ELECTRONIC AUTHENTICATION: TRUST AND SECURITY FOR ELECTRONIC TRANSACTIONS

BENKHADRA ZAHIRA[1], RADIA BOUDIA[2]
[1,2]Lecturer A, University of lounici Ali, Blida 2 (Algeria).
The Author's E-mail: z.benkhadra@univ-blida2.dz[1], r.boudia@univ-blida2.dz [2]
Received: 09/2023 Published: 03/2024

Abstract:
To achieve trust and security in electronic transactions over the Internet, electronic certification authorities are relied upon as a neutral and reliable mediator that verifies the validity and integrity of transactions.
Certification authorities work to verify the authenticity of electronic signatures and ensure that they are issued by the person concerned.
Electronic certification authorities also issue certificates of authenticity that prove the validity and authenticity of electronic signatures. These certificates are relied upon by users to ensure that the electronic transaction is valid and has legal value.
***Keywords**: Electronic authentication, Electronic certification service provider, Electronic authentication certificate.*

INTRODUCTION:

With the growing reliance on e-commerce worldwide, the Algerian legislator faced a significant challenge in legitimizing electronic documents. In the past, handwritten paper documents were the primary means of proving the authenticity of transactions. However, with the advent of e-commerce, it became necessary to find new solutions that ensure the security and efficiency of electronic transactions.

The electronic signature, accompanied by an electronic certificate of authenticity, was the optimal solution to overcome the challenges faced by the Algerian legislator. An electronic signature is a digital signature used to verify the identity of the person who signed an electronic document. Electronic certificates of authenticity are issued by accredited entities that guarantee the validity of these signatures.

Recognizing the importance of electronic signatures in facilitating electronic transactions, the Algerian legislator acknowledged their evidentiary value in the amended and supplemented Civil Code (Law No. 05/10 of June 20, 2005). This approach was further supported by Law No. 15/04 of February 1, 2015[1], which set out the general rules for electronic signatures and electronic certification, followed by implementing texts on electronic certification authorities. These laws demonstrate the state's genuine commitment to granting legal validity to electronic signatures accompanied by an electronic certificate of authenticity. This aims to ensure the security and safety of electronic transactions and boost the e-commerce sector in Algeria, especially after the enactment of the E-Commerce Law No. 18/05.

With the increasing prevalence of e-commerce, the need for trust and security in electronic transactions has also grown. In the absence of direct interaction between individuals, the need arose for a neutral third party to act as a mediator to ensure the validity and integrity of transactions. This third party is known as a certification authority, which is responsible for issuing electronic certificates of authenticity.

Therefore, the problem at hand is: **What is the role of electronic certification in ensuring the security and safety of electronic transactions?**

[1] -Law No. 15-04 of February 1, 2015, determining the general rules relating to electronic signatures and authentication, J.O. No. 6, issued on February 10, 2015.

From this perspective, we will study the problem by addressing the concept of electronic certification (first) and then the entities responsible for granting the certificate of authenticity (second) using the descriptive analytical approach.

First: The Concept of Electronic Certification

Electronic certification is a relatively new term in the field of electronic transactions. Its emergence coincided with the spread and increased use of various modern technological techniques that contributed to the transformation of various actions or transactions (legal, commercial, and banking) from their physical nature to legally recognized electronic media. Given its importance, it is necessary to address its definition and significance.

01- Definition of Electronic Certification:

Proving the validity of electronic signatures is one of the major legal challenges facing its implementation. Under the general rules of international and national law, a party cannot create evidence for itself. Therefore, there was a need for a neutral third party to document the electronic signature, verify the identity of the signer, and authenticate their signature.

