Decree-Law nr. 290-D/99 of the 2nd of August

Council of Ministers Resolution nr. 115/98, of the 1st of September decided that the definition of the legal framework applicable to electronic documents and digital signatures, is one of the objectives to be achieved within the ambit of the National Electronic Commerce Initiative, which is necessary for the establishment of electronic commerce. Open electronic networks, such as the Internet, are increasingly important in the daily life of the general public and the business community, and provides a network of global commercial relations. It is necessary to create a secure environment for electronic authentication, so that advantage can be taken of these opportunities, in the best way possible. The fact is that electronic communications and commerce require electronic signatures and the services associated therewith, which permit the electronic data authentication. Electronic signatures make it possible for users of data sent electronically, to check the source thereof (authentication) and whether the data has been altered in the meantime (security). So far as electronic signatures are concerned, this decree-law is based on the prevailing technology: i.e. digital signatures produced by cryptographic techniques. The studies available of digital signature technologies, based on public key cryptography, confirm that the digital signature is currently the most recognised electronic signature technique and affords a high level of security for data exchange in open networks. This awareness of the state of the technology has led foreign legislation to give preference to this type of electronic signature. However, given the constant technological progress, this data authentication solution may be technically outdated in a short time, and be replaced by other forms of electronic signature. The legal framework envisaged in this decree-law can accordingly be applied to other forms of electronic signature, which comply with digital signature security requirements. The checking of data authenticity and security afforded by electronic signatures, in general, and by digital signatures, in particular, does not necessarily prove the identity of the signatory, who created the electronic signatures. It was therefore deemed necessary to create a system in which confirmation is provided by certification agencies, in accordance with the internationally accepted and technically recommended practises, which are responsible for ensuring the high levels of system security, which are indispensable for the creation of confidence in signatures of electronic documents. In this context, this decree-law, on the one hand, regulates the recognition and legal value of electronic documents and digital signatures, and, on the other hand, entrusts the control of the certification of signatures to an authority to be designated and defines the powers and procedures thereof, and the terms on which certification business may be licensed and the rights and duties of certification agencies. The business of the certification of digital signatures, in accordance with the approach already adopted in other European Union countries, is not subject to prior administrative licensing. It is therefore necessary for the State to control the reliability and security afforded by certification agencies, thus providing the general public and the market with the guidance and quality guarantees, which are indispensable for the creation of confidence in new documentation and signature methods. A voluntary system, in which the certification bodies are licensed and supervised by the proper authority, is therefore envisaged, in accordance with this approach. This decree-law is the first step taken in Portugal to give legal recognition to electronic signatures and adopts the solutions proposed within the European Union and in the draft European Parliament and Council directive, regarding a community legal framework for electronic signatures. Technological progress, which is constant in this area, means that the legal framework established by this decree-law will have to be revised, adapted and extended in the medium term.

Accordingly: the Government decrees the following, pursuant to the provisions of paragraph a) of nr. 1 of article 198 of the Constitution, as a general law of the Republic:

CHAPTER I
Electronic documents and juridical acts

Article 1
Subject-matter

1. This decree-law regulates the validity, efficacy and evidential value of electronic documents and digital signatures.

2. The legal framework envisaged in this decree-law may be applied to other forms of electronic signature, which comply with the same security requirements as digital signatures.

Article 2
Definitions

For the purposes of this decree-law the following terms shall have the following meanings:

a. Electronic document: a document created by electronic data processing;

b. Electronic signature: the result of electronic data processing, which can be the subject-matter of an exclusive individual right and be used to indicate the authorship of an electronic document, in which it is included, so that:

i. It unequivocally identifies the holder as the author of the document;
ii. The inclusion thereof depends only on the holder;
iii. The link between the signature and the document is such that it is possible to detect all subsequent alterations thereof;

