Law and Humanities Quarterly Reviews

Alhamad, A. M. G. Electronic Documentation as a Mechanism for Protecting Electronic Contracting: A Comparative Study Between Jordanian and Algerian Law. ***Law and Humanities Quarterly Reviews,*** **3(3), 1-11.**

ISSN 2827-9735

DOI: 10.31014/aior.1996.03.03.121

The online version of this article can be found at:
https://www.asianinstituteofresearch.org/

Published by:
The Asian Institute of Research

The Asian Institute of Research Law and Humanities Quarterly Reviews is a peer-reviewed International Journal of the Asian Institute of Research. The journal covers scholarly articles in the interdisciplinary fields of law and humanities, including constitutional and administrative law, criminal law, civil law, international law, linguistics, history, literature, performing art, philosophy, religion, visual arts, anthropology, culture, and ethics studies. The Law and Humanities Quarterly Reviews is an Open Access Journal that can be accessed and downloaded online for free. Thus, ensuring high visibility and increase of citations for all research articles published. The journal aims to facilitate scholarly work on recent theoretical and practical aspects of law.

ASIAN INSTITUTE OF RESEARCH
Connecting Scholars Worldwide

The Asian Institute of Research
Law and Humanities Quarterly Reviews
Vol.3, No.3, 2024: 1-11
ISSN 2827-9735

DOI: 10.31014/aior.1996.03.03.121

Electronic Documentation as a Mechanism for Protecting Electronic Contracting: A Comparative Study Between Jordanian and Algerian Law

Amjed Muflih Ghanem Alhamad[1]

[1] Assistant Professor - Irbid National University - Private Law. Email: a.rheme@inu.edu.jo / amjadalrheme@yahoo.com

Abstract
Due to the development in the field of information and communication technology, which has contributed significantly to the dematerialization of various commercial and banking transactions into legally recognized electronic platforms, the use of electronic contracting has spread. To protect this latter, both Jordanian and Algerian legislators have provided for electronic documentation, which is carried out by issuing a third-party neutral or an accredited entity for the electronic certification between two parties dealing electronically. Its content confirms the validity of the data exchanged between the parties through following certain complex technical and procedural measures. This party is a specialized natural or legal entity operating under a license from the competent authorities in the country and under their supervision, within the provisions that define its system and the obligations imposed on it, as well as delineating its responsibility for damages inflicted on clients or others. The electronic certification certificate serves to prove the electronic exchange and to determine the moment the contract is concluded. However, electronic documentation can only protect electronic contracting if the certification entity adheres to a set of obligations such as verifying the signer's identity, maintaining confidentiality, issuing electronic keys, issuing the electronic certification, and finally, conducting mandatory insurance.

Keywords: Electronic Documentation, Electronic Certification, Certification Certificate, Certification Entity, Electronic Contracting, Jordanian Law, Algerian Law

1. Introduction

The advancements in information and communication technology have impacted all areas of life and various interactions between individuals. Electronic contracting now goes hand in hand with traditional contracting, and in many cases, it surpasses it. Through the conclusion of electronic contracts made over the internet and various electronic mediums, this method of dealing has imposed itself on a wide scale.

Electronic contracting, like traditional contracting, involves selling, buying, distributing, and providing services between consumers and producers or service providers. Due to the different contracting environments between

traditional and electronic contracting, the latter is more susceptible to fraud and scams against the consumer contractor, as the transactions are done remotely and virtually, with the contractor, store, and goods all being presumed.

As a result, trust between the parties will be very lacking, if not nonexistent. Therefore, it was necessary to have guarantees that secure electronic transactions and their development. Both the Jordanian and Algerian legislators recognized the need for guarantees to ensure the protection of the electronic consumer and the commercial transaction. They introduced laws to protect electronic contracting, and by creating a reliable mechanism trusted by both parties, they ensure legally and technically the authenticity of the contracting will and the identity of the contracting parties. This mechanism is represented in electronic authentication, or as the Algerian legislator called it, electronic certification.