Electronic certification can be defined as follows:

- A secure technical means of verifying the authenticity of a signature or document by verifying its attribution to a specific person; This is done by a neutral party called a certification service provider or electronic documentation provider[1].
- Electronic certification or documentation refers to the process of verifying the authenticity of electronic writing and electronic signatures [2],This process is carried out by a neutral and independent party from the parties to the electronic contract. This party can be an individual, a company, or a designated entity, and is called a "certification service provider", "authentication service provider", or "certification authority". The terminology varies from one legislation to another, and the role of the electronic notary or authenticator is to document electronic transactions for individuals, in order to give them confidence in their documents to prove their legal actions. They have been called "Agents of Proof".
- Electronic certification is a procedure carried out by a third party that meets the legal requirements to secure and confirm a specific service. It is a process that ensures the authenticity and reliability of the user's identity using other devices and entities through information and communication systems[3].
- The nature of the certification process, which is based on verifying the identity of the contracting party and the content of the transaction to be documented, leads some to consider the role of this entity as similar to that of a notary public. Therefore, the electronic certification authorities have been called "electronic notaries". However, there is a fundamental difference between them. The task of the certification authority is not to create and store legal documents, but rather to verify electronic legal transactions and issue a certificate to the interested parties[4].
- Some define electronic certification as the process of verifying that an electronic signature has been executed by a specific person. This is done using analytical tools to identify symbols, words,

[1] Mohamed Okoubi, "Technical and Legal Mechanisms for the Protection of Electronic Signatures", Fikr Magazine, No. 18, Algeria, 2019, p. 306.

[2]-Ibrahim Al-Dosouqi Abu Al-Layl, Documentation of Electronic Transactions and the Responsibility of the Documentation Authority Towards the Affected Third Party, Conference on Electronic Banking Transactions Between Sharia and Law, Faculty of Sharia and Law, United Arab Emirates University, Volume 5, May 1 and 6, 2013, p. 929.

[3] -Osama bin Ghanem Al-Obeidi, "Electronic Certification and Its Applications in the Saudi System", Judicial Magazine, Volume 04, Issue 179, Year 2012, p. 169.

[4] -Abed Fayed Abdel Fattah Fayed, Electronic Writing in Civil Law, Dar Al Nahda Al Arabiya, Cairo, 2016, pp. 60-61.

and numbers, as well as decryption, reverse engineering, and any other means or procedures that achieve the desired goal [1].

Therefore, electronic certification means the intervention of a third party to secure the electronic exchange of data in the electronic field, in order to achieve safety and confidence in electronic transactions.

Consequently, the certification procedure is an acknowledgement of the authenticity of the signature and seal on a document or instrument. It aims to secure e-commerce websites through the electronic certification system. This stage is carried out by the intervention of a neutral third party known as the certification authority, which is a designated body or entity that issues certificates called electronic certification certificates[2].

2- The importance of electronic certification in ensuring the security and effectiveness of electronic transactions

Electronic certification is an essential element for ensuring the security and effectiveness of electronic transactions. It creates a secure electronic environment through electronic certification authorities that act as a trusted intermediary between the contracting parties.

The electronic signature verification stage is considered the most important stage in the conclusion of electronic transactions of all kinds. This is due to the prominent role of this stage in the formation of the contract and ensuring the accuracy of the data contained therein, as well as verifying the authenticity of the signature and attributing it to its location.

This is what the Algerian legislator stipulated in Article 28 of Law 18-05 on the Regulation of Electronic Commerce[3].

One of the functions of an electronic certification service provider is to issue a document of authentication. This document is linked to the electronic signature and, in order for the authority to reach the stage of issuing this document, it must have taken all the necessary verification and compliance measures with the information obtained electronically from the sender. This is so that the latter can be given the character of authenticity and legal security[4].

2-1-The role of electronic certification authorities is manifested in:

-Verifying the identity of the contracting parties and determining their eligibility for electronic transactions: Electronic certification authorities verify the identity of the contracting parties in electronic transactions by ensuring the accuracy of their personal data and matching it with official documents[5]. They also verify their eligibility for electronic transactions by ensuring that they have reached the age of majority and that there are no legal restrictions preventing them from doing so.

- Ensuring the integrity and reliability of data circulating over the network: Electronic certification authorities ensure the integrity and reliability of data circulating over the network by using encryption and electronic documentation techniques. They also prevent any attempt to tamper with or modify data without the permission of the owners.

- Issuing trusted electronic certificates: Electronic certification authorities issue trusted electronic certificates that are used to verify the identity of the contracting parties and ensure the integrity and reliability of data circulating over the network. These certificates include:

---

[1] -Ghazi Nassima, Legal Mechanisms for the Protection of Electronic Payment Methods in Algerian Legislation, Journal of Political and Administrative Research, Volume 06, Issue 10, p. 291.

