Law No. 53-05 on the electronic exchange of legal data (complete)

Dahir n ° 1-07-129 of 19 kaada 1428 (November 30, 2007) promulgating Law n ° 53-05 on the electronic exchange of legal data.

Law No. 53-05 on the electronic exchange of legal data

Preliminary chapter

Article 1:

This law establishes the regime applicable to legal data exchanged electronically, to the equivalence of documents drawn up on paper and in electronic media and to electronic signature.

It also determines the legal framework applicable to operations carried out by electronic certification service providers, as well as the rules to be observed by them and the holders of the electronic certificates issued.

Title 1: The validity of documents drawn up in electronic form or transmitted by electronic means

Article 2:

Chapter 1 of Title 1 of Book 1 of the Dahir forming the Code of Obligations and Contracts is supplemented by Article 2-1 as follows:

"Article 2-1. - When a writing is required for the validity of a legal act, it can be drawn up and kept in electronic form under the conditions provided for in articles 417-1 and 417-2 below.

When a written statement is required by the very hand of the party obliging himself, the latter may affix it in electronic form, if the conditions of this affixing are such as to guarantee that it can only be done by him- even.

However, acts relating to the application of the provisions of the Family Code and acts under private signature relating to personal or real securities, of a civil or commercial nature, are not subject to the provisions of this law, to the exception of acts established by a person for the needs of his profession. "

Article 3:

Title 1 of Book 1 of the Dahir forming the Code of Obligations and Contracts is supplemented by a Chapter 1 bis designed as follows:

"Chapter 1 bis . - The contract concluded in electronic form or transmitted electronically. **Section I: General provisions** *Article 65-1.* - Subject to the provisions of this chapter, the validity of the contract concluded in electronic form or transmitted by electronic means is governed by the provisions of chapter 1 of this title.

Article 65-2. - The provisions of Articles 23 to 30 and 32 above are not applicable to this chapter.

Section II: The offer

Article 65-3. - Electronic means can be used to make contractual offers or information on goods or services available to the public with a view to concluding a contract.

The information requested for the conclusion of a contract or that which is sent during its execution may be transmitted by e-mail if the recipient has expressly accepted the use of this means.

Information intended for professionals can be sent to them by e-mail, once they have communicated their e-mail address.

When the information must be entered on a form, it is made available electronically to the person who must complete it.

Article 65-4. - Anyone who offers, in a professional capacity, by electronic means, the supply of goods, the provision of services or the transfer of business assets or one of their elements makes the applicable contractual conditions available to the public in a manner that allows their conservation and reproduction.

Without prejudice to the conditions of validity provided for in the offer, its author remains bound by it, either for the period specified in the said offer, or, failing this, as long as it is accessible electronically by him.

The offer also includes:

1 - the main characteristics of the good, the service offered or the business concerned or one of its elements;

2 - the conditions of sale of the good or the service or those of transfer of the business or one of its elements;

3 - the different steps to follow to conclude the contract electronically and in particular the terms according to which the parties release themselves from their reciprocal obligations;

4 - the technical means enabling the future user, before the conclusion of the contract, to identify errors made in entering data and to correct them;

5 - the languages offered for the conclusion of the contract;

6 - the procedures for archiving the contract by the author of the offer and the conditions for accessing the archived contract, if the nature or subject of the contract justifies it;

7- the means of consulting, by electronic means, the professional and commercial rules to which the author of the offer intends, if applicable, to abide by.

Any proposal which does not contain all of the statements indicated in this article cannot be considered as an offer and remains a simple advertisement and does not commit its author.

Section III: Conclusion of a contract in electronic form

Article 65-5. - For the contract to be validly concluded, the recipient of the offer must have had the opportunity to check the details of his order and its total price and to correct any errors, and this before confirming the said order to express his acceptance. .

The author of the offer must acknowledge receipt, without undue delay and by electronic means, of the acceptance of the offer addressed to him.

The recipient is irrevocably bound to the offer upon receipt.

The acceptance of the offer, its confirmation and the acknowledgment of receipt are deemed to have been received when the parties to whom they are addressed can have access to it.