c. Digital signature: an electronic signature process, based on an asymmetric cryptographic system, comprising an algorithm or series of algorithms, which generate a pair of asymmetric, exclusive and interdependent keys, one of which is private while the other is public, which permit the holder to use the private key to indicate the authorship of the electronic document, to which the digital signature is affixed, and acceptance of the contents thereof, and which permits the person, who receives the document, to use the public key to confirm that the signature was created using the corresponding private key and top check whether the document has been altered since the signature was affixed thereto;

d. Private key: one of a pair of asymmetric keys, which is known only to its holder, which is used by the holder to affix a digital signature to an electronic document, or which is used to decipher an electronic document encrypted with the corresponding public key;

e. Public key: one of a pair of asymmetric keys to be publicised, which is used to check the digital signature affixed to an electronic document by the holder of the pair of asymmetric keys, or to encrypt an electronic document to be transmitted to the holder of the said pair of keys;

f. Licensing: the act which confirms that an organisation, which applies to be licensed and carries on the business of a certification agency, referred to in paragraph h) of this article, complies with the requirements of this decree-law for the purposes hereof;

g. Licensing authority: the proper agency responsible for the licensing and supervision of certification agencies;

h. Certification agency: a licensed organisation, private individual or corporation, which creates or provides the means to create keys, issues signature certificates, publicises the same and provides other services in connection with digital signatures;

i. Signature certificate: an electronic document authenticated with a digital signature, which certifies holdership of a public key and the validity period thereof;

j. Chronological validation: a statement by a certification agency, which attests to the time and date of the creation, sending or reception of an electronic document;

l. Electronic address: identification of computer equipment, which is capable of receiving and storing electronic documents.

Article 3
Form and evidential effect

1. An electronic document shall comply with the legal requirement that it be in writing, when its contents can be represented as a written statement.

2. An electronic document with the content referred to in the preceding number, shall have the same evidential value as a private signed document, in accordance with the provisions of article 376 of the Civil Code, when it bears a digital signature certified by a licensed body, which complies with the requirements of this decree-law.

3. An electronic document, the contents of which cannot be represented as a written statement, shall

have the evidential value, in accordance with the provisions of article 368 of the Civil Code and article 167 of the Criminal Procedure Code, when it bears a digital signature certified by a licensed body, which complies with the requirements of this decree-law.

4. The provisions of the preceding numbers shall not prevent the use of other means to prove the authorship and security of electronic documents, including electronic signatures, which do not comply with the provisions of this decree-law, provided that the said means are adopted by the parties pursuant to a valid agreement regarding evidential value or are accepted by the person against whom the document is raised.

5. The evidential value of electronic documents, which do not contain an electronic signature certified by a licensed body, which satisfies the requirements of this decree-law shall be considered according to the general provisions of the law.

Article 4
Copy documents

Copies of electronic documents, on an identical or different support, shall be valid and effective in accordance with the general provisions of the law and shall have the same evidential value as photocopies, in accordance with no. 2 of article 387 of the Civil Code and article 168 of the Criminal Procedure Code, provided that the requirements stipulated therein are complied with.

Article 5
Electronic documents issued by public agencies

1. Public agencies may issue electronic documents bearing a digital signature, which complies with the provisions of this decree-law.

2. The creation, issue, storage, reproduction, copying and transmission of electronic documents, which formalise administrative acts, via computer systems, including the transmission thereof by telecommunications, the data with regard to the agency concerned and the person who practised each administrative act shall be stated so as to render them readily identifiable and so as to record the function or position of the person who signs each document.

Article 6
Communication of electronic documents

1. Electronic documents sent by telecommunications shall be deemed to be sent and to be received by the addressee, if transmitted to and received at an electronic address stipulated by agreement between the parties.

2. The date and time of the creation, transmission or reception of an electronic document, which contains a chronological validation issued by a certification agency, may be raised between the parties thereto and in dealings with third parties.