[2] Saliha Merbah, The Role of Electronic Certification in Proving and Preserving Electronic Transactions, Journal of Comparative Legal Studies, Volume 07, Issue 1, 2021, p. 869.

[3] - Law No. 18-05 on E-Commerce, dated May 10, 2018, J.O.No. 28, issued on May 16, 2018.

[4]Youssef Rahmane, Electronic Certification Authorities in Algerian Legislation According to Law 15-04, A Comparative Study, Journal of Legal and Political Studies, Volume 2, Number 1, Year 2017, p. 183.

[5] Bahia Fatima, Electronic Certificate of Authentication, Journal of Legal and Political Science Research, Volume 1, Issue 2, Year 2015, P. 395.

Ordinary or simple certificate: This certificate is used to verify the identity of the holder only.
Described certificate: This certificate is used to verify the identity of the holder and ensure the integrity and reliability of data circulating over the network.

2-2- The Algerian legislator has distinguished between two types of electronic certificates:

2-2-1 Ordinary electronic certificate:

An electronic document that proves the link between the electronic signature verification data and the signatory[1].

2-2-2- Described electronic certificate:

An electronic certificate that meets the following requirements[2]:

1- Granted by a trusted third party or an electronic certification service provider in accordance with the electronic certification policy approved by the regulatory authority.

2- Granted to the signatory and no one else.

3- Must include:

-An indication that it is granted as a described electronic certificate.

-The identity of the trusted third party or the electronic certification service provider that issued the certificate and the country in which they are established.

-The name of the signatory or the pseudonym that allows their identification.

-The possibility of including a specific capacity for the signatory, if necessary, depending on the purpose of using the electronic certificate.

Data related to the verification of the electronic signature and in accordance with the data of the creation of the electronic signature.

-An indication of the start and end date of the validity period of the electronic certificate.

-An identification code for the electronic certificate.

-The electronic signature of the electronic certification service provider or the trusted third party that issued the electronic certificate.

-The limits of use of the electronic certificate, if necessary.

-The limits of the values of the factors that may be used for the electronic certificate, if necessary.

-An indication of the document that proves the representation of another natural or legal person, if necessary.

In general, it can be said that an electronic certificate of authentication is a certificate issued by an authority licensed by government agencies to practice its activity to play the role of verifying that the electronic signature was made in the correct manner and in accordance with the required standards and conditions[3], with the identification of the signature to its owner so that it can be used as evidence.

Second: Electronic Certification Authorities:

Electronic certification authorities are neutral entities accredited by the state or a competent international body that play a fundamental role in ensuring the validity and security of electronic transactions.

These entities issue electronic certificates of authentication, which are used to verify the identity of signatories to electronic documents and ensure that their data has not been tampered with.

01- Definition of an electronic certification authority:

In order to provide complete confidentiality of information and data, and to ensure their legal security, it is necessary to store and authenticate them by a neutral party with these powers. Therefore, it is necessary to define its nature.

1-1-Jurisprudential Definitions of Electronic Certification Service Providers

[1]Article 2, paragraph 7 of Law 15-04 on Electronic Signature and Certification.

[2] Article 15 of Law 15-04 on Electronic Signature and Certification.

[3] Souad Yahyaoui, Electronic Authentication: A Technical Mechanism to Ensure and Protect Electronic Commercial Transactions in Law, Journal of Comparative Legal Studies, Volume 08, Issue 1, 2022, p. 698.

There are many jurisprudential definitions of electronic certification service providers. One definition is:

-"A licensed or accredited entity that issues electronic certificates through electronic means to ensure the authenticity of the data contained in the document or the validity of the electronic signature of the person who issued the document."[1]

- Any independent neutral public or private organization or entity that acts as an intermediary between parties to document their electronic transactions[2].

- A public or private entity that works to fulfill the need for a trusted third party in e-commerce by issuing certificates that prove the authenticity of a certain fact related to the subject of e-exchange, to confirm the attribution of the electronic signature to a specific person and to confirm the attribution of the public key used to its owner[3].

- Some define it as an entity or institution managed by a natural or legal person that operates under a license from a state institution, and its function is to issue electronic certification certificates that link a person (natural or legal) to their public key or any other task related to the electronic signature[4].

