

DECREE No. 335-03

WHEREAS: The promulgation of Law No. 126-02 on Electronic Commerce, Documents, and Digital Signatures constitutes a significant milestone for the insertion of the Dominican Republic in the information society, as an agent of competitiveness of the productive sector, of modernization of public institutions, and socialization of information through universal access to the telecommunications services which influence these changes, such as telephony and the Internet;

WHEREAS: The volume of exchange by electronic means has grown notably in the Dominican Republic, one example of which is the increase in transactions of automatic tellers and debit operations in the terminals of points of sale;

WHEREAS: That the possibility of performing commercial transactions over electronic mediums encourages the creation and increase of new and faster services, with greater degree of personalization and quality, and decreases the costs of transaction, for both consumers and suppliers;

WHEREAS: Despite the great advantages of electronic commerce, the incorporation of legal security in the transactions occurring over this medium is a basic point in order to encourage its expansion to the benefit of persons or companies who participate in it, insofar as the celebration of contracts over digital mediums requires the full identification of the persons who perform the transactions and the verification of the integrity of the contents of electronic documents, in order to guarantee the eventual value of proof, judicially and extrajudicially, of digital signatures and data messages;

WHEREAS: Law No. 126-02 and the Regulation of Application which approves the present Decree attempt to provide the Dominican Republic with an adequate legal framework required by the development of electronic commerce, complimenting the norms of law in effect in civil, commercial, and administrative matters, by providing the adequate legal acknowledgement of transactions in digital format, and adopting measures which will permit one to identify in a trustworthy form the persons who participate, for the purpose of acknowledging respective rights and obligations, as well as guaranteeing their value as proof;

WHEREAS: The effective implementation of Law No. 126-02 will permit the providing of clear rules for electronic commerce on perfecting the commitments assumed through expressions of will over the electronic medium, which will provide a framework of security and trust for the development of electronic transactions with full identification of their participants and certainty regarding the integrity of the contents of digital documents and data messages issued by the latter;

WHEREAS: At the same time, this legal and regulatory regime will allow the development of the “Electronic Government” and will facilitate access by the community to information and services offered by the State, increasing the efficiency of its organizations, by means of the digitalization of its procedures, remote access to data bases, and expediting of information and communication of public services, with the consequent corresponding reduction of processing time, as well as a reduction of the costs associated with supplying of same;

WHEREAS: Given the nature of the electronic transactions in which it is possible to perform commercial operations which generate rights and obligations, between parties located in remote places, beyond the scope of application of this legal order, the Dominican Republic must adopt legal and technical norms which will permit inter-operability between the different systems with which it is interconnected internationally;

WHEREAS: That in that line of ideas, it is necessary to have regulatory and administrative mechanisms of recognition of legal

validity of digital certificates issued outside of the country, and used by persons located abroad, in their exchanges with the Dominican Republic, recognizing, for such ends, the power of the Dominican Telecommunications Institute (INDOTEL), in its capacity as regulatory body, to make agreements of mutual recognition (acknowledgment) of certificates with other countries;

WHEREAS: That a fundamental element for the push towards electronic commerce is the setting up of an Infrastructure of Public Password (Key) for the Dominican Republic, which will permit the reliable identification of persons or companies signing digital certificates;

WHEREAS: Law No. 126-02 establishes that the entities of certification must fulfill the requirements established in the regulations of application;

WHEREAS: One of the essential functions of the certification entities is that of validating the data of identity of the subscribers/signers of digital certificates, which activity it develops for itself or for third parties, according to international usages;

WHEREAS: This activity, developed by the Registry Units, merits a specific regulation, given the transcendence of its role as axis of the system of trust which is implied by a Public Password Infrastructure;

WHEREAS: Another relevant aspect is the determination of the official day and time, at a given moment, in the electronic mediums, as well as the design of the mechanisms of communication and distribution of the official date and time on the Internet, so that, both public entities and certification entities proceed to take from this mechanism the exact date and time as input for its registry and subsequent distribution, and for the supplying of the service of registry and chronological stamping;

WHEREAS: On the other hand, the possibility of having the certain or true date and time in electronic mediums and in the Internet will permit the celebration or performance of acts and agreements for which the reliable determination of the precise moment of occurrence of a fact generating rights or obligations constitutes an essential

element in the formation and manifestation of the will, such as in the presentation of evidence in digital format in judicial and administrative instance, as documentary proof, in the making of electronic purchases or in electronic notifications;

WHEREAS: Pursuant to Law No. 126-02, there is recognized the legal efficacy of the mechanisms of identification of authorship which have been agreed to by the parties, even in the event that it not be a question of digital signature;

WHEREAS: Nevertheless, Law No. 126-02 does not use any special denomination or name for those mechanisms of identification agreed upon between the parties to a digital transaction not subject to solemn forms, which do not constitute a digital signature due to the absence of any of its elements, although the Law itself recognizes the legal efficacy of said mechanisms of identification of authorship;

WHEREAS: Comparative law, both in the legislation in effect and in the model laws of the United Nations Commission for International Mercantile Law – CNUDMI, on which Law No. 126-02 is based, denominates as an electronic signature those mechanisms of identification in the virtual world which do not constitute advanced digital signatures or electronic signatures;

WHEREAS: The interpretation which should be given to the alternatives contemplated by Law No. 126-02 with regard to the mechanisms of authentication agreed to between the parties which do not constitute a digital signature is oriented by the same Law when it states the general principles which inspire it and the criteria which should be resorted to for its interpretation;

WHEREAS: In its article 3, Law No. 126-02 establishes as criteria of interpretation the recommendations of multilateral bodies on the subject, the need to promote the uniformity of its application, and the observation of good faith, and it points out as general principles the facilitating of electronic commerce, validating of transactions between parties, promoting and supporting of the implementation of new technologies, and the support of commercial practices;

WHEREAS: Pursuant to what is established by Law No. 126-02, it is in order to denominate as an electronic signature the mechanisms of authentication agreed to between the parties, in consonance with comparative law both of the legislation in effect in the various countries, and that contained in the Model Laws of the United Nations Commission for International Mercantile Law – CNUDMI;

WHEREAS: Likewise, the international systems of electronic signature or digital signature, in general, contemplate voluntary schemes of accreditation, in accordance with the principle of freedom of trade;

WHEREAS: Nevertheless, it is necessary, for purposes of protecting the rights of consumers and users of digital signatures, to regulate, minimally, the rendering of certification services performed by providers of electronic signature;

WHEREAS: The United Nations Commission for International Mercantile Law – CNUDMI, as well as the legislations based on its principles, expressly foresee systems of voluntary accreditation of the providers of certification services before specific regulatory bodies, differentiating the legal effects of the digital certificates issued by authorized certifiers with full legal value of handwritten signature, with respect to the certificates issued by unauthorized certifiers, which do not enjoy the same legal value which the norms assign to the digital signature, but which do not lack all value, because they are considered as an electronic signature;

WHEREAS: In such cases, one assigns the same legal effect which is granted to the handwritten signature to the digital signature (sic), also called advanced electronic signature, which is a reliable electronic signature, only when said signatures are generated from digital certificates issued by certification entities authorized by the corresponding regulatory body, foreseen for each norm in particular in comparative law;

WHEREAS: In accordance with the above aspects, it is necessary to acknowledge the existence of providers of certification services who choose not to request authorization or comply with the requirements established by INDOTEL for providing digital signature services,

with value equivalent to that granted in the legal order in effect to the holographic signature, expressly establishing that their certificates shall not have the effects of a digital signature;

WEHREAS: The Regulation which approves the present Decree is intended to encourage the development of technological initiatives linked to electronic commerce, by promoting the use of these services, and disseminating their use among the population in order to familiarize a greater number of persons with the system;

WHEREAS: Likewise, it is deemed convenient to create a Registry of Certification Entities which will permit its permanent consultation over the Internet in order to facilitate the confirmation of the relevant aspects of the Public Password Infrastructure of the Dominican Republic, by subscribers and users of digital signatures;

WHEREAS: Law No. 126-02 on Electronic Commerce, Digital Documents and Signatures, in its article 61, establishes a term period of six (6) months, as of the publication of the said Law, for the Executive Power to pronounce the corresponding Regulation of Application;

WHEREAS: Law No. 126-02 on Electronic Commerce, Digital Documents and Signatures of the Dominican Republic, was published in the Official Gazette No. 10172 on the twenty-ninth (29th) day of the month of September of the year two thousand two (2002);

WHEREAS: Pursuant to the provisions of article 56 of the said Law, which empowers **INDOTEL** to propose to the Executive Power the implementation of policies regarding the regulation of activities of the certification entities, as well as to approve the internal regulations of the rendering of services, among other functions, on the seventeenth (17th) day of the month of March of the year two thousand three (2003), the Board of Directors of the **Dominican Telecommunications Institute (INDOTEL)** approved, by means of its Resolution No. 042-03, the draft of the General Regulation of Application of the Law on Electronic Commerce, Digital Documents, and Signatures, to be submitted for the approval of the Executive Power, which was drafted by said institution with the participation of international consultants, after having exhausted several rounds of

consultations, in which representatives of the telecommunications sector, of the financial sector, of associations of accountants and auditors, of the public sector, and of the professional associations and non-profit organizations of the Dominican Republic participated.

WHEREAS: By express delegation made by the Board of Directors of the **Dominican Telecommunications Institute (INDOTEL)**, on the twenty-fourth (24th) day of the month of March of the year two thousand three (2003), the President of the Board of Directors of said institution, Lic. Orlando Jorge Mera, remitted to the Office of the Legal Consultant of the Executive Power, the said Draft of Regulation for purposes of approval, pursuant to the provisions of the Law.

SEEN: The Constitution of the Dominican Republic;

SEEN: The Civil, Commercial, Civil Procedure, and Criminal Procedure Codes of the Dominican Republic;

SEEN: Law No. 126-02 on Electronic Commerce, Digital Documents and Signatures of the Dominican Republic, promulgated on the fourth (4th) day of the month of September of the year two thousand two (2002);

SEEN: Resolution No. 042-03 issued by the Board of Directors of the Dominican Telecommunications Institute (INDOTEL), on the seventeenth (17th) day of the month of March of 2003;

SEEN: The application for approval of the General Regulation of Application of the Law on Electronic Commerce, Digital Documents and Signatures of the Dominican Republic, presented to the Executive Power by the President of the Dominican Telecommunications Institute (INDOTEL), Lic. Orlando Jorge Mera, on the twenty-fourth (24th) day of the month of March of the year two thousand three (2003).

