Translated by Donna L. Hicks de Pérez-Mera
Santo Domingo Speakers Bureau, S.A.
Tel.: (809) 566-3085; Fax.: (809) 289-0080;
E-mail: donna.hicks@codetel.net.do

Law No. 126-02 concerning Electronic Commerce, Documents, and Digital Signatures

THE NATIONAL CONGRESS
In the Name of the Republic

Law No.126-02

WHEREAS: The accelerated change in information technology and telecommunications, together with the exponential growth of the digital interconnection of nations, is generating a profound transformation of human activities in all of their dimensions, and therefore of the social order and the global economy;

WHEREAS: This technological convergence has revolutionized the way in which society produces, stores, and uses information;

WHEREAS: The rapid growth of networks across national borders has erased the geopolitical and economic limits between those who provide, supply, and originate information, democratizing access of countries and persons to knowledge and to global markets;

WHEREAS: The new technologies are transforming traditional practices of trade by permitting the direct interconnection of the critical systems of trade and their key components, clients, providers, distributors, and employees, which make possible electronic commerce in its different manifestations;

WHEREAS: That worldwide electronic commerce is responsible for the profound changes recorded in the way of doing business, so that it alters the relationship between producers and consumers of goods and services, and stimulates the rapid integration of global markets. Also, insofar as worldwide electronic commerce grows, companies seek a permanent structure for the transactions of electronic commerce supported and acknowledged by national governments;

WHEREAS: Electronic commerce makes markets efficient by increasing exponentially the options and choices which providers and consumers have available, and tends to facilitate the exchange between the contracting parties of information, optimum practices, and feedback in the market in real time;

WHEREAS: The transactions of exchange of goods, of information, and of services, between persons and /or companies will be benefitted enormously by the efficiency, legal security, and global scope granted to them by the fact of their orderly and regulated performance over digital means of storage and transportation fo data over global information networks;

WHEREAS: The institutions and regulatory systems of the State must increase their productivity and effectiveness in order to guarantee the trust, protection, legal security of the parties involved in electronic econmic transactions within the scope of technological globalization;

WHEREAS: The authentication and security of digital documents and messages are fundamental in order to ensure the parties involved that their electronic commerce transactions are performed in an environment free from illegal attacks or infractions, or that, if these occur exceptionally, said transactions satisfy the necessary conditions to be able to address conflicts, assign responsibilities, and repair harm as may be the case;

WHEREAS: The civil and commercial codes of the Dominican Republic govern matters of commerce, contracts, and civil liability, and therefore are the essential basis of the country´s electronic commerce.

TITLE I

GENERAL PROVISIONS

ARTICLE 1.- Scope of application. The present law shall be applicable to all types of information in the form of a digital document or data message, excepting in the following cases:

a) In the obligations contracted by the Dominican State pursuant to international conventions or treaties;

b) In the written warnings which, because of legal provisions, must necessarily be printed on certain types of products because of the risk implied by their marketing, use, or consumption.

ARTICLE 2.- Definitions. For effects of the present law the following shall be understood:

a) Electronic commerce: Every relationship of a commercial nature, whether contractual or not, structure based on the use of one or more digital documents or data messages or of any other similar medium. The relationships of a commercial nature comprise but are not limited to the following operations:

- Every commercial operation of supplying or exchanging goods, services, or information;

- Every distribution agreement;

- Every operation of representation or commercial mandate;

- Purchasing of accounts receivable, at a discount price (factoring);

- Rental or leasing;

- Construction of works;

- Consulting;

- Engineering;

- Granting of licenses;

- Investment;

- Financing;

- Banking industry;

- Insurance;

- Every agreement of concession or exploitation of a public service;

- Joint venture and other forms or industrial or commercial cooperation;

- Transportation of merchandise or passengers by air, ocean, rail, or highway.

b) Digital document: The information coded in digital form on a logical or physical back-up or support, in which electronic, photolithographic, optical, or similar

methods are used which are constituted in representation of acts, facts, or data legally relevant;

c) **Data messages:** The information generated, sent, received, stored, or communicated by electronic, optical, or similar means, such as, among others, the electronic exchange of data (EDI), electronic mail, telegram, telex, or telefax;

d) **Electronic data exchange (EDI):** The electronic transmission of information from one computer to another, when the information is structured according to a technical standard agreed upon to such effect;

e) **Initiator:** Every person who, in accordance with a data message, has acted for his account or in whose name one has acted, in order to send or generate said message before being filed, if such is the case, but who has not done so as intermediary with respect to said message;

f) **Addressee:** The person designated by the initiator to receive the message, but who is no acting as intermediary with regard to said message;

g) **Intermediary:** The person who, in relation to a particular data message, acting for account of another, sends, receives, or files said message or provides some other service with regard to it;

h) **Information system:** By this will be understood any system used to generate, send, receive, file, or process in any other form digital documents or data messages;

i) **Digital signature:** It will be understood as a numerical value attached to a data message and which, by using a known mathematical procedure, linked to the password of the initiator and to the text ot the message, allows one to determine that this value has been obtained exclusively with the inititator´s password and the text of

the message, and that the initial message has not been modified after the transmission has been effected;

