



Legal Framework for Electronic Signature Security in Algerian Legislation and European Directive



Received: 01/05/2024; Accepted: 20/06/2024

Naouel Loucif

faculty the law, university of Constantine 1 “Mentouri brothers”, Algeria. nawel.loucif@umc.edu.dz

Abstract

In the latest amendment, Article 62 of the constitution specifically addresses the responsibility of public authorities regarding consumer protection, ensuring their safety, health, and economic rights. This underscores the necessity of a legal framework regulating e-commerce, particularly as it has become a global phenomenon requiring the authentication of written documents linked to electronic signature security. E-commerce contracts demand signatures from the contracting parties, making electronic signatures a crucial pillar of electronic banking operations. Consequently, this has required the intervention of specialized authorities to regulate the electronic commercial environment, known as certifying authorities. These authorities, as stipulated by law, are subject to the central authority in their creation and performance of duties, as outlined in Law No. 15/04, which sets the general rules for electronic signatures and certification being studied.

Keywords

Constitutional founder;
Electronic signature;
Electronic banking operations;
Certifying authorities;
Law no. 15/04.

الكلمات المفتاحية

المؤسس الدستوري؛
التوقيع الإلكتروني؛
العمليات المصرفية الإلكترونية؛
سلطات التصديق؛
القانون رقم 04/15.

التأطير القانوني لأمن التوقيع الإلكتروني في التشريع الجزائري والتوجيه الأوروبي

ملخص

خص المؤسس الدستوري في آخر تعديل و في المادة 62 منه الحديث عن مسؤولية السلطات العمومية فيما يخص حماية المستهلكين بشكل يضمن لهم الأمن ، السلامة ، الصحة و حقوقهم الاقتصادية ، و هو ما يعني التأكيد على ضرورة وجود إطار قانوني يضبط التجارة الالكترونية ، خاصة و أن هذه الأخيرة أصبحت ظاهرة عالمية استلزمت توثيق المحرر الكتابي الذي يرتبط بتأمين التوقيع الإلكتروني ، خاصة و أن عقود التجارة الإلكترونية تتطلب توقيع الأطراف المتعاقدة ، ما جعل التوقيع الإلكتروني بهذا الشكل أحد أهم دعائم العمليات المصرفية الإلكترونية ، و هو ما تطلب بالنتيجة تدخل سلطات مختصة لضبط البيئة التجارية الإلكترونية تدعى بنص القانون سلطات التصديق ، أين تخضع هذه الأخيرة في طريقة إنشائها و أدائها لمهامها للسلطة المركزية ، و هو ما جاء في القانون رقم 04/15 المحدد للقواعد العامة للتوقيع و التصديق الإلكترونيين محل الدراسة .

* Corresponding author: nawel.loucif@umc.edu.dz

Doi:

I- Introduction:

The emergence of the World Wide Web (Internet) has changed traditional balances and rules. This network has become a space for contracting in the field of commercial deals, leading to the rise of what is called electronic securities, which means moving away from traditional securities. This, in turn, has facilitated the development of signatures, taking a digital numeric form known as the electronic signature, which is linked with e-commerce due to the necessity of using it in electronic bonds and contracts. The electronic signature has thus become an urgent necessity imposed by international and national transactions, due to its features that facilitate the performance and completion of transactions between different parties quickly and easily. This aligns with global trade agreements that require the parties to quickly complete international commercial transactions, otherwise, they face penalties.

Given the importance of transactions over digital networks and the novelty of legislative interest in it, the Algerian legislator dedicated a legal space to it in 2005 under Law No. 05/10 dated June 20, 2005, concerning the amended and supplemented civil law. However, in our opinion, this was not sufficient, which led the Algerian legislator to reconsider drafting and issuing a law specific to signatures, taking into account its importance and its close relationship with e-commerce.

I.1. Study problem:

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

Did the Algerian legislator, by virtue of Law No. 15/04 defining the general rules for electronic signature and authentication, establish a general framework for the electronic signature that aligns with international developments in this field?

To answer this question, we follow a plan in which we discuss Algeria's transition from paper-based transactions to a new system that relies on electronic signatures, considering this legal step that we value through Law No. 15/04. This transition is a bold step in the electronic system and necessitated the establishment of specialized authorities to oversee electronic signature operations, which we believe is an important link in maintaining the security of the latter.