Exercising the powers conferred on me by article 55 of the Constitution of the Dominican Republic, I pronounce the following

DECREE:

GENERAL REGULATION OF APPLICATION OF LAW No. 126-02 ON ELECTRONIC COMMERCE, DIGITAL DOCUMENTS, AND SIGNATURES

TITLE I DEFINITIONS AND SCOPE

ARTICLE 1.- Definitions.-

In addition to the definitions established in the Law, the expressions and terms employed in the present Regulation shall have the meaning indicated below:

1.1. Authorization: The legal act by means of which, in written and formal manner, INDOTEL grants to a Certification Entity the right to issue digital certificates with legal value of digital signatures, and to provide other certification services foreseen by Law No. 126-02 and its regulatory norms;

1.2. Certificate (Digital Certificate): The digital document issued and signed digitally by a Certification Entity, which identifies a signer unequivocally during the period of effectiveness of the certificate, and which is built on proof that said signer is the source or originator of the contents of a digital document or data message which incorporates its associated certificate;

1.3. Private cryptographic password: The numerical value or values or binary characters which, used together with a known mathematical procedure, serve to generate the digital signature of a data message or of a digital document;

1.4 Public cryptographic password: The numerical values or binary characters which are used to verify that a digital signature was generated with the private password of the subscriber or signer of the digital certificate which has issued the data message or digital document;

1.5 Technical Reliability: The quality of the totality of equipment for computing, software, protocols of communication, and related security and administrative procedures which fulfill the following requirements:

- a) Protection against the possibility of intrusion or unauthorized use;
- b) Guarantee of availability, reliability, confidentiality, and correct functioning;
- c) Appropriateness for the performance of the specific functions;
- d) Compliance with the appropriate security or safety standards, in accordance with the international standards on the subject; and
- e) Compliance with the technical and auditing standards INDOTEL may establish;

1.6 Cryptography: The branch of mathematics applied to the science of information systems which concerns itself with the transformation of digital documents or data messages, from their original representation to an unintelligible and undecipherable representation which protects and preserves their contents and form, and the recuperation of the original document or data message from the latter;

1.7 Asymmetrical Cryptosystem: The algorithm which uses a pair of keys or codes or passwords, a private password to sign digitally, and its corresponding public password to verify said digital signature, in this manner, one password cannot operate without the other, and in such a form that the user who is familiar with the public password cannot derive from it the private password;

1.8 Data of creation of a digital signature: Those unique data, such as private cryptographic codes or passwords, which the subscriber or signer uses to create his digital signature;

1.9. Data of verification of digital signature: Those unique data, such as public cryptographic codes or passwords, which are used to verify the digital signature, the integrity of the digital document or data message, and the identity of the signer;

1.10. Addressee: The person designated by the initiator to receive the message, but who is not acting as intermediary with regard to said message;

1.11. Device of creation of digital signature: The hardware or software device technically reliable which permits one to sign digitally;

1.12. Device of verification of digital signature: The device of technically reliable hardware or software which permits one to verify the integrity of the digital document and the identity of the signer;

1.13 Digital document: The information encoded in digital form over a logical or physical support, in which electronic, photolithographic, optical, or similar methods are used which become the legally relevant representation of acts, facts, or data;

1.14 Certifying Entity: That institution or company which, being authorized pursuant to the Law, or the present Regulation and the norms which may be pronounced by INDOTEL, is empowered to issue certificates in relation to the digital signatures of persons, to offer or facilitate the services of registry and chronological stamping of the transmission and receipt of data messages, as well as to fulfill other functions related to communications based on digital signatures;

1.15. Chronological Stamp or Digital Certification of date and time: The indication of the certain date and time, assigned to a document or electronic registration by a Certifying Entity and digitally signed by the latter;

1.16. Digital Signature: It shall be understood as a numerical value adhering to a data message and which, using a known mathematical procedure, linked to a password of the initiator and to the text of the message, permits one to determine that this value has been obtained exclusively with the password/key of the initiator and the text of the message, and that the initial message has not been modified after the transmission was made;

1.17. Electronic Signature: An electronic signature is understood to be the body of electronic data integrated, linked, or associated in a

logical manner with other electronic data, which by agreement between the parties, is used as a means of identification between the sender and the addressee of a data message or a digital document and which lacks some of the legal requirements to be considered a digital signature;

1.18. INDOTEL: The initials which denominate the Dominican Telecommunications Institute, the regulatory body for telecommunications and electronic commerce, digital documents and signatures, pursuant to Laws No. 153-98 General Telecommunications Law, and No. 126-02 on Electronic Commerce, Digital Documents and Signatures, of the Dominican Republic, respectively;

1.19. Initiator: Every person who, with respect to a data message, has acted on his own 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 which has not done it as an intermediary with respect to said message;

1.20. Law: This refers to the Law on Electronic Commerce, Digital Documents and Signatures, number 126-02;

1.21. Telecommunications Law: This refers to the General Telecommunications Law, number 153-98;

1.22. 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, according to its initials in English), electronic mail, telegram, telex, or telefax;

1.23. Procedures Manual: The body of practices used by the Certifying Entity in the issuing and administration of certificates. In English, Certification Practice Statement (CPS);

1.24. Plan for Cessation of Activities: The body of activities approved by INDOTEL, to be developed by the Certifying Entity in the event that it terminates the rendering of its services;

1.25. **Contingency Plan:** The body of procedures to be followed by the Certifying Entity given the occurrence of unforeseen situations which could compromise the continuity of its operations;

1.26. **Security Plan:** The body of policies, practices, and procedures destined for the protection of the resources of the Certifying Entity;

1.27. **Certification Practices:** The body of information concerning the compliance with the requirements of authorization and operation which each Certifying Entity must publish according to what is established in article 38 of Law No. 126-02;

1.28. **Certification Policies:** The rules defined by the Certifying Entities and approved by INDOTEL, in which are established the criteria for issuing and use of digital certificates. In English, Certification Policy (CP);

1.29. **Procedure for verification of digital signature:** The process used to determine the validity of a digital signature. Said process must consist at least of the following steps:

- a) The verification that said digital signature has been created during the period of validity of the digital certificate of the subscriber;
- b) The determination that said digital signature has been created by using the data of creation of digital signature corresponding to the data of verification of digital signature indicated in the signer's certificate; and
- c) The verification of the authenticity and validity of the certificates involved;

1.30. **Provider of Services of Electronic Signature:** Every company, whether domestic or foreign, public or private, who renders certification services and whose digital certificates have no legal value as digital signature, without prejudice of the rest of the services which they may perform;

1.31. **Registry of Certifying Entities:** The registry of public access which INDOTEL maintains in which are recorded the information concerning the Certifying Entities;

1.32. National Registry: The registry, established in Chapter IX of the Regulation of Concessions, Registrations in Special Registries and Licenses for the Providing of Telecommunications Services in the Dominican Republic, which keeps a list of all authorizations granted by INDOTEL;

1.33. Regulation: This refers to the present Regulation of Law No. 126-02;

1.34. Repository: A system of information for the storage and recuperation of certificates or other type of information relevant for the issuing and validation of same;

1.35. Revoking a certificate: Definitively finalizing the period of validity of a certificate, from a specific date thereafter;

1.36. Signer or owner/title-holder of a digital certificate: The person who contracts with a Certifying Entity for the issuing of a certificate, so that he be named or identified in it. Said person has the obligation to keep under his strict and exclusive control the procedure to generate his digital signature;

1.37. Suspending a certificate: Temporarily interrupting the operational period of a certificate from a specific date thereafter;

1.38. Unit of Registry: Every person or company, or public entity, enabled to validate the data of identity of persons and companies, signing certificates and able to provide other validation services related to digital signatures, according to the authorization granted for such ends by INDOTEL. In English, Registration Authority (RA);

1.39. User: The person who, without being a signer and without contracting the services of issuance of certificates from a Certifying Entity, can nevertheless validate the integrity and authenticity of a digital document or data message, based on a certificate of the signer originating the message;

1.40. Validating the integrity and authenticity of a digital document or data message: The procedure for verification of digital signatures applied to a digital document or data message.

ARTICLE 2.- Scope.-

2.1. The present Regulation constitutes the regulatory framework which will be applied throughout the national territory for the rendering of services of digital certification, in the framework of Law No. 126-02 on Electronic Commerce, Digital Documents, and Signatures, and regulates the entities comprised in the Law and in the present Regulation.

2.2. Subjects regulated by the Law, by the present Regulation, and by the complimentary norms which INDOTEL may pronounce, are the certifying entities, the providers of services of electronic signatures, and units of registry, as well as the providers of support services or infrastructure operationally linked to same in regard to their contractual relationship.

2.3. The present Regulation must be interpreted pursuant to the Law, to the regulations and norms pronounced by INDOTEL, and there shall be taken into account the international norms and recommendations on the subject.

2.4. INDOTEL shall approve the norms which compliment the present Regulation, which may be expanded, modified, or repealed accordance to the evolution of internationally accepted standards.

ARTICLE 3.- Authority.-

3.1. INDOTEL shall watch out for the faithful compliance with the present Regulation, shall stipulate the technological, legal, economic, and procedural standards applicable in matters of digital signature, digital documents, and data messages, and shall issue the corresponding resolutions in order to guarantee the effective application of the Law and of the present Regulation.

3.2. INDOTEL constitutes the only institution of the State with legal capacity to authorize the installation and operation of public and private services of digital certification in national territory, and this

power may not be substituted by any centralized, autonomous, or decentralized authority of the State.

TITLE II REGULATED SUBJECTS

PART I CERTIFYING ENTITIES

ARTICLE 4.- Categories.-

4.1. The Certifying Entities, the Registry Units, and the Providers of Services of Electronic Signature are regulated by the Law, by the present Regulation, and by its complimentary norms, as well as by the applicable norms of common law.

4.2. Certifying Entities: They are those which, being domestic or foreign companies, public or private, and the Chambers of Commerce and Production, domiciled in the Dominican Republic, which, after application, are authorized by INDOTEL pursuant to the Law, to the present Regulation, and to the norms which INDOTEL may pronounce, are empowered to issue certificates in relation to the digital signatures of persons, to offer or facilitate the services of registration and chronological stamping of the transmission and receipt of data messages, as well as to fulfill other functions related to communications based on digital signatures, without prejudice to the rest of the services which they may perform.

4.3. Providers of Services of Electronic Signature: They are those companies, domestic or foreign, public or private, which grant digital certificates which lack legal value of digital signature, without prejudice to the rest of the services which they may perform.

ARTICLE 5.- Rendering of Services of Electronic Signature.-

5.1. The providing of services of digital certification by Providers of Services of Electronic Signature does not require prior authorization by INDOTEL.

5.2. For purposes of protecting the rights of consumers, INDOTEL shall determine the information to be presented and the procedures to be complied with by the Providers of Services of Electronic Signature.

ARTICLE 6.- Effects of the Certificates issued by Providers of Services of Electronic Signature.-

6.1. The certificates and other services of certification rendered by the Providers of Services of Electronic Signature do not have the legal value that the Law grants to the digital signature, this circumstance must be recorded in the information which they provide on their services both in printed form and in digital format, on the Internet site they have available, and in general, in all communications linked to same.

6.2. The Providers of Services of Electronic Signature must communicate such circumstance expressly to the applicants and/or signers of digital certificates which they issue and to every third party who has contact with said Provider of Services of Electronic Signature.

ARTICLE 7.- Norms.-

Compliance with the norms set for the application of the present Regulation is obligatory for the Certifying Entities. INDOTEL has the power to effect, by office or at the request of the party, verifications of compliance with the legal and regulatory provisions in the Certifying Entities when it may deem so necessary, in the form provided by the Law and by its regulatory norms.

ARTICLE 8.- Updating of the norms.-

8.1. The administrative acts which imply the modification of norms for the rendering of services of digital certification shall establish the term periods in which the Certifying entities must adjust themselves to same.

8.2. Failure to comply with the provisions of the new norms shall be qualified as a very serious fault, and shall empower INDOTEL to leave the authorization without effect, pursuant to articles 56 and 57 of the Law and the present Regulation.

ARTICLE 9.- Certification Practices.-

9.1. The Certifying Entities shall have specific rules on their certification practices, which consist of a detailed description of the policies, procedures, mechanisms, and conditions for providing the services, as well as the obligations which they assume.

9.2. The Certification Practices must declare compliance with the requirements indicated in article 68 of the present Regulation, with the exception of the insurance policy which is accredited by means of the presentation of same.

9.3. Certification Practices must be objective and non-discriminatory, must be published pursuant to article 38 of the Law, and the present Regulation, and must be communicated to the signers and users in a simple manner and in the Spanish language.

9.4. The Certification Policies shall be subject to the approval of INDOTEL and must be remitted together with the application for authorization.

9.5. The Certification Policies must be published and updated permanently and must be accessible to the public by electronic means, at the address corresponding to the site available to the Certifying Entity, in INDOTEL's bulletin, and in INDOTEL's Internet site.