j) **Cryptography**: The branch of applied mathematics and information science which concerns the transformation of digital documents or data messages from their original representation to a representation which is unintelligible and undescipherable, and which protects and preserves its contents and form, and which also concerns the recuperation of the original document or data message based on the latter;

k) **Certifying entity**: That institution or company which, being authorized pursuant to the present law, is empowered to issue certificates in relation to the digital signatures of persons, to offer or facilitiate services of registration and chronological stamping of the transmission and receipt of data messages, as well as to fulfill other functions relating to the communications based on digital signatures;

l) **Certificate**: The digital document issued and signed digitally by a certifying entity, which identifies a signer unequivocally during the period of effectiveness of the certificate, and which constitutes proof that said subscriber is the source or originator of the contents of a digital document or data message which incorporates its associated certificate;

m) **Repository**: An information system for the storing and recuperation of certificates or other type of information relevant to the issuing and validation of same;

n) **Signer**: The person who contracts with a certifying entity the issuing of a certificate, so that it be named or identified in it. Said person keeps under his strict and exclusive control the procedure to generate his digital signature;

ñ) **User:** The person who, without being a signer and without contracting the services of issuing of certificates of a certifying entity, may nevertheless validate the integrity and authenticity of a digital document or data message, based on a certificate of the subscriber originating the message;

o) **Revoke a certificate**: To terminate definitively the period of validity of acertificate, from a specific date, onwards;

p) **Suspend a certificate:** To interrupt temporarily the operational period of a certificate from a specific date onwards.

ARTICLE 3.- Interpretation. In the interpretation of the present law, the recommendations of multilateral organizations concerning the subject shall be taken into account as well as the need to promote the uniformity of their application and the observance of good faith.

Questions relating to matters governed by the present law, and which are not expressly resolved in any text, shall be addressed pursuant to the general principles which inspire the present law, including but not limited to:

1. Facilitating electronic commerce between and within nations;

2. Validating transactions between parties which have been performed by means of the new information technologies;

3. To promote and support the implementation of new technologies;

4. To promote the uniformity of application of the law, and

5. To support commercial practices.

ARTICLE 4.- Legal acknowledgement of digital documents and data messages. Legal effects, validity or obligatory force shall not be denied to any type of information for the sole reason that it is in the form of a digital document or data message.

TITLE II

APPLICATION OF THE LEGAL REQUIREMENTS OF DIGITAL DOCUMENTS AND DATA MESSAGES

ARTICLE 5.- Written proof. When any norm requires that information be presented in writing, said requirement shall be satisfied with a digital document or data message, if the information which it contains is accessible for its subsequent consultation and if the digital document or data message fulfills the requirements of validity established in the present law.

The provisions of the present article shall be applied both if the requirement established in any norm constitutes an obligation, and if the norms foresee consequences in the event that the information is not in written form.

ARTICLE 6.- Signature. When any norm requires the presence of a signature or establishes certain consequence in the absence of same, it shall be understood that said requirement is satisfied with regard to a digital document or data message, if the latter has been signed digitally and the digital signature fulfills the requirements of validity established in the present law.

Paragraph.- In any interaction with a public entity which requires a signed document, said requirement shall be satisfied with

one or more digital documents or data messages which are signed digitally in accordance with the requirements contained in the present law. The reglamentation of the present law shall specify in detail the conditions for the use of a digital signature, certificates, and certifying entities indocumentary interactions between entities of the State or between private parties and state entities.

The provisions of the present article shall be applied both if the requirement established in any norm constitutes an obligation, and if the norms simply foresee consequences in the event that a signature does not exist.

ARTICLE 7.- Original. When any norm requires that the information be presented and preserved in its original form, said requirement shall be satisfied with a digital document or a data message if:

a) There exists a reliable guarantee that the integrity of the information has been preserved, as of the moment in which its definitive form was generated for the first time, as a digital document, data message, or other form;

b) If it is required that the information be presented, if said information can be shown to the person to whom it must be presented.

Paragraph.- The provisions of the present article shall be applied both if the requirement established in any norm constitutes an obligation, and if the norms simply foresee consequences in the event that the information is not presented or preserved in its original form.

ARTICLE 8.- Integrity of the digital document or data message. For effects of the previous article, it shall be considered that the information consigned in the digital document or data message is entire (integral or complete), if the latter has remained complete and unaltered, excepting for the addition of some endorsement or of some

change which may be inherent to the communication process, filing, or presentation. The degree of reliability required shall be determined in accordance with the purpsoes for which the information was generated, and of all of the circumstances relevant to the case.

ARTICLE 9.- Admissibility and proving force of digital documents and data messages. Digital documents and data messages shall be admissible as means of proof, and shall have the same proving effect granted to acts under private signature in the Civil Code and in the Code of Civil Procedure.

Paragraph.- In administrative or judicial acts efficacy, validity, or obligatory and proving force shall not be denied to any type of information in digital document or data message form, because of the sole fact that it deals with a digital document or data message or because it has not been presented in its original form.

ARTICLE 10.- Criteria to evaluate as proof a digital document or data message. When evaluating the proving force of a digital document or data message, one shall take into consideration the reliability of the form in which the digital document or message has been generated, filed, or communicated, the reliability of the form in which the integrity of the information has been preserved, the form in which its creator or initiator is identified, and any other pertinent factor.

