



International Journal of Electronic Security and Digital Forensics

ISSN online: 1751-9128 - ISSN print: 1751-911X
<https://www.inderscience.com/ijesdf>

The legal authority of the electronic authentication certificate and its role in proving e-commerce transactions

Lana Al-Khalaileh, Tareq Al-Billeh, Ali Al-Hammouri

DOI: [10.1504/IJESDF.2025.10068183](https://doi.org/10.1504/IJESDF.2025.10068183)

Article History:

Received:	28 May 2023
Last revised:	06 July 2023
Accepted:	13 July 2023
Published online:	23 December 2024

The legal authority of the electronic authentication certificate and its role in proving e-commerce transactions

Lana Al-Khalaileh*, Tareq Al-Billeh and
Ali Al-Hammouri

Department of Law,
Applied Science Private University,
Al Arab St 21, Amman, Jordan
Email: l_khalileh@asu.edu.jo
Email: Lanahmoud@yahoo.com
Email: t_billeh@asu.edu.jo
Email: a_alhammouri@asu.edu.jo

*Corresponding author

Abstract: This article analyses the concept of the electronic authentication certificate and shows its types issued by electronic authentication authorities according to the function they perform and the purpose of their issuance. It will also show the legal recognition of electronic certificates by referring to the national legislations in Jordan, Egypt, France and Tunisia, and the extent to which these legislations comply with international requirements. In this study, light will also be shed on achieving trust and safety among dealers through modern means of communication, especially via the Internet, and on encouraging dealing with electronically signed documents through the use of a reliable, neutral third party. This party will be responsible for verifying the integrity of the electronic certificates and the validity of their issuance, as well as ensuring the seriousness of the dealing and that it is free from fraud.

Keywords: electronic documentation; legal authority; electronic documents; international requirements; electronic commerce; electronic transactions.

Reference to this paper should be made as follows: Al-Khalaileh, L., Al-Billeh, T. and Al-Hammouri, A. (2025) 'The legal authority of the electronic authentication certificate and its role in proving e-commerce transactions', *Int. J. Electronic Security and Digital Forensics*, Vol. 17, Nos. 1/2, pp.267–282.

Biographical notes: Lana Al-Khalaileh is an Assistant Professor Faculty of Law, Department of Law – Applied Science Private University (ASU) and practices the legal profession, and worked as a lawyer and legal advisor. She has many refereed research papers published in scientific journals. Her research areas focus on cyber law, family law, and environmental law and electronic commerce and Intellectual property and civil law and research interests and criminal laws and electronic crimes and rights and freedoms in the age of technology and private international law. She specialised in national and international environmental legislation and specialised in the subject from an academic point of view, and my career objectives contribute to raising the legal scientific level of students.

Tareq Al-Billeh is an Assistant Professor at the Faculty of Law, Department of Law – Applied Science Private University (ASU), and received a letter of thanks from Johns Hopkins University/Washington (SAIS), and practices the legal profession. He worked as a lawyer and legal advisor with the Jordan Petrol Refinery PLC (Legal Affairs & Risks Management Unit). He has many refereed research papers published in scientific journals. His research areas focus on cyber law, family law, and environmental law and administrative law and administrative judiciary and constitutional law and constitutional judiciary and criminal laws and electronic crimes and rights and freedoms in the age of technology.

Ali Al-Hammouri is an Assistant Professor at the Faculty of Law, Department of Law – Applied Science Private University (ASU) and practices the legal profession, and worked as a lawyer and legal advisor. He has many refereed research papers published in scientific journals. His research areas focus on cyber law, family law, and environmental law and public international law and climate justice and human rights and environmental justice and electronic crimes and rights and freedoms in the age of technology. He specialised in national and international environmental legislation and specialised in the subject from an academic point of view, and my career objectives contribute to raising the legal scientific level of students.

1 Introduction

The current rapid technological and technological progress has resulted in the introduction of new means that have contributed to the speed and convenience of getting and spreading information, regardless of its geographical and spatial remoteness (Reed, 2001). However, the fast advancement of electronic transactions in the current period is still hampered by various issues and barriers that prevent their widespread use. The most notable of them are the lack of security and secrecy in electronic transactions as a result of hacking, the difficulty of proving these transactions and recording their content, and guaranteeing that no modifications or changes are done to this material (Bromby, 2010).

Due to the escalation of breaches and abuses in the electronics sector, impartial parties were enlisted to document electronic transactions by developing an electronic documentation system that strives to ensure a safe electronic environment for Internet transactions (Greenwood and Campbell, 1997). Electronic authentication authority act as a trustworthy and unbiased intermediary between dealers in electronic exchanges, authenticating the parties' identities and assessing their eligibility for dealing (Bennett, 1997).

The electronic documentation system also ensures the content of the data circulated between them, which is accomplished through the issuance of an electronic certificate by electronic authentication authorities, the function of which is to link the holder of the electronic signature with its public key. It also ensures that no side will contest the electronic signature on the document (Wang, 2010).

In addition, it is a clear and explicit indication that the signer owns the private cipher key. So, he is the one who signed. Hence, these certificates constitute an important and sure guarantee for people who wish to deal with him. They also ensure the fulfilment of important functions, namely confidentiality, safety and authenticity (Al-Zahra and Jamila, 2019). This prompts us to question the importance and role of the electronic

authentication certificate and specifically about the extent of its contribution to providing confidence and security for customers using electronic means of communication.