Section IV: Miscellaneous provisions

Articles 65-6. - The requirement of a detachable form is satisfied when, by a specific electronic process, it is possible to access the form, to complete it and to return it by the same means.

Article 65-7 . - When a plurality of originals is required, this requirement is deemed to be met, for documents drawn up in electronic form, if the document concerned is drawn up and kept in accordance with the provisions of articles 417-1, 417-2 and 417-3 below and that the process used allows each of the interested parties to have a copy or to have "access to it." "

Article 4:

Section II of Chapter 1, Title Seventh, Book 1 of the Dahir forming the Code of Obligations and Contracts is completed by Articles 417-1, 417-2 and 417-3 as follows:

“Section II: Literal proof

Article 417-1. - Writing on electronic media has the same probative force as writing on paper.

A written document in electronic form is admitted as evidence in the same way as a written document on paper, provided that the person from whom it emanates can be duly identified and that it is drawn up and kept under conditions such as to guarantee it. 'integrity.

Article 417-2. - The signature necessary for the perfection of a legal act identifies the person who affixes it and expresses his consent to the obligations arising from this act.

When the signature is affixed before a public officer empowered to certify, it confers authenticity to the act.

When it is electronic, it is advisable to use a reliable identification process guaranteeing its link with the act to which it relates.

Article 417-3. - The reliability of an electronic signature process is presumed, until proven otherwise, when this process uses a secure electronic signature.

An electronic signature is considered secure when it is created, the identity of the signatory assured and the integrity of the legal act guaranteed, in accordance with the laws and regulations in force in this area.

Any document on which a secure electronic signature is affixed and which is time-stamped has the same probative force as the document whose signature is legalized and of a certain date. "

Article 5:

The provisions of Articles 417, 425, 426, 440 and 443 of the Dahir forming the Code of Obligations and Contracts are amended and supplemented as follows:

" *Article 417*. - the literal proof …….. Under private signature.

It can also result from ……. And private documents or from any other signs or symbols endowed with an intelligible meaning, whatever their medium and their methods of transmission.

When the law has not set other rules and, in the absence of a valid agreement between the parties, the court rules on conflicts of literal evidence by any means, whatever the medium used.

Article 425. - Deeds under private signature ……. In the name of their debtor.

They only have a date against third parties:

1 ° …… ..

…… ……

6 ° - when the date results from the secure electronic signature authenticating the act and its signatory in accordance with the legislation in force.

The successors and successors …… ..in the name of their debtor.

Article 426. - The act …… by it.

The signature …… .. at the bottom of the deed; a stamp or seal cannot replace it and are considered as not affixed.

In the case of a secure electronic signature, it should be included in the document, under the conditions provided for by the applicable laws and regulations.

Article 440 . - The original …… copies.

Copies of a legal document drawn up in electronic form are admitted as evidence provided that the document meets the conditions referred to in articles 417-1 and 417-2 and that the process for keeping the document allows each party to of a copy or to have access to it.

Article 443. - Agreements and other legal facts …… and exceeding the sum or the value of ten thousand dirhams cannot be

proved by witnesses. An authentic act or private signature must be signed, possibly drawn up in electronic form or transmitted electronically. "

Title II: Legal regime applicable to secure electronic signature,

cryptography and electronic certification

Chapter 1 : Secure electronic signature and cryptography

Section I: Secure electronic signature

Article 6:

The secure electronic signature, provided for by the provisions of article 417-3 of the Dahir forming the Code of Obligations and Contracts, must meet the following conditions:

- be specific to the signatory;
- be created by means that the signatory can keep under his exclusive control;
- guarantee with the act to which it is attached such a link that any subsequent modification of said act is detectable.

It must be produced by a device for creating an electronic signature, certified by a certificate of conformity.

The secure electronic signature verification data must be mentioned in the secure electronic certificate provided for in article 10 of this law.

Article 7:

The signatory, referred to in Article 6 above, is the natural person, acting for his own account or for that of the natural or legal person he represents, who implements a signature creation device electronic.