ARTICLE 11.- Preservation of digital documents and data messages. When the law requires that certain documents, records, or information be preserved, said requirement shall be satisfied by means of the preservation of the digital documents and/or data messages as may be the case, so long as they fulfill the following conditions:

1. That the information which they contain be accessible for their subsequent consultation;

2. That the digital documents or data messages be preserved in the format in which they were generated, sent, or received, or in a format which will allow one to demonstrate that it proces exactly the information originally generated, sent, or received;

3. In the case of the data messages which preserves, if there is any, all of the information which will allow one to determine the origin, destination, date, and hour on which the message was sent or received, and

4. In the case of a digital document which is preserved for legal effects, all information which will allow one to determine the date and hour on which the digital document was delivered for its preservation, the person or persons who created the document, the person who delivered the document, and the person receiving same for its preservation.

Paragraph.- The information which is solely intended to facilitate access to the digital document or the sending or receiving of data messages shall not be subject to the obligation of preservation, excepting that information which is associated with a data message which constitutes proof of its transmission from its origin to its destination, including but not limited to the routing of the message within the respective data network, its unique sequential number, and exact times of receipt and retransmission, and universal identifiers of each server or communications node which is involved in the original transmission of the message.

ARTICLE 12.- Preservation of digital documents and data messages through third parties. Compliance with the obligation to preserve documents, records, or information in data messages may be performed through third parties, so long as the conditions indicated in the abovegoing paragraph are fulfilled.

TITLE III

PART I

COMMUNICATION OF DIGITAL DOCUMENTS AND DATA MESSAGES

ARTICLE 13.- Formation and validation of contracts. In the formation of the contract, excepting an express agreement between the parties, the offer and its acceptance may be expressed by means of a digital document, data message, or a data message bearing a digital document, as may be the case. Validity or obligatory force may not be denied to a contract because of the sole reason that in its formation one or more digital documents or data messages have been used.

ARTICLE 14.- Acknowledgement of digital documents and data messages by the parties. In the relations between the initiator and the addressee of a data message, or between the parties signing a digital document, when there are any, legal effects, validity, or obligatory force shall not be denied to a manifestation of will or other declaration because of the sole reason that it has been made in the form of a digital document or data message.

ARTICLE 15.- Communication and attribution of digital documents. A digital document can be communicated between parties, whether by delivery of the digital document in a physical medium from one party to the other, or through a data message which, in addition to its own contents, includes a faithful and verifiable representation of the digital document.

Paragraph.- It shall be understood that a digital document comes from that person or those persons who digitally sign the document, independently of the support or back-up on which said document has been recorded or of its means of communication. In the case of the transmission of the digital document by data message and the absence of the internal digital signature to the document, it shall be understood that the digital document comes from the initiator of the data message in accordance with Article 16 of the present law.

ARTICLE 16.- Attributions of a data message. It shall be understood that a data message comes from the initiator when the latter has been sent by:

1. The initiator itself;

2. By any person empowered to act in the name of the initiator with regard to said message, or

3. By an information system programmed by the initiator, or in its name, so that it operate automatically.

ARTICLE 17.- Presumption of origin of a data message. It shall be presumed that a data message has been sent by the initiator, and therefore the addressee can act in consequence, when:

1. The procedure agreed to previously with the initiator in order to establish that the data message effectively came from the latter has been applied adequately, and

2. The data message which the addressee receives results from the acts of a person whose relationship with the initiator, or with any of his representatives, has given it access to any method used by the initiator to identify a data message as its own.

ARTICLE 18.- Agreement of the data message sent with the data message received. So long as a data message comes from the initiator, or is understood to come from him, or so long as the addressee has the right ot act in accordance with this supposition, in the relationships between the initiator and the addressee, the latter shall have the right to consider that the data message received corresponds to that which the initiator wished to send, and he may proceed in consequence. The addressee shall not enjoy this right if he knew or would have known, if he had acted with the due diligence or

had applied an agreed upon method, that the transmission had given rise to an error in the data message received.

ARTICLE 19.- Duplicate data messages. It is presumed that each data message received is a different data message, excepting insofar as it duplicates another data message, and that the addressee knows, or should have known, if he had acted with due diligence or had applied an agreed upon method, that the new data message was a duplicate.

ARTICLE 20.- Acknowledgement of receipt of data messages. If upon sending or before sending a data message, the initiator the initiator requests or agrees with the addressee that acknowledge of receive of the data message be made, but a particular form or method to do so has not been agreed upon between them, acknowledgement of receipt can be made by means of:

a) Any communication of the addressee, whether automated or not, or

b) Any act of the addressee which suffices to indicate to the initiator that the data message has been received.

Paragraph I.- If the initiator has requested or agreed with the addressee the acknowledgement of receipt of the data message, and expressly the former has indicated that the effects of the data message shall be conditioned on the receipt of an acknowledgement of receipt, it shall be deemed that the data message has not been sent until the acknowledgment of receipt has been received.