3. The transmission of an electronic document signed in accordance with the requirements of this decree-law, by a means of telecommunications, which ensures actual reception, shall be equivalent to a document sent by recorded delivery mail, and if reception thereof is proved by a confirmation message addressed to the sender bearing a digital signature received by the sender, it shall be equivalent to a document sent by recorded delivery mail with advice of delivery.

4. Data and documents transmitted by telecommunications shall be deemed to be in the power of the sender until received by the addressee.

5. Operators, which provide the means to transmit electronic documents by telecommunications, shall not become aware of the contents thereof nor shall they, in any way, copy them or provide third parties with any information regarding the existence or contents of the said documents, including a summary or extract thereof, save when this information is intended to become public, either at the express request of the sender or because of the nature thereof.

CHAPTER II
Digital signatures

Article 7
Digital signature

1. The inclusion of a digital signature in an electronic document or in a copy of an electronic document, shall be equivalent to a hand-written signature on written paper documents and shall give rise to the presumption that:

a. The person who included the digital signature is the holder of the signature or is an authorised representative of the juristic person, which owns the digital signature;
b. The digital signature was included with the intention to sign the electronic document;
c. The electronic document has not been altered since the digital signature was included therein, whenever it is used to confirm a public key in a valid certificate, issued by a certification agency licensed in accordance with the provisions of this decree-law.

2. Digital signatures shall be unequivocally linked to only one natural or juristic person and to the document to which it has been affixed.

3. The inclusion of a digital signature shall replace the affixture of paper stamps, rubber stamps, marks or other methods of identifying its holder.

4. A private key, which corresponds to a public key in a valid certificate, issued by a certification agency licensed in accordance with this decree-law, which has neither been suspended nor revoked by decision of the certification agency and which is in force, when the digital signature is included, shall be used to affix digital signatures.

5. The inclusion of a digital signature, at a time when its public key is contained in a revoked, expired or suspended certificate, or which does not comply with the conditions in the certificate, shall be deemed to be equivalent to no signature.

Article 8
Obtaining of keys and certificates

Whosoever intends to use a digital signature for the purposes envisaged in this decree-law shall create or obtain a pair of asymmetric keys, in accordance with the provisions of nr. 1 of article 29 hereof, and obtain a certificate of the public key, issued by a certification agency licensed in accordance with this decree-law.

CHAPTER III
Certification

SECTION I
Access to certification business

Article 9
Free access to certification business

Access to the certification agency business referred to in paragraph h) of article 2 shall be free. The licensing application procedure in articles 11 et seq. hereof shall be optional.

Article 10
Freedom of choice of certification agency

1. The choice of certification agency shall be free.

2. The selection of a specific agency shall not be a condition of the offer or completion of any contract or unilateral obligation.

Article 11
The licensing authority

The licensing of certification agencies for the purposes of this decree-law shall be the responsibility of an authority to be designated in accordance with article 40 hereof, hereinafter referred to as the licensing authority.

Article 12
Approval of the certification agencies

Digital signature certification agencies, which comply with the following requirements, shall be licensed, upon application to the licensing authority:

a. Have sufficient capital and financial resources;

b. Provide assurances of absolute integrity and independence in the conduct of their digital signature certification business;

c. Have technical and human resources, which comply with the security and efficacy standards envisaged in the regulations referred to in article 38;

d. Have a valid contract of insurance, which provides adequate civil liability cover for the certification business.

Article 13
Licensing applications

1. The following documents shall be submitted in support of licensing applications by digital signature certification agencies:

a. The articles of association of juristic persons and companies and the address and full identification of natural persons;
b. In the case of company applicants, a list of all members, stating their holdings and the members of the board of directors and the audit committee, and, in the case of a public limited company, a list of all shareholders with significant direct or indirect holdings therein;
c. Signed declarations by all the natural and juristic persons referred to in nr. 1 of article 15, to whom or which any of the circumstances indicative of good standing, referred in nr. 2 thereof, do not apply;
d. Evidence of the asset base and financial resources available and, in the case of companies, that the share capital is fully paid up;
e. A description of the internal organisation and security plan;
f. A description of the available material and technical resources, including the characteristics and location of all land and buildings used;
g. The name of the security auditor;
h. A general business plan for the first three years;
i. A general description of the business conducted in the last three years or since incorporation, if less, plus the balance sheets and profit and loss accounts of the corresponding financial years;
j. Proof of the existence of a valid contract of insurance, which provides adequate civil liability cover for the certification business.

