Mohamed Boudiaf University M'sila
Faculty of law and political sciences
Master 1 field - section 2

English legal Terminologie
Lexus Metandus
Program
Teacher Dr Debbih Hatem

Doc 3

ELECTRONIC SIGNATURE IN ALGERIAN LEGISLATION

The adoption of the law N ° 15-04 expresses a will of Algeria to take the step of the modernization of its economy and its administration. This perceptible desire already for several years, began with the computerization of civil registration and the establishment of a national identifier for each citizen, currently, it is even question of electronic payment and e-trade in a near future.

The main purpose of this law is to dematerialize and streamline commercial and administrative **transactions** by introducing the recognition of the electronic signature as the legal equivalent of the handwritten signature, the only signature, previously accepted, as the legal basis for identifying the signatory.

Thus it introduces for the first time a legal framework allowing the exchange between actors in a fully connected environment. In order to give everyone the power and the freedom to assert their identity at any moment wherever they are, on the one hand and to ensure in an open network such as the Internet, confidentiality, **authentication**, privacy, integrity of the information conveyed and the protection of its authors on the other hand, this law provides for the establishment of an organization and a set of measures that we propose to examine below.

I- The identification of electronic signature

Law 15-04, in its Article 2 Paragraph 1 and Article 6, defines the electronic signature as: " *a set of attached or logically linked* ***electronic data*** *serving as a method of authenticating the identity of the signatory and the adhesion of the latter to the content of the writing in electronic form*".

The text attributes, the quality of equivalence to a handwritten signature, to the only qualified electronic signature (*benefiting from a qualified electronic certificate*), while not depriving all other electronic signatures of their legal **effectiveness**, unless at the origin this signature was conditioned by its manuscript character in which case except the certified electronic signature can ensure this effectiveness (Articles 7,8 & 9).

In addition Article 7 adds that for an electronic signature to be designated as qualified, it must meet the following main **requirements**:

- being performed on the basis of a qualified electronic certificate,
- being designed by secure means of electronic signature creation, so that any subsequent modification of the data is detected,
- being created by means that the signatory can keep under its exclusive control.

A- Qualified electronic certificate

As defined by the Model Law of the ***United Nations Commission on International Trade Law*** (UNCITRAL) and Law No. 15-04, **the Electronic Certificate** means a document in electronic form attesting the link between the verification data of a qualified electronic signature and the signatory.

The qualified electronic certificate is a digital certificate that meets the following main requirements:

1. To be issued by **a trusted third party** authorized by the *Government Electronic Certification Authority* with respect to interveners in the Government Branch and by **a Service Provider** authorized by the *Electronic Economic Certification Authority* for other operators and the public,

2. Must contain mainly:

. An indication that the electronic certificate is issued as a qualified certificate,

. The identification of the certification service provider or authorized trusted third party who issued the electronic certificate and the country in which it's established,

. The name of the signatory or a pseudonym to identify it,

. The signature verification data that corresponds to the electronic signature creation data and in particular **the public cryptographic key** issued by one of the two governmental or economic authorities, as the case may be,

. The indication of the beginning and the end of the period of validity of the electronic certificate,

. The identity code of the electronic certificate,

. The qualified electronic signature of the electronic certification provider who issued the electronic certificate,

. The transaction value limits for which the electronic certificate can be used if applicable.

B- The government branch

Includes institutions, administrations and public institutions as defined by the legislation in force.

C- The public cryptographic key: is a series of numbers issued by government or economic authority and inserted in the electronic certificate certified by the suppliers of this certificate.

It should be noted that the governmental and economic authorities are part of the public authorities of control and regulation to be put in place by the State.

II- Qualified electronic certificate providers:

The text provides for two authorized suppliers of certified electronic certificates: the trusted third party and the service provider.

1- The trusted third party:

The Trusted Third Party is a legal entity, authorized by the Government Authority, responsible for issuing qualified electronic certificates to actors of the Government Branch.

2- the service provider:

The Service Provider is a natural or legal person, authorized by the Economic Authority, responsible for issuing qualified electronic certificates to actors other than those of the Government Branch, including individuals.

The electronic certificate provider is responsible for the registration, **issuance**, **revocation**, publication and **retention** of certificates in accordance with the policy approved by the relevant Authority.

It has the obligation to verify **the veracity** of the data and information related to the issued certificates and to preserve the confidentiality.

It is also obliged to transfer to the authority concerned the information relating to the electronic certificates after their **expiration** with a view to their retention by them.

Any electronic certificate provider must be under Algerian law or Algerian nationality in the case of a normal person.

The normal person or the manager of the legal person (corporation) must have the necessary financial capacities, appropriate qualifications and proven experience in the field of information technology and not have been **convicted** of an incompatible crime or **misdemeanor** with the electronic certification activity.

3- Device for creating and verifying electronic certificate

This device must be approved by the competent services, which will be defined by regulation. It must make it possible to generate an electronic signature provided with a private cryptographic key, linked to the public cryptographic key contained in the qualified electronic certificate issued by the trusted third party or the service provider, as the case may be, so as to:

- that the data used can only be found once or can not be found by deduction,
- the data and the electronic signature are protected against any **intrusion**, **falsification** or **fraudulent** use by any technical means available at the time of **the homologation**.