Paragraph II.- If the initiator has requested or agreed with the addressee that an acknowledgment of receipt of the data message be given, but the former did not expressly indicated that the effects of the data message are conditioned to the receipt of the acnowledgment of receipt, and if the acknowledgment of receipt has not been received

in the term set or agreed to, no term has been set or agreed to, (*sic*) in a term of forty-eight (48) hours, as of the moment of the sending or the expiration of the term set or agreed to, the initiator:

a) May give notice to the addressee that it has not received the acknowledgment of receipt by verifiable means, and to set a new term for its receipt, which shall be forty-eight (48) hours, counting from the moment of the sending of the new data message, and

b) If the acknowlegement of receipt is not received within the term indicated in the above going clause, it may, by giving notice of such to the addressee, consider that the data message has not been sent, or exercise any other right which it may have.

ARTICLE 21.- Acknowledgement of receipt of digital documents. Likewise acknowledgment of receipt of a digital document may be performed by means of:

a) Any communication whether automated or not, from the party receiving the digital document to the party which delivers it directly or through a duly authorized person, and

b) Any act of the receiving party which suffices to indicate to the party who delivers the digital document that the same has been received.

In the case of delivery of digital documents by means of data messages, the provisions of Article 20 of the present law shall be taken into account. In such case, the acknowledgment of receipt of the digital document is identical to the acknowledgment of receipt of the data message used for the sending of such digital document.

ARTICLE 22.- Presumption of receipt of a data message. When the initiator recives an acknowledgement of receipt from the addressee, it shall be presumed that the latter has received the data message.

Said presumption shall not imply that the data message corresponds to the message received. When in the acknowledgment of receipt it is indicated that the data message received fulfills the technical requirements agreed uponor stated in some applicable technical norm, it shall be presumed that it is so.

ARTICLE 23.- Legal effects. Articles 20, 21, and 22 of the present law govern only the effects related to the acknowledgement of receipt. The legal consequences of the digital document or of the data message shall be governed pursuant to the norms applicable to the legal act or business contained in said digital document or data message.

ARTICLE 24.- Time of sending of a data message. Unless otherwise agreed between the initiator and the addressee, the data message shall be deemed to have been issued when it enters an information system which is not under the control of the initiator or of the person who sent the data message in the latter´s name.

ARTICLE 25.- Time of receipt of a data message. Unless otherwise agreed between the initiator and the addressee, the moment of receipt of a data message shall be determined as follows:

a) If the addressee has designated an information system for the receipt of data messages, the receipt shall take place:

    1. At the moment when the data message enters the designated information system;

    2. If the data message is sent to an information system of the addressee which is not the designated information

system, at the moment in which the addressee recuperates the data message.

b) If the addressee has not designated an information system, the receipt shall take place when the data message enters an information system of the addressee.

Paragraph.- The provisions of the present article shall be applicable even though the information system is located in a place other than where the data message is considered to have been received in accordance with the following article.

ARTICLE 26.- Place of sending and receiving of data message. Unless the initiator and the addressee agree otherwise, the data message shall be considered to have been issued in the place where the initiator has its establishment, and shall be deemed to have been received in the place where the addressee has his place of establishment. For purposes of the present article:

a) If the initiator or addressee has more than one establishment, his establishment shall be the one with the closest relationship to the underlying operation, or, if there is not underlying operation, his main establishment;

b) If the initiator or addressee does not have any establishment, his habitual place of residence shall be taken into account.

ARTICLE 27.- Time and place of sending and receiving a digital document. For those digital documents which are delivered in physical back-up, such as magnetic media, photolithographical media of writing only, optical media or similar, the time of sending and receiving and the place of sending and receiving the digital document shall be determined in the same way as if the document had been delivered in a physical paper medium or similar.

For those digital documents which are delivered by means of data messages, the norm specified in Articles 25 and 26 of the present law shall be applied.

ARTICLE 28.- Concession of rights or acquisition of obligations by means of digital documents or data messages. When transferring a right to a particular person and to no other, or when the latter acquires any obligation, and the law requires that in order for said act to have effect, the right or obligation must be transferred to that person by means of the sending or use of a document issued on paper, said requirement shall be satisfied if the right or obligation is transferred by means of the sending or use of one or more digital documents or data messages, so long as a reliable method to guarantee the singularity oruniqueness of said digital documents or messages is used.

Paragraph I.- For purposes of the present article, the level of reliability required shall be determined in light of the purposes for which the right or obligation was transferred and of all of the circumstances of the case, including any pertinent agreement.

Paragraph II.- When a legal norm is applied obligatorily to a registered contracted or one of which proof has been left in a document issued on paper, said norm shall not fail to be applied to said contract of which proof has been left in one or more data messages for the reason that the contract consists of said data message or messages instead of being recorded in documents issued on paper.

PART II

ELECTRONIC COMMERCE IN MATTERS OF TRANSPORTATION OF MERCHANDISE

ARTICLE 29.- Acts related to contracts for transportation of merchandise. Without prejudice ot the provisions in the present law, the present chapter shall be applicable but not limited to any of

the following acts which are related to a contract for transportation of merchandise, or to its compliance:

1. Acts relating to the receipt and shipment of merchandise:

    a) Indication of the brands, number, quantity, or weight of the merchandise;

    b) Declaration of the nature or value of the merchandise;

    c) Issuance of a receipt for the merchandise;

    d) Confirmation of having completed the shipment of the merchandise.