II– Transition from paper-based transaction systems to the use of information and communication technologies in public administration:

Economic thought literature suggests that the concept of electronic management, which emerged at the beginning of the twentieth century, and the idea of information and communication technologies are interconnected concepts. The concept of electronic management is derived from the English term "e-government," which has been evolving remarkably due to the demands imposed by information and communication technologies that have influenced the nature of the administrative process itself.

The emergence of the World Wide Web (Internet) has altered traditional balances and rules, as this network has become the primary link in the exchange of information and services.

The term "electronic management" has received significant attention and scholarly interest from researchers and scholars in the field of electronic management, offering various definitions. Some refer to it as "e-government," due to the overlap and connection between the concepts. One of the key definitions of electronic management:

Electronic management (E- Management) is simply the transition from performing transactions and providing public services in a traditional manual way to an electronic format, for optimal use of time, money, and effort.

In other words, it involves performing administrative transactions and providing public services via the internet, without clients having to physically go to the offices to complete their transactions, thereby avoiding a waste of time, effort, and resources (Hamed, 2012, p. 76).

It is also a process of mechanizing all tasks and activities of the administrative institution by relying on necessary information technologies, aiming to achieve the new management goals of reducing paper use, simplifying procedures,

and eliminating the routine to accurately and quickly handle tasks and transactions, preparing each administration to later connect with the electronic government (Jamal, 2009, p. 28).

Another definition attempts to simplify the concept and bring it closer to reality, describing electronic management more than delving into theoretical dimensions by saying: "It is the transformation of traditional administrative works and services and lengthy, complicated procedures using paper into electronic tasks executed with high speed and utmost precision (Al-Hasan, 2019, p. 04)." Ghoneim defines it as "performing operations among a group of partners through the use of advanced information technology to increase efficiency and effectiveness of performance (Al-Meer, 2007, p. 15)."

Some have focused on certain procedural issues relied upon by electronic management, defining it as "the organization's ability to exchange information and provide services between itself, citizens, and business sectors quickly, accurately, and at minimal cost over the internet, while ensuring the confidentiality and security of the exchanged information (at any time and place), based on two principles (Djilali, 2016, pp. 32-33):

- **Technical:** It involves the technological preparation of information and its transmission over the internet, ensuring its accuracy and confidentiality.
- **Procedural:** It involves the remote execution of information and services, ensuring their validity and credibility.

From the above, we conclude that the most comprehensive and optimal definition of electronic management is: "A management strategy for the information age that aims to provide better services to citizens, institutions, and its customers, optimally utilizing available information resources by employing available human and moral resources within a modern electronic framework to optimally utilize time, money, and effort, and to meet targeted demands with the required quality."

From the above, we can derive the features of electronic management (Al-Kubaisi, 2008, pp. 32-33):

- A strong, fast, and secure network infrastructure.
- A strong information infrastructure (strong and compatible information systems).
- A human cadre trained to use modern technologies.
- A technical human cadre capable of performing continuous technical support and developing various information systems.

The electronic signature, like the traditional signature, serves as a tool for expressing the signer's will and is also considered a means of proof. The prevalence of e-commerce transactions and the growing use of electronic bonds and contracts have played a role in enforcing legal protection for the electronic signature (Shenin, 2013, p. 158).

Algeria adopted the electronic signature system for the first time in 2005 by virtue of Law 05-10 dated June 20, 2005, which amended and supplemented the civil law. This law recognized electronic writing as a means of proof by adding Articles 323 bis and 323 bis1. This moved the focus of the Algerian legislator from the idea of an electronic signature to issuing a specific law for it, thereby confirming the transition from paper-based to electronic transactions by defining its concept, because this is linked to defining the forms of the electronic signature.

II.1. The interest of the Algerian and European legislators in defining the electronic signature:

The electronic signature is a set of numbers, symbols, electronic characters, or signs used by a person in their electronic dealings, which identifies the signer uniquely as the one who agrees to the transaction being documented (Zirzoor, 2011, p. 144). Generally, the Algerian legislator took a more clarifying approach through the Executive Decree No. 07/162 concerning the exploitation system on wired and wireless communication networks and electrical wires, as stated in Article 3 of it: (The electronic signature is a working method that meets the conditions specified in Articles 323 bis and 323 bis1, where it is considered that the secured electronic signature is an electronic signature that meets the following requirements:

- It is unique to the signer.
- It is made by means that the signer retains under his exclusive control.
- It ensures that any subsequent modification to the connected action is detectable), (Article 3 of Executive Decree No. 07/162 amends and supplements Decree No. 01/123 concerning the exploitation system applied to all types of networks including electric wireless and various wire and wireless communication services) , which is adopted by the Algerian legislator through Law No. 15/04 dated February 1, 2015, which sets the general rules related to electronic signature and certification, in Articles 6 to 14, especially Article 13 which included what was mentioned in Article 3 of Executive Decree No. 06/167.