It must also be able to check the electronic signatures received in such a way:

- The data used for the verification are identical to those of the signature,
- The authenticity and validity of the electronic certificate and the identity of the signatory are verified in a secure manner.

The *Private Cryptographic Key* is a series of numbers held exclusively by the signer and used to create a qualified electronic signature; it is linked to a public cryptographic key.

4- Responsibilities of qualified electronic certificate holder

Once the qualified electronic certificate has been obtained, the holder is responsible for:

- the confidentiality of the signature creation data,
- to revoke the electronic certificate by the supplier of this certificate in case of doubt about confidentiality or **the conformity loss** with the data contained in the electronic signature,
- the non-use of signature creation data related to a revoked or expired certificate, to sign or to have another certificate issued by another supplier with its same data.
- to use his qualified electronic certificate only for the purposes for which it was established.

III- Supervisory and regulatory authorities

The text provides for the establishment of three State administrative bodies responsible for the control and regulation of the electronic certification activity. It is a national authority created by the Prime Minister and which constitutes the highest authority and two governmental and economic authorities with the Minister of Posts and Telecommunications.

1- The national electronic certification authority:

It is an independent administrative authority under the responsibility of the Prime Minister, enjoying legal personality, financial autonomy and equipping the State budget. In charge of the promotion and the development of the signature and the electronic certification, it has as main missions:

- The elaboration of the national general policy on electronic certification after approval of the Prime Minister,
- The approval of the certification policies issued by the governmental and economic authorities,
- The proposal of any draft legislative text to the Prime Minister for approval,
- **The audit** of governmental and economic authorities.

2- The governmental electronic certification authority:

It is an Authority placed under the responsibility of the Minister in charge of the post office, information and communication technologies, enjoying legal personality and financial autonomy. Responsible for monitoring and controlling the electronic certification activity of trusted third parties, its main missions are:

- Development of its electronic certification policy and **submission** for approval to the National Authority,
- Approval of electronic certification policies issued by trusted third parties and ensure their application,
- Retention of expired electronic certificates and related data for the purposes of legal action where appropriate,
- Publication of the public cryptographic key electronic certificate for trusted third parties,
- The audit of trusted third parties.

3- The economic authority for electronic certification

The Authority currently in charge of postal and telecommunications regulation is designated for the purposes of the Law as the Economic Authority for *Electronic Certification. Responsible* for **the monitoring** and control of the electronic certification activity of Service Providers, its main missions are:

- Development of its electronic certification policy and submission for approval to the National Authority,
- The approval of the electronic certification policies issued by the Service Providers, and to

authorize their activities after approval of the National Authority, Retention of expired electronic certificates and related data for the purposes of legal action where appropriate,

• Publication of the public cryptographic key electronic certificate for Service Providers,

• to supplement the activity of a Service Provider in the event of his incapacity to fulfil his obligations,

• The audit of service providers before their authorization or during their activity.

IV- DOCUMENTS ELIGIBLE FOR ELECTRONIC SIGNATURE

The law is not restrictive to any document signed electronically, whether it is electronically signed in a qualified manner (*with a qualified electronic certificate*) or not. It even states that any document sent or received electronically is not **deprived** of its legal efficiency.

The main purpose of this Law is **to emphasize** that when the document, according to the previously existing laws, requires a handwritten signature, the latter may legally validly be replaced by a qualified electronic signature.

However, we think it is useful to point out that certain special circumstances may arise where the handwritten signature may still be required, for example, a notarial act where the physical presence of **witnesses** is required by law to validate legally the signature of this document, or the case where a document requiring the affixing of a wet tax stamp or notary apostille.

Finally, we believe that the application of this law will only take its full measure depending on the efforts made by the economic or administrative operators in the dematerialization of their own information process.

V- PECUNIARY, ADMINISTRATIVE AND CRIMINAL PENALTIES

The Law in order to ensure **compliance** with its requirements establishes a series of **offenses** subject to financial and / or criminal penalties. These offenses are summarized below:

• Any service provider that doesn't comply with the provisions of its terms of reference or its electronic certification policy approved by its Authority,

• Anyone guilty of **false statements**,

• Any service provider who has failed to inform his Authority of his cessation of business within the required time,

• Anyone guilty of using another person's electronic signature creation data,

• Anyone who knowingly fails to identify the electronic certificate applicant,

• Any service provider who has not preserved the confidentiality of data and information related to electronic certificates,

• Any service provider who has not obtained the consent of the person concerned before the use of his personal data,

• Any service provider exercising without authorization or after the withdrawal of the latter,

• Any person in charge of an audit who **reveals** confidential information collected during this audit, to others,

• Anyone who uses his electronic certificate for purposes other than those for which it was issued or continues to use it after its expiration or revocation.

As regards normal persons, **the penalties incurred**, depending on the gravity of the offense, can range from the simple withdrawal of authorization and seizure of equipment to **fines** up to a maximum of 5 million Dinars and penalties of up to imprisonment of up to 3 years. When a legal person is guilty of one of the offenses mentioned above, incurs a fine equivalent to five (5) times the maximum provided for the natural person.

QUESTIONS:

- TRANSLATE THE UNDERLINED TERMS INTO ARABIC.
- GIVE AN ABSTRACT (IN ARABIC) TO THE TOPIC.