2. Acts related to the contract and conditions of transportation:

    a) Notification to any persons of the clauses and conditions of the contract;

    b) Communication of instructions to the transporter.

3. Acts related to the conditions of delivery of the merchandise:

    a) Claiming of the delivery of the merchandise;

    b) Authorization to proceed with the delivery of the merchandise;

    c) Notification of the loss of merchandise or damage which it may have suffered.

4. Any other notification or declaration related to compliance with the contract.

5. Promise to make delivery of the merchandise to the person designated or to a person authorized to claim said delivery.

6. Concession, acquisition, waiver, restitution, transfer, or negotiation of any right to the merchandise.

7. Acquisition or transfer of rights and obligations in accordance with the contract.

Paragraph.- Complimenting the provisions established in the present law, for contracts concerning the transportation of merchandise, there shall be taken into account the provisions established by the Commercial Code of the Dominican Republic concerning the obligations of commissioners for ground and ocean transportation and of the carrier.

ARTICLE 30.- Transporting of documents.- Subject to the provision in Paragraph II of the present article, in those cases in which the law requires that any of the acts indicated in Article 38 of the present law be performed in writing or by means of a document issued on paper, said requirement shall be satisfied when the act is performed by means of one or more digital documents or data messages.

Paragraph I.- The above shall be applicable both if the requirement foreseen in it is expressed in the form of an obligation, or if the law simply foresees consequences in the event that the act not be carried out in writing or by means of a document issued on paper.

Paragraph II.- When using one or more digital documents or data messages to carry out any of the acts indicated in numbers 6 and 7 of Article 29, no document issued on paper to perform any of these acts shall be valid unless an end has been made to the use of a digital document or data message to substitute it for the documents issued on paper. Every document with back-up on paper which is issued under those circumstances must contain the declaration in this regard. The substitution of digital documents or data messages for documents issued on paper shall not affect the rights or obligations of the parties.

Paragraph III.- Article 28 of the present law, and in particular Paragraph II of said article, shall be applicable to contracts for transporting of merchandise which are consigned or of which proof on paper has been left (recorded).

TITLE IV

DIGITAL SIGNATURES, CERTIFICATES, AND CERTIFYING ENTITIES

CHAPTER I
DIGITAL SIGNATURES

ARTICLE 31.- Attributes of a digital signature. The use of a digital signature shall have the same force and effect as the use of a handwritten signature, if it incorporates the following attributes:

1. It is unique to the person who uses it;

2. It is susceptible to being verified;

3. It is under the exclusive control of the person who uses it;

4. It is linked to the information, digital document, or message to which it is associated, in such a way that if they are changed, the digital signature is invalidated, and

5. It is in accordance with the regulations adopted by the Executive Power.

ARTICLE 32.- Safe/secure digital signature. A secure digital signature is that one which can be verified in conformance with a security procedure system which complies with the guidelines outlined by the present law and by its regulation.

ARTICLE 33.- **Data messages signed digitally**. It shall be understood that a data message has been signed digitally if the symbol or methodology adopted by the party complies with an authentication or security procedure established by the regulation of the present law.

When a digital signature has been fixed in a data message, it is presumed that the signer of same had the intention of accrediting that data message and of being linked to the contents of same.

ARTICLE 34.- **Digital documents signed digitally**. It shall be understood that a digital document has been signed digitally by one or more parties if the symnbol or methodology adopted by each one of the parties complies with an authentication or security procedure established by the regulation of the present law. When one or more digital signatures have been set in a digital document, it is presumed that the signing parties had the intention of accrediting said digital document, and of being linked to the contents of same.

CHAPTER II

CERTIFYING ENTITIES

ARTICLE 35.- Characteristics and requirements of the certifying entities. Without prejudice to what is established in the present article, certifying entities may be companies, both public and private, of national or foreign origin, and the chambers of commerce and production which, after application, are authorized by the Dominican Telecommunications Institute (INDOTEL), and which comply with the requirements established in the regulations of application pronounced based on the following conditions:

a) Having the economic and financial capacity sufficient to provide the services authorized as certifying entity;

b) Having the necessary technical capacity and elements for the generation of digital signatures, the issuing of certificates concerning the authenticity of same, and the preservation of data messages in the terms established in the present law;

c) Without prejudice to the regulatory provisions which govern to such effect, the legal representatives and administrators may not be persons who have been condemned to imprisonment; or who have been suspended from the exercise of their profession because of serious fault against ethics or who have been excluded from same. Said prohibition shall be in effect for the same period in which the criminal or administrative law indicates for such effect, and

d) The certificates of digital signatures issued by foreign certifying entities may be acknowledged in the same terms and conditions of certificates in the law for the issuing of certificates by national certifying entities, so long as such certificates are recognized by an authorized certifying entity which guarantees, in the same manner as it that with its own certificates, the regularity of the details of the certificate, as well as its validity and term of effectiveness.

In any case, the providers of certification services are subject to the national norms concerning liability.

Paragraph.- It is a power of the Monetary Board, among its prerogatives, to standardize everything concerning the financial operations and services associated with electronic means of payment performed by the national financial system, and the supervision of same corresponds to the Superintendency of Banks, under shelter of the banking legislation in effect.

