Article 1:
This Law establishes the regime applicable to legal data exchanged electronically, to the equivalence of documents drawn up in paper and electronic format and to the electronic signature.

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

Title One: The validity of documents drawn up in electronic form or transmitted electronically

Article 2:
The first chapter of the first title of the first book of the Dahir forming code of obligations and contracts is completed by an article 2-1 thus conceived:

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

Where a written mention is required from the hand of the person who binds himself, the latter may affix it in electronic form, if the conditions of such affixing are such as to guarantee that it can be carried out only by him. even.

However, acts relating to the application of the provisions of the Family Code and private documents relating to personal or real security, of a civil or commercial nature, are not subject to the provisions of this Act, to the except for acts established by a person for the purposes of his profession. "

Article 3:
The first title of the first book of the Dahir forming the Code of Obligations and Contracts is completed by a first chapter bis, as follows:

"Chapter first 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 electronically shall be governed by the provisions of Chapter I of this Title.

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

Section II: The Offer
Article 65-3. - The electronic way can be used to make available to the public contractual offers or information on goods or services for the conclusion of a contract.

Information which is requested for the conclusion of a contract or which is sent in the course of its execution may be transmitted by electronic mail if the addressee has expressly accepted the use of this means.

Information intended for professionals can be sent to them by e-mail, as soon as they have provided their e-mail address.

When the information has to be put on a form, it is put electronically at the disposal of the person who has to fill it out.

Article 65-4. - Anyone who proposes, in a professional capacity, by electronic means, the supply of goods, the provision of services or the transfer of goodwill or any of their elements shall make available to the public the contractual conditions applicable in a manner allowing their conservation and reproduction.

Without prejudice to the conditions of validity envisaged in the offer, its author remains committed by this one, either for the duration specified in said offer, or, failing that, as long as it is accessible by electronic means of its fact.

The offer includes, in addition:

1 - the main characteristics of the property, the proposed service or the business concerned or one of its elements;

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

3 - the various steps to follow to conclude the contract electronically and in particular the procedures according to which the parties are released from their reciprocal obligations;

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

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

6 - the conditions of archiving of the contract by the author of the offer and the conditions of access to the archived contract, if the nature or the object of the contract justifies it;

7- the means to consult, electronically, the professional and commercial rules to which the author of the offer intends, if necessary, to submit.

Any proposal that does not contain all the statements mentioned in this article can not be considered as an offer and remains a mere advertisement and does not engage 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 before confirming the order to express his acceptance .

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

The recipient is irrevocably bound to the offer upon receipt.

Acceptance of the offer, its confirmation and acknowledgment of receipt are deemed to be received when the parties to whom they are addressed may have access to it.

Section IV: Miscellaneous Provisions
Articles 65-6. - The requirement of a detachable form is satisfied when, by a specific electronic procedure, it is possible to access the form, to fill it out and to send it back by the same way.

Article 65-7 . - Where a plurality of originals is required, this requirement shall be deemed to be satisfied, 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 interested party to have a copy or to have access to it. "

Article 4:
Section II of Chapter I, of the seventh title, of the first book of the Dahir forming the Code of Obligations and Contracts is supplemented by Articles 417-1, 417-2 and 417-3 as follows:

"Section II: Literal proof
Article 417-1. - Electronic writing has the same probative force as writing on paper.

The written form in electronic form is admitted in evidence in the same way as the writing in paper form, provided that the person from whom it emanates can be duly identified and that it is established and preserved in conditions of a nature to guarantee the 'integrity.

Article 417-2. - The signature necessary for the perfection of a legal act identifies the person who affixes it and expresses its 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 necessary to use a reliable identification process to guarantee its connection with the act to which it attaches.

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

An electronic signature is considered secure when it is created, the identity of the insured signatory and the integrity of the guaranteed legal act, in accordance with the relevant legislation and regulations.

Every act on which a secure electronic signature is affixed and which is time stamped has the same probative force as the act whose signature is legalized and of 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 modified and completed as follows:

" *Article 417.* - literal proof .....
It may also result ..... .and private documents or any other signs or symbols with an intelligible meaning, whatever their medium and their means of transmission.