1.1. Study Problem

The problem of this study can be formulated in the following main question:

How does electronic authentication ensure the protection of electronic contracting under Jordanian and Algerian law?

The following sub-questions fall under this problem:

- What does the legal system for electronic authentication entail?
- What role does electronic authentication play in protecting electronic contracting?

1.2. Study objectives

This intervention aims, with its importance, to highlight electronic authentication as a mechanism to protect electronic contracting in both Jordanian and Algerian law. The Jordanian and Algerian legislators have recognized that electronic contracting is an inevitable matter and a necessity of current life that must be protected and secured. These guarantees can only be established through the mechanism of electronic authentication.

1.3. Study Approach

To address this issue, we followed both the analytical and comparative methods, which are most suitable for such a study. The analytical method involves analyzing the legal texts in the Jordanian Electronic Transactions Law and the Algerian Law specifying the rules for electronic signatures and certification. The comparative method involves comparing the legal texts in both laws under study and identifying the similarities and differences between them.

Consistent with our research methodology, we divided the intervention into two main sections: the first section discusses the legal system of electronic authentication, while the second section addresses the role of electronic authentication in protecting electronic contracting.

2. The Legal System for Electronic Authentication

Electronic authentication is a relatively new term in the field of electronic transactions. It emerged concurrently with the spread and increased use of various modern technological techniques, which have contributed significantly to abstracting various actions or commercial and banking transactions from their physical nature to legally recognized electronic supports. To understand the legal system of electronic authentication, this axis will cover its concept and then the provisions of the electronic authentication certificate.

2.1. The Concept of Electronic Authentication

To protect the electronic signature and consequently protect the electronic consumer and electronic contracting, the Jordanian and Algerian legislators have implemented a series of mechanisms that regulate electronic contracting. Among these mechanisms is the electronic authentication certificate, issued by electronic authentication bodies. To understand this, we need to go through the definition of electronic authentication, followed by the definition of the electronic authentication certificate, its types, and finally, the electronic authentication bodies.

2.1.1. Definition of Electronic Authentication

Electronic authentication is defined as a procedure conducted by a neutral third party or an accredited entity through following some complex technical and technical procedures. This party is a specialized natural or legal entity operating under a license from the competent authorities in the country and under their supervision, within provisions that define its system and the obligations laid upon it, as well as delineating its responsibility for any damages inflicted on clients or others. Since the electronic fulfillment process is conducted over the internet, without the physical presence -real- of the concerned parties, banks have found it necessary to resort to a neutral and reliable third party, which ensures the safety of the fulfillment process in its own ways and according to a mechanism that instills trust and reassurance among the users of the electronic fulfillment system (Al-Muzail, 2017, p. 222).

Electronic authentication is also defined as "a technical means that contributes to verifying the validity of an electronic signature or electronic document so that it can be attributed to a specific person or entity, issued by a trusted entity or a neutral party called an application service provider" (Al-Shanraqi, 2013, p. 79). It is also known as the verification that an electronic signature was executed by a specific person, using analytical methods to recognize symbols, words, numbers, decryption, reverse engineering, and any other means or procedures that achieve the intended purpose" (Musadiq, 2020, p. 38). The Jordanian legislator defined it in Article 02 of (Law N°15, 2015) as verifying the identity of a user of an electronic authentication certificate to prove the attribution of an electronic signature to a specific person based on approved authentication procedures. Meanwhile, the Algerian legislator has not defined electronic authentication.

2.1.2. Definition of the Electronic Authentication Certificate

Jurisprudence defines the electronic authentication certificate as a security instrument and a certificate issued by an intermediary or third party between two parties engaging electronically. Its content verifies the accuracy of the data exchanged between the parties, for example, over the internet. Accordingly, the intermediary issues this digitally authenticated certificate, which certifies the authenticity of one of the contracting parties' electronic signature, in addition to other data that the certificate may be allowed to include, resulting in trust between the contracting parties, thus finalizing the contract (Yahiaoui, 2022, p. 697).