The importance of the study lies in defining the role of documenting electronic transactions, as it is the personal identity through which electronic transactions are conducted via the internet, and proving the identity of the electronic signature holder and the validity of the electronic transaction. An electronic signature documented by an electronic certificate issued by a competent authority enjoys the necessary legal authority in evidence, like a traditional signature. This was confirmed by most of the legislations that regulated the work of the authorities concerned with issuing electronic authentication certificates.

The study aims to demonstrate: the compliance of national legislation with international requirements in electronic documentation; the most prominent types of certificates that can be issued by electronic documentation agencies according to the function they perform and the purpose of issuing them; the legal recognition of this type of electronic document by referring to the national legislations in Jordan, Egypt, France and Tunisia; and achieving trust and safety for customers through modern means of communication, especially via the internet.

The problem of the study is manifested in the absence of a clear and well-defined legislative framework for the legal authority enjoyed by electronic authentication certificates. In the Electronic Transactions Law, the Jordanian legislator contented himself with setting a general regulation for the authenticity of electronic documents without allocating the electronic authentication certificate with special provisions. The same applies to the aforementioned law, as its texts dealt with electronic documents in general without referring specifically to commercial ones. From this issue, the main study problem emerges, which is the answer to the question related to the extent of the legal authenticity enjoyed by the electronic authentication certificate, whether certificates issued by national or foreign authentication bodies. Does it have the same authenticity as traditional documents? Does it have evidentiary power that can be relied upon in the event of a dispute between its parties?

Therefore, the study seeks to answer several legal questions, the most important of which are: What is the concept of the electronic authentication certificate issued by the electronic authentication authorities? What are the electronic authentication authorities? What are its main functions? What is the validity of the electronic authentication certificate in Jordanian and comparative legislation?

This study adopted the descriptive, analytical and comparative approach. Through the descriptive approach, the position of the Jordanian legislator will be described by listing the different rules. As for the analytical approach, its purpose is to analyse the legal texts contained in the Jordanian legislation related to the study to determine their effectiveness and shortcomings in addressing the issue of authenticity of electronic authentication certificates. In addition, the comparative approach is used to compare what the Jordanian legislator stated regarding the authenticity of electronic authentication certificates with some comparative legislation to assess the most prominent aspects of agreement and disagreement, and to benefit from the legal experiences of other countries in dealing with this legal problem in this regard.

2 What is the electronic authentication certificate?

Electronic authentication plays an essential role in the security of e-commerce transactions. It is not possible to achieve practical results in the field of these transactions without raising the level of people's confidence in the security of the electronic system and the legal protection of electronic transactions in the various laws and legislations. This can only be achieved through the existence of a modern secure technology system aimed at identifying the parties to e-commerce documents and verifying their electronic signatures. It is the electronic authentication authority (Moqaddam and Issa, 2014; Masadeh, 2023).

2.1 *Concept of electronic authentication certificate*

Dealers in the field of electronic transactions and contracts need a way to ensure the security of their transactions, whether individual or commercial, so as to remove their fears of others breaking into the confidentiality of their electronic data and contents, and to assure them of the identity of the other party and the validity of his signature. This role has been entrusted with an electronic authentication certificate. In view of the importance of these certificates, it prompts us to define their concept by reviewing the various definitions that have been developed for them and addressing the various types that derive from them (Al-Dakhili, 2018).

2.1.1 *Definition of electronic authentication certificate*

Many legislations that regulated electronic transactions defined the term electronic authentication certificate. The UNCITRAL Model Law on Electronic Signatures defines them in Article (2/b) thereof as: "a data message or other record confirming the connection between the signatory and the signature creation data". From this definition, it becomes clear to us that the legislator in UNCITRAL law has mentioned the nature of the certificate as a data message and the purpose of its issuance, which is to indicate the existence of a link between the personality of the signer and the signature creation data, or to confirm the existence of this link. However, this definition has been subjected to several criticisms, the most prominent of which is that it neglected to specify the authority issuing this certificate, which is the electronic authentication authority (Al-Safadi, 2010).

The guiding Arab law of proof using modern technologies defines the electronic authentication certificate as: "A certificate proving the relationship between the signatory and the electronic document attributed to him, issued by the authentication authority". However, this definition is criticised for not showing the nature of the certificate and not specifying the data contained therein. It also did not indicate whether the certification body should be licensed or accredited.

As for the European directive on electronic signatures, it was more precise in its definition of the electronic authentication certificate. It distinguished between the simple electronic certificate and the electronic certificate described in the ninth and tenth paragraphs of Article (2) thereof. It defined the first as the electronic certificate that links the electronic signature verification data to a specific person and confirms the identity of that person. As for the described certificate, it defined it as a certificate that fulfils the requirements stipulated in the first appendix, which is submitted by the person assigned

to the authentication service who fulfils the requirements stipulated in the second appendix (Al-Khafaji and Hussein, 2016).

