in writing, the submission of its electronic record shall have the same legal consequences under the following conditions: a. The information stated in the electronic record may be accessed. b. The possibility of storing the electronic record and the ability to refer to it at any time without making any changes to it."

Article History
Submitted 13 July 2024 - Revision Required 30 December 2024 - Accepted 30 April 2025

JURNAL HUKUM NOVELTY
Volume 16, Issue 1, 2025, pp. 120-139
P-ISSN: 1412-6834
E-ISSN: 2550-0090

Nevertheless, legal and technical conditions must be available to legitimize the electronic bond and consider it producing its legal effects.

Conditions of Electronic Bond

The electronic bond must meet two basic conditions: electronic writing and signature. Electronic writing consists of symbols, letters, or numbers that form an algorithm implemented through data entry and output operations in the computer (Al-Billeh et al., 2023). This is done by providing the device with this information through the input units, and this writing is stored on a magnetic tape, CD, digital disk, or any other perceptible means. Electronic writing depends on its ability to be stored and preserved electronically and its stability and continuity. Under these conditions, electronic writing gives electronic bonds legal authority on par with a traditional written bond (Al-Billeh, 2023; Qouteshat, 2016).

An electronic signature is a digital representation of a person's signature initiated by different means and used to sign electronic documents and records. It serves a person's intent to agree to the content of an electronic document, just like a handwritten signature does on a physical paper document (Khashashneh et al., 2023). It derives from computer data storage media, contains information and saved data, is readable and written, and is legally protected against electronic pirate activities (Al-Khawajah et al., 2023).

The use of handwritten electronic signatures has proliferated across diverse applications, resulting in heightened demand for identification. In contrast to handwritten signatures, handwritten electronic signatures provide the benefit of capturing dynamic feature data, such as pressure, velocity, and acceleration of the writing (Yang et al., 2024).

According to the UNCITRAL Uniform Rules for Electronic Signatures, an electronic signature is any data in electronic form that is affixed to, included in, or logically connected to a data message. It serves to determine the signatory's identity in connection with the data message and to show that the signatory agrees with the information in the data message (Monaghan, 2022).

The Jordanian legislature has acknowledged the legitimacy of electronically organized bonds and accords them with the same legal status and strength as conventional regular bonds. He did not confine it to a particular method. This authority can be found in the Jordanian Evidence Law, which states it is part of the proof-based evidence. Article 13 of the Evidence Law specifies that:

1. Signed correspondence has the same probative force as a means of proof as an informal document unless the signatory proves that he did not send or assign anyone to send them.
2. The same probative force will apply to telegrams if the original, left at the office of dispatch, is signed by the sender.

JURNAL HUKUM
NOVELTY
Volume 16, Issue 1, 2025, pp. 120-139
P-ISSN: 1412-6834
E-ISSN: 2550-0090

3. a. With regard to the provisions of this paragraph, faxes, telexes, e-mails, and similar modern means of communication shall have the same probative force as common bonds have if they are accompanied by the testimony of the person who sent them to support their issuance or the testimony of the person to whom they were received to support his receipt of them unless proven otherwise; b. E-mail correspondence has the probative force as a means of proof without being accompanied by a certificate if they meet the conditions required by the in force electronic transactions law; c. Data transferred or saved using modern technologies using a secret number agreed upon between the parties will be deemed evidence for each party. They can be used to prove the transactions that took place based on that data; d. Certified or signed computer outputs have the same probative value unless the person to whom they are attributed proves that he did not extract, authenticate, sign, or assign anyone to do so.

The type of electronic data that forms the basis of an electronic signature is what distinguishes it from a traditional signature. In contrast to a handwritten signature, which is easily falsified, an electronic signature unquestionably offers a high level of security, privacy, and protection. The foundation of an electronic signature is a collection of codes, symbols, and numbers that only the owner knows what they imply. This is essentially different from a conventional hand-gesture-based signature. An electronic signature is a useful tool for recording transactions carried out via electronic media.

The Jordanian judiciary has recognized electronic messages as evidence of probative value in many of its rulings. In a ruling by the Jordanian Court of Cassation, it was stated,

> "And since electronic messages serve as evidence in this case, the two parties, within the general conditions, have agreed that messages via e-mail, fax, and signature are the method of communication and dealing between them to complete the project, and they serve as evidence following the provisions of Article 13C from the law of evidence."

The Jordanian legislator also allocated by-laws in the Electronic Transactions Law that dealt with the electronic bond, trying to remove ambiguity and clarify its provisions, as stipulated in Article 18:

> "a. The electronic bond shall be transferable if the conditions of a negotiable bond apply to it following the provisions of the Commercial law, except the condition of writing, provided that the drawer has approved its negotiability; b. The holder of the electronic bond shall have the authority over the transferable electronic bond if the drawer has approved the negotiability of such bond and provided that it has an authenticated electronic signature."