2. If the juristic person has not, as yet, been incorporated, the application shall be supported by the submission of the following documents, instead of the documents referred to in paragraph a) of the preceding number:

a. The minute of the meeting at which the decision to incorporate was taken;
b. Draft articles of association;
c. An undertaking, signed by all the subscribers, to the effect that the asset base required by law will be fully paid up, at the time and as a precondition of the act of incorporation.

3. The undertakings envisaged in paragraph c) of nr. 1 may be submitted following the submission of the application, on such terms and within such time limits as the licensing authority shall specify.

4. Holdings of 10% or more of the share capital of a public limited company shall be deemed to be significant holdings for the purpose of this decree-law.

Article 14
Asset requirements

1. Private certification agencies, which are juristic persons, shall have a share capital of at least 40 000 000$00, or an equivalent asset base, if not companies.

2. The asset base and the minimum share capital of companies, shall be fully paid up on the date the license is granted, if the juristic person has already been incorporated, or shall be fully paid up when the juristic person is incorporated, when incorporation occurs subsequently.

3. Certification agencies, which are natural persons, shall have assets, free of onuses and encumbrances, with a value equivalent to that indicated in nr. 1, for as long as they continue to trade.

Article 15
Good standing

1. Natural persons and the members of the board of directors and audit committee, employees, agents and representatives of juristic persons, which are certification agencies, who have access to acts and instruments of certification, company shareholders, and, in the case of public limited companies shareholders with significant holdings, shall always be of recognised good standing.

2. The fact that, in addition to other relevant circumstances, the following applies to a person shall be deemed to indicate lack of good standing:

a. Conviction, in Portugal or abroad, of the crime of theft, robbery, fraud, computer and communications fraud, extortion, breach of confidence, infidelity, forgery, misrepresentation, criminal insolvency, negligent insolvency, fraudulent preference, issuing of cheque without provision, misuse of a guarantee or credit card, unlawful appropriation of state or co-operative property, wrongful mismanagement of a unit in the public or co-operative sector, usury, bribery, corruption, unauthorised reception of deposits or other reimbursable funds, unlawful acts or operations in the context of insurance business or pension funds, money laundering, insider trading, stock market manipulation or a crime envisaged in the Commercial Companies Code;
b. Has been declared, by a Portuguese or foreign court, to be bankrupt or insolvent or held liable for the bankruptcy or insolvency of an enterprise dominated by him or her or when he or she was a member of its board of directors or audit committee;
c. Has had penalties imposed, in Portugal or abroad, for offences against legal provisions or regulations, which govern the business of the production, authentication, registration and conservation of documents, i.e. those governing notaries, public registries, court officials, public libraries and the certification of digital signatures.

3. Failure to comply with the requirements of good standing, stipulated in this article, shall be grounds to refuse and cancel licences, in accordance with the provisions of paragraph c) of nr. 1 of article 21.

Article 16
Security auditor

1. All certification agencies shall have a security auditor, which shall be a natural or juristic person and which shall prepare an annual security report and send it to the licensing authority, by the 31st of March of each calendar year.

2. The appointment of security auditors shall be subject to the prior approval of the licensing authority.

Article 17
Obligatory civil liability insurance

The Minister of Finance shall define the characteristics of the civil liability insurance contract referred to in paragraph d) of article 12, in a statutory instrument.

Article 18
Decision

1. The licensing authority may request applicants to provide additional information and conduct or order the conduct of such investigations, enquiries and inspections as it deems necessary, in order to consider applications.