As for the Arab legislation, we find that the Jordanian legislator has defined the electronic authentication certificate in Article (2) of the Electronic Transactions Law as: "The certificate issued by the electronic authentication authority to prove the attribution of an electronic signature to a specific person based on approved authentication procedures". The same applies to the Egyptian legislator, who defined the certificate in Article (1) of the law regulating the electronic signature as: "The certificate issued by the authority authorized to ratify and proves the link between the signatory and the signature creation data". It is the same definition contained in Article 1/8 of the executive regulations. What is noted about these two previous definitions for both the Jordanian and Egyptian legislators is that they are very similar to the definition provided by the UNCITRAL Model Law on Electronic Signatures in that they did not address the certificate issued by an accredited authority, nor did they clarify the nature of the data that should be mentioned in the certificate. It was also emphasised that the purpose of the electronic authentication certificate is limited to proving the validity of the electronic signature and its association with its holder, and clarifying his identity.

The Tunisian legislation also defined the authentication certificate, or as it called it the "electronic authentication certificate," as: "the electronic document secured by the electronic signature of the person who issued it, who certifies through it the effect of inspection on the validity of the data it contains". It is clear from this definition, unlike most of the definitions that have been dealt with, that the nature of the certificate was mentioned when it was stated that it is an electronic document, and it also specified its function of proving the validity of the data it contains. However, it did not address the originating or issuing authority of the certificate, nor the mechanisms used in issuing it. Nor did he distinguish between the ordinary authentication certificate and the accredited or prescribed authentication certificate (Al Saadi, 2017).

Turning to the jurisprudential aspect, we find that many legal scholars have set several definitions for the electronic authentication certificate, including: "The certificate issued by the electronic authentication service provider, according to which it certifies the validity of the electronic signature and its attribution to the person who issued it, and that it fulfills the conditions and criteria necessary to recognise its authority in proof" (Kamil, 2009). While others went to define it as: "an identity issued by a neutral person to identify the person who carries it and to authenticate his electronic signature and the transactions he conducts via the Internet" (Al-Mazouri, 2018). It was also defined as: "An identity or electronic card issued by a competent authentication authority, which includes a set of basic data related to the certificate and the identity of the sender. It proves the identity of the person who sent the electronic message by linking his private key to the public according to certain controls" (Hassan, 2009).

Accordingly, we can deduce from the aforementioned definitions, whether legislative or jurisprudential, that they revolve around one axis that the certificate is an electronic document issued by a trustworthy and neutral party that includes a set of data whose primary function is to prove the identity of the signatory, and to verify the validity of his signature and attributing it to him, in addition to ensuring the validity of the data included in the electronic transaction (Nuseirat, 2005).

2.1.2 Types of electronic authentication certificate

The certificates that can be issued by electronic authentication bodies vary according to the function they perform and the purpose of issuing them. Most notably are (Al-Zahra and Jamila, 2019):

- *Electronic signature authentication certificate*: This certificate is one of the most common types of certificates and the most important because the authentication authority issues it and certifies the authenticity of the signature and its attribution to the person it was issued by. This certificate also contains the public key as well as information indicating the identity of the holder of the corresponding private key, i.e., the identity of the person to whom the electronic signature is attributed. It also shows the right and authority of the signatory and his power to conclude various legal actions (Haj Ali, 2013).
- *Identifications certificate*: This certificate works to identify the person by keeping names on the Internet or on smart cards, while the task of the electronic authentication authority is to verify people's identities. It should be noted here that the name in the world of digital communications does not necessarily have to be a unique name or a real name, but rather a pseudonym may be used. The person's name, address or ID card number may be used. After issuing definition certificates, the documentation authority publishes them on its website so that they are available to all. These certificates are often used in bank or banking transactions (Hassan, 2009).
- *Certificate of authorisation*: It is the certificate by which additional information about a person is provided beyond merely identifying him or her. For example, information is provided regarding his work and qualifications, place of residence, or licenses he possesses. The role of this certificate is not limited to merely providing general information about the applicant, but it works to introduce him in a comprehensive and accurate way (Daze Yee, 2016).
- *Statement certificate*: This type of certificate is not issued in order to link a specific person to a specific key or code, as is the case with the authorisation and identification certificates, but rather its mission is to indicate the validity of a specific event or incident and specify the time of its occurrence.
- *Certificate documenting the time and date of issuing the electronic signature*: It is the certificate that is concerned with documenting the date and time of issuing the electronic signature. This is achieved by the holder of the message, after signing it, sending it to the authentication authority, which records the date and signature on it, and then sends it back to the sender. This type of certificates is very important, because there are cases in which it is very important to state exactly when the incident occurred, and to prove whether it occurred before or after a certain date. Therefore, the role of this certificate lies in establishing evidence of the date and time in which the electronic signature of the document concerned took place (Hassan, 2009).

The aforementioned types may be for national or foreign authentication certificates. As for the national authentication certificate, it is issued by the national electronic authentication authorities. As for the foreign authentication certificate, it is issued by

recognised foreign electronic authentication agencies. Its evidentiary authority has been recognised in legislation related to electronic transactions (Al-Aish, 2008).

2.2 Electronic documentation authorities

The availability of the elements of trust and safety among the parties to e-commerce transactions is one of the most important things that must be available in such transactions, given that e-commerce transactions generally depend on an open network for their procedures. Most of the contracts concluded between its parties are considered to be contracts concluded between absentees, for whom the place and time of the contract differ. In order for this trust to exist between the parties to the contract, the presence of a neutral third party is required to verify the authenticity of the electronic signature and its attribution to the signer, as well as to give it the evidentiary power. This party is called the electronic authentication authority (Ibrahim, 2010).