ARTICLE 36.- Activities of the certifying entities. The certifying entities authorized by the Dominican Telecommunications Institute (INDOTEL) in this country may provide the following services, without prejudice to the regulatory power of the regulatory entity to modify the following list:

a) To issue certificates with regard to the digital signatures of persons or companies;

b) To offer or facilitate the services of creation of certified digital signatures;

c) To offer or facilitate the services of chronological recording and stamping in the transmission and receipt of data;

d) To issue certificates in relation to the person who possesses a righ with respect to the documents indicated in numbers 6 and 7 of Article 27 of the present law.

ARTICLE 37.- Audit of the certifying entities. The Dominican Telecommunications Institute (INDOTEL) retains the same power of inspection conferred by the General Telecommunications Law No. 153-98 dated May 27, 1998, and, in the event of express modification of said text, the present article shall be interpreted in such a manner as to be in accordance with the legislation on the subject of telecommunications.

ARTICLE 38.- Manifestation or declaration of practice of the certifying entity. Each authorized certifying entity shall publish, in a repository of the Dominican Telecommunications Institute (INDOTEL) or in the repository which the regulatory entity may designate, a manifestation or declaration of practice of certifying entity which contains the following information:

a) The name, address, and telephone number of the certifying entity;

b) The present public password of the certifying entity;

c) The results of the evaluation obtained by the certifying entity in the last audit performed by the Dominican Telecommunications Institute (INDOTEL);

d) Whether the authorization to operate as a certifying entity has been revoked or suspended. In both cases the public password of the certifying entity shall be considered to have been revoked or suspended. Said recording must include also the date of the revocation or suspension of operation;

e) The limits imposed on the certifying entity in the authorization to operate;

f) Any event which substantially affects the ability of the ceritfying entity to operate;

g) Any information which may be required by means of regulation.

ARTICLE 39.- Remuneration for the rendering of services. Remuneration for the services of the certifying entities shall be established freely by the latter, unless the Dominican Telecommunications Institute (INDOTEL), by means of motivates resolution, should determine that, in a concrete case, there do not exist on the market of services, the conditions sufficient to ensure effective and sustainable competition.

ARTICLE 40.- Obligations of the certifying entities. The certifying entities shall, among others, have the following obligations:

a) To issue certificates pursuant to requests or agreements with the signer;

b) To implement the security systems to guarantee the issuing and creation of digital signatures;

c) To guarantee the protection, confidentiality, and due use of the information supplied by the signer;

d) To guarantee the permanent providing of the service of certifying entity;

e) To attend punctually to the applications and claims made by the subscribers (signers);

f) To make the notices and publications in accordance with what is established in the present law and its regulations;

g) To supply the information which the competent administrative or judicial entities may require in relation to the digital signatures and certificates issued, and in general, about any data message which is under its custody and administration;

h) To update its technical elements for the generation of digital signatures, the issuing of certificates on the authenticity of same, the preservation and filing of supported documents in data messages and every other service authorized, subject to the regulations necessary to guarantee the protection of the consumers of its services;

i) To facilitate the performing of the audits by the Dominican Telecommunications Institute (INDOTEL);

j) To publish in a repository its practice of audit of certification, subject to the terms and conditions provided in the regulations.

ARTICLE 41.- Unilateral termination. Excepting by agreement between the parties, the certifying entity may terminate the agreement of relationship with the signer, by giving prior notice in a term no less than ninety (90) days. Once this term has expired, the certifying entity shall revoke the certificates which are pending expiration.

Also, the signer may terminate the relationship agreement with the certifying entity by giving prior notice of a term period no less than thirty (30) days.

ARTICLE 42.- Liability of the certifying entity. Excepting by agreement between the parties, the certifying entities shall be liable for the damages and harm which they cause to any person.

ARTICLE 43.- Cessation of activities by the certifying entities. The authorized certifying entities can cease to exercise or perform their activities, after notification to the Dominican Telecommunications Institue (INDOTEL) in a term period no less than ninety (90) days prior to the ceasing of activities by the certifying entity, without prejudice to the power of the regulatory entity to regulate whatever is necessary in order to preserve the protection of the consumers of its services. In the application of the present article, and in the event that its interpretation should be necessary, it will be taken into account that the obligation subsists of guaranteeing the protection, confidentiality, and due use of the information supplied by the signer.

CHAPTER III

THE CERTIFICATES

ARTICLE 44.- Contents of the certificates. A certificate issued by an authorized certifying entity must contain, besides the digital signature of the certifying entity, at least the following requirements:

1. Name, address, and domicile of the signer;
2. Identification of the signer named in the certificate;
3. Name, address, and place where the certifying entity performs activities;
4. The user´s public password;

5. The methodology to verify the signer´s digital signature put in the data message;

6. The series number of the certificate; and

7. Date of issuance and expiration of the certificate.

ARTICLE 45.- Expiration of a certificate. A certificate issued by a certifying entity expires on the date indicated on same. The regulation of the present law shall determine all of the conditions in addition to the term of effectiveness and expiration of certificates.

ARTICLE 46.- Acceptance of a certificate. It is understood that a signer has accepted a certificate when the latter or a person in the latter´s name has published it in a repository or has sent it to one or more persons.