Legally, the Jordanian legislator defined it in Article 02 of (Law N°15, 2015) as the certificate issued by the electronic authentication body to prove the attribution of an electronic signature to a specific person based on approved authentication procedures. Meanwhile, the Algerian legislator defined it in Article 02 of (Law N°15, 2015) as a document in electronic form.

2.1.3. Types of Authentication Certificates

Referring to the Jordanian and Algerian law, we find that each has specified two types of authentication certificates, namely the ordinary authentication certificate (A) and the qualified authentication certificate, or as the Algerian legislator calls it, the described certification certificate (B).

A. Ordinary Authentication Certificate

The ordinary authentication certificate is a document issued by the competent authentication body without specifying prior data, which can be used as evidence in court in case of a dispute, with proof that the certificate was issued in an authenticated manner, or it is a certificate linked to specific data from an electronic scan and a

particular person, confirming their identity (Yahiaoui, 2022, p. 698). This type of certificate is used to authenticate electronic messages conducted via email (Al-Saadi & Al-Hasan, 2017, p. 590).

B. Qualified Authentication Certificate

The described authentication certificate is a document issued by the competent authority for electronic authentication certificates with the purpose of confirming the accuracy of the data in the electronic signature and verifying its attribution to its owner. This certificate includes numerous data elements that provide security requisites for the parties involved (Baha, 2015, pp. 391-392).

The Jordanian legislator has named it the "qualified authentication certificate" and defined it in Article 02 of the Jordanian Electronic Transactions Law as "an electronic authentication certificate issued by electronic authentication bodies to themselves to enable other authentication bodies to trust the certificates they issue." Meanwhile, the Algerian legislator has named it the "described certification certificate," and defined it in Article 15 of Law 15/04, 2015, as an electronic certification certificate that meets a set of requirements:

- It must be granted by a trusted third party or by an electronic certification service provider, in accordance with the approved electronic certification policy.
- It must be granted to the signatory exclusively.

It must specifically include an indication that this certificate was granted on the basis that it is a described electronic certification certificate, identifying the trusted third party or the licensed electronic certification service provider issuing, the certificate Electronic certification, as well as the country of residence of the certifying party, the name or pseudonym of the signatory allowing for identification, and the possibility of including a specific attribute for the signatory when necessary, according to the purpose of using the electronic certification certificate. It includes data related to the verification of the electronic signature and matches the data for creating the electronic signature. It indicates the start and end dates of the validity period of the electronic certification certificate, the identification code of the electronic certification certificate, the described electronic signature of the service provider or the trusted third party granting the electronic certification certificate when necessary, the limits of the use of the electronic certification certificate, the transaction value limits for which the electronic certification certificate may be used when necessary, and the reference to the document proving the representation of another natural or legal person when necessary, referring to French law, we find that it stipulates similar data.

2.1.4. Definition of Electronic Authentication Parties

Definition of Electronic Authentication Parties The third party or neutral entity responsible for electronic authentication is referred to by multiple names. Some scholars call it "certification service providers," defining it as "a public or private body or institution that issues electronic certificates, acting as an electronic registry securing the electronic signature, identifying the signatory, and associating the public key with him. Another scholarly view refers to the entities specializing in electronic authentication as "publicity authorities," defining them as "a neutral public or private entity that provides security services in electronic commerce by issuing certificates that verify the authenticity of a specific fact related to the subject of electronic exchange, to authenticate the identity of the individuals using the digital signature (Al-Muzail, 2017, p. 223).

A public or private entity operates under the supervision of the executive authority and usually consists of three different levels of authority. The highest level is the "main authority," which specializes in the technological certification of practices for all parties licensed to issue pairs of encryption keys or certificates related to the use of those keys. Following this is the certification authority, which is responsible for certifying that a user's public key corresponds to that user's private key. At a lower level, there is a local registration authority whose task is to receive applications from individuals seeking to obtain public and private encryption key pairs. It also verifies the identity and persona of these users and grants certification certificates that validate the client's signatures (Qarawish, 2017, p. 413).