Given the importance of the role played by this authority in providing guarantees to determine the identity of customers, considering that the electronic documentation stage is the most important in electronic contracting, because it plays a prominent role in proving the conclusion of the contract and verifying the correctness of the information contained therein, and not being subject to forgery or alteration, we must explain what this authority is in terms of its definition, and clarify the functions it performs (Daze Yee, 2017; Al-Billeh, 2022a).

2.2.1 The concept of the electronic authentication authority

To begin with, it is necessary to point out the multiplicity of jurisprudential and legislative definitions in terms of electronic authentication. There is also no unified designation for this authority in the legislation of the different countries that regulate its work and responsibility. It has been called by several names, such as: the electronic certification body, the electronic signature authentication body, and the electronic certification services provider. Despite the different names, it remains only a formal difference (Darawshah, 2018). For example, the UNCITRAL Model Law on Electronic Signatures called it a “provider of certification services” and defined it as: “a person who issues certificates and may provide other services related to electronic signatures”. The same applies to the European legislator, who used the same name and defined it in the European Directive on Electronic Signatures issued in 1999 as: “Every natural or legal person who undertakes the task of issuing electronic authentication certificates or provides other services related to electronic signature.” The services related to the electronic signature mean the technologies that allow the issuance of a model signature, or publishing, viewing and other informational services such as archiving (Mason, 2012).

As for the French legislation, it called it “the person in charge of the electronic authentication service” and defined it in Decree No. (272/2001) issued March 30, 2001 as: “every person who issues electronic certificates or provides other services related to electronic signature”.

We note that the three aforementioned definitions contained in UNCITRAL law, European directives and French law agree that the person who provides documentation services can be a natural or legal person. Although the European directive mentioned this explicitly, the UNCITRAL law and the French law mentioned only the word “person”, which is a general word that includes the natural and legal person. We believe that in

practice it is not conceivable that a natural person would do this work, because electronic documentation services require high and very expensive material and technical capabilities that only a legal person can do, whether it is a general legal person or a private legal person.

As for Arab legislation, the Jordanian legislator called it the “electronic authentication authority” and defined it in Article (2) of the Electronic Transactions Law No. (15) of 2015 as: “the authority licensed or approved by the Telecommunications Regulatory Authority or legally authorised to issue authentication certificates and provide any services related to these certificates in accordance with the provisions of this law and the regulations and instructions issued pursuant thereto”. The Tunisian legislator defined it under the name “electronic authentication services provider” in the Tunisian Exchange Law as: “every natural or legal person who creates, delivers and disposes of authentication certificates and provides other services related to electronic signature”. The legislator of the Emirate of Dubai also defined it as a “certification services provider” in the Dubai Electronic Transactions and Commerce Law as: “any accredited or recognized person or authority that issues electronic authentication certificates or any services or tasks related to electronic signatures organized under the provisions of Chapter Five of this law”.

It is clear from the previous texts that despite the multiplicity and different designations used for this authority, it focused in defining the concept of the authentication authority on stating the basic function of this authority and its purpose, which is to issue an electronic authentication certificate to prove the validity of the electronic signature and the extent of its association with its holder, in addition to providing any other services related to signature certificates, i.e. related to the authenticated electronic signature.

There are also many jurisprudential definitions in terms of electronic authentication. It has been defined as: “an official or private organization entrusted with confirming and documenting an electronic transaction to instill confidence in users of open networks by following a number of procedures and technical means necessary to secure or protect the transactions between them from tampering as long as they are preserved and to issue an approved electronic certificate that proves all of this, protects it, and inspires confidence in it, in order to ensure the creation of a safe electronic environment for dealing through the network” (Al-Rajwani, 2014). Others defined it as: “An organization or a public or private authority that issues electronic certificates that secure the validity of the signatory or the authenticity of his signature, confirm his identity, and enable him to know the public key” (Darawsheh, 2018).

Based on the aforementioned legislative and jurisprudential definitions of the electronic authentication entity, we can define it as: “a natural or legal person, public or private, subject to the supervision and control of the state, who plays the role of an electronic mediator by issuing electronic authentication certificates, which determine the identity of the contracting parties and the percentage of the electronic signature.” to them, in addition to any other services related to electronic signature.

Based on the aforementioned legislative and jurisprudential definitions of the electronic authentication authority, we can define it as: “a natural or legal person, public or private, subject to the supervision and control of the state, who plays the role of electronic mediator by issuing electronic authentication certificates, which identifies the contracting parties and attributes the electronic signature to them, in addition to any other services related to the electronic signature”.