ARTICLE 47.- Guarantee deriving from the acceptance of a certificate. At the moment of accepting a certificate, the signer guarantees to all persons of good faith exempt of blame who rely on the information contained in it, that:

a) The digital signature authenticated by means of the latter is under its exclusive control;

b) That no person has had access to the procedure of generation of the digital signature, and

c) That the information contained in the certificate is true and corresponds to that provided by the latter to the certifying entity.

ARTICLE 48.- Suspension and revocation of certificates. The signer of a certified digital signature may request the certifying entity which issued it a certificate, to suspend or revoke

such certificate, which suspension or revocation will be done in the manner foreseen in the regulations of application of the present law.

ARTICLE 49.- Causes for the revocation of certificates. The signer of a certified digital signature is obligated to request the revocation of the corresponding certificate in the following cases:

a) Due to loss of the private password;

b) The private password has been exposed or runs the risk that it will be given undue or inappropriate use.

In the event that any of the above indicated situations should arise, if the signer did not request the revocation of the certificate, he shall be liable for the damages and harm which may be incurred by third parties who are exempt from blame and who relied on the contents of the certificate.

A certifying entity shall revoke an issued certificate for the following reasons:

1. At the petition of the signer or a third party in his name and legal representation;

2. Due to the death of the signer, subject to the means of proof and publishing prescribed by common law;

3. Due to the absence or disappearance definitively declared by a competent authority, in accordance with the prescriptions of common law;

4. Due to liquidation of the signer in the case of companies;

5. Deu to the confirmation that any information or fact contained in the certificate is false;

6. The private password of the certifying entity or its security system has been compromised in such a material manner as to affect the certificate´s reliability;

7. Due to the cessation of activities of the certifying entity, and

8. By judicial order or order of a competent administrative entity.

ARTICLE 50.- Notification of a suspension or renewal (*sic*) of a certificate. Once the suspension or revocation of a certificate is recorded, the certifying entity must publish immediately a notice of suspension or revocation in all of the repositories in which the certifying entity published the certificate. It must also notify of this fact the persons who request information about a digital dignature verifiable by remission to the suspended or revoked certificate.

If the repositories in which the certificate was published do not exist at the moment of the publication of the notice, or if the same are unknown, the certifying entity must publish said notice in a repository which the Dominican Telecommunications Institute (INDOTEL) may designate for such effect.

ARTICLE 51.- Record of certificate. Every authorized certifying entity shall carry a record of all certificates issued, which will be available to the public, in which they must indicate the dates of issuance, expiration,and the records of suspension, revocation, or reactivation of same.

ARTICLE 52.- Term of conservation of records. The records of certificates issued by a certifying entity must be preserved for the term of forty (40) years, counting from the date of revocation or expiration of the corresponding certificate.

CHAPTER IV

SIGNERS OF DIGITAL SIGNATURES

ARTICLE 53.- Duties of the signers. The duties of the signers are:

a) To receive the passwords from the certifying entity, or to generate the passwords, using a security system required by the certifying entity;

b) To provide complete, precise, and accurate information to the certifying entity:

c) To accept the certificates issued by the certifying entity, demonstrating approval of its contents by means of the sending of same to one or more persons or requesting the publication of same in repositories;

d) To maintain the control of the private reserved password from the knowledge of third persons;

e) To perform opportunely the corresponding requests for suspension or revocation.

Paragraph.- A signer ceases to be obligated to comply with the abovegoing duties as of the publication of a notice of revocation of the corresponding certificate by the certifying entity.

ARTICLE 54.- Request for information. The signers may request from the certifying entity information concerning every matter related to the certificates and digital signatures which constitutes public information or which corresponds to them, and the certifying entity shall be obligated to respond within the terms prescribed by the regulation of the present law.

ARTICLE 55.- Liability of the signers. The signers shall be liable for falseness or error in the information supplied to the certifying entity and which is the material object of the contents of the certificate. They shall also be liable in those cases in which they do not give prompt notice of revocation or suspension of certificates in the cases indicated above.

CHAPTER V

REGULATORY ENTITY

ARTICLE 56.- Functions.- The Dominican Telecommunications Institute (INDOTEL) shall exercise the function of watchdog entity controlling the activities performed by the certifying entities. It shall especially have the following functions:

1. To authorize, pursuant to the regulation issued by the Executive Power, the operation of certification entities within national territory;

2. To ensure the proper functioning and efficient provision of the service by the certifying entities, and the full compliance with the legal and regulatory provisions of the activity;

3. To perform the audits deal with by the present law;

4. To define regulatorily the technical requirements which qualify the appropriateness of the activities performed by the certifying entities;

5. To evaluate the activities performed by the authorized certifying entities in accordance with the requirements defined in the technical regulations;

6. To revoke or suspend the authorization to operate as a certifying entity;

7. To require at any time that the certifying entities provide information related to the certificates, the digital signatures issued, and the information systems backup documents which they administer or have under custody;

8. To impose sanctions on the certifying entities for noncompliance or partial compliance with the obligations deriving from the rendering of the service;

9. To order the revocation or suspension of certificates when the certifying entity issued them without fulfilling the legal formalities;

10. To designate the repositories and certifying entities in the cases foreseen in the law;

11. To propose to the Executive Power the implementation of policies in regard to the regulation of the activities of the certifying entities and the adaptation of the technological advances for the generation of digital signatures, the issuing of certificates, the preservation and filing of documents in electronic back-up;

12. To approve the internal regulations for the providing of the service, as well as their reforms;

13. To issue certificates regarding the digital signatures of the certifying entities, and

14. To ensure the observance of the constitutional and legal provisions concerning the promotion of restrictive commercial practices and competition in the markets covered by the certifying entities.