Article 8:

The electronic signature creation device consists of hardware and / or software intended to apply the electronic signature creation data, comprising the distinctive elements characterizing the signatory, such as the private cryptographic key, used by him to create an electronic signature.

Article 9:

The certificate of conformity, provided for in paragraph 2 of article 6 above, is issued by the national authority for the approval and supervision of electronic certification, provided for in article 15 of this law, when the electronic signature creation device meets the following requirements:

1) guarantee by technical means and appropriate procedures that the electronic signature creation data:

a) cannot be established more than once and their confidentiality is ensured;

b) cannot be found by inference and that the electronic signature is protected against any forgery;

c) can be satisfactorily protected by the signatory against use by third parties.

2) not cause any alteration or modification of the content of the deed to be signed and not prevent the signatory from having exact knowledge of it before signing it.

Article 10:

The link between the electronic signature verification data and the signatory is attested by an electronic certificate, which consists of a document drawn up in electronic form.

This electronic certificate can be simple or secure.

Article 11:

The electronic certificate, provided for in Article 10 above, is a secure electronic certificate, when it is issued by a

provider of electronic certification services approved by the National Authority for the approval and monitoring of electronic certification and that it includes the following data:

a) a statement indicating that this certificate is issued as a secure electronic certificate;

b) the identity of the provider of electronic certification services, as well as the name of the State in which it is established;

c) the name of the signatory or a pseudonym where it exists, the latter then having to be identified as such, holder of the secure electronic certificate;

d) where applicable, an indication of the quality of the signatory according to the use for which the electronic certificate is intended;

e) the data which allow the verification of the secure electronic signature;

f) identification of the start and end of the validity period of the electronic certificate;

g) the identity code of the electronic certificate;

h) the secure electronic signature of the electronic certification service provider issuing the electronic certificate;

i) where applicable, the conditions of use of the electronic certificate, in particular the maximum amount of transactions for which this certificate can be used.

Section 2: Cryptography

Article 12:

The main purpose of the cryptographic means is to guarantee the security of the exchange and / or storage of legal data by electronic means, in a manner which ensures their confidentiality, their authentication and the control of their integrity.

By means of cryptography is meant any hardware and / or software designed or modified to transform data, whether information, signals or symbols, using secret conventions or to perform the reverse operation, with or without a secret convention.

The term “cryptography service” is understood to mean any operation aimed at the use, on behalf of others, of means of cryptography.

Article 13:

In order to prevent use for illegal purposes and to preserve the interests of national defense and internal or external security of the State, import, export, supply, exploitation or use of cryptography means or services are subject to:

a) upon prior declaration, when the sole purpose of this means or service is to authenticate a transmission or to ensure all the data transmitted electronically;

b) with prior authorization from the administration, in the case of a subject other than that referred to in paragraph a) above.

The government fixes:

1. the means or services meeting the criteria referred to in paragraph a) above.

2. the modalities according to which the declaration is signed and the authorization is issued, referred to in the previous paragraph.

The government may provide for a simplified declaration or authorization regime or the exemption from declaration or authorization for certain types of cryptography means or services or for certain categories of users.

Article 14:

The supply of cryptography means or services subject to authorization is reserved for providers of electronic certification services, approved for this purpose in accordance with the provisions of Article 21 of this law. Failing this, the persons who intend to provide cryptography services subject to authorization must be approved for this purpose by the administration.

Chapter II: Certification of the electronic signature

Section 1: The National Authority for the approval and oversight of electronic certification

Article 15:

The national authority for the approval and monitoring of electronic certification, hereinafter designated by the national authority, has the mission, in addition to the powers devolved to it by virtue of other articles of this law:

- propose the standards of the accreditation system to the government and take the necessary measures for its implementation;
- to approve providers of electronic certification services and to control their activities.

Article 16:

The national authority publishes an extract from the approval decision in the " *Official Bulletin* " and keeps a register of approved electronic certification service providers, which is subject, at the end of each year, to a publication in the " *Official Bulletin* ".

Article 17:

The national authority ensures that the providers of electronic certification services issuing secure electronic certificates comply with the commitments provided for by the provisions of this law and the texts adopted for its application.