9.6. The provisions of Certifying Practices must contain and list at least the following information:

- a) General data:
 - i) The name, physical address, and telephone number of the Certifying Entity;
 - ii) The number of the National Taxpayer's Registry (RNC);

- iii) The electronic address, at which the communications and notifications shall be valid;
- iv) The digital certificate which contains the present public password of the Certifying Entity;
- v) The results of the evaluation obtained by the Certifying Entity in the last hearing held by INDOTEL;
- vi) If the authorization to operate as a Certifying Entity has been revoked or suspended, this registration must include the date of revocation or suspension to operate for all of the cases in which it has been produced;
- vii) The limits imposed on the Certifying Entity in the authorization to operate; and
- viii) Any event which would substantially affect the capacity of the Certifying Entity to operate.

b) **Certification Policies** which contemplate at least the following contents:

- i) **Introduction**, which will contain a summary of the certification practices in question, mentioning both the entity which signs the document and the type of signers and products to which they are applicable;
- ii) **General considerations**, which shall contain information on obligations, responsibilities, compliance with audits, confidentiality, and intellectual property rights, with respect to all of the parties involved;
- iii) **Identification and authentication**, in which are described the processes of authentication applied to the applicants of certificates, as well as the processes to authenticate same when they request the suspension or revocation of a certificate. In the event of operations with a Unit of Registration, the entity shall supply the data of this Unit;
- iv) **Operational requirements**, which shall contain operational information and procedures to be followed for the processes of application for certificates, issuing of certificates, suspension, and revocation of certificates, processes of auditing, security, storage of relevant information, change of data of creation of a digital signature, overcoming critical situations, cases of *force majeure*, chance, and procedure of termination of certification service;

- v) **Personal and physical controls of procedure**, they shall describe the non-technical security controls used by the certifying entity to ensure the functions of generation of data of creation of the digital signature, the authentication of users, issuing of certificates, suspension and revocation of certificates, auditing, and storage of relevant information;
- vi) **Controls of technical security**, they will indicate the security measures adopted by the Certifying Entity to protect the data of creation of their own digital signature;
- vii) **Profiles of certificates and of the registration of public access**, they shall specify the formats of the certificate and of the registration of public access;
- viii) **Specifications of administration of the certification policy**, they shall indicate the form in which same is contained in the Practice, and the procedures to change, publish, and notify said policy.

c) Plan for Cessation of Activities

d) Contingency Plan

- e) **Policy for Protection of Personal Data**, in accordance with the complimentary norms to be pronounced by INDOTEL.
- f) **The acknowledgement of foreign certificates by the Certifying Entity**, if applicable.

ARTICLE 10.- Registry of Digital Certificates.-

10.1. Each Certifying Entity and each Provider of Services of Electronic Signature shall maintain a Registry of certificates accessible to the public, in which is guaranteed the availability of the updated information contained in it regularly and continuously.

10.2. Said Registry shall contain the certificates issued by the Certifying Entities and by the Providers of Services of Electronic Signature, indicating the status of the certificates in such a manner that they indicate at least the following:

- a) If same are in effect, revoked, suspended, or reactivated;
- b) If they are acknowledged by the Certification Entity in the event that they have been issued by a foreign Certifying Entity;
- c) The Certification Policy under which it was issued;
- d) The dates of issuance and expiration; and
- e) All relevant mentions for the use of same.

10.3. The Certifying Entities and the Providers of Services of Electronic Signature shall guarantee the public access in a permanent manner to said Registry by electronic means.

ARTICLE 11.- Communication of cessation of activities.-

11.1. Certifying Entities. In the event that a Certifying Entity cease to render the service, it shall notify such situation to the signers of the certificates issued by it in the following manner:

11.1.1. Voluntary Cessation. With no less than NINETY (90) working days in advance, and pointing out to the signers that there does not exist any objection to the transfer of the certificates to another Certifying Entity, which will be indicated in said notification, within the term period of FIFTEEN (15) working days after receipt of the communication, it shall be understood that the signer has consented to the transfer of same.

11.1.2. Involuntary Cessation. The cancellation of the authorization shall be notified immediately to the signers. In the event that the Certifying Entity is in a situation of transferring the certificates to another Certifying Entity, it shall inform of such situation in the manner and term period indicated in clause 11.1.1.

11.2. If the signer of the certificate communicates that he is opposed to the transfer in the term period established, the certificate shall be revoked without any additional procedure.

ARTICLE 12.- Voluntary cessation of activities.-

12.1. Certifying Entities. In the event that the cessation of the providing of the service should occur at the will of the Certifying Entity, the latter shall request of INDOTEL by means of a document signed by its representative, NINETY (90) working days in advance, the cancellation of its registration in the Registry of Certifying Entities, communicating to it the destination which it will give to the certificates, specifying, in its case, those which it is going to transfer and to whom, when applicable.

12.2. Providers of Services of Electronic Signature. In the event of cessation of activities, the Providers of Services of Electronic Signature must report such circumstance to INDOTEL NINETY (90) working days in advance, by means of a document signed by its representative.

ARTICLE 13.- Subsistence of the Obligations.-

13.1. INDOTEL shall regulate the procedures applicable to the cessation of activities of the Certifying Entities and of the Providers of Services of Electronic Signature based on the need to preserve the protection for the rights of the consumers.

13.2. The Certifying Entities shall contemplate in their Plans for Cessation of Activities, approved by INDOTEL, the subsistence of the obligations relating to the protection, confidentiality, and due use of the information supplied by the signers of certificates.

ARTICLE 14.- Preservation of the Documents and Support Data for the Issuing of Certificates.-

14.1. The data supplied by the signers of digital certificates, and the support documents, shall be preserved by the Certifying Entities at least for TWENTY (20) years after the revocation or expiration of the certificates.

14.2. In the event that the Certifying Entities cease their activities, they shall transfer said data to another Certifying Entity or to a company specializing in the custody of electronic data duly authorized by INDOTEL, for the time remaining to complete the TWENTY (20) years after revocation or expiration of each certificate. This situation must be seen reflected in both the Registry of Certifying Entities and in the Certification Policy approved by INDOTEL.

ARTICLE 15.- Preservation of the Registry of Certificates.-

15.1. The Certifying Entities shall preserve the data contained in the registries mentioned in article 51 of the Law for a term period of FORTY (40) years, counting from the date of revocation or expiration of each certificate.

15.2. In the event that the Certifying Entities cease their activities, they shall transfer said data to another Certifying Entity, or to a company specializing in the custody of electronic data, duly authorized by INDOTEL, for the time remaining to complete the FORTY (40) years after revocation or expiration of each certificate. This situation must be reflected in both the Registry of Certifying Entities and in the Certification Policy approved by INDOTEL.

ARTICLE 16.- Insurance.-

The Certification Entity will have insurance in effect in accordance with the responsibilities assumed, which will comply with the requirements which may be established by the complimentary norm on the policies of accreditation or authorization which INDOTEL may pronounce.

ARTICLE 17.- Obligations of the Certifying Entities.-

In addition to the provisions of article 40 of the Law, the Certifying Entities have the following obligations:

- a) To determine by themselves or through a Registry Unit, in which such function has been delegated, the identity or other data of the applicants which is considered relevant for the procedures of verification of identity prior to the issuance of the digital certificate, according to the Certification Policy under which the certificate is requested;
- b) To make permanently available to the public the Certification Policies and Procedures Manual, in those aspects which do not contain confidential information, in the formats approved by INDOTEL for such ends;
- c) To comply faithfully with the Certification Policies agreed to with the signer and with its Procedures Manual, its noncompliance being considered a serious fault;
- d) To guarantee the established providing according to the levels defined in the services agreement made with the signer, concerning the services for which it requested authorization;
- e) To report to the applicant of a digital certificate, in clear and accessible language in the Spanish language, regarding the characteristics of the certificate requested, the limitations to the liability/responsibility, if applicable, the prices of the services of certification, use, administration, and other related, including additional charges and forms of payment, the levels of service to be provided, the obligations which the signer assumes as user of the certification service, his domicile in the Dominican Republic, and the means to which the signer can resort in order to request clarifications, to give an account of improper functioning of the system or to present his claims;
- f) To have available a service of attention to signers of certificates and users, by means of personal, telephone, and Internet access, which will allow them to send the consultations and the prompt reply to the request for suspension or revocation of certificates;
- g) To guarantee public, efficient, and free access for signers and users to the registry of certificates issued, suspended, revoked, reactivated, or acknowledged;

- h) To keep updated the registries of certificates issued, suspended, revoked, or reactivated for the term of FORTY (40) years, starting with the date of revocation or expiration of each certificate;
- i) To adopt the reliable security procedures and safeguards, as established by INDOTEL, to guarantee that the private passwords of the signers not remain in their power nor be able to be used by third parties in the event that it provide the service of generation of passwords;
- j) To inform INDOTEL immediately of the occurrence of any event which compromises the correct providing of the service;
- k) To guarantee the integrity of the information which they maintain under their control;
- l) To respect the right of the signer of the digital certificate not to receive advertising of any type through its intermediation, excepting with the express consent of the latter;
- m) To publish by electronic means and in a newspaper of national circulation, the certificate of public password corresponding to the certification policy for which it obtained authorization;
- n) To comply with the norms and precautions established for the protection of personal data, as well as the rest of the norms approved by INDOTEL;
- o) To comply with the requirements established by Law, by the present Regulation, and by the norms which INDOTEL may pronounce which motivated the authorization obtained for the providing of certification services;
- p) In those cases of revocation of certificates contemplated in number 6 of article 49 of the Law, it must substitute free of charge that digital certificate which has ceased to be safe or secure with another one which will comply with said requirements. INDOTEL shall establish the process of

replacement of certificates in these cases. In those cases in which a digital certificate has ceased to be safe due to reasons attributable to its signer, the Certifying Entity shall not be obligated to substitute the digital certificate;

- q) To send the reports of statements of operations as a sworn statement as INDOTEL may request on the dates and in the formats determined by the regulation pronounced by INDOTEL for such ends;
- r) To have ideal and reliable personnel, with professional backgrounds in accordance with the function they perform, without prejudice to the legal responsibilities which it assumes due to the services provided;
- s) To comply with the requirements performed pursuant to the sentence with value of an irrevocably judged matter or authorization of a judge to deliver the data;
- t) To respond to the petitions for reports by the users of certificates regarding the validity and scope of a digital certificate issued by it; and
- u) To report to INDOTEL the termination of the contract or the modifications regarding the scopes or amounts of the coverage of the insurance.

ARTICLE 18.- Responsibility of the Certifying Entities.-

In no case may the responsibility which could emanate from a certificate made by a Certifying Entity compromise the civil liability of the State in its capacity as entity of control and surveillance, nor in particular the civil liability of INDOTEL, as public entity with legal personality.

ARTICLE 19.- Resources/Recourses of the Certifying Entities.-

19.1. For the adequate development of the activities for which it requests authorization, the Certifying Entity shall evidence that it has a team of professionals, the physical and technological infrastructure and financial resources, as well as the procedures and security systems which will permit it:

- a) To generate, in a safe environment, the digital signatures themselves and all of the services for which it requests authorization;
- b) To comply with what is foreseen in its policies and procedures of certification;
- c) To guarantee the reliability of the systems in accordance with the standards approved by INDOTEL;
- d) To issue certificates which will comply with the following:
 - i. What is provided for in article 44 of the Law;
 - ii. The technological standards approved by INDOTEL; and
 - iii. The corresponding Certifying Policy;
- e) To guarantee the existence of physical and logical security systems in its installations which will ensure restricted access to the equipment which manages the operational systems of the Certifying Entity;
- f) To protect the handling of the private password of the Certifying Entity by means of a security procedure which will prevent access to same by unauthorized personnel;
- g) To protect the access and use of the private password by means of procedures which will require the participation of more than one person;
- h) To register the transactions performed, in order to identify the author and the moment of each one of the operations;
- i) To use exclusively the systems which fulfill the functions of certification with that purposes, without any other function's being assigned to them;
- j) To protect all of the systems used directly or indirectly in the certification function with procedures of authentication and security with a high level of protection, which must be updated in accordance with technological advances in order to guarantee the correct rendering of the certification services;
- k) To guarantee the continuity of the operations by means of a Contingency Plan updated and tested; and

- l) To have available financial resources adequate for the type of certification activity which it develops, in accordance with the levels of responsibility deriving from same.