- It is also called an electronic certification service provider, a third party that issues a certificate that includes the identity of the website and its relationship to the signature[5]. It is a link between the sender and the receiver, and thus strengthens the element of trust between electronic traders, which encourages e-commerce.

1-2-Legal Definition of Electronic Certification Service Providers

From a legal perspective, the Algerian legislator defined it under Law No. 15/04 of 2015, which determines the rules related to electronic signature and certification.

Article 2 of the law states that electronic certification bodies are divided into two categories:

1-2-1-Trusted Third Party:

-A legal entity.

-Issues qualified electronic certificates.

-May provide other services related to electronic certification.

-For stakeholders in the government sector.

1-2-2- Electronic Certification Service Provider:

-A natural or legal person.

-Issues qualified electronic certificates.

-May provide other services in the field of electronic certification.

2-Types of Electronic Certification Authorities According to Algerian Law:

From the texts of the Algerian law on electronic signature, it can be concluded that there are two types of electronic certification authorities:

2-1- Trusted Third Party:

[1] Hammoud, Mohammad Nasser, Al-Aqeed Al-Douli Al-Electroni Al-Mubram Abeer Al-Internet, 1st ed., Dar Al-Thaqafah for Publishing and Distribution, Jordan, 2012, p. 349.

[2] Eman Mamoun Ahmed Suleiman, Conclusion of the Electronic Contract and its Proof: Legal Aspects of the Electronic Commerce Contract, Dar Al-Jamia Al-Jadida, Alexandria, 2008, p. 390.

[3] Alaa Ahmed Mohamed Haj Ali, Legal Regulation of Electronic Signature Certification Authorities, Master's Thesis, Faculty of Graduate Studies at An-Najah National University in Nablus, Palestine, 2013, p. 12.

[4] Ghassan Rabdi, Issa, The Rules of Electronic Signature, 2nd ed., Dar Al-Rayah for Publishing and Distribution: Amman 2012, p. 116.

[5] Ayad Ahmed Saeed Al-Sari, The Legal System for the Conclusion of Electronic Contracts, Halabi Legal Publications, Lebanon, 2016, p. 110.

A Trusted Third Party, a legal entity that issues qualified electronic certificates, may also provide other electronic certification services for stakeholders in the government sector[1], including public institutions and administrations, public bodies, national independent institutions and regulatory authorities, participants in interbank exchanges, and any person belonging to the government sector by nature of their work or tasks[2].

A Trusted Third Party is subject to supervision and monitoring of its activity by the Government Authority for Electronic Certification.

The Government Authority for Electronic Certification is an administrative authority under the Ministry of Post and Information Technology with financial independence and legal personality[3].

It is also subject to the control of the National Authority for Electronic Certification, which is at the top of the pyramid of electronic certification authorities[4].

The Government Authority for Electronic Certification ensures the application of electronic certification policies by the Trusted Third Party through two bodies[5]:

-The Steering Council.

-The Director General of the Government Authority.

2-2-Electronic Certification Service Providers:

An Electronic Certification Service Provider is a natural or legal person that issues qualified electronic certificates and may provide other electronic certification services to the public[6].

Electronic Certification Service Providers are subject to the control of the Economic Authority for Electronic Certification, which is an economic authority under the authority responsible for regulating mail and wired and wireless communications[7].

They are also subject to the control of the National Authority for Electronic Certification, which is at the top of the pyramid of electronic certification authorities.

Algerian Law No. 15-04 regulates Electronic Certification Service Providers and specifies their obligations in ensuring the security and integrity of electronic transactions.

These obligations relate to several aspects, including the accuracy and confidentiality of personal data[8].

The Electronic Certification Service Provider must verify the accuracy of the data provided by the signatory using available legal means such as a national identity card or passport.

In addition, the Electronic Certification Service Provider must maintain the confidentiality of the data and not disclose it except in accordance with the law. This is done by issuing electronic keys, whether the private key used to encrypt the electronic transaction and which is specific to the site only, or the public key used to decrypt it[9].These keys rely on data encryption standards that ensure their confidentiality and non-disclosure.

---

[1] Article 2/11 of Law No. 15/04

[2]. Article 2/13 of Law No. 15/04.

[3] Article 26 of Law No. 15/04.