An electronic bond is a bond that is initiated using electronic means and represents the obligation of the initiator over the other party in such a way that this bond is transferable and negotiable. In the case of an electronic bond, the same conditions

Article History
Submitted 13 July 2024 - Revision Required 30 December 2024 - Accepted 30 April 2025

JURNAL HUKUM NOVELTY
Volume 16, Issue 1, 2025, pp. 120-139
P-ISSN: 1412-6834
E-ISSN: 2550-0090

apply to a regular bond under the Jordanian Commercial Law for bills of exchange, promissory notes, and checks, except for the writing requirement.

The Jordanian Electronic Transactions Law has specified the requirements for considering the electronic bond transferable that grants rights and establishes obligations comparable to those of a traditional bond. Article 19 specifies that:

> "Unless agreed otherwise, the holder of an electronic bond shall have the authority over a transferable bond and shall have the same rights and claims entitled to the ordinary bond holder following any legislation in force, provided that it met all conditions stipulated thereof."

However, if we examined Article 20 of the same law, it also granted the debtor of a transferable electronic bond the same right as the debtor of a paper negotiable bond. Article 20 states, "The debtor of a transferable electronic bond shall enjoy the same rights and claims enjoyed by a debtor of a paper negotiable bond."

The method of delivering the electronic bond is established as follows: the initiator sends the information message to the other party via an electronic means that expresses his will to conclude the contract and is considered an offer (Caprioli, 2014). The electronic bond is ascribed to the initiator unless the latter proves the opposite, as ascribing the bond to the initiator is a simple legal presumption that can be proven to the contrary under the text of Articles 9 and 10 of the Electronic Transactions Law, which Article 9 stipulates: "The information message shall be deemed as a mean of expressing the will legally admissible to convey offer or acceptance for establishing a contractual intent." Article 10 of the same law stipulates that:

> "The information message shall be deemed to be issued by the Initiator whether it was sent by the initiator for his/ her account, by a person working on his/ her behalf, or by an electronic intermediary that is set to work automatically in the initiator's name or on his/ her behalf."

We argue here that since signed electronic bonds are equivalent to traditional bonds in value and authenticity, they are deniable, and the allegation of forgery is acceptable. If the electronic bond is denied, the court must investigate any technical work to prove the authenticity of the electronic bond (Rabadi, 2012).

It is worth noting that regarding judicial precedents, the courts recognized the validity of the electronic bond as the identity of the initiator is acknowledged. The Court of First Instance for the Province of New Brunswick in Canada ruled in the ruling issued on 26 April 2012, specifies that

> "The electronic correspondence exchanged between the two opponents resulted in the conclusion of a binding contract, and it also confirmed that the e-mail messages contained the essential terms of the agreement and that the electronic correspondence met the requirements for a sales contract because they were received in written form."

JURNAL HUKUM NOVELTY
Volume 16, Issue 1, 2025, pp. 120-139
P-ISSN: 1412-6834
E-ISSN: 2550-0090

Conditions of Electronic Signature

A signature is traditionally defined as any character created with the intention of endorsing a document. Nonetheless, the global information technology revolution necessitates the adoption of electronic signatures in place of traditional ink-based signatures. The utilization of electronic signatures is not as straightforward as that of ink signatures, since it encounters both technological and legal obstacles. States are legalizing electronic signatures by introducing legislation to overcome legal problems (Haileyesus, 2021).

Traditional signatures are created using different methods. They can be handwritten signatures using a pen, a personal mark affixed to the paper document, fingerprints, or symbols stamped by a seal. All important is that it is attributable to a signer, expresses his legal will, and shows his acceptance of an offer. In contrast, an electronic signature is a digital representation of an individual's signature (Al-Momani, 2003). It can be letters, digits, codes, or symbols affixed to or associated with an electronic record. It is created using an electronic device, such as a computer or a smart card. It is typed and stored in a card, provided that the signatory controls the electronic intermediary for creating the signature and that the signature is linked to an electronic authentication certificate issued by an electronic certification body (Al-Kilani, 2021).

Based on those mentioned above, regardless of the traditional or electronic method used for the signature, whether in writing, symbol, or code, it should be obvious and demonstrate the signatory's will to adhere to the bond terms unless proven otherwise (Al-Arayshi, 2016).

Authentically Identify the Identity of the Signatory

The signatory's identity is determined through authenticated symbols, signals, or marks with a unique character that distinguishes him from others. It is stored electronically and is easy to refer to at any time (Hegazy, 2003). For example, a signature with a password can identify the signatory's identity because no one knows it except its user, as well as a digital signature and an electronic pen signature (Al-Bashkani, 2009).

One of the essential legal prerequisites for trust in the digital world is the ability of individuals and legal entities to exercise their rights in the area of electronic signatures. This includes having faith in the dependability of electronic transactions and being certain of the legal significance and potential repercussions of using electronic means (Solovyanenko, 2022).