Where the law has not laid down other rules and, in the absence of a valid agreement between the parties, the court rules on conflicts of literal evidence by any means, regardless of the medium used.

Article 425. - Acts under private seings ..... in the name of their debtor.

They have a date against third parties only:
1 ° ....
....

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

Successors and successors .... on behalf of their debtor.

Article 426. - The act ..... by it.

The signature .... at the bottom of the act; a stamp or stamp can not make up for it and are considered as not affixed.

In the case of a secure electronic signature, it must be entered in the act, under the conditions laid down in the relevant legislation and regulations.

Article 440 . - The original copies .....
Copies of a legal act drawn up in electronic form are admitted into evidence as long as the act meets the conditions referred to in Articles 417-1 and 417-2 and the process of keeping the document allows each party to dispose of it. 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 can not be
proved by witnesses. It must be authenticated or in private, possibly in electronic form or transmitted electronically. "

**Title II: The 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 satisfy the following conditions:

- be specific to the signatory;

- be created by means that the signatory can keep under his exclusive control;

- to guarantee with the act to which it attaches a link such that any subsequent modification of that act is detectable.

It must be produced by an electronic signature creation device, attested by a certificate of conformity.

The verification data of the secure electronic signature shall 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 on his own behalf 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 implement 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, shall be issued by the national accreditation and supervisory authority for electronic certification provided for in Article 15 of this law, when the electronic signature creation device meets the following requirements:

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

(a) can not be established more than once and their confidentiality is assured;

(b) can not be found by deduction and the electronic signature is protected against forgery;

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

2) not to alter or modify the content of the act to be signed and not to prevent the signatory from having an exact knowledge of it before signing it.

Article 10:
The link between the electronic signature verification data and the signatory is evidenced 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 issued by an electronic certification service provider approved by the National Authority for Accreditation and Supervision of the certification and includes the following data:

(a) a statement that the certificate is issued as a secure electronic certificate;

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

(c) the name of the signatory or a pseudonym when it exists, which must then 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 that allows verification of the secure electronic signature;

f) identification of the beginning 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, including the maximum amount of transactions for which that certificate may be used.

Section 2: Cryptography

Article 12:
The purpose of the cryptographic means is to guarantee the security of the exchange and / or the storage of legal data by electronic means, so as to ensure their confidentiality, their authentication and the control of their integrity.

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

The term "cryptography service" means any operation for the use, on behalf of others, of cryptographic means.

Article 13:
In order to prevent the use for illegal purposes and to preserve the interests of national defense and internal or external security of the State, the import, export, supply, exploitation or use of means or services of cryptography are subject to:

(a) a prior declaration, where the sole purpose of the means or service is to authenticate a transmission or to ensure the completeness of the data transmitted by electronic means;

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

The government sets:

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

2. the conditions under which the declaration and the authorization are subscribed, referred to in the preceding paragraph.

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

Article 14:
The provision of means or services of cryptography subject to authorization is reserved for electronic certification service providers, 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: National Certification and Surveillance Authority for Electronic Certification

Article 15:
The National Authority for the Accreditation and Supervision of Electronic Certification, hereinafter referred to as the National Authority, has as its mission, in addition to the powers conferred on it by other articles of this law:

- to propose to the government the standards of the accreditation system and to take the necessary measures for its implementation;

- to certify electronic certification service providers and to control their activities.

Article 16:
The national authority shall publish an extract of the approval decision in the " *Official Bulletin* " and keep a register of approved electronic certification service providers, which shall be subject, at the end of each year, to a publication in the " *Official Bulletin* ".

Article 17:
The national authority shall ensure compliance by the electronic certification service providers issuing secure electronic certificates 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 conformity of the activities of an electronic certification service provider issuing secure electronic certificates with the provisions of this **article.** law or texts taken for its application. It may use experts to carry out 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 designated by it, have, on the basis of their qualifications, the right to access any establishment and take cognizance of all the 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 electronic certification service providers approved under the conditions laid down by this Law and the texts adopted for its application may issue and issue secure electronic certificates and administer the services related thereto.