2.2.2 Electronic documentation functions

The electronic documentation has several functions that can be summarised as follows (Hassan, 2017):

- *Verification of the identity of the signatory:* The main obligation of this authority is to verify the identity of the signatory. This is done by issuing an electronic authentication certificate stating the authentication of an electronic signature in a specific contract, by which it certifies the validity of that signature and its attribution to the person who issued it. If one of the parties puts his electronic signature on an electronic document and the authentication authority guarantees its authenticity, this confirms the issuance of the electronic signature by its holder. It also entails verifying the identity of the signatory through the authentication authority, determining the legal capacity of the contractor, as well as verifying the authorities and functional competencies of this person (Qandil, 2002).
- *Verification of the content of the electronic exchange:* The electronic authentication authorities are in charge of verifying the content of the electronic exchange between the parties, and the extent of its safety, seriousness, and its distance from fraud and deception. Therefore, we find that the authentication authorities track commercial websites to investigate their seriousness and credibility. If it becomes clear to them that these sites are not real or not serious, they warn the dealers.
- *Determination of the moment of concluding the contract:* Determining the time for concluding the legal act is not a condition for the validity of this act. However, defining that moment is necessary, as the time of concluding the contract is considered the moment when the legal effects begin to apply to its parties. Therefore, the electronic authentication authority records the process of issuing and receiving electronic messages, seals this process, and provides dating services, i.e. the dated signature on a summary of the message exchanged between the contracting parties (Al-Hajjar, 2002).
- *Issuance of digital signatures:* This authority is responsible for issuing digital signatures, whether by issuing the private key by which electronic messages and signatures are encrypted, or the public key through which decryption takes place, while keeping a copy of the public key without the private one, which remains in the possession of its holder and no one has the right to view it. As for the public key, it is usually kept by those authorities and sent by e-mail to everyone who wishes to deal with the holder of the electronic signature, and thus the validity of the signature is verified (Abu Al-Layl, 2003).

3 The legal authenticity of the electronic authentication certificate

An electronic authentication certificate has full legal value like any other document. Different international and local legislation stipulated the authenticity of these certificates in their relevant laws, and recognised the equality of electronic signatures and documents with their traditional counterparts in terms of legal value and authenticity of proof. Hence, it is necessary to give the electronic authentication certificate complete authenticity and legal value because of the extreme importance of this certificate, by

which the electronic signature gains authenticity, just like the regular (traditional) signature (Al Saadi, 2017).

3.1 The legal authenticity of national electronic authentication certificates

The Jordanian legislator indicated in the Electronic Transactions Law No. (15) for 2015 that one of the objectives of this law is to provide the legal framework for the electronic means used in conducting electronic transactions, as well as to grant legal authority to those transactions, including the electronic authentication certificate and electronic signature. Article (17) thereof recognised the authenticity of electronic records associated with an electronic signature in several cases, as it stated in the following: “a. The electronic record associated with a protected electronic signature shall have the same authority as a regular document, and the parties to an electronic transaction may invoke it b. The electronic record associated with an authenticated electronic signature shall have the same authority as an ordinary document, and the parties to an electronic transaction and others may invoke it c. In cases other than those stipulated in paragraphs (a) and (b) of this article, the electronic record that bears an electronic signature shall have the same authority as the regular document against the parties to the electronic transaction, in the event of denial, the burden of proof falls on those who invoke the electronic record d. The electronic record that is not linked to an electronic signature shall have the authority of the unsigned papers in the proof e. Any official document may be issued or authenticated by electronic means, provided that its electronic record is linked to an authenticated electronic signature”.

It appears from the previous text that the Jordanian legislator has affirmed that electronic actions have the same authority and effect as traditional actions, and that the electronic record can be invoked by the parties to an electronic transaction if it is linked to a protected electronic signature. Likewise, it can be invoked by the parties to the transaction and third parties if it is linked to a certified electronic signature. On the contrary, if this signature is not authenticated, it cannot be an authority against others. The legislator authorised the issuance of any official document or its authentication by electronic means, provided that the electronic record linked to it is a certified electronic signature. Accordingly, the electronic authentication certificate that certifies the validity of the electronic signature shall have the same force and authority granted to the electronic signature.

The Jordanian legislator also considered, in Article 6 thereof that electronic means represented in electronic contracts and documents produce the same effects as the use of traditional means, provided that the electronic record of these means can be viewed, stored and referred to at any time without any change or modification to its content.

The Jordanian Evidence Law No. (30) of 1952, as amended, in paragraph (c/3) of Article (13) thereof, indicated that certified or signed computer outputs have the power of ordinary documents that include the signature of the one who issued it in terms of proof, unless the one to whom it is attributed proves that he did not issue it or did not assign anyone to issue it.

Accordingly, it can be said that the local electronic authentication certificates issued by the accredited authentication authorities, if they meet the conditions of their validity as electronic records and are signed by the electronic signature of these authorities, then they acquire the same authority as the regular fixed-date document, as it is an authority

for the parties to the electronic transaction and third parties, provided that the electronic record is linked to an authenticated electronic signature.

As for the Egyptian legislation, the Egyptian Electronic Signature Law No. (15) of 2004 did not specify the authenticated electronic signature cases, as did the Jordanian Electronic Transactions Law. Article (14) thereof sufficed with the equality of authenticity between the authenticated electronic signature and the written signature in general, as it states that: "The electronic signature in the scope of civil, commercial and administrative transactions shall have the same authenticity prescribed for signatures in the provisions of the Law of Evidence in civil and commercial rules if the conditions stipulated in this law and the technical controls specified by the executive instructions of this law are taken into account in its creation and completion".

The same applies to the Tunisian legislator. The Tunisian Electronic Exchange and Commerce Law did not provide for the legal value of the electronic authentication certificate, or in other words, did not provide for the legal value of the electronic authentication certificate (Al-Safadi, 2010; Isa et al., 2022).