19.2. The criteria of evaluation of the provisions in the preceding paragraph shall be established by INDOTEL in accordance with international standards and the regulation pronounced for such ends.

ARTICLE 20.- Services of third parties.-

20.1. In those cases in which the Certifying Entity should require or use the technological services or infrastructure provided by a third party, it must foresee within its Contingency Plan the procedures to be followed in case of interruption of such services, in such a way as to permit the continuation of the providing of its certification services without any prejudice to the signers.

20.2. The contracts between the Certifying Entity and the Providers of Services or Infrastructure must guarantee the execution of the procedures contemplated in the Plan for Cessation of Activities approved by INDOTEL. The Certifying Entity authorized or which has initiated the procedure to obtain the authorization shall facilitate for INDOTEL all that information contained in the contracts which is linked to the providing of the certification services and to the implementation of the Plan for Cessation of Activities and the Contingency Plan.

ARTICLE 21.- Effects of the Authorization.-

Without prejudice to any other obligations imposed under the Law, legal or regulatory provisions, or other obligations contracted particularly or privately, the Certifying Entities are obligated to the following:

- a) To provide the services authorized by INDOTEL in a continuous manner in accordance with the terms, conditions, and time periods established in the Law, in the present Regulation, in the

Resolutions which INDOTEL may pronounce to that effect, and in the respective authorization;

- b) To comply with the minimum economic, technical, and legal requirements which have been required by INDOTEL and pursuant to which the Authorization has been granted, as well as to comply with any other requirement established by INDOTEL;
- c) To comply with the Certification Policies for which it obtained authorisation, which support the issuing of its certificates, with the Procedures Manual, with the Security Plan, with the Plan for Cessation of Activities, and with the Contingency Plan approved by INDOTEL, as well as with the complimentary norms pronounced by INDOTEL on the subject of technological standards, certification procedures, safeguarding of the security and confidentiality of the information, protection of personal data of the signers of certificates, and all other norms issued by INDOTEL.
- d) To adopt the measures necessary to guarantee the confidentiality of the information and the protection of the personal data of the signers of digital certificates;
- e) To pay punctually the costs and duties established in the present Regulation, as well as any taxes, contributions, or other obligations deriving from the Authorization;
- f) To cooperate with INDOTEL in its work in defense of the interests of signers and users of services of digital certification;
- g) To admit as client or user of the services which it supplies, in a non-discriminatory manner, to all persons who wish it and who comply with the technical and economic conditions established, without any limitations other than those deriving from the capacity of the service;
- h) To supply to INDOTEL, in the term period required, the information and reliable data which the latter may request of them, concerning the regulated activity; and

- i) To cooperate with INDOTEL in its work of detection of fraudulent activities related to the services of digital certification which are the object of the present Regulation.

ARTICLE 22.- Exclusive Use of the Expression “Certifying Entity”

The use of the expression “Certifying Entity” and similar phrases is of the exclusive use of the providers of services of digital certification which have been authorized to operate as Certifying Entities to such effect by INDOTEL by means of resolution and incorporated into the Registry of Certifying Entities.

PART II UNITS OF REGISTRY

ARTICLE 23.- Functions and Obligations of the Units of Registry.-

Without prejudice to whatever could be provided by the regulation pronounced by INDOTEL, the Units of Registry shall have the following functions and obligations:

- a) Receipt of the applications for issuing of digital certificates;
- b) Validation of the identity and authentication of the data of the applicants of digital certificates;
- c) Validation of other data of the applicants of digital certificates which are presented to it whose verification is delegated by the Certifying Entity, for the granting of digital certificates with particular powers, such as for example the capacity as representative of a legal person, capacity as functionary of an organization, capacity as a member of a professional organization, among others;
- d) Remission of the applications approved to the Certifying Entity with which it is operationally linked;

- e) Receipt and validation of the applications for suspension or revocation of digital certificates, and directing them to the Certifying Entity with which they are linked, once the corresponding verifications of identity are performed;
- f) Identification and authentication of the applicants for suspension or revocation of digital certificate issued by the Certifying Entity;
- g) Preservation and filing of all support documentation of the process of validation of identity, according to the procedures established by the Certifying Entity;
- h) Compliance with the legal norms applicable, as well as those which INDOTEL may pronounce in relation to the protection of personal data, the confidentiality of the information, and other subjects linked to the activity;
- i) Compliance with the provisions established by the Certifying Policy and the Procedures Manual of the Certifying Entity with which it is linked, in the part which is applicable; and
- j) Collaboration for the performance of inspections or audits by the Certifying Entity, INDOTEL, or its auditors.

ARTICLE 24.- Delegation.-

24.1. The Certifying Entities may delegate in the Registry Units the function of validation of identity and other data of the signers of certificates, as well as the function of registration of the presentations and of the bureaucratic processes which may be formulated.

24.2 In order to perform this delegation, both the Certifying Entities and the Registry Units must comply with the norms and procedures established in the Law, in the present Regulation, and in the provisions dictated by INDOTEL.

24.3 The Certifying Entities shall be authorized by INDOTEL to perform this delegation.

ARTICLE 25.- Responsibility of the Certifying Entity with regard to the Registry Unit.-

25.1. A Registry Unit may incorporate itself as a single unit or as several units hierarchically dependent on each other, and may delegate its operation in other Registry Units, so long as it has the approval of the Certifying Entity and the respective authorization of INDOTEL.

25.2. The Certifying Unit is responsibility in accordance with what is established by Law, even in the event that it should delegate part of its operation in Registry Units, without prejudice to the right of the Certifying Entity to claim from the Registry Unit the compensations for damages and harm which it may suffer as a consequence of the latter's acts or omissions.

ARTICLE 26.- Title Holders of Registry Units.-

The following may fulfill the function of Registry Unit: notaries public, the offices of Civil Registry, professional associations for their members, the Chambers of Commerce for their members, the banking entities for their clients, and in relation to the Certifying Entities belonging to public entities, the areas of personnel of the jurisdictions or other dependencies, which fulfill the requirements established by INDOTEL for such ends. This list is not limited but may be modified by INDOTEL in the use of its regulatory power.

ARTICLE 27.- Supervision by INDOTEL.-

27.1. The Registry Units are subject to the regulatory powers and inspection of INDOTEL as watchdog and control entity in matters of digital signatures.

27.2. INDOTEL shall authorize the functioning of the Registry Units based on compliance with the precautions established in the procedures which it may pronounce to such end.

27.3. The Registry Units are subject to the same obligations as the Certifying Entities in the following matters:

- a) Preservation of data of signers of certificates;
- b) Protection of rights of the consumer;
- c) Confidentiality of information;
- d) Protection of personal data; and
- e) In all other aspects which INDOTEL may establish by means of norms which compliment the present Regulation.

PART III COSTS AND DUTIES

ARTICLE 28.- Costs and duties.-

28.1. Every regulated entity is subject to the payment of the following costs and duties, which shall be applied by INDOTEL:

- a) Costs of Processing, which refer to costs directly involved in administrative processing, Authroization, registration in the Registry of Certifying Entities, and other bureaucratic processes which INDOTEL may determine; and
- b) Right/duty of supervision, corresponding to the peforming of ordinary and extraordinary inspections and audits.

28.2. The costs of processing shall be applied by service, and shall be collected concomitantly with the presentation of the following applications:

- a) Application for Authorization to incorporate as Certifying Entity;
- b) Application for Authorization to incorporate as Registry Unit;
- c) Application for Authorization for a transer, concession, lease, granting of right of use, incorporation of liens or transer of control of a Certifying Entity, of a Provider of Services of Electronic Signature, or of a Registry Unit in effect; and
- d) Every any presentation which INDOTEL includes in the abovegoing list.

28.3. The processing costs shall be paid, as appropriate. Said costs shall not be restituted in the event that the authorization or registration is not granted due to noncompliance or non-fulfillment of the legal and regulatory requirements and obligations.

28.4. The right of supervision shall comprise the costs corresponding to the ordinary and extraordinary inspections and audits. The amount must be paid within the NINETY (90) calendar days following the date of the Resolution which sets them, based on the costs which the inspections and audits demand from INDOTEL.

28.5. The amounts of the costs of processing, of the rights of supervision, and of the fines shall be established by INDOTEL, by means of Resolution.

TITLE III DIGITAL CERTIFICATES

ARTICLE 29.- Contents of digital certificates.-

29.1. Without prejudice to whatever INDOTEL could establish, the digital certificates provided by the Certifying Entities shall contain at least the following data:

- a) Digital signature of the Certifying Entity;
- b) Name and electronic address of the signer;
- c) Identification of the signer named in the certificate;
- d) Name, electronic address and place where the Certifying Entity's activities are performed, and the background of the authorization obtained;
- e) Public password of the signer;
- f) Methodology used to verify the digital signature of the signer;
- g) Series number of the certificate;
- h) Date and time of issuance and expiration of the certificate; and
- i) Identification of the Certification Policy under which the certificate was issued.

29.2. INDOTEL may modify the minimum contents of the certificates, in accordance with the progress of international technological standards.

ARTICLE 30.- Incorporation of Additional Contents.-

30.1. The Certification Entities must introduce in the certificates which they issue, the data mentioned in the previous article, and that which occasionally INDOTEL so orders, in the time periods foreseen in the present Regulation.

30.2. The additional powers which the Certifying Entities introduce for purposes of incorporating limits to the use of the certificate, must not make difficult or impede the reading of the data indicated in the previous article nor its recognition by third parties.

ARTICLE 31.- Secure digital signature.-

31.1. For the issuing of certificates of secure digital signature contemplated in article 32 of the Law, the Certifying Entity must determine reliably the identity of the applicant before its issuance, and comply with the technical and procedural norms which INDOTEL may dictate.

31.2. The Certifying Entity may make said determination by itself or by means of Registry Units, requiring the personal and direct appearance of the applicant or of its legal representative in the case of a company.

31.3. The determination of the data of identity of the persons who request the issuance of a digital certificate framed in a Certification Policy for secure digital signature shall be made based on the number of the Personal and Electoral Identification Card, on the Identification Carnet, the Passport, or any other official document of personal identification which the Dominican State may adopt in future.

31.4. In the event that the individual is not of Dominican nationality, the determination of the identification data of the applicant of a digital certificate framed in a Certification Policy for secure digital signature shall be made based on the Passport number.

31.5. INDOTEL shall establish the procedures and documents which will be considered for the determination of the identity of the persons who are minors and who request the issuance of a digital certificate.

ARTICLE 32.- Securing of the private password.-

32.1. The data for creation of a signature, when generated by the Certifying Entity, must be delivered to the signer of the certificate in order to guarantee receipt of same in a personal and confidential form. As of this moment the private password is under the control and responsibility of the signer for the effects foreseen in the Law and in its regulation.

32.3. It is prohibited for the Certifying Entity to maintain a copy of the data for creation of the digital signature once they have been delivered to its signer, from which moment the latter will begin to be responsible for keeping them under his exclusive control.

32.3. Failure to comply with the provisions on safeguarding of the private password provided in the above articles constitutes a very serious fault which will give rise to the immediate suspension of the authorization, without prejudice to the criminal and civil liability which may correspond to it.