Generally speaking, the accuracy of the electronic signature may be higher than that of a traditional signature in serving the purpose of distinguishing the signatory since it is created by an accredited electronic authentication party (Al-Khawajah et al., 2023). The electronic signature is distinguished by stability, trustworthiness, and

Article History
Submitted 13 July 2024 - Revision Required 30 December 2024 - Accepted 30 April 2025

P-ISSN: 1412-6834
E-ISSN: 2550-0090

difficulty in forging compared to the traditional signature, which is susceptible to forgery, distortion, and manipulation (Khashashneh et al., 2023).

It is worth noting that the body certifying the electronic signature requires that the signatory has the legal capacity that grants him the right to conclude contracts and legal actions. In one of its rulings, the Jordanian judiciary approved using electronic signature provided it is certified and demonstrates the signatory's identity. For instance, the Jordanian Court of Cassation stated:

> "And since the expert report was based on legal accounts on the computer used to organize the plaintiff company's records, documents, and financial statements, which a legal auditor audited. And that the accounting program that was selected works in such a way that it does not allow for any modification or deletion of any additions to the entered data. The entered data includes the electronic signature of its enterer, and therefore, these accounts are suitable for conducting experiments".

This is achieved through reliable procedures proving the signatory's identity, as no one can decode his signature. The signatory uses his private key and signature to demonstrate his will and adherence to the electronic bond content. We can say that the pen used for signing to show acceptance and will is replaced by an e-signature based on creating a whole data system (Qouteshat, 2016).

The electronic signature on the electronic document is created electronically using modern means of communication. The signature must be linked to the electronic bond and can only be modified by the contractor. In a digital signature, which relies on two public and private keys, no one can view the document except the contractor who owns the private key (Mason, 2014; Alsheyab, 2023).

The authentication of legal declarations by natural beings is a fundamental requirement of electronic administration. The utilization of electronic signatures is a valid and effective method for ensuring authenticity; yet, it is not widely adopted by individuals. A trust service provider may generate an electronic signature for an individual, with client authentication achieved using two-factor dynamic handwritten signature verification. This approach, augmented with other safeguards, would establish a secure and dependable foundation for the authentication of electronic legal statements (Kiss & Klimkó, 2020; Zainuddin & Ramadhani, 2021).

Electronic Signature Forms and Legal Validity

The electronic signature can be accomplished through various methods. It can involve using an electronic pen to write your signature on a computer screen physically, or it can be generated through biometric means like your personal fingerprint, iris scan, facial recognition, or vocal tone, which are then stored electronically on the computer screen. An electronic signature can also be a digital signature comprising encrypted numbers or symbols (Martin & Pascarelli, 2014; Alkhseilat et al., 2024).

Since electronic signatures occur remotely between individuals who do not physically meet, it is essential to have legal assurances to verify the parties' identities, such as

JURNAL HUKUM NOVELTY
Volume 16, Issue 1, 2025, pp. 120-139
P-ISSN: 1412-6834
E-ISSN: 2550-0090

having a neutral third party acting as an intermediary between the contracting parties to validate the authenticity of electronic procedures which is called accredited electronic authentication party "accreditation authorities" (Krawczyk, 2014; Wong & Muhamad, 2022). These authorities issue electronic certificates and determine the identities of the contracting parties, whether through the private encryption key or the public key, decrypted through special records that ensure complete confidentiality and enhance electronic trust between the parties (Linh, 2014; Quintanilla et al., 2014; Prasetya & Bawono, 2022).

Electronic accredited authorities are subject to state supervision, which establishes necessary instructions and precautionary measures to ensure the security of electronic signatures to prevent hacking, with criminal and civil liability penalties (Elsonbaty, 2014). When it comes to electronic signatures, if the required conditions for signatures are met, such as verifying the identity of the signatory, associating the signature with the electronic bond, and the ability to access the signature is limited to the signatory, does it enjoy probative force? And, is it required to be authenticated? This inquiry leads us to the issue of electronic signatures and the validity of each type.

Authenticated and Protected Electronic Signature

The signatory assumes responsibilities and is granted rights if the signature is authenticated. It enjoys the same legal probative value as a traditional bond. Nevertheless, the signature shall be authenticated. By this, we mean a licensed authentication party in the State should issue it. The electronic signature should also meet several conditions to be deemed protected and authenticated (Casamento & Hatfield, 2014; Azhari et al., 2021). These conditions are stipulated in Article 15 of the Electronic Transactions Law, which are: If it is unique in its connection to the signatory and distinguishes him/her from others; If it identifies its owner; If the private key is under the control of the signatory when he signs; If it is connected to the electronic record in a way that does not allow modification on such record after signing it and without making any changes on that signature.