As for the French legislation, in Article (1316/1) of the Civil Code, it equated electronic writing with traditional writing. Thus, it has given electronic documents the same legal authority as traditional documents. However, Article (1312/4) thereof stipulated that in order for electronic documents to enjoy the aforementioned authenticity, they must be sealed and secured by an electronic signature that is reliable in its validity and that can be attributed to the signer, and that it is preserved in a secure way as well. Therefore, if the electronic signature enjoys the legal authority, then it is a foremost priority that its authentication certificate enjoys the legal authority of proof as ordinary documents do (Al-Khafaji and Hussein, 2016).

3.2 The legal authenticity of foreign electronic authentication certificates

Electronic actions and transactions usually take place in a virtual digital medium that does not recognise the geographical borders of countries. This applies to electronic authentication certificates, as they may be issued by local and national authentication authorities, or by international authentication authorities. This requires that this certificate have a global legal value that goes beyond the borders of the country in which it was issued. In order to recognise the universality of the electronic authentication certificate, equality must be achieved between the authentication certificate issued by the national service provider and the certificate issued by the foreign service provider (Al Saadi, 2017; Al-Billeh, 2022b).

In application of this, the Jordanian Electronic Transactions Law went to grant the electronic signature that was created outside the Kingdom the same authority as evidence if it was authenticated by an approved authentication certificate. The Electronic Transactions Law granted foreign authentication certificates the same effect as national authentication certificates if they were issued by an entity licensed by a competent authority in the foreign country. The ruling regarding the digital signature must not differ, given that the authentication certificate is linked to it and was created to authenticate it. The same applies to the Egyptian legislator, as Article (22) of the Egyptian Electronic Signature Law stipulated that, in order to recognise a foreign electronic authentication certificate, the foreign authentication service provider must first be recognised, which is regulated by the Technology Industry Development Authority.

As for the UNCITRAL Model Law on Electronic Signature of 2001, it is considered one of the clearest laws when it deals directly with the issue of recognising foreign electronic authentication certificates (Massa'ada, 2018; Marshall and Allen, 2018). It stressed that the authentication certificate issued in a specific country is considered as if it was issued in all countries of the world alike (in terms of authenticity). It can be recognised and has a value equal to the value of the national authentication certificate in terms of reliability and dependability. This gives flexibility to the authentication certificates themselves without the need to associate their authenticity with the approval of the issuing authorities (Al-Dimiati, 2009; Al-Billeh, 2022c). This is evident in the text of Article (3/12) thereof, which established a set of rules related to the issue of recognition of foreign certificates and signatures issued by different countries within the framework of common relations regulating electronic transactions. The most important of these rules can be summed up in the following points (Al-Zahra and Jamila, 2019; Khashashneh et al., 2022):

- Not taking into account the geographical location in which the certificate issuance process took place, nor the geographical location of the workplace of its issuer, as long as it is valid and has not been suspended or revoked.
- Acknowledgment and legal recognition of foreign certificates. That is, the foreign certificate has the same level and legal effect as the national certificate, provided that it enjoys the same level of reliability, namely, that it has the same guarantees of safety and confidence established in the certificate of national origin. In order to determine whether foreign certificates provide the same degree of reliability, the applicable international standards in this regard must be taken into account, in addition to any other relevant factors, such as the principle of reciprocity between the country in which the electronic authentication certificate was issued and the other country in which recognition of the authenticity of that certificate is required (Seddah, 2009; Gao and Zeng, 2021; Al-Billeh, 2022d).
- In the event that the parties agree among themselves to use certain types of certificates without observing the aforementioned rules, that is, without subjecting those certificates to the equivalence test indicated in paragraphs 2 and 3 of Article (12), these agreements are considered a sufficient basis for the recognition of certificates across borders, and their validity is not suspended unless they are legally incorrect, or contradict the law of the country in which they are required to be enforced, as if they are contrary to public order or public morals in that country.
- The same is the case with regard to the Arab guiding law of proof using modern technologies. It went towards equality between the foreign and national electronic authentication certificate in terms of legal value and authenticity of proof if some conditions required by the law are met in the authentication service provider at one time and in the authentication certificate at another.
- Therefore, we conclude from the foregoing, that national laws and international legislation have equated the foreign electronic authentication certificate with the electronic authentication certificate issued by a national authentication authority in terms of authenticity and legal value. The issue of recognition is a matter that is handled by the competent authorities in the country, as it bears the task of accrediting foreign authentication bodies by concluding multiple agreements with countries and

other international organisations to coordinate and organise this issue (Rabadi, 2012).

4 Conclusions

The study dealt with the electronic authentication certificate and its role in authenticating electronic transactions. It is considered the personal identity through which electronic transactions take place over the Internet. It also proves the identity of the electronic signature holder and the validity of the electronic transaction. An electronic signature authenticated by an electronic certificate issued by a competent authority enjoys the necessary legal authority in evidence, like a traditional signature. This is confirmed by most of the legislations that regulate the work of the authorities concerned with issuing electronic authentication certificates.

Therefore, in view of the importance of the role played by electronic authentication certificates, it was necessary to have a special law system that defines the work of this certificate and its different types. There is also the need to provide for the legal authenticity and its impact on the parties dealing with it in the field of electronic transactions, and not to be satisfied with what has been stipulated in relation to the authenticity of electronic documents in general.