According to Article 02 of the (Law N°15, 2015), the third party authorized to carry out the authentication task is termed "Electronic Authentication Entity." This entity is defined in the aforementioned article as the body licensed or accredited by the Telecommunications Regulatory Authority or legally authorized to issue authentication certificates and provide any services related to these certificates according to the provisions of this law and the regulations and instructions issued thereunder. Article 05 of the (Law N°15, 2015) that the Ministry of Digital Economy and Entrepreneurship serves as the electronic authentication entity for ministries, official public institutions, public entities, and municipalities and is responsible for issuing electronic authentication certificates for use in any of their transactions.

The Cabinet, based on the recommendation of the Minister of Communications and Information Technology, may entrust any public official entity or governmental body with the tasks stated in paragraph (a) of this article. Moreover, paragraph two of Article 23 of the (Law N°15, 2015) that the Telecommunications Regulatory Authority is the competent authority to license, accredit, and regulate the activities of electronic authentication entities in accordance with the regulations and instructions issued under the provisions of this law.

It is worth noting that the Jordanian legislator has set strict financial penalties for any entity that operates as an electronic authentication entity without obtaining a license or accreditation according to the provisions of the law. Article 26 of the Electronic Transactions Law stipulates that anyone who practices the activity of electronic authentication entities within the Kingdom without obtaining a license or accreditation according to the provisions of this law and the regulations issued thereunder shall be fined no less than 50,000 Jordanian Dinars and no more than 100,000 Jordanian Dinars.

The Algerian legislator, referring to Article 02 of (Law N°15/04, 2015), distinguishes between two types of entities responsible for electronic certification. The first entity is named the "Trusted Party" and is defined as a legal entity that issues described electronic certification certificates and may provide other services related to electronic certification for stakeholders in the governmental sector. The second entity is named by the Algerian legislator as the "Electronic Certification Service Provider," and Article 02 previously mentioned defines it as a natural or legal person who issues described electronic certification certificates and may offer other services in the field of electronic certification.

2.2. The legal force of the electronic authentication certificate

In this section, we address the legal force of electronic authentication (01) and then the termination and suspension of the electronic authentication certificate (02).

2.2.1. The Validity of Electronic Authentication

Referring to Article 05 of (Article 2 of the Directive N 1999/93, 1999), it specifies two types of signatures: the simple electronic signature and the secured electronic signature. The simple electronic signature does not meet the security requirements and requires the establishment of proof in court that it was executed in a reliable manner, while the secured electronic signature is characterized by a high degree of security and has various legal conditions set so that it can be valid for proving authenticity (Baha, 2015, p. 395).

Referring to the Jordanian legislator in Article 17 of the (Law N°15, 2015), it states that the electronic record associated with a protected electronic signature has the same validity as an ordinary document and may be invoked by the parties to the electronic transaction. The electronic record linked to a verified electronic signature has the same validity as an ordinary document and may be invoked by both the parties to the electronic transaction and others. This article clarifies that legal actions have the same validity and effect as traditional actions and can be contested by the parties to the transaction if linked to a protected electronic signature, or by others and the parties if linked to a verified electronic signature. Article 16 of the (Law N°15, 2015) specifies the conditions that must be met in the electronic signature for it to be considered reliable. These are the same

conditions specified by the Algerian legislator in Article 07 of (Law N°15/04, 2015), termed the described electronic signature. These conditions include:

- If it is linked to an electronic authentication certificate: issued at the time of creating the electronic signature by a licensed electronic authentication entity in the Kingdom, or an accredited electronic authentication entity or any other government entity approved by the Council of Ministers, the Ministry of Digital Economy and Entrepreneurship, and finally the Central Bank of Jordan in relation to banking or financial electronic transactions. This was expressed by the Algerian legislator as being based on a described electronic certification certificate.
- If it is uniquely used by the owner of the signature to distinguish it from others: meaning it is linked exclusively to the signer: This implies that the signature owner has a unique code and data that differ from other signers, so for the signature to perform its functions, it must be directly related to the signer. The owner of the signature, as defined by Article 02 of the (Law N°15/04, 2015), is the person who has been issued an electronic authentication certificate and holds both the public and private keys, whether he signs himself or through a representative or agent. The Algerian legislator defined it in Article 02 of (Law N°15/04, 2015) as a natural person who possesses the data for creating the electronic signature and acts on his own behalf or on behalf of the natural or legal person he represents.
- If it identifies the owner of the signature
- If the private key is under the control of the signature owner at the time of signing
- If it is linked to the electronic record in a way that does not allow for modifications to that electronic record after signing without altering that signature.

As for the Algerian legislator, when we refer to Article 07 of (Law N°15/04, 2015), we find that a set of conditions have been established for the electronic signature to be considered valid. These conditions include:

- It must be linked exclusively to the signer:
- It must be able to identify the identity of the signer, which is the same condition stipulated in the Jordanian law.
- The private key must have been under the control of the signer at the time of signing: The Algerian legislator expressed this by stating that it must be created by means that are under the exclusive control of the signer.
- It must be linked to the electronic record in such a way that does not allow for modifications to that electronic record after signing without altering that signature. The Algerian legislator expressed this by stating that it should be linked to its specific data, in such a way that any subsequent changes to these data can be detected, and it should be designed by a secure mechanism specifically for creating the electronic signature, The secure mechanism for creating the electronic signature is the electronic signature creation mechanism which must be according to Article 11 of (Law N°15/04, 2015):

    - It must be ensured by appropriate technical means and procedures at least the following:
        - Practically, it is not possible to accidentally generate the data used to create the electronic signature more than once, and their confidentiality must be guaranteed by all available technical means at the time of accreditation.
        - It must be impossible to deduce the data used to create the electronic signature and that this signature is protected from any forgery by the technical means available at the time of accreditation.
        - The data used to create the electronic signature must be reliably protected by the legitimate signer from any use by others.
    - The data subject to the signature must not be altered and must not prevent these data from being presented to the signer before the signing process. It is noted that these conditions are purely technical and technical in nature. If these conditions are met, the electronic signature is authenticated and has validity. The availability of these conditions depends on the presence of an electronic certification certificate. This concerns the validity of the national electronic authentication certificate, while regarding the validity of the foreign electronic authentication certificate, the Algerian legislator in Article 63 of (Law N°15/04, 2015) equated the national

and foreign electronic authentication certificates issued by a foreign authentication service provider in terms of validity, provided that the foreign service provider acted within the framework of a mutual recognition agreement concluded by the authority.

2.2.2. Suspension and Cancellation of the Authentication Certificate

The competent authority issuing the electronic authentication certificate is obliged to cancel or suspend its operation in certain cases, such as if it becomes aware of the forgery of documents presented to it by stakeholders, or if it finds from its investigations that the person named in the certificate has become bankrupt, lost their legal capacity, or their job.

Therefore, this authority is responsible if it delays taking the necessary measures to cancel the authentication certificate. The cancellation and suspension of operation can be based either on a request from the signer directed to the electronic authentication entity or by the electronic authentication entity itself on its own accord based on justified reasons that will be mentioned in this point.

Suspension of operation refers to the temporary cessation of the certificate's validity, which means disabling the legal effect associated with it until one of two things occurs: either the resumption of its operation after the removal of the impeding reason or its final cancellation. Notably, some of the prominent cases of suspending the certificate's operation are:

- Based on a request from the certificate owner: Whether as an individual on their behalf or as the legal representative of a legal entity, however, the response to the owner's request to suspend the certificate is contingent upon the justification of this request, out of concern for the rights of others involved.
- The presence of evidence, based on documented data that indicates a violation of the electronic signature creation system or the use of the certificate for fraudulent purposes, which requires the accredited authentication entity to promptly suspend the certificate operation on its own initiative, otherwise, it will be civilly and criminally liable for this violation.