The electronic signature shall also be deemed authenticated if all of the aforementioned conditions stipulated in Article 16 of this Law are fulfilled and if it was connected to an electronic authentication certificate issued at the time the electronic signature was created, following the provisions of this law and the regulations and instructions issued hereunder by: An electronic authentication party licensed in Jordan; An accredited electronic authentication party; Any governmental body legally authorized by the Council of Ministries, whether it was a ministry, public official institution, public institution, or municipality, provided that it fulfills the requirements of the Telecommunications Regulatory Commission; The Ministry of Information and Communications Technology; or, The Central Bank of Jordan, concerning the banking or financial electronic operations.

Article History
Submitted 13 July 2024 - Revision Required 30 December 2024 - Accepted 30 April 2025

JURNAL HUKUM NOVELTY
Volume 16, Issue 1, 2025, pp. 120-139
P-ISSN: 1412-6834
E-ISSN: 2550-0090

Through Article 16 of the Electronic Transactions Law, we notice that the Jordanian legislator has established a presumption regarding the electronically authenticated bond, considering it to be issued by its owner, and it does not burden the owner with proving the validity of the electronic signature. Rather, the opposing party disputes this bond to prove the contrary by presenting evidence of the inauthenticity of the electronic signature (Caprioli, 2014; Qian, 2008).

The Jordanian legislator granted the electronic bond with a protected signature, a probative value equivalent to a traditional bond. The parties to the electronic transaction may invoke it (Rabadi, 2012). As stated by Article 17(a) of the Electronic Transactions Law: "The electronic record that carries a protected electronic signature shall have the same evidential weight designated to the ordinary bond, and the parties of the electronic transaction may use it in an argument to prove evidence." Nonetheless, in this context, we ponder: What if the signature remains authenticated?

An electronic signature is deemed protected when it meets the conditions stipulated in Article 15. The Jordanian legislator has differentiated between protected signatures, which must meet specific conditions, and authenticated signatures, which an accredited authentication entity must issue. Under Jordanian law on electronic transactions, the electronically protected record associated with an electronic signature has the same legal validity as a traditional bond, and authentication is not a requirement (Al-Momani, 2003). Parties engaged in electronic transactions can rely on the electronic record to support their claims, whether protected or authenticated. However, those not party to the transaction can only object if the record is protected or authenticated. The Jordanian legislator has granted legal validity to an electronically signed record that is neither protected nor authenticated, equivalent to a regular bond between parties. In cases where the electronic record is not linked to the electronic signature, it carries the same probative value as the unsigned bond for proofing evidence (Al-Kilani, 2021; McIsaac & Fohr, 2014).

Consequently, an electronic signature can either be an electronic signature that includes the identification of its owner, its exclusive use by the owner, and its distinctiveness from others, or it can be a protected electronic signature that identifies its owner, distinguishes it through its use and has a private key controlled by the owner, which is associated with an electronic record preventing any alterations to that record (Al-Bashkani, 2009). Alternatively, it can be a protected and authenticated electronic signature issued by an entity authorized to perform electronic authentication (Al-Arayshi, 2016; Al-Khalaileh et al., 2025).

Unprotected and Unauthenticated Electronic Signature

This situation arises when the electronic bond lacks one of the conditions outlined in Articles 15 and 16 of the Electronic Transactions Law, which pertain to authentication and protection. In such a case, its probative value is equivalent to that of a traditional paper bond. It suffices for the document's creator to assert its authenticity, shifting

JURNAL HUKUM
NOVELTY
Volume 16, Issue 1, 2025, pp. 120-139
P-ISSN: 1412-6834
E-ISSN: 2550-0090

the burden of proof to the opponent party. If the bond is challenged, it becomes the responsibility of the party defending the flawed electronic signature to prove the integrity of the technical means used to generate the electronic signature data (Hegazy, 2003).

The digital society revolution propels the concept of the extent and efficacy with which the public sector and government are prepared to utilize digital instruments. One such instrument is the "electronic signature," extensively utilized in the private sector as a valid means of identifying the individual executing a document (Donchevska, 2020; Ouyang et al., 2022).

The ongoing transition to digital transactions underscores the necessity for strong Qualified Electronic Signature standards that protect integrity and privacy. The primary problem Remote Qualified Electronic Signatures (QESs) pose to end users is the decision to submit either the complete document or solely its digest to the Trust Service Provider (TSP). The first alternative jeopardizes the document's confidentiality, whilst the second necessitates the creation of signature software that adhere to sophisticated signature formats, a process that frequently demands extra time and resources (Aciobăniței et al., 2024).