Article 21: In
order 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 Kingdom and:

1 - fulfill technical conditions guaranteeing:

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

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

c - the availability of staff with the necessary qualifications for the provision of electronic certification services;

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

e - the precise determination of the date and time of issue and revocation of an electronic certificate;

f - the existence of a security system capable of preventing the falsification of electronic certificates and ensuring that the data for creating the electronic signature correspond to the data of its verification when both creation data and verification data of the electronic signature.

2 - to be able to retain, possibly in electronic form, all the information relating to the electronic certificate that may be required to prove the electronic certification in court, provided that electronic certificate retention systems ensure that:

a - the introduction and modification of the data is restricted to the persons authorized for this purpose by the service provider;

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

c - any change likely to compromise the security of the system may be detected;

3 - commit to:

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

3-2 - ensure at the time of issuance of the electronic certificate:

(a) the information it contains is accurate;

(b) 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 an electronic certification services contract:

(a) the terms and conditions of use of the certificate;

(b) dispute and dispute resolution procedures;

3-4 - to provide those who rely on an electronic certificate with the elements of the information provided for in the preceding point which are useful to them;

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

3-6 - take out insurance to cover the damages resulting from their professional mistakes;

3-7 - revoke an electronic certificate, when:

(a) it turns out that it was issued on the basis of incorrect or falsified information, that the information contained in the certificate is no longer true or that the confidentiality of the data relating to the signature creation has been raped;

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

Article 22:
Notwithstanding 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 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 party or of a bilateral agreement of reciprocal recognition between Morocco and the country of establishment of the provider;

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

Article 23:
The electronic signature certification service provider that issues, issues and manages the electronic certificates shall inform the administration in advance, within a maximum of two months, of its intention to terminate its activities.

In which case, he must ensure that the latter is taken over by an electronic certification service provider guaranteeing the same level of quality and security or, failing that, revokes the certificates within a maximum of two months after having warned the holders.

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

Article 24:
Providers of electronic certification services are bound, for themselves and their employees, the respect of the professional secrecy, under penalty of the sanctions provided by the legislation in force.

They are responsible, in terms of common law, for their negligence, incompetence or professional incompetence vis-à-vis their co-contractors as well as third parties.

The electronic certification service providers must keep the certificate creation data and are obliged, by order of the Attorney General, to communicate them to the judicial authorities, under the conditions provided by the legislation in force. In this case, and notwithstanding any legislative provision to the contrary, electronic certification service providers shall inform the users concerned without delay.

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

- in respect of the administrative authorities, duly authorized in accordance with the legislation in force;

- with regard to the agents and experts of the National Authority and agents and officers referred to in Article 41 below in exercising the powers provided for in Articles 19 and 41 of this Law;

- the holder of the electronic signature has consented to the publication or communication of the information provided to the electronic certification service provider.

Section 3: The obligation of the electronic certificate holder

Article 25:
From the moment of the creation of signature creation data, the holder of the electronic certificate is solely responsible for the confidentiality and integrity of the data related to the signature creation that he uses. Any use of these is deemed, unless proven otherwise, to be its act.

Article 26:
The holder of the electronic certificate is required, as soon as possible, to notify the certification service provider of any change in the information contained therein.

Article 27:
In case of doubt as to the maintenance of the confidentiality of the data relating to the creation of signature or loss of conformity with the reality of the information contained in the certificate, its holder is obliged to have it revoked immediately in accordance with the provisions of the Article 21 of this law.

Article 28:
When an electronic certificate has expired or been revoked, the holder can no longer use the corresponding signature creation data to sign or have this data certified by another electronic certification service provider.

Chapter III: Sanctions, Preventive Measures and the Recognition of Offenses

Article 29:
Is punished with a fine of 10,000 to 100,000 DH and imprisonment from three months to one year, whoever has provided secure electronic certification services without being approved under the conditions provided for in Article 21 hereof. above or will have continued its activity despite the withdrawal of its authorization or has 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 by imprisonment of one month to six months and a fine of 20,000 DH to 50,000 DH whoever divulges, incites or participates to divulge the information entrusted to him in the framework for the exercise of its activities or functions.

However, the provisions of this article are not applicable to the publication or the communication authorized, in writing in paper form or electronically, by the holder of the electronic certificate or to the publication or the communication authorized by the legislation in force. .