The definition presented above focuses on the idea of a secured electronic signature, bound by conditions. In contrast, the European directive distinguishes between the advanced electronic signature and the simple electronic signature, where the former type is certified by an electronic certification service provider and is granted a certificate that verifies the validity of this signature after confirming its attribution to the owner, while the latter type has legal validity in case it is not denied (Bougmiha, 2017, p. 363), which is not different from what the Algerian legislator has gone to as we will mention below.

Where it is stated in Article 323 bis1 of the amended and supplemented civil law: (Proof by writing in electronic form is considered as proof by writing on paper, provided that the identity of the person who issued it can be verified and it is prepared and preserved under conditions that ensure its integrity) (Article 323, 2005, p. 24), and in a legal reading of the above text, we note the equality between writing in electronic form and writing on paper media, which means not completely abandoning classic contracts and documents.

As for the text of Article 327 from the same legislation mentioned earlier: (The electronic signature is regarded according to the conditions mentioned in Article 323 bis1) (Article 327, p. 24), which means that the availability of conditions is considered evidence of its validity until proven otherwise, and thus the two necessary conditions required in electronic writing are:

- The ability to verify the person who signed. The reason for this condition is that the signature, whatever its method, must leave a distinctive trace linked to a specific person.
- That this signature is preserved under conditions that ensure its integrity, meaning that for the electronic signature to be considered, there must be the possibility to detect any modification or alteration in the electronic signature data, and this will only be possible if it is preserved under conditions that ensure its integrity, which aligns with the European directive.

The electronic signature is thus legally reliable if it meets the conditions stipulated in Article 7 of Law No. 15/04 related to electronic signature and certification (Article 7 of Law No. 15/04 , 2015, p. 08), which we summarize as:

- It must be specific to the signer alone.
- It must be created by electronic means that the signer exclusively controls.
- It must ensure that the signature is connected to the electronically sealed document in a way that allows detection of any modification, alteration, or distortion in the document's data or elements of the signature.

Additionally, the Algerian legislator has established legal protection for the data mentioned above under Article 301 of the amended and supplemented Penal Code (Article 301 of the amended and supplemented Penal Code: "Punishable by imprisonment from one month to six months and a fine from 500 to 5000 DZD.... and all persons entrusted by virtue of reality, profession, permanent or temporary position with secrets entrusted to them and disclosed them in cases not mandated by law to disclose and they are authorized to do so....", although some legal scholars believe that the text of Article 301 of the Penal Code is not suitable for protecting electronic personal data since the scope of the crime of disclosing secrets is confidential data, which must either be official secrets or related to certain professions based on trust (Shenin, 2013, p. 198).

II.2. The Proving Power of Electronic Signature Types:

It is worth noting that the electronic signature requires the capacity to express will electronically, which implies two things:

- **The first matter:** The personal or professional status of the contracting person based on which the agreement is made.
- **The second matter:** The complete legal capacity as required by law (Nachnach, 2018, p. 247). Since this is related to the electronic signature, it must meet certain conditions such as being written (a line and personal mark), identifying the signer and expressing their will, and the necessity of linking the signature to the document (Zirzoor, 2011, pp. 146-147). It must also be readable and its existence characterized by continuity.

Accordingly, there are several types of electronic signatures, the most important of which are:

II.2.1 The scanned handwritten signature (transferring the handwritten signature via a scanner) (Kandeel, 2006, p. 66):

This signature is made by the signer themselves who manually transfers the signed document to a scanner. The device reads, images, and transfers the signature as a set of graphic images stored inside the computer, converting it into an electronic signature that can be added to the document to be signed (Bougmiha, 2017, p. 365).

This signing mechanism appears easy, but it is not secure at all because it can be accessed by anyone who can use or seize that device. Therefore, this signature is not widely used and is not recognized as a legally reliable signature.

II.2.2 The electronic signature using a PIN code:

Also known as signing using magnetized credit cards with a PIN (Kandeel, 2006, pp. 67-69), where this signature is made by inserting a magnetized card into a suitable machine, then entering the PIN and pressing the approval button to complete the desired transaction.