Unsigned Electronic Bond

Article 17(d) of the Electronic Transactions Law stipulates, "The electronic record that does not carry an electronic signature shall have the same evidential weight designated to unsigned documents for the purpose of proofing evidence." By this law, we can say that the Jordanian legislator has granted the unsigned electronic bond the same value as unsigned papers as and with less value than a regular bond. Referring to the provisions of the Jordanian Evidence Law, Article 18 stipulates that:

> "Registers and private papers have no probative force against the person from whom they have issued, except in the two following cases: 1. If he expressly mentions that he has been repaid the debt, 2. If he expressly mentions his intention, the contents of these papers shall take the place of a title in favor of a person from whom the entries establish a right."

Keep in mind that private papers and registers are the memos that people write, and they are not intended for proof and do not take a specific form, and people are not obligated to organize them.

These documents do not hold validity for their owner if the matter is civil. However, they serve as evidence against their owner in two situations: first, if he explicitly mentions that a debt has been settled (Krawczyk, 2014). The second is that if he expressly states his intention, the contents of these papers shall take the place of a title in favor of a person from whom the entries establish a right. In these two cases, as exceptions to the general rule that does not compel a party to provide evidence against themselves, the law does not require these documents to be signed or written in the owner's handwriting. Instead, the legislator requires explicit statements within

Article History
Submitted 13 July 2024 - Revision Required 30 December 2024 - Accepted 30 April 2025

JURNAL HUKUM NOVELTY
Volume 16, Issue 1, 2025, pp. 120-139
P-ISSN: 1412-6834
E-ISSN: 2550-0090

them, either acknowledging the debt settlement or recognizing a debt owed (Elsonbaty, 2014; Al-Billeh et al., 2024a). Consequently, in these circumstances, an electronic bond does not have probative force for its owner if the dispute involves a civil party. Still, it serves as evidence against the owner if it explicitly states that a debt has been settled or indicates electronically that it is intended to serve as a document for a legitimate interest (Martin & Pascarelli, 2014; Linh, 2014).

Traders' paper books are another type of unsigned paper. It was covered under Articles 15 of the Jordanian Evidence Law, which stipulates that:

> "'Traders' paper books shall not be considered proof against other than traders. However, where these books contain particulars as to supplies made by traders, the court may, based on these particulars and within the limits of matters that could be established by the witness's testimony, call upon any of the parties to take the suppletory oath."

Article 16 of the same Law specifies that:

> "The compulsory traders' books, whether legally regulated and kept or not: 1. Shall have probative force against their owner, whether they are legally regulated or not, but it is not permissible for anyone to extract evidence from them for his own interest to split what is stated and exclude what is opposing his claim. 2. It shall have probative force in favor of its owner in his transactions related to his trade if it is organized and the dispute is between him and a trader."

Accordingly, the electronic bond is considered a legal traders' paper book, even if it is not signed, and it gains a probative value the same as the traders' paper books (Mason, 2014).

Another type of unsigned paper is called indication. Indication on papers is covered under Article 19 of the Jordanian Law of Evidence. However, it states that:

> "1. Indication on the bond by the creditor establishes the quittance of the debtor. And it shall be deemed evidence against him until proof to the contrary is made even if it is not dated or signed, so long as bond remains in his possession; 2. The provision shall apply if the creditor proves by his handwriting and without his signature the quittance of the debtor in a duplicate original copy of a bond or discharge is in the hand of the debtor."

We conclude from the earlier Articles that, provided that the bond is in the creditor's control, any indication made by him on an unsigned electronic bond uttering that the debtor has paid him the debt is regarded as evidence against him (Qouteshat, 2016; Al-Billeh et al., 2024b).

Conclusion

The widespread use of electronic authentication and signature systems may be a significant step towards decreasing trade documentation and associated expenses in international transactions. While the quality and security of technology solutions heavily influence the pace of growth in this field, the legislation may play an important role in enabling the use of electronic authentication and signature systems.

JURNAL HUKUM
NOVELTY
Volume 16, Issue 1, 2025, pp. 120-139
P-ISSN: 1412-6834
E-ISSN: 2550-0090

Therefore, the Jordanian Electronic Transactions Law has granted electronic signatures the same probative value as traditional signatures if the signatory's identity is established, distinguishing him from others, and if it expresses his intent to engage in a legal transaction. Technical and legal prerequisites must be met to confer probative value on electronic signatures.

In fact, electronic signatures may be either secured and verified or unsecured and unverified. The technical specifications for an authenticated electronic signature vary from those for a secured one. Authenticated electronic signatures necessitate authentication by a recognized and accredited organization. The Jordanian Electronic Transactions Law acknowledges the evidentiary validity of unprotected and unauthenticated electronic signatures.

For the electronic signature statute, the Jordanian legislator must set up a mechanism known as the "electronic examiner." It is the responsibility of this system to ascertain whether the electronic signature and the information and documents connected to it are authentic or fraudulent. It's also critical to stress that certification service providers are required to secure users' private information, prevent exposure, and face legal and criminal consequences for any unlawful concealment. However, legislators and policymakers must comprehend the distinctions among domestic liability regimes and their common aspects to formulate suitable methods and procedures for the recognition of signatures validated by international certificates. The domestic laws of different nations may already offer basically identical responses to the concerns addressed in this article, due to shared legal traditions or membership in a regional integration framework.