Article 31:
Without prejudice to more severe penal provisions, is punished by imprisonment of one year to five years and a fine of 100,000 DH to 500,000 DH, who made knowingly false statements or handed false documents to the provider electronic certification services.

Article 32:
Anyone who has imported, exported, supplied, exploited or used any of the means or services of cryptography without the required declaration or authorization shall be punished by one year's imprisonment and a fine of 100,000 DH. in Articles 13 and 14 above.

The court may, in addition, pronounce 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 offense or to facilitate its preparation or commission, the maximum penalty shall be freedom incurred is noted as follows:

- he is brought to life imprisonment when the offense is punishable by 30 years' imprisonment;

- it is extended to thirty years' imprisonment, when the offense is punishable by twenty years of criminal imprisonment;

- it is brought to twenty years 'imprisonment, when the offense is punishable by fifteen years' imprisonment;

- he is brought to fifteen years 'imprisonment, when the offense is punishable by ten years' imprisonment;

- it is brought to ten years 'imprisonment, when the offense is punishable by five years' imprisonment;

- it is doubled when the offense is punishable by up to three years' imprisonment.

However, the provisions of this article shall not apply to the perpetrator or accomplice of the offense who, at the request of the judicial or administrative authorities, has provided them with the plain text version of the encrypted messages, as well as the necessary secret agreements. to decryption.

Article 34:
Except to demonstrate that they have not committed willful misconduct or negligence, persons providing cryptography services for the purposes of confidentiality are liable, in respect of such benefits, for the harm caused to persons entrusting them with the management of their secret agreements in the event of breaches of the integrity, confidentiality or availability of data processed using these agreements.

Article 35:
Anyone who illegally uses personal signature creation elements relating to the signature of others shall be punished by imprisonment for one to five years and a fine of DH 10,000 to DH 100,000.

Article 36:
Is punished with a fine of 10,000 DH to 100,000 DH and imprisonment from three months to six months, any provider of electronic certification services that does not respect the obligation of information of the national authority provided in Article 23 above.

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

Article 37:
Any holder of an electronic certificate who continues to use the expired or revoked certificate is liable to a fine of 10,000 DH to 100,000 DH and imprisonment for 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 whoever uses unduly, a company name, an advertisement and, in a general way, any expression making believe that it is approved in accordance with the provisions of Article 21 above.

Article 39:
Where, on the report of its agents or experts, the national authority finds that the electronic certification service provider issuing secure certificates no longer meets one of the conditions laid down in Article 21 above. or its activities are not in conformity with the provisions of this Act or the regulations made for its application, it invites it to comply with the said conditions or provisions, within the time it determines.

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

Where the activities of the offender are such as to affect the requirements of national defense or internal or external security of the State, the national authority is empowered to take all necessary measures to stop such activities, without prejudice to criminal proceedings they call.

Article 40:
When the perpetrator is a legal person, and without prejudice to the penalties that may be applied to its leaders, the perpetrators of any of the offenses set out above, the fines provided for in this chapter shall be double.

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

- the partial confiscation of his property;

- the confiscation provided for in Article 89 of the Criminal Code;

- the closure of the establishments or establishments of the legal person used to commit the offenses.

Article 41: In
addition to officers and judicial police officers and customs officers in their field of competence, the agents of the national authority authorized for this purpose and sworn in the forms of common law may search and record, by minutes , infringements of the provisions of this law and of the texts taken for its application. Their minutes are transmitted within five days to the King's Prosecutor.

The officers and officers referred to in the preceding paragraph may enter the premises, grounds or means of transport for professional use, request the disclosure of all professional documents and take a copy, collect, on convocation or on the spot, the information and justifications. .

They may proceed, in those very places, to the seizure of the means referred to in Article 12 above on the order of the King's Prosecutor or the investigating judge.

The means seized are recorded in the minutes drawn up on the spot. The original minutes 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 the real rights are fixed by decree.

Article 43:
Notwithstanding the provisions of the first paragraph of Article 21 above, the Government may, on the proposal of the national authority referred to in Article 15 and subject to the interest of the public service, approve legal persons governed by public law to issue and issue secure electronic certificates and to administer the related services under the conditions laid down by this Law and the texts adopted for its application.