This type of electronic signature is common in Automated Teller Machines (ATMs) at banks for obtaining account statements, withdrawing cash, or making financial transfers to another account. To address the issue of the proving power of this method, banks have concluded a special agreement with the customer to acknowledge its full legal validity (Sudah, 2009, p. 77).

II.2.3 The biometric electronic signature (Shaweesh, 2018, p. 04):

This type of signature relies on unique human characteristics such as fingerprints, retinal patterns, voice timbre, DNA, and other inherent human traits that cannot be forgotten. Since distinctive features such as fingerprints, retinal patterns, and voiceprints differ from person to person, they are reliable means of identifying an individual and are therefore permissible in affirming legal actions conducted through an electronic intermediary (Tharwat, 2007, p. 61).

However, it can be noted that some human characteristics may change due to circumstances like the loss of fingers, or the facial features of twins might make the electronic signature less significant in an electronic environment.

II.2.4 The digital electronic signature:

This is one of the most prominent types of electronic signatures used to authenticate electronic correspondences and transactions. It involves using a series of numbers, letters, or a combination of both, chosen by the sender to identify themselves, known only to them or to those they inform. This signature relies on digital encryption techniques that use algorithms or mathematical formulas to securely encrypt information and communications by converting them into a format that is only understandable by the relevant parties (Zirzoor, 2011, p. 144).

The electronic signature is made using a specific key to encrypt the electronic message, and then the recipient decrypts the message using another key to access the sent information. If the message appears clear and readable after decryption, the sender's signature is verified as correct (Sudah, 2009, p. 74).

For example, a merchant offering goods on the internet thereby allows every buyer to read the message without being able to modify its terms, by providing the buyers with a public key that permits reading without altering the format. Meanwhile, the buyer controls a private key, which allows them to resend the contract attached with their signature in a file that the merchant cannot modify because they do not possess this private key.

This digital electronic signature operates using a two-key technology, one public and one private. These keys are massive sequential digital data that cannot be altered. If the content is agreed upon and the commitments within are accepted, the signer places their signature using the private key. Here, it is noted that the public key can be used by everyone to verify the reliability of the signature and confirm the identity and personality of the signer according to the law (Tharwat, 2007, p. 63).

This type of electronic signature is the most important and commonly used technology due to its ease and being the least expensive among other types of signatures (Lalouch, 2012, pp. 53-67).

Thus, the difference between these two signatures lies in the level of trust that the legislator bases on the signature's validity in proving it. If the same level of trust is present in the electronic signature, it equals the traditional signature in its legal validity in proving.

III- The Procedural and Regulatory Framework for the Electronic Signature

Verifying the identity of the signer is extremely important, especially when linked to proving financial or commercial transactions. In reviewing Algerian legislation prior to the enactment of Law No. 15/04, we notice an almost complete absence of legal solutions aimed at cases of fraud and manipulation in such transactions (Nachnach, 2018, p. 253). However, electronic signatures were included under the protection provided by the penal code in the section concerning crimes of assault on processing systems and forgery (Articles 394, 394 bis 1, 394 bis 2, 301 from the amended and supplemented Penal Code) , within the framework of achieving information security, meaning the protection of information and its critical components, including the systems and devices that use, store, and transmit this information (Al-Qahtani, 2015, p. 85).

Therefore, when the signature is legally valid, it facilitates the electronic certification process, which is a document in electronic form that verifies the connection between the electronic signature verification data and the signer (This definition appears in the text of Article 2, Paragraph 7 of Law No. 15/04, which sets the general rules related to electronic signatures and certifications). This process is overseen by authorities known as electronic certification authorities.

III.1 Electronic Certification A Mechanism to Verify Data Conformity with the Signer:

The electronic notary is a neutral third party, which may be individuals, companies, or independent neutral entities that act as intermediaries between the parties to authenticate their electronic transactions. The primary function of an electronic notary or electronic certification authority is to verify the identities of the parties in electronic transactions, ascertain their legal capacity to transact, and ensure the content of the transaction is secure, serious, and free from fraud and forgery (Zirzoor, 2011, p. 148). This is done through electronic identity technology or what is known as smart cards, not forgetting to verify the identity of the will's owner using biometric methods (hand or fingerprint, eye print, voice print, facial recognition) (Nachnach, 2018, pp. 257-258).