[4] Article 16 of Law No. 15/04.

[5] Executive Decree No. 16/135 of April 25, 2016, defining the nature, composition, organization and operation of the Government Authority for Electronic Certification, Official Gazette, No. 26, 2016.

[6] Article 12/02 of Law No. 15/04.

[7] Articles 29 and 30 of Law No. 15/04.

[8] Samir Dahmani, "Documentation in Electronic Transactions, A Comparative Study," Master's Thesis in International Business Law, Faculty of Law, Mouloud Mammeri University, Tizi Ouzou, 2010, p. 94.

[9]Ministry of Post and Information and Communication Technologies, "Electronic Signature and Certification." Accessed June 12, 2023, at 8:30 PM, on the website **www.mpt.gov.dz/en/electronic-signature**.

The obligations of the Electronic Certification Service Provider also include issuing and revoking electronic certificates.

An electronic certificate contains information about its owner, such as their name, address, and legal representative, and provides security and confidentiality for electronic transactions. An electronic certificate is revoked in specific cases such as a request from the certificate holder, obtaining false information, the death of the certificate holder, or the expiration of the certificate. The Electronic Certification Service Provider must notify the certificate holder of its cancellation and transfer the information related to the certificate to the Economic Authority for Electronic Certification after its expiration.

The Electronic Certification Service Provider also determines the time and date of the conclusion of the electronic contract and the limitation period that may apply to this type of legal act[1].The date and time of the electronic signature must be linked to the validity period of the electronic certificate[2].

These obligations aim to guarantee the reliable and secure implementation of electronic certification services and achieve trust and legal security in electronic transactions.

The main difference between the two parties is that the first party, or the third party that issues qualified electronic certificates, must be a legal entity. This entity is considered trustworthy and is a source of qualified electronic certificates for the benefit of stakeholders in the government sector only, meaning that the public does not benefit from the services of this entity, and that it must be subject to the supervision of the regulatory authorities in the field of electronic certification, which is the government authority responsible for electronic certification.

The second party, which is the electronic certification service provider, is responsible for providing electronic certification services. It can be a legal entity or a natural person. This entity issues detailed qualified certificates and simple certificates for the benefit of the public. It is subject to the supervision of the economic authority responsible for electronic certification, which is affiliated with the authority responsible for regulating mail and wire and wireless communications.

These entities that provide services to the public must obtain a prior license from the regulatory authorities[3], in accordance with Law No. 2000 issued on August 5, 2000[4], which defines the general rules related to mail and wire and wireless communications in the field of electronic certification, and in accordance with the conditions specified in Article 33 of the same law and the procedures mentioned in Article 34 of Law No. 15-04. After obtaining the license, electronic certification bodies begin to practice their main activity, which is issuing electronic certificates, in addition to other activities that they can carry out in accordance with the law and the regulatory license in the field of electronic certification.

CONCLUSION:

Electronic signatures ensure the authenticity and integrity of electronic transactions. By implementing them, we can achieve trust in electronic transactions and encourage their widespread use, which contributes to the development of the digital economy and its benefits for all.

RECOMMENDATIONS:

1. Develop electronic systems to process applications for electronic certificates.
2. Spread awareness about the importance of electronic certificates.
3. Create a unified electronic platform to receive requests for electronic certificates from various stakeholders, which facilitates the application process and speeds up the issuance of certificates.

[1] Mohamed Fawaz El-Matlaqa, "Electronic Signature," Dar Al-Jamia Al-Jadida, Alexandria, Egypt, 2014, p. 90.

[2]Samir Dahmani, Op. cit,P96.

[3] Souad Yahiaoui, , Op. cit,P706..

[4] -Law No. 2000-03 of August 5, 2000, determining the general rules relating to mail and wired and wireless communications, J.O. No. 48, issued on August 6, 2000.

4. Use artificial intelligence and machine learning techniques to verify the identity of the applicant and the accuracy of the data provided, which improves the efficiency of the process and reduces errors.
5. Provide workshops and seminars to provide detailed information about electronic certificates to the target audience, such as institutions, companies and individuals.
6. Establish a national and international cooperation framework to exchange experiences and unify standards and policies related to electronic signatures.
7. Exchange best practices between electronic signature providers to enhance the efficiency and effectiveness of their services and improve the quality of electronic certificates offered.