ARTICLE 33.- Scope of the Use of Digital Certificates.-

33.1. The digital certificate may be used by its signer pursuant to the provisions established in the Policy of Certification of the Certifying Entity with which the issuance and administration of same has been contracted.

33.2. The digital certificate must permit the person who receives it to verify directly or by means of electronic consultation or by any other medium reasonably available, that it has been issued by a Certifying Entity for the purpose of determining the validity of same.

ARTICLE 34.- Suspension of Digital Certificates.-

The Certifying Entities shall proceed to suspend the effectiveness of the certificate when any of the following circumstances is verified:

- a) Request by the signer of the certificate;
- b) Beginning of the processing of absence with presumption of death of the signer of the certificate, or due to the initiation of a procedure of declaration of disability, in both cases, by means of provisional decision of the competent Judge;
- c) Decision of the Certifying Entity by virtue of technical reasons, which circumstance will be communicated immediately in a maximum term of TWENTY-FOUR (24) hours to the signer of the certificate and to INDOTEL, by the mediums established in article 51 of the present Regulation;
- d) By means of ruling of a court with authority of an irrevocably judged matter; and
- e) By virtue of the rest of the causes provided for in the Certification Policy of each Certifying Entity duly approved by INDOTEL.

ARTICLE 35.- Effects of the Suspension of the Certificate.-

35.1. The effect of the suspension fo the Certificate is the temporary cessation of its legal effects in accordance with the uses proper to it and prevents the legitimate use of same by the signer, as of the notification and during the time the latter endures.

35.2. The suspension of the Certificate shall terminate for any of the following causes:

- a) Because of the decision of the Certifying Entity to revoke the Certificate, in the cases foreseen in the Law, in the present regulation, and the complimentary technical norms;
- b) Because of the decision of the Certifying Entity to lift the suspension of the Certificate, once the causes which originated it cease;
- c) Due to the decision of the signer of the certificate, when the suspension has been requested by the latter, and this fact is communicated to the Certifying Entity;

- d) Because of ruling of the court with authority of an irrevocably judged matter which declares the disability, or temporary absence with presumption of death or death due to definitive absence of the signer of the certificate (sic), which implies its revocation; and
- e) By virtue of the rest of the causes provided in the Certification Policy duly approved by INDOTEL;

ARTICLE 36.- Revocation of Digital Certificates.-

36.1. Digital certificates shall remain without effect due to the revocation practiced by the Certifying Entity.

36.2. The revocation shall take place when the Certifying Entity determines and communicates formally by the means established in article 51 of the present Regulation any of the following circumstances:

- a) The request of the signer of the digital certificate;
- b) The request of a legal representative of the signer of the certificate, with the accreditation of the representation invoked;
- c) If it is determined that a digital certificate was issued based on false information which at the moment of the issuance would have been the object of verification;
- d) If it is determined, by virtue of the audit performed, that the procedures of emission and/or verification have failed to be secure;
- e) Due to special conditions defined in the Certification Policies;
- f) Due to judicial decision or decision of a competent administrative entity, duly motivated;
- g) Due to the death of the owner or dissolution fo the signing company;
- h) Due to judicial declaration of absence with presumption of death of the signer;
- i) Due to declaration by means of ruling with authority of an irrevocably judged matter of the legal disability of the signer;
- j) Due to the determination that the information contained in the certificate has ceased to be valid;

- k) Due to the cessation of the relationship of representation, whether labor or contractual relationship, with respect to a company or a public entity;
- l) In the case of revocation, ordered by INDOTEL, of the authorization to function granted to the Certifying Entity, so long as it has not been decided to transfer the certificate to another Certifying Entity; and
- m) Due to the cessation of activities of the Certifying Entity and so long as it has not been decided to transfer the certificate to another Certifying Entity.

36.3. The effect of the revocation of the digital certificate is the permanent and definitive cessation of the legal effects of the latter pursuant to the uses proper to it, and it impedes its legitimate use as of the moment of the revocation.

ARTICLE 37.- Procedure of Suspension or Revocation.-

37.1. The revocation of a digital certificate may be produced officially or at the request of its signer due to the concurrence of some of the causes foreseen in the Law, in the present Regulation, in the complimentary norms, or in the certification policies duly approved by INDOTEL.

37.2. The request for suspension or revocation, as applicable, shall be addressed to the Certifying Entity or to the Registry Unit dependent on same, in any of the forms foreseen by its Certification Policies.

37.3. The suspension or revocation of the certificate must be notified immediately in a maximum term of TWENTY-FOUR (24) hours to its signer, by the means established in article 51 of the present Regulation, without prejudice to the fact that it must be published in the Registry of public access indicated in article 51 of the Law.

37.4. When it is a matter of the suspension due to technical reasons or the revocation of the digital certificate due to circumstances foreseen in clauses b), I), or j) of the previous article, said decision must be communicated to the signer at least TWENTY-FOUR (24) hours prior

to its being put into practice, indicating the cause and the moment in which it will be made effective, by the means established in article 51 of the present Regulation.

37.5. The term of effectiveness of the certificate shall be opposable to third parties from the moment of the publication of the suspension or revocation in the registry of public access indicated by article 51 of the Law.

ARTICLE 38.- Acknowledgement of Foreign Certificates.-

38.1. The Certifying Entities may acknowledge the digital certificates issued by foreign Certifying Entities, under their responsibility.

38.2. For such, the Certifying Entity shall demonstrate to INDOTEL that the certificates to be acknowledged by it have been issued by a provider of services of certification not established in the Dominican Republic which complies with technical norms and procedures equivalent to those established in the Law, in the present Regulation, in its complimentary norms and modifications, for the development of the activity. Particularly, it must accredit the fact that the certificates to be acknowledged by it comply with the provisions referring to minimum contents of the certificates, established in the Law, in the present Regulation, and in the norms issued by INDOTEL.

38.3. INDOTEL shall verify compliance with the legal and regulatory provisions, and shall publish the information on the acknowledgement in the Registry of Certifying Entities. In the event that the Certifying Entity not accredit the compliance with the legal and regulatory precautions for the acknowledgement of foreign certificates, INDOTEL, by means of motivated resolution, shall reject the request for acknowledgement.

38.4. Once the acknowledgement is practiced, the Certifying Entity, in a term of THREE (3) working day, shall communicate such situation to INDOTEL and shall publish it immediately in a maximum term of TWENTY-FOUR (24) hours, in the Registry of public access contemplated in article 51 of the Law.

38.5. The acknowledgement of certificates must be declared in the Practices of Certification.

TITLE IV REGULATORY BODY

ARTICLE 39.- Regulatory Power.-

INDOTEL is empowered to establish the following:

- a) The technological standards applicable in consonance with international standards in effect;
- b) The procedures for signature and verification in consonance with the technological standards defined in the preceding clause;
- c) The minimum conditions for issuance of digital certificates;
- d) The cases in which the digital certificates must be suspended or revoked;
- e) The data considered public contained in the digital certificates;
- f) The mechanisms which guarantee the validity and authorship of the lists of certificates revoked;
- g) The information which the regulated subjects must publish over the Internet;
- h) The information which the Certifying Entities must publish in the mediums established by the present regulation;
- i) The minimum procedures for revocation of the digital certificates whatever their source of issuance, and the minimum procedures for preservation of the back-up documentation of the operation of the Certifying Entities, in the event that the latter should cease their activity;
- j) The system of inspection and auditing of the regulated subjects, including the modes of dissemination of the auditing reports and the requirements for preparation of entities to perform audits and the criteria and minimum standards of auditing which they must cover;
- k) The conditions and procedures for the granting and revocation of the authorizations;
- l) The procedure of instruction and grading of sanctions foreseen in the Law, by virtue of reincidence and/or opportunity;
- m) The applicable procedures for the recognition of foreign certificates;

- n) The agreements of mutual acknowledgement of digital certificates with other countries;
- o) The conditions for application of the Law and the present regulation in the Dominican public sector, including the authorization to provide digital certification services for its entities and jurisdictions;
- p) The minimum contents of the policies of certification according to national and international standards;
- q) The minimum conditions which must be fulfilled in the case of cessation of activities of a Certifying Entity;
- r) The types of risks which will be covered by the insurance which must be contracted by the Certifying Entities, and the amounts corresponding to contracting and coverage;
- s) The conditions for providing other services in relation to the digital signature and other aspects contemplated in the Law; and
- t) The modification and updating of the subjects considered in the abovegoing clauses.

ARTICLE 40.- Procedure for formulation and modification of technical norms.-

40.1. At the request of a party or in official capacity, and for the purpose of formulating or modifying the norms established by the present Regulation, INDOTEL may initiate the procedure to draft and set the norms.

40.2. To such ends, the public will be informed of the opening of the procedure of reformulation of norms, and it shall be submitted to public consultation as provided by means of Resolution pronounced by INDOTEL.

40.3. If necessary, alternative bodies of technical norms may be set for the providing of the service for purposes of permitting the use of various technologies and electronic mediums, in accordance with the Law and with the present Regulation.

ARTICLE 41.- Agreements of Mutual Acknowledgement.-

In accordance with the provisions of articles 37 and 55 of the Constitution of the Dominican Republic, the head of INDOTEL is delegated with the power to make agreements of reciprocity with the governments of foreign countries, whose purpose is to grant validity, in their respective territories, to the digital certificates issued by authorized certifying entities of both countries, while verifying compliance with the conditions established by the Law, by the present Regulation, by the complementary norms, and their modifications for the digital certificates issued by certifying entities authorized by INDOTEL.

ARTICLE 42.- Certification Policies.-

INDOTEL shall define the minimum contents of the Certification Policies, in accordance with the international standards in effect, and with national legislation, which must contain at least the following information:

- a) Identification of the Certifying Entity;
- b) Policy of administration of the certificates and list of the services;
- c) Procedures for verification of the identity of the signers of the certificates;
- d) Obligations of the Certifying Entity, of the Registry Unit in its case, and of the signers of the certificates;
- e) Treatment of the information supplied by the signers, and safeguarding of the confidentiality in its case;
- f) Admitted scopes and limits of liability.

ARTICLE 43.- Functions of INDOTEL.-

Without prejudice and in addition to the functions assigned by Law, INDOTEL shall exercise the function of watchdog and control entity over the activities developed by the regulated subjects. It shall especially have the following functions:

- a) To authorize, according to the Law, the present Regulation and the complementary norms, the operation of Certifying Entities in national territory;

- b) To watch over the proper functioning and efficient rendering of the service by the regulated subjects, and the full compliance with legal and regulatory provisions of the activity;
- c) To perform the inspections and audits foreseen in the Law, in the present Regulation, and in the complimentary norms;
- d) To define in terms of regulation the technical requirements which will quality the appropriateness of the activities developed by the regulated subjects;
- e) To approve the certification policies, the procedures manual, the security plan, the plan for cessation of activities, and the contingency plan, presented by the Certifying Entities which require authorization;
- f) To evaluate the activities developed by the regulated subjects in accordance with the requirements defined in the technical regulations;
- g) To refuse, to revoke, or to suspend the authorization to operate of the Certifying Entities who do not fulfill the requirements established by Law, by the present Regulation, and by the complimentary norms;
- h) To require at any moment that the regulated subjects provide information related to the certificates, the digital signatures issued, and the information systems support documents which they administer or are under their custody;
- i) To order the process of instruction and subsequent application of sanctions for noncompliance with the obligations deriving from the rendering of service;
- j) To order the revocation or suspension of certificates when the Certifying Entity issues them without fulfilling the legal formalities;

- k) To issue certificates in relation to the digital signatures of the Certifying Entities, in the event that it should be deemed necessary;
- l) To publish on the Internet or on the public access network of transmission or broadcasting of the data which shall it shall substitute in the future, permanently and uninterruptedly, of the domiciles, telephone numbers, Internet addresses, and digital certificates of:
 - i) The Certifying Entities
 - ii) The Certifying Entities whose authorizations have been revoked;
- m) To administer the resources generated according to the provisions of article 44 of the present regulation, coming from the various financing sources;
- n) To establish, in concrete cases, the concept/justification and amounts of all types of costs, duties, and fines foreseen in the Law and in article 28 and 44 of the present regulation;
- o) To request the expansion or clarification on documentation presented by the regulated subjects;
- p) To guarantee the correct handling and maintenance of confidentiality by the regulated subjects, of the information on the signers and their respective digital certificates.
- q) To watch out for the observance of the legal provisions on the promotion of competition and protection of the rights of the consumers and users, in the marketplaces attended by the certifying entites.
- r) To permit permanent public access to the updated information of the Registry of Certifying Units and to the certificates of public password of same, by means of publicly accessible telecommunications connections. This also is applied to information on names, incorporated domicile, electronic address, and proper telephone numbers, of the Certifying Entities and the Registry Units;

- s) To supervise the execution of the plan for cessation of activities of the Certifying Entities who cease their functions;
- t) To record the presentations which may be formulated to them, as well as the process conferred on each one of them;
- u) To supervise the execution of contingency plans of the Certifying Entities;
- v) To perform tasks of control of compliance with the recommendations made in the rulings of audits on the regulated subjects, in order to determine, in each case, whether the audited party has taken the corresponding corrective actions;
- w) To receive the claims of the signers and users of digital certificate related to the providing of the service by the regulated subjects; and
- x) In its capacity as signer of a digital certificate, it must fulfill identical obligations as the signers of certificates and the Certifying Entities, in relation to the safeguarding of security measures on its private password and its digital certificate.