The European Directive number 93 of 1999 adopted the idea of an electronic notary and termed it as Certification Service Providers, the same designation adopted by the Algerian legislator in Executive Decree 07-162. To engage in the electronic certification activity, one must obtain a license granted by the postal and telecommunications authority, which comes with a specification book that outlines the rights and duties of the service provider and the user. As for the individuals who are legally permitted to engage in this activity, they must meet the same conditions as those required for providing internet services in Algeria.

Thus, the concept of electronic certification is present in the definition of electronic signature, which the legislator linked to the certification method under Article 2 of Law No. 15 / 04, which defines the general rules related to electronic signature and certification (Article 4 of Law No. 18/04, 2018, p. 02). Additionally, according to the law on postal and electronic communications, the state ensures the security and safety of electronic communication networks, and this direction necessitates the inclusion of certification authorities, which will be discussed in the following section.

III.2 Electronic Certification Authorities:

Initially, it is important to note that electronic certification authorities, also known as authentication entities, are responsible for issuing electronic certificates alongside digital signatures by maintaining special registries for electronic signatures to ensure their secure usage (Article 62, 2020, p. 16).

Article 2 of the European Directive defines accreditation certificates and specifies their characteristics as follows: "An electronic certificate links a signing tool to a specific individual and confirms the identity of the signature owner by meeting the conditions stated in Annex 1, and is issued by an authority specialized in providing these services after fulfilling the conditions listed in Annex 2 (Zirzoor, 2011, p. 149)."

The European legislator requires electronic certification authorities to maintain the confidentiality of personal data, ensuring that it can only be accessed by the person themselves or with their explicit consent, and only if such data are necessary for issuing the certificate (Kessi, 2012, p. 218). Given the importance of these certificates, in cases where there is a duplication between two electronic signatures, one simple and the other advanced, priority is given to the advanced signature because it possesses elements of security and trust that are not available in the simple signature.

In the same context, the Algerian legislator has addressed electronic certification authorities and divided them into three categories⁽¹⁾, listed as follows:

- The National Authority for Electronic Certification: The aforementioned law specifies in its Articles (16) to (25) the composition, tasks, and operations of the National Authority for Electronic Certification. This authority, under the supervision of the Prime Minister and acting as an independent administrative authority, defines the national policy for electronic certification. It is charged with promoting and developing the use of electronic signatures and certifications, in addition to ensuring and monitoring their correct usage.
- The Governmental Authority for Electronic Certification: This is the first branch of the National Authority, affiliated with the Ministry of Post, Information Technology, and Communication. It manages the certificates used in electronic exchanges between departments, thus eliminating the physical aspect of correspondences between ministries and between the administration and institutions, such as the National Centre for the Commercial Registry, which issues electronic commercial registries, and between the administration and citizens, especially through the remote issuance of civil status documents. Other trusted parties within the governmental branch also oversee the issuance of electronic certificates, which are then ratified by the government.
- The Economic Authority for Electronic Certification: This authority is responsible for managing certificates used in electronic exchanges between businesses, either among themselves or with citizens (e-commerce, email exchanges).

In conclusion, these authorities play a significant role in maintaining the security of electronic signatures against any action that constitutes an assault on electronic commerce transactions, thus qualifying it as a crime of aggression against the electronic signature online (Harwal, 2014, pp. 299-308).

IV- Conclusion:

The electronic signature process involves a series of data appended to the electronic message to ensure its validity, identify the signature, and link the content to the signer, thus protecting the recipient from fraud committed by the sender and countering any attempts at deceit and manipulation. The electronic signature provides effective means to ensure the validity and integrity of any document during its validity period, which is evident during the creation process and when verifying the electronic signature using the available information to validate and ensure the integrity of the received invoice.

In conclusion of our study on the topic of electronic signatures, we can say that in the era of technology and especially the era of speed relating to electronic payment methods or the extraction of administrative documents, Algeria was quite delayed in keeping up with developments. However, we appreciate the legal initiative represented by Law No.

15/04, which sets the general rules for electronic signatures and certifications, as well as Law No. 18/04 which sets the general rules related to postal and electronic communications, and Law No. 18/05 related to e-commerce. We await the issuance of ministerial decisions in each concerned sector to activate the electronic processing of transactions in line with the idea of developing and updating public services according to international standards, especially concerning electronic signatures on official and administrative documents. In this context, we recommend:

- The necessity of recognizing the legal validity of electronic signatures and generalizing them.
- The establishment of specific statutes regulating the encryption process in electronic transactions.