ARTICLE 57. Faults and sanctions. The Dominican Telecommunications Institute (INDOTEL) may impose, according to the nature and gravity of the fault, the following sanctions on the

certifying entities which do not comply with, or who violate the norms to which their activity must be subject:

1. Warning;

2. Fines up to the equivalent of two thousand (2,000) minimum monthly salaries. The amount of the fine shall be graduated according to theimpact of the infraction on the quality of the service offered, and the factor of reincidence. The fined entities may be repeated against those who have performed the acts or omissions which gave rise to the sanction;

3. To suspend immediately any or all of the activities of the entity committing the infraction;

4. To remove the responsible administrators or employees from the positions which they occupy in the sanctioned certifying entity.

5. To prohibit the certifying entity committing the infringement from providing directly or indirectly the services of certifying entity for the term of ten (10) years, and

6. Definitive revocation of the authorization to oeprate as a certifying entity, when the application of the above listed sanctions has not been effective, and one attempts to avoid real or potential harm to third parties.

CHAPTER VI

REPOSITORIES

ARTICLE 58.- Recognition and activities of the repositories. The Dominican Telecommunications Institute (INDOTEL) shall authorize theoperation of only those repositories

which are kept by the authorized certifying entities. The repositories authorized to operate must:

a) Maintain a data base of certificates in accordance with the regulations which the Executive Power may issue to such effect;

b) Guarantee that the information which they maintain is preserved as integral or complete, exact, and reasonably reliable;

c) Offer and facilitate the services of recording and chronological stamping in the transmission and receipt of data messages;

d) Offer the services of filing and preservation of data messages, and

e) Maintain a record of the publications of the certificates recoked or suspended.

CHAPTER VII
VARIOUS PROVISIONS

Article 59.- Reciprocal certifications. The digital certificates issued by foreign certifying entities may be recognized in the same terms and conditions required in the law for issuance of certificates by national certifying entities, so long as such certificates are recognized by an authorized certifying entity which will guarantee, in the same form as with its own certificates, the regularity of the details of the certificate, as well as its validity and effectiveness.

ARTICLE 60.- Incorporation by issuance. Apart from an agreement otherwise between the parties, when in a digital document or data message total or partial remission is made to directives, norms, standards, agreements, clauses, conditions, or terms easily accessible with the intention of incorporating them as part of the contents or making them legally binding, it is presumed that said terms are

incorporated by remission to said digital document or data message. Between the parties, and pursuant to the law, said terms shall be legally valid as if they had been incorporated in their totality into the digital document or data message.

TITLE V

REGULATION AND EFFECTIVENESS

CHAPTER I

REGULATION

ARTICLE 61.- Regulation. The Executive Power shall regulate the present law within the six (6) months following the date on which it takes effect.

Pursuant to the regulation which may be pronounced, the Dominican Telecommunications Institute (INDOTEL) shall have an additional term of six (6) months to organize and assign to one of its dependencies the function of control and effectiveness of the activities performed by the certifying entities, without prejudice to the fact that, to such effect, the Executive Power may create a specialized unit.

CHAPTER II

EFFECTIVENESS AND REPEALS

ARTICLE 62.- Effectiveness and repeals. The present law rules from the date of its publication and repeals the norms which may be contrary to it, with the exception of the norms destined for consumer protection.

GIVEN in the Hall of Sessions of the Chamber of Deputies, Palace of the National Congress, in Santo Domigno de Guzmán, National District, Capital of the Dominican Republic, on the nineteenth (19^{th}) day of the month of March of the year two thousand two (2002); year 159 of the Independence and 139 of the Restoration.

Rafaela Alburquerque
President

Ambrosina Saviñón Cáceres — Secretary
Germán Castro García — Secretary Ad-Hoc

GIVEN in the Hall of Sessions of the Senate, Palace of the National Congress, in Santo Domingo de Guzmán, National District, Capital of the Dominican Republic, on the fourteenth (14) day of the month of August of the year two thousand two (2002); year 159 of the Independence and 139 of the Restoration.

Andrés Bautista García
President

Ramiro Espino Fermín — Secretary
Julio A. González Burell — Secreatry Ad-Hoc.

HIPOLITO MEJIA
President of the Dominican Republic

Exercising the powers conferred on me by Article 55 of the Constitution of the Republic.

I PROMULGATE the president Law and order that it be published in the Official Gazette for its knowledge and compliance.

GIVEN in Santo Domingo de Guzmán, National District, Capital of the Dominican Republic, on the fourth (4^{th}) day of the month of September of the year two thousand two (2002); year 159 of the Independence and 140 of the Restoration.

HIPOLITO MEJÍA