ARTICLE 44.- Setting of Costs and Duties.-

44.1. INDOTEL may set and collect from the subjects regulated by the Law and by the present Regulation, duties for the costs of processing and for supervision, in order to cover totally or partially its operational cost and the cost of inspections and audits performed by itself or by third parties contracted to such effect.

44.2. INDOTEL's own resources shall be composed of:

- a) The amounts coming from the costs and duties, foreseen in the previous clause, corresponding to the following services:
 1. digital certification services;
 2. digital certification services of certain date and time;
 3. services of secure storage of digital documents;

4. services rendered by Registry Units;
 5. services rendered by reliable third parties;
 6. services of certification of digital documents digitally signed; and
 7. other services or activities related to the digital signature.
-
- b) The amounts coming from the duties of supervision applied to the regulated subjects;
 - c) The subsidies, inheritances, legacies, donations, or transfers under any title which it may receive;
 - d) Income perceived from the payment of fines applied to the regulated subjects;
 - e) Budgetary assignments which in their case are assigned to it by the Central Government, in the Budget of Income and Law of Public Expenditures; and
 - f) The rest of the funds, goods, or resources which may be assigned to it pursuant to the Telecommunications Law; and
 - g) Contributions coming from applications which use digital signatures, to be determined by the respective norms.

ARTICLE 45.- Power of Inspection.-

45.1. For purposes of performing audits, INDOTEL shall exercise the power of inspection conferred by Law No. 126-02 and the Telecommunications Law.

45.2. INDOTEL shall exercise the power of inspection over the Certifying Entities, the Registry Units, and the Providers of Services of Electronic Signature, and shall guarantee compliance with the legal and regulatory provisions by same. With respect to the Certifying Entities, INDOTEL shall watch over the observation of the requirements which were approved at the moment that the authorization was granted, and the obligations imposed by the Law, by the present Regulation, and by the complimentary norms.

45.3. INDOTEL shall exercise the power of auditing and inspection of the systems and procedures of the providers of services or infrastructure contracted by the Certifying Entity, according to the provisions of the previous article.

45.4. The power of inspection comprises both ordinary inspection and extraordinary inspection. Ordinary inspection consists of the power to practice periodic audits of the installations of the entities subject to the control and vigilance of INDOTEL, as well as to perform permanent monitoring of the development of the activity. Extraordinary inspection will be practiced in an official capacity or by motivated denunciation of the rendering of the service, ordered by INDOTEL by means of a resolution with basis.

45.5. Inspections may be made by officials of the plant (in-house personnel) or by experts especially contracted and prepared for such ends by INDOTEL, who in the exercise of their functions, may require the entities subject to supervision and control, to provide additional information beyond that originally supplied.

45.6. The information requested by INDOTEL must be provided within the term of five (5) working days, counting from the date of its request.

45.7. INDOTEL shall set the criteria which must be complied with by the third parties contracted to perform the inspections and audits.

ARTICLE 46.- Registry of Certifying Entities.-

46.1. INDOTEL shall maintain a Registry of Certifying Entities, which will form part of the National Registry. Without prejudice to what INDOTEL may order, the Registry of Certifying Entities shall contain the following data:

- a) Number of resolution granting the authorization;
- b) Name or company of the Certifying Entity, its domicile, the name of its Legal Representative, its telephone number, the electronic address of its domain site, and of the electronic mail account in which the notifications will be valid, as well as the data of the insurance company with which it has contracted the insurance policy, if appropriate;

- c) The Digital Certificate which contains the public password of the Certifying Entity;
- d) The date on which the authorization to operate expires;
- e) The results of the evaluation obtained by the Certifying Entity in the last audit and inspection performed by INDOTEL; and
- f) The status of the authorization to operate, pointing out if it has at any moment been revoked, suspended, or has expired.

46.2. The access to public data of the Registry of Certifying Entities must be able to be made both in printed support and by electronic means. Regular and continuous access must be guaranteed, as well as the permanent updating of the information.

ARTICLE 47.- Protection of the Rights of the Signers and Users.-

47.1. For purposes of attending the claims presented by signers and users of certification services, INDOTEL shall pronounce a complimentary norm on protection of the rights of the signers and users.

47.2. The regulated subjects must have available an operator to answer telephone calls from users TWENTY-FOUR (24) hours per day, SEVEN (7) days per week, or must electronically record the complaints and calls from users. A combination of operators and recorded can be used. In the event that they use recorders, the company must contact the user at the latest on the next working day after receipt of the recorded message. Likewise they must also provide the service of attention to consultations by means of Internet access.

47.3. The regulated subjects must supply to the users, through a telephone line of free access or electronic address, dedicated to client service, the following information:

- a) Registration number in the Registry of Certifying Entities;

- b) Receiving and accepting reports, applications for revocation or suspension of certificates;
- c) Applicable rates and taxes;
- d) Expiration date of the authorization if one exists; and
- e) Consultations or other relevant information for the use of the service;

ARTICLE 48.- Standards of Conduct.-

48.1. No executive or employee of INDOTEL may reveal confidential information obtained during the performance of his functions. The revelation of such information shall be sanctioned with the cessation of the functions of said employee, without prejudice to other civil or criminal actions against him.

48.2. This obligation of confidentiality shall extend to the auditing entities contracted by INDOTEL.

48.3. No executive or employee of INDOTEL, so long as he is performing his charge, may receive any payment whatsoever for any reason from companies subject to the regulatory power of INDOTEL. Neither may they have any labor relationship, share participation, or other link with any regulated entity. This prohibition shall extend for a period of ONE (1) year subsequent to the abandonment of the charge or function.

48.4. Informal or individual contacts are forbidden between the interested parties and INDOTEL personnel, on subjects pending resolution. Said communications must be formal and accesible to the interested parties or their representatives in cases of acts of general scope, whether they are participating in the meetings or hearing the respective presentations or acts or minutes, in the form regulated by INDOTEL.

48.5. INDOTEL executives shall be subject to the INDOTEL Code of Ethics.

ARTICLE 49.- Conflict of Interest for Auditing Entities.-

49.1. For compliance with or fulfillment of the functions of watchdog and control entity foreseen in the Law and in the present Regulation, INDOTEL may contract experts, whose contracts shall incorporate the norms of conduct foreseen in the previous article.

49.2. Audits made not be made by the auditing entities or persons who are directly or indirectly linked to the regulated subjects.

ARTICLE 50.- Powers of the Monetary Board and the Superintendency of Banks.-

50.1. The Monetary Board, using the regulatory power conferred on it by Law No. 126-02 and Law No. 183-02 the Monetary and Finance Law on matters of financial operations and services associated with electronic means of payments performed by the national financial system, shall establish the requirements concerning the conditions of use of the certification services in said system.

50.2. The Superintendency of Banks, in its capacity as supervisor of the national financial system, shall pronounce the instructions and circulars which it may deem necessary for purposes of having the financial intermediary entities give faithful compliance with the conditions established by the Monetary Board.

TITLE V PROCEDURES

PART I GENERAL ASPECTS

ARTICLE 51.- Notifications.-

51.1. All notifications referred to by the Law and by the present Regulation shall be formulated in writing, using at least one of the following methods:

- a) Digital documents or data messages signed digitally, transmitted by protocols of electronic communication such as electronic mail, file transfer, among others.
- b) Facsimile, under the condition that the sender be able to have proof of receipt;
- c) Correspondence with acknowledgement of receipt;
- d) Those performed by accredited functionaries of INDOTEL by means of notification communiques;
- e) Bailiff's Act; or
- f) Any other physical or electronic medium by means of which INDOTEL can have proof of the certainty of its receipt.

51.2. For the effects of the present Regulation, all notification made pursuant to letters c), d), and e) must be delivered, in the case of an individual person, to the person or in the incorporated domicile, and in the case of a company, delivered to the person of its legal representative or an accredited functionary of the notified party, or in its incorporated domicile, in both cases, leaving proof of the day, time, and place in which the notification was made, as well as the name of the person who received it and his relationship with the notified party. Whenever applicable, a complete copy must be delivered of the Resolution or document in question.

51.3. In the event that the person to be notified refuses to receive or sign the notification, the INDOTEL functionary or acting Bailiff shall draft an act giving record of such circumstance and shall proceed pursuant to the provisions of the Dominican Code of Civil Procedure.

51.4. Every notification to an individual person or company whose domicile is unknown shall be made pursuant to the provisions of the Dominican Code of Civil Procedure.

51.5. The notifications performed by the accredited functionaries of INDOTEL shall have faith of its contents, until proven to the contrary.

51.6. INDOTEL has the power to modify the mechanisms to perform the notifications foreseen in the present Regulation.

51.7. The Certifying Entities, the Registry Units, and the Providers of Services of Electronic Signature must incorporate an electronic mail address for INDOTEL's information where the communications and notifications will be deemed valid.

51.8. The provisions of the present article apply equally to the communications between the regulated subjects and the users and signers of digital certificates.

ARTICLE 52.- Incorporation of Domicile.-

52.1. The Certifying Entities, the Registry Units, and the Providers of Services of Electronic Signature must incorporate domicile with INDOTEL when depositing their application for Authorization, or at the moment of making their first presentation.

52.2. The changes of incorporated domicile must be reported to INDOTEL.

52.3. In the case of companies, they must inform INDOTEL of the names and changes which occur among the members of their Board of Administration or Board of Directors.

ARTICLE 53.- Presentation of Observations or Objections.-

Every person who accredits a legitimate and direct interest in an application for authorization which is being made to INDOTEL shall have the opportunity to present observations or objections related directly to said application, following the applicable procedures. The observations received shall not be binding on INDOTEL.

ARTICLE 54.- Confidentiality.-

54.1. Every applicant for an Authorization may request in writing that certain information not be subject to public inspection. Said request for confidentiality must:

- a) Identify the document which contains the information, describe the reasons which motivate it, and the term period during which the confidentiality of the information is required; and
- b) Explain the form and measure in which the revelation of the information could result in a substantial competitive harm for the applicant.

54.2. INDOTEL shall review the application, and shall issue its decision with a term period of FIFTEEN (15) calendar days counting from the receipt of same, recording in the event that the application is accepted, the term during which the information shall remain of a confidential nature.