The prominent cases for the cancellation of the authentication certificate are:

- Cancellation of the certificate upon the request of its owner, which is a personal right granted to the owner alone. Even if others have rights related to the certificate, they do not have the right to request its cancellation; their right is limited to seeking compensation from the owner if they suffer any harm as a result.
- Cancellation of the certificate due to the death of the natural person or dissolution of the legal entity, in addition to the bankruptcy of the person in whose name the certificate was issued or loss of their legal capacity, as these are reasons that obligate the authentication entity to cancel the certificate.
- Cancellation of the certificate if the reason leading to its temporary suspension is proven to be valid, and also if the information contained in the suspended certificate is found to be inaccurate.
- Cancellation of the certificate due to a change in the information contained in the certificate.

In practical reality, authentication entities place the numbers of certificates whose operations have been suspended or cancelled in a dated and signed list on their websites, enabling everyone to identify the certificates that have been suspended or cancelled. The obligation of the electronic authentication entity is a commitment to achieve a result if it is based on the orders of the certificate owner, and its responsibility arises simply from the failure to achieve this result. However, when assuming that the authentication entity takes the initiative on its own, its commitment is classified as an exercise of due diligence, because the reasons for cancelling or suspending the certificate are based on the credibility of the authenticated information and its changes. It is perhaps impossible to absolutely guarantee the accuracy of this information under all circumstances (Darawsha, 2018, pp. 31-33).

3. The Role of Electronic Authentication in Protecting Electronic Transactions

For electronic authentication to protect electronic signatures from manipulation and fraud, thereby protecting electronic transactions from tampering, authentication entities must adhere to a set of obligations. In this axis, we will discuss these obligations: verifying the identity of the signer, maintaining confidentiality, proving electronic exchange, determining the moment the contract is concluded, issuing electronic keys, issuing electronic authentication certificates, and mandatory insurance.

3.1. Verifying the identity of the signer

Verifying the identity of the signer is the primary obligation that falls on the certification authorities, which is done through various identification documents provided by the subscriber, such as personal identification and passport. They issue an electronic authentication certificate that certifies the electronic document in a specific contract, thereby attesting to its authenticity and its attribution to the issuer. If one of the parties places an electronic signature on the electronic data message and a neutral entity guarantees its accuracy, this confirms that the signature originated from its owner and entails verifying the identity of the signer by determining the legal capacity of the contracting party (Musadiq, 2020, pp. 39-40).

Due to the critical nature of this obligation, the electronic authentication entity is required to provide compensation if the certificate contains inaccurate data, as long as the client has no way to verify the accuracy of the information and data in the electronic authentication certificate. Some believe that the authentication entity is only responsible for the accurate data that is provided by the client, but it must examine this data to ensure its consistency with the submitted documents.

Therefore, if it is later proven that the data was falsified by its owner or its validity has expired, and if the appearance of this data did not indicate this, then the authentication entity that issued the certificate does not bear any responsibility. Moreover, the competent entity issuing the authentication certificate is not allowed to make any reservations about the accuracy of the data in the electronic certificate; it is obligated to verify all the data legally required for issuing the certificate. In the case of missing data or proof of forgery, it must refrain from issuing the certificate, noting that the obligation on its part is a duty of care (Darawsha, 2018, p. 29) and not a duty to achieve a result.

3.2. The Obligation of Confidentiality

The obligation to maintain confidentiality by electronic authentication entities is one of the most critical obligations imposed on them, and it is one of the obligations that could assess the liability of the authentication entities towards the owner of the electronic certificate, whether it is civil or criminal liability. All this supports trust among parties interacting through electronic means, especially since most electronic transactions occur between people who do not meet and do not know each other. Without these guarantees, people would not engage in concluding contracts and completing transactions (Kabisi, 2012, p. 218).

The Algerian legislator, in Article 42 of (Law N°15/04, 2015), obliges the providers of electronic authentication services to maintain the confidentiality of the data and information related to the electronic authentication certificate.