Through the definitions that we have touched on, whether legislative or jurisprudential definitions, it is clear that the electronic authentication certificate is an electronic document issued by an authentication entity licensed or accredited by competent authorities in the country. This certificate includes a set of basic data whose function is the link between the electronic signature verification data and the signatory. It also acknowledges and certifies that the electronic signature fulfils all the legal conditions necessary to rely on it and that it is valid and attributed to the one who issued it, and that the data contained in the signed electronic document are correct and have not undergone any kind of modification or change.

The electronic authentication certificate enjoys full legal authority as proof, just like official and customary papers. This is if a set of conditions stipulated by the law are met. At the forefront of these conditions is that they are issued by a competent, licensed or accredited authority, in addition to containing a set of data and meeting the requirements of safety and reliability.

In fact, most of the legislation regulating electronic transactions, including the Jordanian legislation, in terms of authenticity and legal value, equated the foreign electronic authentication certificate with the authentication certificate issued by a national authentication authority. However, these legislations have restricted the issue of acknowledging with certain conditions or standards of a technical legal nature. These conditions revolve primarily around the issue of ensuring that those certificates contain the necessary elements of trust and safety.

Finally, we hope that the national legislation, in particular the Jordanian legislator in the current Electronic Transactions Law No. (15) of 2015, will benefit from the UNCITRAL Model Law on Signatures from detailed provisions on this issue. Especially this is with regard to the issue of the legal authority granted to foreign electronic authentication certificates and its legal impact on the parties to the electronic transaction and on third parties. This necessitates expediting the amendment of some texts of the law and including in it special provisions that regulate in detail the legal validity of this type

of electronic documents, and not to be satisfied with the texts that dealt with the issue of the authenticity of electronic documents in general.

References

- Abu Al-Layl, I. (2003) *Legal Aspects of Electronic Transactions: A Study of the Legal Aspects of Dealing through Modern Electronic Communication Devices*, Scientific Publishing Council, Kuwait.
- Al Saadi, G. (2017) 'The legal system for electronic authentication certificate: a comparative study', *Al-Mohaqiq Al-Hilli Journal of Legal and Political Sciences*, Vol. 9, No. 2, pp.580–623 [online] <https://www.asjp.cerist.dz/en/downArticle/110/10/1/91415> (accessed 1 April 2023).
- Al-Aish, A. (2008) *Digital Writing as A Way to Express Will and Evidence for Proof: A Study of the Laws of Electronic Transactions in the Light of General Rules*, Manshaat Al-Maarif, Alexandria.
- Al-Billeh, T. (2022a) 'Legal controls of the crime of publishing a program on the internet in Jordanian legislation', *Pakistan Journal of Criminology*, Vol. 14, No. 1, pp.1–14.
- Al-Billeh, T. (2022b) 'The correction of the invalidity of the civil trials procedures in Jordanian and Egyptian legislation: the modern judicial trends', *Kutafin Law Review*, Vol. 9, No. 3, pp.486–510, <https://doi.org/10.17803/2713-0525.2022.3.21.486-510>.
- Al-Billeh, T. (2022c) 'Judicial oversight on the administrative contracts in the Jordanian legislation and the comparison: the modern qualitative jurisdiction of the administrative judiciary', *Indian Journal of Law and Justice*, Vol. 13, No. 2, pp.1–28 [online] <https://ir.nbu.ac.in/handle/123456789/4763> (accessed 2 April 2023).
- Al-Billeh, T. (2022d) 'Freedom of religious belief and the practice of religious rites according to the Jordanian legislation: difficult balance between international and regional requirements as well as the national legislative controls', *Balkan Social Science Review*, Vol. 20, pp.117–137 [online] <https://js.ugd.edu.mk/index.php/BSSR/article/view/5503/4660> (accessed 1 April 2023).
- Al-Dakhili, A. (2018) *The Legal System for Electronic Documentation: A Comparative Study*, Zain Legal and Literary Library, Lebanon.
- Al-Dimiati, T. (2009) *Evidence of Electronic Contracting via the Internet*, Dar Al-Nahda Al-Arabiya, Cairo.
- Al-Hajjar, W. (2002) *Electronic Evidence*, Sader Bookshop Publishers, Lebanon.
- Al-Khafaji, W. and Hussein, A. (2016) 'The legal authenticity of electronic signature certification certificates: a comparative study', *Al-Mohaqiq Al-Hilli Journal of Legal and Political Sciences*, Vol. 8, No. 4, pp.289–338 [online] <https://www.iasj.net/iasj/download/6f6e920edd783715>.
- Al-Mazouri, H. (2018) *The Legal System for Authenticating Electronic Transactions: A Comparative Analytical Study*, New University Publishing House, Alexandria.
- Al-Rajwani, J. (2014) 'Electronic authentication certificate', *Journal of Judges' Tribune: Regional Office of the Hassania Ouadatia for Judges*, Vol. 1, No. 1, pp.80–96.
- Al-Safadi, A. (2010) *The Legal System for Electronic Authentication*, Wael Publishing House, Amman.
- Al-Zahra, B. and Jamila, H. (2019) 'Electronic certification certificate as a mechanism for enhancing confidence in electronic transactions', *Journal of Legal and Political Sciences*, Vol. 10, No. 1, pp.892–911 [online] <https://www.asjp.cerist.dz/en/article/91415> (accessed 3 April 2023).
- Bennett, R. (1997) *Electronic Authentication and Digital Signature*, DIANE Publishing, Darby, PA, USA.