Referrals and References:

- [1]. Al-Hasan, H. b. (2019). Electronic Management Between Theory and Application. *International Conference for Administrative Development Towards Outstanding Performance in the Public Sector*. Riyadh.
- [2]. Al-Kubaisi, K. M. (2008). Requirements of Electronic Management at the Information Systems Center of the Electronic Government in the State of Qatar. *Master's Thesis in Business Administration*. International Virtual University.
- [3]. Al-Meer, E. K. (2007). Requirements for Human Resources Development for the Implementation of Electronic Management, An Applied Study on the Employees of the General Traffic Administration at the Ministry of Interior in the Kingdom of Bahrain. *Master's Thesis Department of Administrative Sciences*. Riyadh: Naif Arab University for Security Sciences.
- [4]. Al-Qahtani, D. b. (2015). *Information Security*. Riyadh: King Fahd National Library.
- [5]. Article 323. (2005). Article 323 bis 1 of Law No. 05/10, amends and supplements Order No. 75/78 containing the amended and supplemented Civil Law. Algeria: Official Gazette.
- [6]. Article 327. (n.d.). Article 327 of Law No. 05/10 amends and supplements Order No. 75/78 containing the amended and supplemented Civil Law.
- [7]. Article 4 of Law No. 18/04. (2018, 05 10). sets the general rules related to postal and electronic communications. Algeria: Official Gazette.
- [8]. Article 62. (2020). the 2020 Constitution. Official Gazette.
- [9]. Article 7 of Law No. 15/04 . (2015). defines the general rules related to electronic signatures and certifications. Algeria: Official Gazette.
- [10]. Bougmiha, N. B. (2017, 06 75). Proof of the Electronic Contract. *Journal of Law and Humanities*, 10(02).
- [11]. Djilali, B. (2016). Electronic Management in Algerian Institutions - Reality and Prospects. *Doctoral Thesis in Management Sciences Specialization in Business and Marketing Management*.
- [12]. Hamed, F. M. (2012). *Electronic Administration* (1 ed.). Amman: Dar Al-Mustaqbal for Publishing and Distribution.
- [13]. Harwal, H. N. (2014). Internet Crimes (Comparative Study). *dissertation submitted for the Ph.D. degree, Faculty of Law and Political Science*. Tlemcen: University of Abou Bekr Belkaid.
- [14]. Jamal, M. (2009). The Feasibility of Implementing Electronic Management at the UNRWA Gaza Regional Office and Its Role in Improving Staff Performance. *Master's Thesis in Business Administration*. Gaza: Islamic University of Gaza.
- [15]. Kandeel, S. E.-S. (2006). *The Electronic Signature – Its Nature, Forms, and Validity in Proof between Circulation and Quotation*. Alexandria: Dar Al-Jamea Al-Jadeeda.
- [16]. Kessi, Z. (2012). The Legal System for Electronic Certification (Authentication) Entities. *Notebooks of Politics and Law*.

- [17]. Lalouch, R. (2012). Security of the Electronic Signature. *thesis submitted for the Master's degree in International Business Law*. Tizi Ouzou: Mouloud Mammeri University of Tizi Ouzou.
- [18]. Nachnach, M. (2018). The Impact of Digital Technology on Assigning Will and Verifying Capacity in Electronic Contracts. *Legal and Political Research Journal*.
- [19]. Shaweesh, W. M. (2018). The Validity of the Electronic Signature in Sharia Court. *Updates in Sharia Judiciary – Contemporary Means of Proof*. Al Ain: Institute of Applied Technology.
- [20]. Shenin, S. (2013). Criminal Protection of E-commerce (Comparative Study). *dissertation submitted for the degree of Doctorate in Private Law*. Tlemcen: University of Abou Bekr Belkaid.
- [21]. Sudah, I. M. (2009). The Validity of Electronic Documents in Evidence (Comparative Study). *thesis submitted for the Master's degree in Private Law*. Palestine: Al-Najah National University.
- [22]. Tharwat, A. H. (2007). *The Electronic Signature – Its Nature, Risks, and How to Counter Them, Its Validity in Evidence*. Alexandria: Dar Al-Jamea Al-Jadeeda.
- [23]. Zirzoor, W. K. (2011). The Electronic Signature as Evidence in the Light of the Provisions of the Amended Iraqi Evidence Law No. 107 of 1979. *Risala al-Huquq Journal*.

Note:

- ¹- Law No. 15/04 sets the general rules related to electronic signatures and certifications