54.3. If the conditions which motivate the request are maintained, and the expiration date of the term set by INDOTEL approaches, the applicant may request an extension of the indicated term period, so long as it presents the application at least TEN (10) calendar days prior to expiration of same.

54.4. INDOTEL shall review the application and shall act in conformance with article 54 number 2 of the present Regulation.

54.5. INDOTEL shall not reveal for any reason information declared to be confidential, excepting in the following cases:

- a) It becomes of the public domain for causes not attributable to an illicit act, or to an omission by INDOTEL or because of the expiration of the term period during which the confidential nature was granted to the information; or
- b) It becomes available by means of another source, in good faith and without any limit in terms of its use.

ARTICLE 55.- Change of Information.-

55.1. The Certifying Entities, the Registry Units, and the Providers of Services of Electronic Signature have the obligation to report to INDOTEL any change of the information they have presented, which does not require the prior approval of INDOTEL, but which could affect the authorization granted, within the THIRTY (30) calendar days following the effective date of the change.

55.2. Failure to comply with this obligation shall constitute a very serious fault, and shall be sanctioned pursuant to the Law.

55.3. If the information should become necessary for the solution of a process or controversy, INDOTEL may require the abbreviation of the term period.

ARTICLE 56.- Resolutions and their Contents.-

56.1. INDOTEL shall make its decisions by means of Resolutions, which shall be dated, numbered consecutively, and recorded in a medium of public access. The resolutions of a general nature, and others of public interest which INDOTEL may determine, must also be published in a newspaper of national circulation.

56.2. INDOTEL's resolutions must be duly motivated and as a minimum, they must include the following:

- a) Description of the positions of the parties and the motives to accept or reject each one of them;
- b) The relevant facts on which their adoption is based;
- c) The applicable norms;
- d) The public interest which is protected; and
- e) The provision of the Resolution.

ARTICLE 57.- Criteria of action.

57.1. In its actions INDOTEL must respect the right to defense of the interested parties, and the protection of the rights of consumers of the services of digital certification.

57.2. The aspects related to the degree of the faults and application of sanctions will be contained in the complimentary norm which INDOTEL will pronounce to such effect.

ARTICLE 58.- Norms of general scope.-

58.1. Before pronouncing resolutions of a general nature, INDOTEL must consult the interested parties, and there must be written proof of the consultation and its responses.

58.2. When the interested parties are of an indeterminate nature, INDOTEL shall call for a public hearing in which, after accreditation and through the procedures foreseen in the regulation which may be pronounced, the possible interested parties may issue their opinion, which shall not be binding on INDOTEL. As an alternative method of consultation, INDOTEL may publish the norm foreseen, in a newspaper of national circulation, establishing a reasonable term period to receive comments from the public.

ARTICLE 59.- Regulatory proposals.-

In those cases in which it is necessary to execute particular actions in benefit of the public interest, this shall be done without prejudice to the obligation of consultation and of the right of participation, and INDOTEL shall pronounce a provisional executory resolution. Said resolution shall be published and will be subject to observations for NINETY (90) calendar days, in which term period a definitive resolution must be taken. In that term, and before the definitive resolution, INDOTEL can modify its provisional regulatory proposal.

ARTICLE 60.- Publicity.-

All actions before INDOTEL and its acts may be consulted by the general public, excepting that, by motivated request of the interested party, in a concrete case and for the time which may be set, INDOTEL, basing itself on reasons of commercial secret or

reservation or other type which is justified, INDOTEL may determine not to make it public.

ARTICLE 61.- Appeals.-

61.1. The decisions of the Executive Director and of the Board of Directors may be object of an appeal for reconsideration, which must be submitted within the term period of TEN (10) calendar days counting from the notification or publication of the act. Both the Executive Director and the Board of Directors must make a pronouncement in a maximum term of THIRTY (30) calendar days after the presentation of appeal.

61.2. Likewise, the decisions of the Executive Director may be the object of an hierarchical appeal before the Board of Directors. The Board of Directors must make a pronouncement within a maximum term of FIFTEEN (15) calendar days after said presentation of appeal.

61.3. The decisions of the Board of Directors shall be the object of a hierarchical appeal before the Jurisdiction of Administrative Contentious Matters, in the form and terms foreseen by the norms which govern the subject.

ARTICLE 62.- Motives for Objection.-

The recourses of appeal against decisions of the Board of Directors may be based only on the following causes:

- a) Exceeding the limits of powers;
- b) Lack of substantial basis in the facts of the cause;
- c) Evident error of right; or
- d) Noncompliance with the applicable procedural norms.

ARTICLE 63.- Obligatory Nature of Administrative Recourse of Appeal

The prior administrative path is obligatory for the regulated subjects who wish to resort to the judicial alternative.

ARTICLE 64.- Execution of the Administrative Act.-

INDOTEL's administrative acts shall be of immediate execution and obligatory compliance, excepting the decision of a competent authority which suspends its execution.

ARTICLE 65.- Delivery of information.-

65.1. INDOTEL may request the regulated subjects to provide reports, accounting data, and statistics in the following cases:

- a) When there exists a controversy in which INDOTEL must intervene;
- b) When there exists an imputation of infraction and same is strictly linked to the imputed fact;
- c) When the information is necessary and has a direct link with the formulation of policies or norms; and
- d) In the auditing processes established by the Law, by the present Regulation, and by the complimentary norms.

65.2. The reports must be provided in the reasonable term periods which are set at each opportunity, which may not be less than FIVE (5) working days. In the cases foreseen, the regulated subjects must permit INDOTEL free access to the books, accounting documentation, and information recorded under any form.

65.3. INDOTEL may directly require the assistance of public force for the exercise of the powers conferred on it by Law.

65.4. INDOTEL may establish the reasonable minimum requirements which the accounting of the regulated subjects will comply with. Likewise, it shall establish the minimum reasonable requirements for the supplying and preservation of accounting, cost, and operational information.

PART II PROCEDURE OF AUTHORIZATION

ARTICLE 66.- Authorization to operate as Certifying Entity.-

66.1. INDOTEL's authorization is required for the providing of the following services linked to digital signatures, according to what is established by articles 35 clause a), 36, and 56 number 1) of the Law, without prejudice to INDOTEL's regulatory power to modify the present list:

- a) Services of issuance, administration, registration, and preservation of digital certificates;
- b) Services of registration and chronological stamping of the transmission and receipt of data messages;
- c) Services of registration and chronological stamping of digital documents;
- d) Services of secure storage of digital documents;
- e) Services provided by Registry Units;
- f) Certification services for digital documents digitally signed;
- g) Other services or activities related to the digital signature to be determined by INDOTEL.

66.2. Authorization is the procedure by virtue of which INDOTEL confirms that the Certifying Entity has the procedures, systems, and human resources necessary to offer digital certification services. In addition, the Certifying Entities must request authorization to perform transfers, cessions, leases, grants of right of use, incorporation of liens or transfer of share control under the terms established in the Law, in the present Regulation, and in the complimentary norms which may be pronounced by INDOTEL.

ARTICLE 67.- Requirements to request authorization.-

67.1. The request for authorization for the rendering of services of digital certification is voluntary.

67.2. In order to obtain it, the applicant must fulfill at least the following conditions:

- a) Demonstrate the reliability necessary of its services in accordance with the technical norms and procedures approved by INDOTEL;
- b) Guarantee the existence of a secure service of consultation of the registry of certificates issued;
- c) Employ personnel qualified for the rendering of the services offered, in the scope of digital signatures and adequate procedures of security and management.
- d) Using reliable systems and products which will guarantee the security of their certification processes;
- e) Having contracted an appropriate insurance under the terms indicated in article 16 of the present Regulation;
- f) Have the technological capacity in terms of information systems and communications necessary for the development of the certification activity; and
- g) Comply with the rest of the precautions established by INDOTEL.

67.3. Compliance with said conditions shall be evaluated by INDOTEL in accordance with the technical and procedural norms applicable to the rendering of the service, during the authorization procedure.

ARTICLE 68.- Contents of the application for authorization.-

68.1. In the application for authorization, the Certifying Entities shall specify the activities or services for which they require authorization, and shall credit the following to INDOTEL by whatever means the latter may determine:

- a) Documentation which demonstrates its legal personality;
- b) Authorization of the corresponding directive entity to initiate the procedure for obtaining authorization to operate as a Certifying Entity, when dealing with institutions;
- c) Certification policies for which it requests authorization, which support the issuance of its certificates, Procedures Manual, Security Plan, Plan for Cessation of Activities, and Contingency Plan in accordance with the requirements established by the norms issued by INDOTEL; and

d) All other documentation required by INDOTEL.

ARTICLE 69.- Procedure for Application.-

69.1. Once the application for authorization has been received, INDOTEL shall proceed to analyze the admissibility of same by means of the verification of the required background, in a term period of TEN (10) working days.

69.2. If the application is admissible, within THREE (3) working days they shall proceed to communicate such situation to the applicant. In said communication, a term period no less than FIFTEEN (15) working days shall be granted so that it complete the background, information or documentation, under warning that otherwise the application will be rejected.

69.3. Once the application is admitted, INDOTEL shall proceed to an examination on the compliance with or fulfillment of the requirements and obligations required by the Law and by the present Regulation in order to obtain the authorization. Said examination shall be performed by means of the drafting of an initial audit, whether by INDOTEL or by third parties, certifying within the term period of NINETY (90) working days counting from the date of the admissibility of the application, extendable one time and for an equal period and for motives with basis, that the interested party fulfills the requirements and obligations to be authorized, and that it has available a term of TWENTY (20) working days to present the insurance policy demanded by the present Regulation, under threat of the application's being rejected.

ARTICLE 70.- Failure to Fulfill the Technical or Procedural Requirements.-

70.1. In the event that INDOTEL should determine that the Certifying Entity does not fulfill the requirements set in the norms for the development of the activity, it shall indicate whether said noncompliance can be remedied, and whether it affects the correct

functioning of the system or the ends foreseen in the Law, in the present Regulation, and in the complimentary norms.

70.2. In the event that the failure to comply is not remediable, INDOTEL shall proceed to pronounce a resolution in which it rejects the application for authorization.

70.3. If the noncompliance or failure to fulfill the requirements is remediable and does not affect the correct functioning of the system nor the ends foreseen in the Law, in the present Regulation and in the complimentary norms, INDOTEL shall grant a term period for the remedying of the noncompliance. Once said term has expired, INDOTEL shall verify whether the corrective measures have been applied, and if so, it shall proceed to give continuity to the processing, or to pronounce a resolution rejecting the application for authorization.

ARTICLE 71.- State of resolution of the processing.-

Once the necessary requirements have been completed, INDOTEL shall proceed to authorize the interested party in the term of TWENTY (20) working days counting, at the petition of the interested party or officially, from when it is certified that the application is in a state of resolution.

ARTICLE 72.- Additional information.-

During the entire authorization process, INDOTEL may request additional documentation, perform visits, and make inspections of the installations of the interested party.

ARTICLE 73.- Scope of the Granting of the Authorization and of the Inscription in the Registry of Certifying Entities.-

73.1. The granting of the authorization does not imply that INDOTEL, the auditing entities, or any State entity guarantees the providing of the certification services or the products offered by the

Certifying Entity. The responsibility for the providing of the services of digital certification corresponds exclusively to each certifying entity.

73.2. The inscription in the Registry does not exempt the Certifying Entity from the obligation to obtain other authorizations necessary to offer other services, and for the effective implementation of the systems authorized.

ARTICLE 74.- Duration of the Authorization.-

74.1. The authorization to function as a certifying entity shall have a term of duration of five (5) years, and may be renewed after favorable ruling of an audit.