3.3. Proving the Content of Electronic Exchange

The authentication authority is responsible for proving the existence and content of the electronic exchange between parties, ensuring its integrity and protection from fraud and deception. To prevent any fraud towards internet users, authentication entities monitor commercial sites by investigating their actual existence and credibility. If it is found that these sites are not genuine or are not serious, they warn the parties involved. These

entities can also be approached before concluding a contract to verify the company with which the contract will be made (Musadiq, 2020, p. 40).

3.4. Determining the Moment of Contract Conclusion

Determining the moment of contract conclusion is not a condition for the validity of the action; however, identifying that moment is necessary because the time of contract conclusion marks the beginning of arranging legal effects. For instance, determining the moment of completing an electronic bank transfer has several implications. It includes determining the end of the transfer upon the bankruptcy of one of the parties, and also determining the possibility of reversing the order of the transfer as long as the amount has not moved from the account of the originator to the account of the beneficiary. Once the transfer is complete, this leads to the impossibility of dealing with the financial amount subject to the transfer order (Musadiq, 2020, p. 40).

3.5. Issuing Electronic Keys

These entities are responsible for issuing electronic keys, both the private key, which is used to encrypt the electronic transaction, and the public key, which is used to decrypt this encryption. Thus, these entities ensure that the public key corresponds by verifying its match and validity.

Additionally, these entities issue the digital signature. The authentication applicant provides the necessary data to the authentication entity, then the private key specific to the signature authentication request is issued. This key can only be used from one computer to ensure that the digital signature originates from its owner. Therefore, the owner of the private key must keep it confidential and not disclose it to anyone. As for the public key, it is usually kept by the authentication entities, which send it by email to anyone wishing to interact with the owner of the electronic signature, thus enabling the verification of the signature's validity. The authentication entity must transmit the electronic signature with its key.

3.6. Issuing the Electronic Authentication Certificate

Issuing an electronic authentication certificate is one of the most important measures that protect the electronic signature and electronic transactions. It is also considered one of the most significant obligations and functions incumbent on the authentication entity, as the authentication certificate confirms the attribution of the signature to its owner, provided its conditions are met.

The authentication entity is committed to issuing and delivering electronic authentication certificates that include all the data legally required to confirm the identity of the signer. If one of the parties places their electronic signature on an electronic data message and the authentication entity guarantees the accuracy of the message with the electronic signature, this confirms that the electronic signature originates from its owner. This leads to determining the contracting party's eligibility. Thus, the purpose of obtaining an authentication certificate becomes clear—it ensures that neither party denies their signature placed on the electronically sent document and serves as proof that the signer possesses a private key and is the one who signed (Sheikh, 2021, p. 276).

The Jordanian and Algerian legislators have obligated authentication entities to issue and grant authentication certificates according to their respective electronic authentication policies, as stipulated by Article 23 of the Jordanian Electronic Transactions Law and Article 41 of the Algerian Law defining the general rules for electronic signatures and authentication.

The obligation of an electronic authentication entity is considered a duty to achieve a result because the purpose of licensing an authentication entity is to enable it to issue accredited authentication certificates based on which transactions are conducted. The goal of obtaining this certificate for a website is to impart a sense of trust and

security to its electronic signature in order to gain the confidence of parties for conducting various commercial transactions (Sheikh, 2021, p. 277).

3.7. Mandatory Insurance

Through Article 60 of (Law N°15/04, 2015), the Algerian legislator has mandated that providers of electronic authentication services must enter into insurance contracts as stipulated in the electronic authentication policy of the economic authority.

Making insurance mandatory helps to instill confidence in electronic transactions and encourages their spread. Given the severe damages that can result from electronic transactions, which authentication entities may be unable to bear, the insurance system from liability is considered an effective solution for compensating these damages.