Article 18:

The national authority may, either ex officio or at the request of any interested person, verify or have verified the compliance of the activities of an electronic certification service provider issuing secure electronic certificates with the provisions of this present law or texts adopted for its application. It may have recourse to experts for the performance of its control missions.

Article 19:

In the performance of their verification mission, referred to in Article 18 above, the agents of the national authority,

as well as the experts appointed by it, have, upon proof of their qualities, the right to access any establishment and become aware of all mechanisms and technical means relating to secure electronic certification services that they deem useful or necessary for the accomplishment of their mission.

Section 2: Electronic certification service providers

Article 20:

Only the electronic certification service providers approved under the conditions set by this law and the texts adopted for its application can issue and deliver secure electronic certificates and manage the related services.

Article 21:

To be able to be approved as an electronic certification service provider, the applicant for approval must be incorporated as a company having its registered office in the territory of the Kingdom and:

1 - meet technical conditions guaranteeing:

a - the reliability of the electronic certification services it provides, in particular the technical and cryptographic security of the functions provided by the cryptographic systems and means it offers;

b - the confidentiality of the electronic signature creation data that it provides to the signatory;

c - the availability of personnel with the necessary qualifications to provide electronic certification services;

d - the possibility for the person to whom the electronic certificate has been issued to revoke this certificate without delay and with certainty;

e - determining, with precision, the date and time of issue and revocation of an electronic certificate;

f - the existence of a specific security system to prevent the falsification of electronic certificates and to ensure that the data for the creation of the electronic signature correspond to the data for its verification when both creation data and electronic signature verification data.

2 - be able to keep, possibly in electronic form, all the information relating to the electronic certificate that may be necessary to provide legal proof of the electronic certification, provided that the electronic certificate retention systems guarantee that:

a - the entry and modification of data are reserved only for persons authorized for this purpose by the service provider;

b - public access to an electronic certificate cannot take place without the prior consent of the certificate holder;

c - any modification likely to compromise the security of the system can be detected;

3 - commit to:

3-1: verify, on the one hand, the identity of the person to whom an electronic certificate is issued, by requiring him to present an official identity document to ensure that the person has the capacity legal to engage, on the other hand, the quality which this person avails and to keep the characteristics and references of the documents presented to justify this identity and this quality;

3-2 - ensure when issuing the electronic certificate:

a) that the information it contains is correct;

b) that the signatory identified therein holds the electronic signature creation data corresponding to the electronic signature verification data contained in the certificate;

3-3 - inform, in writing, the person requesting the issuance of an electronic certificate prior to the conclusion of a contract for the provision of electronic certification services:

(a) the terms and conditions for using the certificate;

b) modalities for contesting and settling disputes;

3-4 - provide the persons who rely on an electronic certificate with the information provided for in the previous point that are useful to them;

3-5 - inform the holders of the secure certificate at least sixty (60) days before the expiry date of the validity of their certificate, of its expiry and invite them to renew it or to request its revocation;

3-6 - take out insurance to cover damage resulting from their professional misconduct;

3-7 - revoke an electronic certificate, when:

a) it turns out that it was issued on the basis of erroneous or falsified information, that the information contained in the said certificate no longer conforms to reality or that the confidentiality of the data relating to the creation of the signature has been raped;

b) the judicial authorities direct him to immediately inform the holders of the secure certificates issued by him of their non-compliance with the provisions of this law and of the texts adopted for its application.

Article 22:

By way of derogation from the provisions of Articles 20 and 21 above:

1 - certificates issued by an electronic certification service provider established in a foreign country have the same legal value as those issued by an electronic certification service provider established in Morocco if the certificate or the certification service provider is recognized in the framework of a multilateral agreement to which Morocco is a party or of a bilateral reciprocal recognition agreement between Morocco and the country of establishment of the service provider;

2 - Electronic certification service providers whose head office is established abroad may be approved, provided that the State on the territory of which they exercise their activity has concluded with the Kingdom of Morocco an agreement for the reciprocal recognition of electronic certification service providers.