2. Notice of the decision regarding licensing applications shall be given to the applicants within three months of the submission of the application, or of the date on which any additional information requested is received or on which any necessary steps are concluded. The said period shall not exceed the period of six months from the date of the submission of the application.

3. Failure to give notice of the decision regarding licensing applications, within the time limits referred to in the preceding number, shall give rise to a presumption of the tacit approval thereof.

4. The licensing authority may include additional conditions in licenses, provided that they are necessary in order to ensure compliance with legal provisions and regulations applicable to the business of the certification agency.

5. The grant of licences shall be accompanied by the issue, by the licensing authority, of the certificate of the keys to be used by the certification agency, in the issue of certificates.

6. Licensing decisions shall be notified to the supervisory authorities of the member states of the European Union.

Article 19
Refusal of licensing applications

1. Licensing applications shall be refused whenever:

a. The licensing application is not supported by all the necessary information and documents;
b. There are errors or falsehoods in the information and documents submitted in support of the licensing application;
c. The licensing authority considers that any of the requirements in articles 12 and 15 are not complied with.

2. If insufficient information or documentation is submitted in support of a licensing application, the licensing authority shall inform the applicant and give it reasonable time to remedy the shortcoming, before refusing the licensing application.

Article 20
Licensing validity periods

1. Licences shall expire if expressly renounced by the applicant, if the applicant does not commence trading within 12 months or, if the applicant is a juristic person, if it is not incorporated within 12 months.

2. Licenses shall, without prejudice the acts necessary for liquidation, also expire is the juristic person is dissolved.

Article 21
Licensing revocation

1. Licenses shall, without prejudice to other applicable penalties, be revoked according to the law, when any of the following circumstances arises:

a. If the licence was obtained by false declarations or other unlawful expedients;
b. If any of the requirements in article 12 cease to be complied with;
c. If the agency ceases certification business or reduces it to an insignificant level, for 12 months or more;
d. In the event of any serious misconduct in the administration, organisation or internal supervision of the agency;
e. In the event that unlawful acts, which negatively affect or imperil public confidence in the licence, are committed in the course of the certification or other activity of the agency;
f. If any of the circumstance indicative of lack of good standing, referred to in article 15, arise in

relation to any of the persons referred to in nr. 1 of article 15.

2. The revocation of licences shall be the responsibility of the licensing authority and be contained in a decision, which states the grounds therefor, and be served on the licensee, within eight working days.

3. The licensing authority shall give proper publicity to decisions to revoke licenses.

4. Decisions to revoke licences shall be notified to the supervisory authorities of the member states of the European Union.

Article 22
Anomalies in management and supervisory bodies

1. In the event that the requirements in the law or the articles of association regarding the normal working of the boards of directors or audit committees, are, for any reason, no longer complied with, the licensing authority shall stipulate a time limit by which the situation is to be remedied.

2. In the event that the situation is not remedied within the time limit fixed, the licence shall be revoked, in accordance with the provisions of the preceding article.

Article 23
Notice of alterations

Notice of any alterations of certification agencies affecting the following matters, shall be given to the licensing authority, within 30 days:

a. Name or Company name;
b. Object;
c. Address of registered office, unless the change is within the same or to a neighbouring municipality;
d. Assets base or assets, provided that it is a significant alteration;
e. Management and supervisory structure;
f. Restriction of the powers of management and supervisory bodies;
g. De-merger, merger and dissolution.

Article 24
Registration

1. Applications to register the persons referred to in nr. 1 of article 15 shall be made to the licensing authority by the certification agency or any of the interested parties, within 15 days of having taken up any of the positions referred to therein, together with evidence that the requirements stipulated in the said article are complied with, failing which the licence shall be revoked.

2. The certification agency or the interested parties, may apply to be registered provisionally, prior to taking up any of the said positions referred to in nr. 1 of article 15. Such registrations shall be converted into definitive registrations within 30 days of talking up office, failing which they shall expire.