REFERENCES:

Articles:

[1] -Law No. 2000-03 of August 5, 2000, determining the general rules relating to mail and wired and wireless communications, J.O. No. 48, issued on August 6, 2000.

[2] -Law No. 15-04 of February 1, 2015, determining the general rules relating to electronic signatures and authentication, J.O. No. 6, issued on February 10, 2015.

[3] Law No. 18-05 on E-Commerce, dated May 10, 2018, J.O.No. 28, issued on May 16, 2018.

[4] Executive Decree No. 16/135 of April 25, 2016, defining the nature, composition, organization and operation of the Government Authority for Electronic Certification, J.O. No. 26, issued on April 28, 2016.

2-Books

[5] Abed Fayed Abdel Fattah Fayed, Electronic Writing in Civil Law, Dar Al Nahda Al Arabiya, Cairo, 2016.

[6] Ayad Ahmed Saeed Al-Sari, The Legal System for the Conclusion of Electronic Contracts, Halabi Legal Publications, Lebanon, 2016.

[7] Eman Mamoun Ahmed Suleiman, Conclusion of the Electronic Contract and its Proof: Legal Aspects of the Electronic Commerce Contract, Dar Al-Jamia Al-Jadida, Alexandria, 2008.

[8] Hammoud, Mohammad Nasser, Al-Aqeed Al-Douli Al-Electroni Al-Mubram Abeer Al-Internet, 1st ed., Dar Al-Thaqafah for Publishing and Distribution, Jordan, 2012.

[9] Ghassan Rabdi, Issa, The Rules of Electronic Signature, 2nd ed., Dar Al-Rayah for Publishing and Distribution: Amman 2012.

[10] Mohamed Okoubi, "Technical and Legal Mechanisms for the Protection of Electronic Signatures", Fikr Magazine, No. 18, Algeria, 2019.

[11] Mohamed Fawaz El-Matlaqa, "Electronic Signature," Dar Al-Jamia Al-Jadida, Alexandria, Egypt, 2014.

Theses

[12] Alaa Ahmed Mohamed Haj Ali, Legal Regulation of Electronic Signature Certification Authorities, Master's Thesis, Faculty of Graduate Studies at An-Najah National University in Nablus, Palestine, 2013.

[13] Samir Dahmani, "Documentation in Electronic Transactions, A Comparative Study," Master's Thesis in International Business Law, Faculty of Law, Mouloud Mammeri University, Tizi Ouzou, 2010.

Articles

[14] -Bahia Fatima, Electronic Certificate of Authentication, Journal of Legal and Political Science Research, Volume 1, Issue 2, Year 2015.

[15] -Ibrahim Al-Dosouqi Abu Al-Layl, Documentation of Electronic Transactions and the Responsibility of the Documentation Authority Towards the Affected Third Party, Conference on Electronic Banking Transactions Between Sharia and Law, Faculty of Sharia and Law, United Arab Emirates University, Volume 5, May 1 and 6, 2013.

[16] -Ghazali Naziha, Legal Mechanisms for the Protection of Electronic Payment Methods in Algerian Legislation, Journal of Political and Administrative Research, Volume 06, Issue 10, 2017.

[17] -Osama bin Ghanem Al-Obeidi, "Electronic Certification and Its Applications in the Saudi System", Judicial Magazine, Volume 04, Issue 179, Year 2012.

[18] -Saliha Merbah, The Role of Electronic Certification in Proving and Preserving Electronic Transactions, Journal of Comparative Legal Studies, Volume 07, Issue 1, 2021.

[19] -Souad Yahyaoui, Electronic Authentication: A Technical Mechanism to Ensure and Protect Electronic Commercial Transactions in Law, Journal of Comparative Legal Studies, Volume 08, Issue 1, 2022.

[20] -Youssef Rahmane, Electronic Certification Authorities in Algerian Legislation According to Law 15-04, A Comparative Study, Journal of Legal and Political Studies, Volume 2, Number 1, Year 2017.

5-Websites

[21] -Ministry of Post and Information and Communication Technologies, "Electronic Signature and Certification." Accessed June12, 2023, at 8:30 PM, on the website **www.mpt.gov.dz/en/electronic-signature.**