4. Conclusion

The foundation of electronic contracting is the existence of trust between the parties involved; without it, one cannot speak of electronic contracting. Electronic authentication is the most important mechanism through which an electronic contract can be concluded and is a significant innovation introduced by both the Jordanian and Algerian legislators. Through this intervention, we have reached a set of results and recommendations, which are summarized as follows:

4.1. Results

- An electronic authentication certificate is an electronic document issued by the authentication entity that includes a set of data related to the parties of the contract or the certificate itself. Its purpose is to prove the validity of the electronic signature and to grant it legal authenticity, making it equivalent to a traditional handwritten signature.
- The electronic authentication certificate contains a variety of data, some related to the service provider, some to the certificate owner, and some to the act subject to the certificate. This data includes both optional and mandatory elements.
- The Algerian and Jordanian legislators have given the electronic authentication certificate the same legal value as official documents, and it has the same evidentiary strength as official writings.
- The Algerian and Jordanian legislators have equated the evidentiary strength of the Algerian authentication certificate with that of a foreign authentication certificate.
- Upon being informed of the death of a natural person or the dissolution of the legal entity owning the certificate, the service provider must immediately cancel it, because electronic authentication is among the contracts based on personal consideration and thus terminates upon the death of the natural person or dissolution of the legal entity owning the certificate.
- The service provider bears any damage caused by their error resulting from the suspension of the service or breach of the obligations incumbent upon them, such as the obligation to notify, unless the certificate owner knew or ought to have known that the certificate had expired.

4.2. Recommendations

- The Jordanian legislator should amend the Electronic Transactions Law by adding and clarifying the cases of cancellation and suspension of the electronic authentication certificate. Similarly, the Algerian legislator should amend Law 15/04 to add cases for the suspension of authentication certificates.
- The Jordanian legislator should stipulate the mandatory insurance.
- Efforts should be made to inform the electronic consumer of their right to resort to electronic authentication authorities to verify the data related to commercial companies.

- It is necessary to secure e-commerce sites with programs that ensure their protection from all methods of fraud and to strengthen penalties against offenders.

Funding: Not applicable.

Conflict of Interest: The authors declare no conflict of interest.

Informed Consent Statement/Ethics Approval: Not applicable.

References

Al-Muzail, S. M. (2017). Electronic Authentication in the Field of Electronic Banking: A Comparative Study. *The Legal Journal*(2).

Al-Saadi, G. J., & Al-Hasan, A. M. (2017). The Legal System for the Electronic Authentication Certificate: A Comparative Study. *AL- Mouhaqiq Al-Hilly Journal for legal and political science*(2).

Al-Shanraqi, H. M. (2013). *Cybercrimes: A Comparative Applied Study on Crimes Against the Electronic Signature.* Egypt: Legal Books Publishing House.

Article 2 of the Directive N 1999/93. (1999, 12 13). The European Directive on Electronic Signatures.

Baha, F. (2015). The Electronic Certification Certificate as a Mechanism to Guarantee the Validity of Electronic Transactions in Light of Law No. 04-15 Related to Electronic Signature and Certification in Algerian Law. *Journal of Research in Law and Political Science, 1*(02).

Darawsha, S. A. (2018). Civil Liability of Electronic Authentication Entities: A Comparative Analytical Study. *Jerash for Research and Studies, 19*(01).

Kabisi, Z. (2012, 06). The Legal System of Electronic Authentication (Certification) Entities. *Notebooks of Policy and Law*(7).

Law N°15. (2015). Jordanian Electronic Transactions Law.

Law N°15/04. (2015, 02 01). defines the general rules related to electronic signing and authentication.

Musadiq, F. Z. (2020). Electronic Authentication as a Means to Protect the Electronic Signature. *Journal of Studies and Researches, 5*(1).

Qarawish, R. (2017). Electronic Authentication Entities under Law 15/04 Related to the General Rules for Electronic Signatures and Authentication (Concept and Obligations). *Journal of Social Sciences*(24).

Sheikh, S. (2021). The Role of Electronic Authentication Entities in Achieving Electronic Information Security. *Journal of Law and Humanities, 14*(01).

Yahiaoui, S. (2022). Electronic Certification: A Technical Mechanism for Ensuring and Protecting Electronic Commercial Transactions in Algerian Law. *Journal of Comparative Legal Studies, 8*(1).