3. In the case of persons returned to office, this fact shall be annotated, upon application by the certification agency or the interested parties.

4. Registration shall be refused, in the event of lack of good standing, in accordance with article 15, notice of refusal shall be given to the interested parties and the certification agency, which shall take the appropriate measures to ensure that those concerned, are removed from office or cease to be in the service of the juristic person, in the position envisaged in the said article. The provisions of article 22 shall apply.

5. Failure to register shall, without prejudice to other applicable legal provisions, not, per se, render the legal acts practised by the person in question, in the exercise of his or her office, void.

SECTION II
Conduct of business

Article 25
Duties of the certification agency

Certification agencies shall:

a. Check the identity of applicants for pairs of keys, the corresponding certificates carefully and their powers of representation, if they are representatives of juristic persons, together with the specific qualities referred to in paragraph i) of no. 1 of article 30, when applicable;

b. Issue pairs of keys or provide the technical resources necessary to create them, issue the signature certificate, in rigorous compliance with the provisions of this decree-law and the applicable regulations, ensuring the functional correspondence between the two keys in each pair and the exactitude of the information in each certificate;

c. At the request of the applicant for a pair of keys, mention the existence of powers of representation or of other titles/capacities connected with professional activity or other positions held;

d. Inform applicants, exhaustively and clearly, regarding the certification procedure and the technical preconditions required for access thereto;

e. Comply with the security rules regarding the processing of personal data, in the corresponding legislation;

f. Ensure that publicity is given to public keys and their certificates and provide information regarding them, by means of appropriate and rapid computer or telecommunications systems, to anyone wishing to consult them;

g. Refrain from becoming aware of the contents of private keys, and accept them for safe keeping, store them, copy them or provide any information with regard thereto;

h. Publicise the revocation or suspension of certificates, in the circumstances provided herein, forthwith;

i. Keep the certificates issued by them, for no less than 20 years;

j. Ensure that the date and time of the issue, suspension and revocation of certificates can be ascertained by chronological validation.

Article 26
Data protection

1. Certification agencies may only collect the personal data necessary for the conduct of their business and shall obtain such data directly from the persons who hold pairs of keys and the corresponding certificates or from third parties, from whom such collection has been authorised by the holder.

2. The personal data collected by the certification agency shall not be used for a purpose other than certification, unless another use is expressly authorised by law or the person concerned.

3. Certification agencies and the licensing authority shall comply with the legal provisions in force regarding the protection, processing and circulation of personal data and privacy in the telecommunications sector.

4. Certification agencies shall inform the judicial authorities whenever so ordered by them, of the data regarding the identity of holders of certificates issued using a pseudonym, in accordance with the provisions of article 182 of the Criminal Procedure Code.

Article 27
Civil Liability

1. Certification agencies shall be civilly liable for the loss and damage sustained by certificate holders or any third parties, as a consequence of the negligent or wilful breach of the duties arising from this decree-law and its regulations.

2. Contractual provisions, which seek to exclude or restrict the liability envisaged in nr. 1, shall be void.

Article 28
Cessation of trading

1. In the event that a certification agency wishes to cease trading voluntarily, it shall give at least three months notice of this fact to the licensing authority and to those persons to whom it has issued certificates, which are in force, identifying the certification agency to which it is going to transfer its documentation, or revoking the said certificates at the expiry of the said period, and shall, in the latter case, deposit its documentation with the licensing authority.

2. Certification agencies threatened with a winding-up order, protection from creditors and reorganisation proceedings or with cessation of trading, for any other reason, which is imposed on it, shall give immediate notice thereof to the licensing authority.

3. In the event that a certification agency ceases to trade, in the circumstances envisaged in the preceding number, the licensing authority shall procure the transfer of the documentation from it to another certification agency or, if such a transfer proves impossible, revoke the certificates issued and keep the information in the said certificates for the same period as the certification agency was required so to do.