Finally, we recommend that the Jordanian legislator intervene to amend the provisions of the Electronic Transactions Law and provide more detailed tasks for assigned electronic authentication entities and the Jordanian legislator should address the responsibilities that arise for electronic authentication entities and establish a contractual relationship between the relevant ministry and the electronic authentication entity, with the responsibility being of a fault-based nature between the electronic authentication entity and electronic users and bridging the gap between technical expertise and legislative competence through specialized training programs related to digital transformation. This would equip the judiciary with human resources trained to understand modern communication methods professionally, positively impacting judicial decisions.

Acknowledgement

The authors would like to thank Zarqa University and Applied Science Private University and Sohar University and Larbi Tebesi University and University Ibn Tofail. Sincere gratitude also goes to anonymous reviewers and editors who have provided constructive feedback so that this manuscript looks worth reading and citing.

Article History
Submitted 13 July 2024 - Revision Required 30 December 2024 - Accepted 30 April 2025

JURNAL HUKUM
NOVELTY
Volume 16, Issue 1, 2025, pp. 120-139

P-ISSN: 1412-6834
E-ISSN: 2550-0090

Declarations

Author contribution	:	Authors 1, 2, 3, 4: initiated the research ideas, instrument construction, data collection, analysis, and draft writing; Authors 2, 3, 4. 5, 6: revised the research ideas, literature review, data presentation and analysis, and the final draft. Authors 3, 4, 5, 6: revised the research ideas, literature review, data presentation and analysis, and the final draft.
Funding statement	:	None
Conflict of interest	:	The authors declare no conflict of interest.
Additional information	:	No additional information is available for this paper.

References

Aciobăniței, I., Arseni, Ștefan C., Bureacă, E., & Togan, M. (2024). A comprehensive and privacy-aware approach for remote qualified electronic signatures. *Electronics (Switzerland)*, 13(4). https://doi.org/10.3390/electronics13040757

Al-Arayshi, O. (2016). *The authenticity of electronic bonds in evidence*. Amman: Al-Hamid Publishing House.

Al-Bashkani, H. (2009). *Legal Regulation of Electronic Commerce*. Egypt: Dar Al-Kutub Al-Qanuni

Al-Billeh, T. (2022). Legal controls of the crime of publishing a program on the internet in Jordanian legislation. *Pakistan Journal of Criminology*, 14(1), 1–14. http://pjcriminology.com/wp-content/uploads/2022/08/1.-Legal-Controls-of-the-Crime-of-Publishing-a-Program-on-the-Internet-in-Jordanian-Legislation.pdf

Al-Billeh, T. (2023). Disciplinary measures consequent on the judges' misuse of social media in Jordanian and French legislation: A difficult balance between freedom of expression and restrictions on judicial ethics. *Kutafin Law Review*, 10(3), 681–719. https://kulawr.msal.ru/jour/article/view/224

Al-Billeh, T. (2024). Jurisdiction regarding administrative proceedings in Jordanian and French legislation: Views on the administrative judiciary in 2021. *International Journal for the Semiotics of Law - Revue Internationale de Sémiotique Juridique*, 37(1), 189–215. https://doi.org/10.1007/s11196-023-10064-5

Al-Billeh, T., Al-Hammouri, A., Khashashneh, T., AL Makhmari, M., & Al Kalbani, H. (2024a). Digital evidence in human rights violations and international criminal justice. *Journal of Human Rights, Culture and Legal System*, 4 (3), 842-871. https://doi.org/10.53955/jhcls.v4i3.446

Al-Billeh, T., Alkhseilat, A., & AL-Khalaileh, L. (2023). Scope of penalties of offences in Jordanian public office. *Pakistan Journal of Criminology*, 15 (2), 341-356. https://www.pjcriminology.com/publications/scope-of-penalties-of-offences-in-jordanian-public-office/

Al-Billeh, T., Hmaidan, R., Al-Hammouri, A., & AL Makhmari, M. (2024b). The risks of using artificial intelligence on privacy and human rights: Unifying global standards. *Jurnal Media Hukum*, 31 (2), 333-350. https://dx.doi.org/10.18196/jmh.v31i2.23480

JURNAL HUKUM NOVELTY
Volume 16, Issue 1, 2025, pp. 120-139
P-ISSN: 1412-6834
E-ISSN: 2550-0090

Al-Khalaileh, L., Al-Billeh, T., & Al-Hammouri, A. (2025). The legal authority of the electronic authentication certificate and its role in proving e-commerce transactions. *International Journal of Electronic Security and Digital Forensics*, 17 (1/2), 267 – 282. https://doi.org/10.1504/IJESDF.2025.143469