- Bromby, M. (2010) 'Identification, trust and privacy: how biometrics can aid certification of digital signatures', *International Review of Law, Computers & Technology*, Vol. 24, No. 1, pp.133–141, <https://doi.org/10.1080/13600861003644541>.
- Darawsheh, S. (2018) 'Civil responsibility of electronic signature authentication entities: a comparative analytical study', *Jerash Journal for Research and Studies*, Vol. 19, No. 1, p.15 [online] <https://jerashrs.com/home/index.php/1?view=publication&task=show&id=721> (accessed 3 April 2023).
- Daze Yee, A. (2016) *The Legal System for Authenticating the Electronic Signature: A Comparative Study*, 1st ed., Dar Al-Fikr Al-Jamei, Cairo.
- Daze Yee, A. (2017) 'The legal system for electronic signature authentication - a comparative study', *Arab Journal of Science and Research Publishing*, Vol. 3, No. 5, pp.57–40, <https://doi.org/10.26389/AJSRP.Z250817>.
- Gao, R. and Zeng, J. (2021) 'Forward secure certificateless proxy multi-signature scheme', *International Journal of Electronic Security and Digital Forensics*, Vol. 13, No. 1, pp.1–27, <https://doi.org/10.1504/IJESDF.2021.111718>.
- Greenwood, D. and Campbell, R. (1997) 'Electronic commerce legislation: from written on paper and signed in ink to electronic records and online authentication', *The Business Lawyer: American Bar Association*, Vol. 53, No. 1, pp.307–338 [online] <https://www.jstor.org/stable/40687785> (accessed 2 April 2023).
- Haj Ali, A. (2013) *Legal Regulation of Electronic Signature Certification Bodies*, Master thesis, An-Najah National University.
- Hassan, L. (2009) *Electronic Authentication and the Responsibility of the Competent Authorities*, Dar Al-Raya for Publishing and Distribution, Amman.
- Hassan, L. (2017) *Electronic Authentication, and the Responsibility of the Competent Authorities in Jordanian Law: A Comparative Study*, PhD thesis, Amman Arab University.
- Ibrahim, K. (2010) *Electronic Signature*, University House, Alexandria.
- Isa, H.A., Alwerikat, N. and Al-Billeh, T. (2022) 'The concept of the public employee in Jordanian law: different constitutional, administrative, and criminal law definitions', *BiLD Law Journal*, Vol. 7, No. 2s, pp.331–337 [online] <https://bildbd.com/index.php/blj/article/view/318> (accessed 3 April 2023).
- Kamil, T. (2009) 'The authenticity of foreign electronic authentication certificates: a comparative study', *The Seventeenth Annual Scientific Conference on Electronic Transactions-E-Commerce*, United Arab Emirates University and the Emirates Center for Strategic Studies and Research, E-Government. Emirates.
- Khashashneh, T., Al-Billeh, T. and Issa, H.A. (2022) 'The authority of the criminal judge to assess digital (electronic) evidence in Jordanian, Egyptian, and French legislation', *Journal of Southwest Jiaotong University*, Vol. 57, No. 5, pp.631–640, <https://doi.org/10.35741/issn.0258-2724.57.5.51>.
- Marshall, S. and Allen, C. (2018) *Digital Signatures for Dummies, Cryptomathic Special Edition. Custom: For Dummies*, John Wiley & Sons, Ltd., The Atrium, Southern Gate.
- Masadeh, S.R. (2023) 'A new encryption system for IoT devices using embedded key cryptosystem', *International Journal of Electronic Security and Digital Forensics*, Vol. 15, No. 1, p.56, <https://doi.org/10.1504/IJESDF.2023.127748>.
- Mason, S. (2012) *Electronic Signatures in Law*, Cambridge University Press, UK.
- Mass'ada, A. (2018) 'Digital signature and authentication certificate: concept and legal implications', *Al-Manara Journal for Research and Studies*, Vol. 11, No. 4, pp.249–282.
- Moqaddam, Z. and Issa, A. (2014) *Electronic Authentication and its Impact on Supporting Commercial Trust: A Comparative Study*, PhD thesis, Omdurman Islamic University.
- Nuseirat, A. (2005) *Authenticity of the Electronic Signature in Evidence – A Comparative Study*, Dar Al Thaqafa for Publishing and Distribution, Amman.
- Qandil, S. (2002) *Electronic Signature*, New University Publishing House, Alexandria.

- Rabadi, I. (2012) *Rules for Electronic Signature*, House of Culture for Publishing and Distribution, Amman.
- Reed, C.H. (2001) 'Legally binding electronic documents: digital signatures and authentication', *The International Lawyer*, Vol. 35, No. 1, pp.89–106 [online] <https://core.ac.uk/download/pdf/216909724.pdf> (accessed 3 April 2023).
- Seddah, I. (2009) *The Extent of the Authenticity of Electronic Documents in Evidence 'A Comparative Study'*, Master thesis, An-Najah National University.
- Wang, F. (2010) *Law of Electronic Commercial Transactions*, Routledge, UK.