SECTION III
Certificates

Article 29
Issue of keys and certificates

1. Certification agencies shall, at the request of an interested natural or juristic person, whose identity and powers of representation, if any, it shall check by a legally reliable and secure method, issue a pair of keys, a private key and a public key, to the said person or provide the said person with the necessary means to create a pair of keys.

2. Certification agencies shall, at the request of the holder of a pair of keys, issue one or more copies of the signature and complementary certificates.

3.Certification agencies shall take proper steps to prevent the forgery or alteration of the data in certificates, ensure compliance with the applicable legal provisions and regulations and use properly qualified staff for this purpose.

4.The certification agency shall provide certificate holders with the following information necessary in order to use their digital signatures securely and correctly:

a. The duties of the certificate holder and the certification agency;
b. The procedure for the affixture and confirmation of a digital signature;
c. The advisability of placing a further digital signature on documents, which already bear a digital signature, in certain technical circumstances.

5.Certification agencies shall create and maintain a permanently up-dated computer record of the certificates issued, suspended or revoked, which shall be accessible to any person, wishing to consult it, including consultation by means of telecommunication. The said record shall be protected against unauthorised alterations.

Article 30
The contents of certificates

1. Signature certificates shall contain, at least, the following information:

a. The name or company name of the signature holder, together with other information necessary to identify the holder clearly and, when there are powers of representation, the name of the holder´s authorised representative or representatives, or the distinctive pseudonym of the signature holder, which shall be clearly identified as such;
b. The name and digital signature of the certification agency, as well as the country where it is established;
c. The public key, which corresponds to the private key held by the holder;
d. The certificate series number;
e. The certificate commencement and expiry dates;
f. The identifiers of the algorithms necessary in order to use the holder´s public key and the certification agency´s public key;
g. Whether the use of the key is restricted to certain types of use, together with any restrictions on the value of transactions for which the certificate is valid;
h. Contractual exclusions of the certification agency´s liability, without prejudice to the provisions of nr. 2 of article 27;
i. Any reference to any specific capacity of the signature holder, as a consequence of the use for which the certificate is intended.

2. Complementary information may be included in signature certificates or complementary certificates, at the holders request, regarding powers of representation granted to the holder by a third party, his or her professional status or other matters, upon production of proof thereof or with the inclusion of a note to the effect that the said information has not been confirmed.

Article 31
Suspension and revocation of certificates

1. Certification agencies shall suspend certificates:

a. On the written request of the holder, being properly identified for the purpose;
b. When there are grounds to believe that the certificate was issued on the basis of incorrect or false information, that the information contained therein is no longer accurate or that the confidentiality of the private key has been compromised.

2. Suspension on one of the grounds envisaged in paragraph b) of the preceding number shall always be explained and notified to the holder promptly and be included in the certificate record forthwith. The suspension may be lifted once the said grounds no longer apply.

3. The certification agency shall revoke certificates:

a. At the written request of the holder, who shall be duly identified;
b. When it is confirmed, following the suspension of a certificate, that it was issued on the basis of incorrect or false information, that the information contained therein is no longer true or that the confidentiality of the private key has been compromised;
c. When the certification agency ceases trading without having first transferred its documentation to the other certification agency;
d. When the licensing authority orders the revocation of the certificate on stated legal grounds;
e. At the expiry of the certificate validity period;
f. When it has notice of the death, legal disability or incapacity of a natural person or of the dissolution of a juristic person.

4. The grounds for decisions to revoke a certificate on one of the grounds envisaged in paragraphs b), c), d) and e) of nr. 3 shall always be stated and served, and registered forthwith.

5. The suspension and revocation of a certificate may be raised against third parties, as from the date on which the same are registered, unless it is proved that the third party already had notice thereof.

6. Certification agencies shall keep the information regarding certificates for 20 years, as from the suspension or revocation of each certificate and shall make it available to any interested parties.