AL-Khalaileh, L., Al-Billeh, T., & Manasra, M. (2024). The legal protection of domain names in Jordanian legislation and the rules of the unified domain name dispute resolution policy issued by ICANN. *Jurnal Hukum Novelty*, 15(1), 1-20. http://journal.uad.ac.id/index.php/Novelty/article/view/28132

Al-Khawajah, N., Al-Billeh, T., & Manasra, M. (2023). Digital forensic challenges in Jordanian cybercrime law. *Pakistan Journal of Criminology*, 15 (3), 29-44. https://www.pjcriminology.com/publications/digital-forensic-challenges-in-jordanian-cybercrime-law/

Alkhseilat, A., Al-Billeh, T., Albazi, M., & Ali, N. A. (2024). The authenticity of digital evidence in criminal courts: A comparative study. *International Journal of Electronic Security and Digital Forensics*, 16(6), 720-738. https://doi.org/10.1504/IJESDF.2024.142010

Al-Kilani, M. (2021). *Rules of evidence and implementation provisions*. Amman: Dar Al-Thaqafa Publishing House.

Al-Momani, O. (2003). *Electronic Signature and Electronic Commerce Law*. Amman: Wael Publishing House.

Alsheyab, M. S. A. (2023). Legal recognition of electronic signature in commercial transactions: A comparison between the Jordanian Electronic Transactions Law of 2015 and the United Arab Emirates Electronic Transactions and Trust Services Law of 2021. *International Journal for the Semiotics of Law*, 36(3), 1281–1291. https://doi.org/10.1007/s11196-022-09967-6

Azhari, R., Ramadhani, W., & Randa, T. O. (2021). Juridical review of electronic signature implementation of duties of notary offices in contracting in agreements in the COVID-19. *Syiah Kuala Law Journal*, 5(1), 26–40. https://doi.org/10.24815/sklj.v5i1.20734

Caprioli, E. A. (2014). Commentary on digital evidence and electronic signature of a consumer credit contract in France. *Digital Evidence and Electronic Signature Law Review*, 11(0). https://doi.org/10.14296/deeslr.v11i0.2160

Casamento, G., & Hatfield, P. (2014). The essential elements of an effective electronic signature process. *Digital Evidence and Electronic Signature Law Review*, 6(0). https://doi.org/10.14296/deeslr.v6i0.1861

Donchevska, B. (2020). Possibilities for application of the electronic signature in the lawmaking process at the assembly of the Republic of North Macedonia. *Balkan Social Science Review*, 15(15), 77–93. https://doi.org/10.46763/bssr20150078d

Elsonbaty, E. M. (2014). The electronic signature law: between creating the future and the future of creation. *Digital Evidence and Electronic Signature Law Review*, 2(0). https://doi.org/10.14296/deeslr.v2i0.1747

Feng, C., Ji, Z., & Zhang, J. (2022). Comparative analysis of dynamic characteristics between electronic signature and conventional signature based on computer vision technology. *Computational Intelligence and Neuroscience*, 2022. https://doi.org/10.1155/2022/4965908

Haileyesus, I. W. (2021). An appraisal of electronic signature law of Ethiopia: Further reforms for improvement. *International Journal of Public Law and Policy*, 7(1), 49–73. https://doi.org/10.1504/IJPLAP.2021.115006

Article History
Submitted 13 July 2024 - Revision Required 30 December 2024 - Accepted 30 April 2025

JURNAL HUKUM NOVELTY
Volume 16, Issue 1, 2025, pp. 120-139
P-ISSN: 1412-6834
E-ISSN: 2550-0090

Hegazy, A. (2003). *Introduction to Arab trade. Book two, the legal system for electronic commerce in the United Arab Emirates*. Alexandria: Dar Al-Fikr Al-Jami'i

Khashashneh, T., Al-Billeh, T., Al-Hammouri, A., & Belghit, R. (2023) The importance of digital technology in extracting electronic evidence: How can digital technology be used at crime scenes?. *Pakistan Journal of Criminology*, 15 (4), 69-85. https://www.pjcriminology.com/publications/the-importance-of-digital-technology-in-extracting-electronic-evidence-how-can-digital-technology-be-used-at-crime-scenes/

Kiss, P. J., & Klimkó, G. (2020). Authentication of electronic legal statements by a trust service provider using two-factor dynamic handwritten signature verification. *In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 12394 LNCS, pp. 147–158). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-030-58957-8_11

Krawczyk, P. (2014). When the EU qualified electronic signature becomes an information services preventer. *Digital Evidence and Electronic Signature Law Review,* 7(0). https://doi.org/10.14296/deeslr.v7i0.1920

Linh, N. D. (2014). The electronic signature law in Vietnam: A note. *Digital Evidence and Electronic Signature Law Review*, 3(0). https://doi.org/10.14296/deeslr.v3i0.1780