Article 23:

The electronic signature certification service provider who issues, issues and manages electronic certificates informs the administration in advance, within a maximum period of two months, of its desire to terminate its activities.

In this case, he must ensure that they are taken back by an electronic certification service provider guaranteeing the same level of quality and security or, failing this, revoke the certificates within a maximum period of two months after having them. warned the holders.

It also informs the national authority, without delay, of the cessation of its activities in the event of judicial liquidation.

Article 24:

The providers of electronic certification services are bound, for themselves and for their employees, to respect professional secrecy, under pain of the sanctions provided for by the legislation in force.

They are responsible, under the terms of common law, for their negligence, lack of work or professional incompetence, both vis-à-vis their co-contractors and third parties.

The providers of electronic certification services must keep the certificate creation data and are required, by order of the Public Prosecutor, to communicate them to the judicial authorities under the conditions provided for by the legislation in force. In this case, and notwithstanding any legislative provision to the contrary, the providers of electronic certification services shall immediately inform the users concerned.

The obligation of professional secrecy, referred to in the first paragraph above, is not applicable:

- with regard to the administrative authorities, duly authorized in accordance with the legislation in force;
- with regard to the agents and experts of the National Authority and the agents and officers referred to in article 41 below in the exercise of the powers provided for in articles 19 and 41 of this law;
- if the holder of the electronic signature has consented to the publication or communication of the information provided to the provider of electronic certification services.

Section 3: The obligation of the electronic certificate holder

Article 25:

From the moment the data relating to the signature creation is created, the holder of the electronic certificate is solely responsible for the confidentiality and integrity of the data relating to the signature creation that he uses. Any use of these is deemed, unless proven otherwise, to be its doing.

Article 26:

The holder of the electronic certificate is required, as soon as possible, to notify the certification service provider of any modification of the information contained therein.

Article 27:

In the event of doubt as to the maintenance of the confidentiality of the data relating to the creation of a signature or of loss of conformity with the reality of the information contained in the certificate, its holder is required to revoke it immediately in accordance with the provisions of the article 21 of this law.

Article 28:

When an electronic certificate has expired or has been revoked, its holder can no longer use the data relating to the creation of the corresponding signature to sign or have these data certified by another electronic certification service provider.

Chapter III: Sanctions, preventive measures and recording of infringements

Article 29:

Is punished by a fine of 10,000 to 100,000 DH and imprisonment of three months to one year, anyone who has provided services of secure electronic certification without being approved under the conditions provided for in article 21 above above or will have continued its activity despite the withdrawal of its authorization or will have issued, issued or managed secure electronic certificates in violation of the provisions of article 20 above.

Article 30:

Without prejudice to more severe penal provisions, is punished with imprisonment from one month to six months and a fine of 20,000 DH to 50,000 DH anyone who discloses, incites or participates in disclosing the information entrusted to him in within the framework of the exercise of its activities or functions.

However, the provisions of this article do not apply to the publication or communication authorized, in writing on paper or by electronic means, by the holder of the electronic certificate or to the publication or communication authorized by the legislation in force. .

Article 31:

Without prejudice to more severe penal provisions, is punished by imprisonment from one year to five years and a fine of 100,000 DH to 500,000 DH, anyone who knowingly made false statements or delivered false documents to the provider electronic certification services.

Article 32:

Anyone who has imported, exported, supplied, exploited or used one of the means or a service of cryptography without the required declaration or authorization is punished by one year of imprisonment and a fine of 100,000 DH in Articles 13 and 14 above.

The court may also order the confiscation of the cryptographic means concerned.

Article 33:

When a means of cryptography, within the meaning of article 14 above, has been used to prepare or commit a crime or an offense or to facilitate its preparation or commission, the maximum of the deprivation of freedom incurred is noted as follows:

- he is brought to life imprisonment, when the offense is punished by thirty years of criminal imprisonment;
- it is increased to thirty years of criminal imprisonment, when the offense is punished by twenty years of criminal imprisonment;

- it is increased to twenty years of criminal imprisonment, when the offense is punished by fifteen years of criminal imprisonment;
- it is increased to fifteen years of criminal imprisonment, when the offense is punished by ten years of criminal imprisonment;
- it is increased to ten years of criminal imprisonment, when the offense is punished by five years of criminal imprisonment;
- it is doubled, when the offense is punished by three years' imprisonment at most.