7. The revocation or suspension of a certificate shall state the date and time from which it takes

effect. The said date and time shall not precede the date and time when the said information was made public.

8. No certificate, in respect of the same keys, shall be issued, by the same or another certification agency, as from the suspension or revocation of a certificate or the expiry of the validity period thereof.

Article 32
The holder´s duties

1. Certificate holders shall take all the technical and organisational steps necessary to prevent loss and damage to third parties and to protect the confidentiality of all information transmitted.

2. Holders shall apply for the suspension of the certificate, if it is suspected that the confidentiality of the private key has been compromised and shall apply that it be revoked, if the said compromise is confirmed.

3. Holders shall be prohibited from using a private key to generate a digital signature, once the certificate has been suspended or revoked or its validity period has expired.

4. Whenever there are proper grounds to revoke or suspend a certificate, the certificate holder shall make the corresponding suspension or revocation application to the certification agency, will all due diligence and speed.

CHAPTER IV
Supervision

Article 33
The duties of certification agencies to inform

1. Certification agencies shall promptly provide the licensing authority with full details of all the information requested by it for the purposes of the supervision of its business and shall permit it to inspect their premises and to examine documents, objects, hardware, software and operational procedures, on-site, to the same end. The licensing authority shall be entitled to make such copies and records as are necessary, during the said inspections.

2. Certification agencies, shall give notice of all relevant alterations to requirements and information in articles 13 and 15.

3. Certification agencies shall send an up-dated version of the lists referred to in paragraph b) of nr. 1 of article 13, by the last working day of each week, to the licensing authority.

Article 34
Official auditors and external auditors

The official auditors in the service of certification agencies and external auditors, which are required by law to provide the said agencies with audit services, shall notify the licensing authority of the serious breaches of the legal provisions or regulations, which are relevant to the supervision thereof, which they detect in the course of their duties.

Article 35
Appeals

In appeals against decisions taken by the licensing authority in the exercise of its licensing and supervisory powers, there shall be a rebuttable presumption that the suspension of the effect of the decision appealed against will seriously harm the public interest.

Article 36
Collaboration with the authorities

The licensing authority may request the police and judicial authorities and any other authorities and public departments to provide it with all such collaboration or assistance as it deems necessary, in order to licence and supervise certification business.

CHAPTER V
Final provisions

Article 37
Certificates issued in other countries

1. Digital signatures, which can be confirmed by a public key in a certificate issued or guaranteed by a certification agency in another member state of the European Union or in another State, which is party to an international agreement, which also binds the Portuguese State, shall be granted equivalent status to digital signatures certified in accordance with this decree-law.

2. The licensing authority shall, whenever possible, publicise the information at its disposal regarding certification agencies licensed in foreign States as it considers appropriate and shall, on request, provide interested parties with the said information.

Article 38
Regulations

1. The regulations of this decree-law, i.e. those regarding technical and security rules, shall be introduced in a regulamentary decree to be approved within 150 days.

2. The departments and agencies of the Civil Service may issue regulations regarding the requirements to be complied with by documents received electronically.

Article 39
Technological progress

The licensing authority shall monitor technological progress in the area of digital signatures, and may propose that the legal framework for digital signatures created by this decree-law, should apply to other forms of electronic signature, which comply with the same security and reliability requirements as such signatures.

Article 40
Designation of the licensing authority

The authority referred to in article 11 shall be appointed in a separate legislation, within 150 days.

Article 41
Commencement

This decree-law shall come into force on the day after the day on which it is published.

Checked and approved in the Council of Ministers on the 22nd of July 1999. - António Manuel de Oliveira Guterres - António Luciano Pacheco de Sousa Franco - José Eduardo Vera Cruz Jardim - José Mariano Rebelo Pires Gago. Promulgated on the 29th of July 1999. To be published. The President of the Republic, JORGE SAMPAIO. Approved on the 29th of July 1999. The Prime Minister, António Manuel de Oliveira Guterres.