Lubis, I. (2021). The validity of the electronic signature in electronic general meeting of shareholders of the limited company's. *Kanun Jurnal Ilmu Hukum*, 23(2), 257–273. https://doi.org/10.24815/kanun.v23i2.21044

Martin, L., & Pascarelli, R. (2014). Electronic signature: value in law and probative effectiveness in the Italian legal system. *Digital Evidence and Electronic Signature Law Review*, 1(0). https://doi.org/10.14296/deeslr.v1i0.1721

Mason, S. (2014). World electronic signature legislation. *Digital Evidence and Electronic Signature Law Review*, 10(0). https://doi.org/10.14296/deeslr.v10i0.2014

Massad, M. (2022). The evidentiary value of electronic documents: A comparative study. *BiLD Law Journal*, 7(2), 359–377. https://bildbd.com/index.php/blj/article/view/321

McIsaac, B., & Fohr, H. R. (2014). Legal update, Canada: PIPEDA's Secure Electronic Signature Regulations have been published. *Digital Evidence and Electronic Signature Law Review*, *2*(0). https://doi.org/10.14296/deeslr.v2i0.1752

Monaghan, N. (2022). Electronic Evidence and Electronic Signatures. A*micus Curiae*, 3(2), 375–380. https://doi.org/10.14296/ac.v3i2.5418

Ouyang, G., Liang, E., & Qi, W. (2022). Electronic signature: Research progress and trend into perspective of document examination. *Forensic Science and Technology*, 47(4), 336–341. https://doi.org/10.16467/j.1008-3650.2022.0021

Prasetya, A. G. N., & Bawono, B. T. (2022). The juridical analysis of the use of electronic signatures on electronic land certificates in the conception of legal certainty. *Sultan Agung Notary Law Review*, 4(3), 771. https://doi.org/10.30659/sanlar.4.3.771-785

Qian, K. (2008). Sealed-bid electronic auction scheme based on new group signature. *Journal of Computer Applications*, *28*(3), 813–815. https://doi.org/10.3724/sp.j.1087.2008.00813

JURNAL HUKUM
NOVELTY
Volume 16, Issue 1, 2025, pp. 120-139
P-ISSN: 1412-6834
E-ISSN: 2550-0090

Qouteshat, O. H. (2016). Challenges of authentication and certification of e-awards in Dubai and before the Dubai International Financial Centre courts: the electronic signature. *Digital Evidence and Electronic Signature Law Review*, 13(0). https://doi.org/10.14296/deeslr.v13i0.2300

Quintanilla, J., Doren, C., & Hernández, D. (2014). The electronic signature in Chile. *Digital Evidence and Electronic Signature Law Review*, *4*(0). https://doi.org/10.14296/deeslr.v4i0.1802

Rabadi, I. (2012). *Rules for electronic signatures*. Amman: Dar Al-Thaqafa Publishing House.

Ruiz-Martínez, A., Sánchez-Martínez, D., Martínez-Montesinos, M., & Gómez-Skarmeta, A. F. (2007). A survey of electronic signature solutions in mobile devices. *Journal of Theoretical and Applied Electronic Commerce Research*. https://doi.org/10.3390/jtaer2030024

Sari, E. M., Kurniawan, K., & Haq, L. M. H. (2023). Notary's responsibility in certification of electronic signatures for discrepancies in verification of personal data of the owner of the electronic signature: Comparative study between Indonesia and the United States of America. *Path of Science*, 9(4), 5009–5015. https://doi.org/10.22178/pos.91-18

Solovyanenko, N. I. (2022). Exercise of the rights of individuals and legal entities in the use of electronic signatures as a condition of trust in the digital environment. *Gosudarstvo i Pravo*, 2022(11), 192–196. https://doi.org/10.31857/S102694520022777-5

Tengku, T., & Wan, W. (2019). The status of electronic signature in the evidence law: An analytical study. *Malaysian Journal of Syariah and Law*, 7(1), 161–170. https://doi.org/10.33102/mjsl.v7i1.90

Wong, H. S., & Muhamad, M. M. (2022). Electronic signature and attestation in conveyancing practice: A Malaysian legal perspective. *F1000Research*, 11, 325. https://doi.org/10.12688/f1000research.73548.3

Yang, Y., Han, X., & Qin, D. (2024). Dynamic feature analysis of handwritten electronic signatures based on Fourier transform. *Journal of Forensic Sciences*, 69(1), 264–272. https://doi.org/10.1111/1556-4029.15386

Zainuddin, Z., & Ramadhani, R. (2021). The legal force of electronic signatures in online mortgage registration. *Jurnal Penelitian Hukum De Jure*, 21(2), 243. https://doi.org/10.30641/dejure.2021.v21.243-252m

Article History
Submitted 13 July 2024 - Revision Required 30 December 2024 - Accepted 30 April 2025