74.2. The Certifying Entities must annually make a report of the statement of operations with the nature of a sworn statement in which is recorded the compliance with the norms established in the Law, in the present Regulation, and in the complimentary norms. The Certifying Entities shall be submitted to periodic audits. The format and procedures for the audit shall be determined by INDOTEL.

ARTICLE 75.- Causes for suspension of the authorization.-

75.1. INDOTEL shall order in its official capacity the suspension of the authorization in the following cases:

- a) Failure to present the report of statement of operations in the form of an annual sworn statement;
- b) False data contained in the report of the statement of operations which has the nature of an annual sworn statement;
- c) Unfavorable ruling of audit based on serious causes;
- d) Unfavorable report of the inspection ordered by INDOTEL based on serious causes;
- e) When the Certifying Entity does not permit the performance of audits or inspections ordered by INDOTEL; and
- f) When the owner of the Certifying Entity has been condemned in a criminal case with ruling of a definitive nature.

ARTICLE 76.- Revocation of the authorization.-

76.1. INDOTEL may leave the authorization without effect by means of a duly motivated Resolution, for the causes foreseen in the following article.

76.2. Said Resolution must order the cancellation of the inscription in the Registry of Certifying Entities.

ARTICLE 77.- Causes for Revocation of the Authorization.-

77.1. The authorization of the Certifying Entities will be left without effect due to the following causes:

- a) Due to request of the Certifying Entity, to INDOTEL, no less than NINETY (90) working days prior to the cessation of the foreseen activities, indicating the destination to be given to the certificates, to the data and the support documentation of same, for which it must comply with the provisions of article 11 of the present Regulation, and guarantee the payment of the notice which must be published in conformance with the provisions of the following article;
- b) Due to loss of the conditions which served as the basis for its authorization, which will be qualified by INDOTEL in compliance with the power of inspection;
- c) Due to reincidence in the causes for suspension of the authorization indicated in the present Regulation;
- d) Due to serious or repeated noncompliance with the obligations established by the Law and by the present Regulation;
- e) Due to the state of cessation of payments of the Certifying Entity, declared by irrevocable ruling of a competent court;

- f) Due to reincidence in the commission of serious or very serious infractions or crimes;
- g) Due to the impossibility of compliance with the corporate purpose of the authorized party according to the mandate of its by-laws insofar as it is related to the authorization granted;
- h) Due to the unjustified suspension of the service;
- i) Due to having made a transfer, cession, lease, granting of right of use, incorporation of liens or transfer of share control without INDOTEL's authorization; and
- j) Due to any other action of the Certifying Entities which INDOTEL may decide, by means of duly motivated resolution and which deliberately goes against the principles of the Law. (sic)

77.2. In the cases of letters b), c), d), e), f), g), h), and i), the Resolution must be adopted after transfer of charges and hearing of the affected party, for which INDOTEL shall give a term period of FIVE (5) working days so that the latter present in writing the response to the charges made. Once it is received, INDOTEL must resolve within the term of FIFTEEN (15) working days, extendable for the same period due to motives with basis.

77.3. In those cases in which noncompliance or objective conditions imply a serious risk to the Infrastructure of Public Password of the Dominican Republic, INDOTEL may preventatively suspend immediately all or any of the activities of the entity committing the infraction, by means of motivated Resolution.

ARTICLE 78.- Communication of the revocation.-

78.1. The Certifying Entities whose inscription in the Registry has been revoked must immediately communicate this fact to the signers of the certificates issued by them, in a maximum term of TWENTY-FOUR (24) hours, and by the means established in article 51 of the present Regulation. Without prejudice to same, INDOTEL shall

publish a notice informing of the revocation of the authorization, whose publication cost shall be charged to the Certifying Entity.

78.2. Said notice must be published in a newspaper of national circulation, without prejudice to the publication of the resolution in the Registry of Certifying Entities. The notice must indicate that as of said publication, the certificates will be without effect and will be revoked immediately, unless they have been transferred to another Certifying Entity.

78.3. In addition, the revocation shall be published on INDOTEL's Internet page and in its Official Bulletin.

TITLE VI CONDITIONS FOR THE USE OF A DIGITAL SIGNATURE IN DOCUMENTARY INTERACTIONS BETWEEN ENTITIES OF THE STATE OR BETWEEN PRIVATE PERSONS AND ENTITIES OF THE STATE

ARTICLE 79.- Validity of the Digital Documents.-

79.1. In the relations between public entities among themselves or between private persons and state entities, legal effects, validity or obligatory force shall not be denied to a statement of will or other declaration for the sole reason of having been made in the form of a digital document or data message.

79.2. The administrative entities of the Dominican State may execute or perform acts, celebrate contracts, and issue any document, within its scope of competence, signing them by means of electronic or digital signature, according to the nature of the act.

79.3. For such effect, the administrative acts, formalized by means of digital documents and which are recorded in decrees or resolutions, in agreements of collegiate or professional entities, as well as the celebration of contracts, the issuing of any other document which expresses the will of a State entity in exercise of its legal powers, and in general, every document which possesses the nature of a public instrument or those which should produce the legal effects of the latter, must be signed by means of a digital signature.

ARTICLE 80.- Providing of certificates for use of the State.-

80.1. State entiteis may contract, according to the norms which govern administrative contracting, the services of certification of digital signature with a Certifying Entity, when by means of resolution with basis, they determine their technical and economic convenience. The estimate of said convenience shall be based on criteria of quality of service and price.

80.2. Otherwise, they may incorporate themselves as provider of services of certification, by requesting of INDOTEL the respective authorization to function as a Certifying Entity.

80.3. In those applications in which the State interacts with the community, the use of Digital Certificates issued by Certifying Entities belonging to the public sector or to the private sector must be admitted, indistinctly. Discriminatory criteria may not be established, insofar as all of the functional, legal, and regulatory requirements are satisfied.

ARTICLE 81.- Units of Registry belonging to the State.-

81.1. In the entities and jurisdictions belonging to entities of the State, the areas of human resources shall fulfill the functions of Unit of Registry for the agents and functionaries of its jurisdiction. In such case, and if the applications inquestion so require, the maximum authority of the entity may in addition assign to another unit the functions of Registry Unit.

81.2. INDOTEL shall authorize the functioning of said Units of Registry and shall supervise their activity.

ARTICLE 82.- Presentation of digital documents.-

82.1. The entities of the State must establish mechanisms which will guarantee the option of remission, receipt, maintenance, and

publication of information in digital format, so long as this is applicable, both for the management of documents between entities and in their interaction with citizens, such as unique electronic window, availability of an electronic mail address, or formula on the Internet page for attending consultations, means of electronic entry, electronic public contractings, follow-up of case files over the Internet, and other applications which will allow the consulting of information, the remission of documentation, and the follow-up of processes over the Internet.

ARTICLE 83.- File of Digital Documents (Repositories).

83.1. The entities of the State Administration which use digital documents must have an electronic Repository or File for purposes of safeguarding and preserving them once their processing has been finalized, in accordance with the norms which regulate their competence.

83.2. The Repository shall be the responsibility of the respective official in charge of the file, without prejudice to the celebration of cooperation agreements between different entities for the safeguarding and preservation of digital documents.

83.3. The Repository must have an authorization in order to operate, which was ordered by INDOTEL.

ARTICLE 84.- Minimum requirements for Digital Document File.-

84.1. The Repository must guarantee the security, integrity, and availability of the information contained in it.

ARTICLE 85.- Electronic communications.-

The entities of the State Administration may be related by electronic mediums with private ones, by using data messages or digital

documents, when the latter have been expressly consented to in this form of communication.

ARTICLE 86.- Setting of the official electronic time.-

86.1. INDOTEL shall analyze the alternatives and regulations necessary for setting the official day and time in the electronic mediums, as well as the design of the distribution mechanisms for the official Internet time, in order that both the public entities and the Certifying Entities proceed to take from there the time as an input for their recording and subsequent distribution, and for the supplying of the service of registry and chronological stamping. This official hour in electronic Internet medium shall be used for the determination of date and true hour in the performance of acts for which the reliable determination of the time constitutes an essential element, such as the presentation of writs in digital format in judicial and administrative instance as a means of documentary proof, the performance of electronic purchases or electronic notifications.

86.2. INDOTEL shall coordinate the actions with the entities of the State which are responsible for setting the official time, in order to draft the norms for the setting of the official time in electronic mediums, and its distribution over the Internet to which the servers of public entities and of regulated subjects must abide (adjust themselves).

86.3. Once said norms are approved, the subjects regulated by the Law, the providers of Internet services, public entities must adjust their servers to the official electronic time set, and shall distribute it in accordance with the regulation which may be pronounced.

86.4. The electronic communications and notifications must have a chronological stamp, based on the certain electronic date and time.

TITLE VII GENERAL PROVISIONS

ARTICLE 87.- Agreement between the parties.-

87.1. In the relationships between the initiator and the addressee of a data message , or between the parties signing a digital document, when there are any, no legal effects, validity, or obligatory nature shall be denied to a manifestation of will or other statement due to the sole reason of having made it in form of digital document or data message.

87.2. The parties may agree on the use of mechanisms to determine the authorship and integrity as such:

- a) Electronic signature;
- b) Electronic signature based on digital certificates issued by providers of services of electronic signature in the framework of the present Regulation;
- c) Digital signature based on digital certificates issued by the Certifying Entities in the framework of the present regulation; and
- d) Digital form based on digital certificates issued by foreign certifiers who have been acknowledged in the following cases:
 - 1- Pursuant to the existence of agreements of reciprocity between the Dominican Republic and in the country of origin of the foreign certifier; and

2 - By a Certifying Entity in the Dominican Republic.

ARTICLE 88.- Preservation.-

88.1. With respect to the preservation of digital documents regarding time of storage, the provisions contained in the norms of merit applicable to the transaction in question are applied.

88.2. Compliance with the legal demand for preservation of documents, registries, or data, in accordance with the legislation in effect on the subject, may be satisfied by the preservation of the corresponding digital documents.

88.3. The documents, registries, or digital data messages must be stored by the parties intervening in each electronic transaction, or by a reliable third party accepted by the intervening parties, during the terms established in the specific norms.

88.4. Legalized copies may be obtained on support paper or indigital format based on the original digital documents, in digital format. The certification of authenticity shall be performed in conformance with the legal procedures in effect for the act in question, identifying the support which from which the copy proceeds.

ARTICLE 89.- Taking of Effect.-

The present Regulation shall take effect as of the date of its publication in the official gazette, or in a newspaper of national circulation.

89.1. **TO ORDER** that Law No. 126-02, its Regulation of Application, and the complimentary norms which INDOTEL may pronounce to such effect, shall govern the use of digital documents, data messages, and digital signatures, the issuing of digital certificates for the persons or companies of private right/law and administration of the State, the providing of the services of certification, the authorization of the certification entities and the generation of rights and obligations of the signers and users of digital documents, data messages, and digital and electronic signatures;

89.2. **TO DELEGATE** in INDOTEL, in accordance with the provisions of articles 37 and 55 of the Constitution of the Dominican Republic, the power to celebrate agreements of reciprocity with governments of foreign countries, whose object is to grant validity in their respective territories to the digital certificates issued by certifying entities authorized in both countries, while compliance is verified of the conditions established by Law No. 126-02, by its Regulation of Application, and by the complimentary or modifying norms for the digital certificate issued by certifying entities;

89.3. **TO ORDER** the Legal Consultant of the Executive Power to remit a complete copy of the present Decree to the Dominican Telecommunications Institute (INDOTEL) for its knowledge, and so that it proceed to publish it in the Official Gazette or in a newspaper of national circulation.

Given in Santo Domingo de Guzmán, National District, Capital of the Dominican Republic, on the eighth (8th) day of the month of April of the year two thousand three (2003), year 160 of the Independence and 140 of the Restoration.

HIPOLITO MEJIA