However, the provisions of this article do not apply to the author or accomplice of the offense who, at the request of the judicial or administrative authorities, has given them the unencrypted version of the encrypted messages, as well as the necessary secret conventions. to decryption.

Article 34:

Unless they can be demonstrated that they have committed no intentional fault or negligence, persons providing cryptography services for confidentiality purposes are liable, under these services, for the damage caused to persons entrusting them with the management of their secret conventions in the event of breaches of the integrity, confidentiality or availability of data transformed using these conventions.

Article 35:

Anyone who illegally uses the elements of creation of personal signatures relating to the signature of others is punished by imprisonment from one year to five years and a fine of 10,000 DH to 100,000 DH.

Article 36:

Is punished by a fine of 10,000 DH to 100,000 DH and imprisonment of three months to six months, any provider of electronic certification services who does not respect the obligation of information of the national authority provided in Article 23 above.

In addition, the culprit may be prohibited, for a period of five years, from the exercise of any activity of providing electronic certification services.

Article 37:

Any holder of an electronic certificate who continues to use said expired or revoked certificate shall be punished with a fine of 10,000 DH to 100,000 DH and imprisonment from six months to two years.

Article 38:

Without prejudice to more severe penal provisions, is punished with a fine of 50,000 to 500,000 DH anyone who improperly uses a company name, an advertisement and, in general, any expression suggesting that he is approved in accordance with the provisions of article 21 above.

Article 39:

When, on the report of its agents or experts, the national authority finds that the provider of electronic certification

services issuing secure certificates no longer meets one of the conditions provided for in Article 21 below. above or that its activities do not comply with the provisions of this law or of the regulations adopted for its application, it invites it to comply with said conditions or provisions, within the time limit that it determines.

After this period, if the service provider has not complied with it, the national authority withdraws the authorization issued, deregulates the service provider from the register of approved service providers and publishes an extract from the " *Official Bulletin* ". the decision to withdraw accreditation.

When the activities of the offender are likely to undermine the requirements of national defense or the internal or external security of the State, the national authority is empowered to take any precautionary measures necessary to put an end to said activities, without prejudice to the criminal proceedings they call.

Article 40:

When the offender is a legal person, and without prejudice to the penalties which may be applied to its managers, perpetrators of one of the offenses provided for above, the fines provided for in this chapter are brought double.

In addition, the legal person may be punished with one of the following penalties:

- partial confiscation of his property;
- confiscation provided for in article 89 of the penal code;
- the closure of one or more establishments of the legal person which were used to commit the offenses.

Article 41: In

addition to the officers and agents of the judicial police and the customs agents in their field of competence, the agents of the national authority authorized for this purpose and sworn in the forms of the common law can seek and establish, by report , infringements of the provisions of this law and of the texts adopted for its application. Their minutes are sent to the King's Prosecutor within five days.

The agents and officers, referred to in the previous paragraph, may access the premises, land or means of transport for professional use, request the communication of all professional documents and take copies thereof, collect, upon summons or on site, the information and justifications .

They may proceed, in these same places, to the seizure of the means referred to in Article 12 above on the order of the King's Prosecutor or the examining magistrate.

The means seized appear in the report drawn up on the spot. The originals of the official report and the inventory are sent to the judicial authority which ordered the seizure.

Chapter VI: Final provisions

Article 42:

The conditions and modalities of application of the provisions of this law to real rights are fixed by decree.

Article 43:

Notwithstanding the provisions of the first paragraph of Article 21 above, the government may, on a proposal from

the national authority referred to in Article 15, and subject to the interest of the public service, approve the legal persons governed by public law to issue and deliver secure electronic certificates and manage the related services, under the conditions set by this law and the texts adopted for its application.

Official Bulletin n ° 5584 of Thursday 6 December 2007