Decree-Law no. 62/2003, of 3 of April

Published in the D.R. no. 79 (Series I-A), of 3 of April

This decree-law aims to align the legal regime for digital signatures established in Decree-Law no. 290-D/99 of 2 August to Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999, on a Community framework for electronic signatures.

In compliance with the above-mentioned directive and the recent legislative developments in Member States of the European Union, a technologically neutral terminology is used. The references that reflected an option for the prevailing technological model, digital signatures produced through cryptographic techniques, are thus deleted. The words “digital signature” are replaced, as appropriate, by “qualified electronic signature” or “qualified electronic signature certified by an accredited certified entity”. References made to “private keys” are replaced by “signature creation data” and references to “public keys” by “signature verification data”.

This decree-law establishes three modalities for electronic signatures: the electronic signature, the advanced electronic signature and the qualified electronic signature, which correspond to different levels of security and reliability.

Accordingly, new definitions are introduced in article 2, and duties of certifying entities that issue qualified certificates are reinforced. The assessment and certification of the compliance of electronic signature products used for the provision of services regarding qualified electronic signatures by a certified entity or for the creation or verification of qualified electronic signatures is assigned to certification bodies. Moreover, in order to ensure a better and larger supervision of these entities by certificate holders and third parties, a register of the accrediting authority is created, which, though it is to be considered as having no more than a declaratory value, is compulsory for certifying entities issuing qualified certificates.

The possibility of certifying entities that issue electronic signatures deemed to be specially secure and reliable, the qualified electronic signatures, requesting the accreditation thereof to the accrediting authority, is retained. Qualified electronic signatures issued by an accredited certified entity is of an equivalent evidential value to that of a private signed document, pursuant to article 376 of the Civil Code, whereas the remaining electronic signature modalities are to be taken into consideration freely in court.

The regime applicable to electronic signatures of legal persons is clarified in the sense that it is clearly stated the legal persons may hold a signature creation device. However, this decree-law does not establish, as far as the representation of legal persons is concerned, a regime different from the one resulting from the provisions governing this

issue. Within the adopted position of technology neutrality regarding the law, it is incumbent upon the certifying entity to assess if the signature ensures the intervention of the natural persons who, under the law or bylaws, represent the legal person.

The provisions as to certificates of other States are likewise amended, so as to ensure a free flow of electronic signature products within the internal market.

Nevertheless, the medium-term technological evolution shall determine the revision and adaptation of the regime established in this statutory instrument.

Therefore:

Pursuant to point a) of paragraph 1 of article 198 of the Constitution, the Government hereby decrees, to be effective as general law of the Republic, the following:

Article 1
Scope

This Decree-Law provides for the transposition to the national legal system of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

Article 2
Amendments to Decree-Law no. 290-D/99 of 2 August

Articles 1, 2, 3, 5, 6, 7, 8, 9, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 37, 38 and 39 of Decree-Law no. 290-D/99 of 2 August are hereby amended to read as follows:

«Article 1
[…]

This statutory instrument governs the validity, effectiveness and evidential value of electronic documents, electronic signatures and the certification activity of certifying entities resident in Portugal.

Article 2
[…]

For the purposes of this statutory instrument:
a) …
b) "Electronic signature" means the result of electronic data processing likely to be subject of an exclusive and individual right and to be used to make the author of the electronic document known;
c) "Advanced electronic signature" means an electronic signature which meets the following requirements:

i. It clearly identifies the signatory as the author of the document;
ii. The placing thereof on the document depends solely on the will of the author;

iii. It is created using means that the signatory can maintain under his exclusive control;
iv. It is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

d) “Digital signature” means a type of advanced electronic signature, based on an asymmetric cryptographic system, comprising an algorithm or series of algorithms, such that a pair of asymmetric, exclusive and interdependent keys is created, one of which is private while the other is public, allowing the author, on the one hand, to use the private key in order to claim authorship of the electronic document on which the signature is placed and to agree with the contents thereof, and the recipient, on the other hand, to use the public key to verify whether the signature was created through the corresponding private key and whether the initial electronic record has been altered since the signature was placed thereon;
e) [Former point d)].
f) [Former point e)].
g) “Qualified electronic signature” means a digital signature or another type of advanced electronic signature that meets the security requirements similar to those of the digital signature, based on a qualified certificate and created by means of a secure signature creation device;
h) "Signature creation data" means unique data, such as private keys, which are used by the signatory to create an electronic signature;
i) "Signature creation device" means configured software or hardware used to implement the signature creation data;
j) "Secure signature creation device" means a signature creation device which, by appropriate technical and procedural means, ensures that:

i. the signature creation data used for signature generation shall practically occur only once, and that their secrecy shall be reasonably assured;
ii. the signature creation data used for signature generation shall not, with reasonable assurance, be derived from other data and the signature shall be protected against forgery using currently available technology;
iii. the signature creation data used for signature generation shall be reliably protected by the legitimate signatory against the use of others;
iv. the data to be signed shall not be altered nor shall it be prevented from being presented to the signatory prior to the signature.

l) "Signature verification data" means data, such as public keys, which are used for the purpose of verifying an electronic signature;
m) “Accreditation” means the act through which the entity requesting it, entitled to provide certification services, is acknowledged to meet the requirements defined in this statutory instrument for the purposes provided for herein;
n) [Former point g)].
o) “Certifying entity” means an entity or a legal or natural person who creates or provides the means to create and verify signatures, issues certificates, ensures the publicity thereof or provides other services related to electronic signatures;
p) "Certificate" means an electronic attestation which links signature-verification data to the holder thereof and confirms the identity of that holder;

q) "Qualified certificate" means a certificate which meets the requirements laid down in Article 29 and is provided by a certifying entity who fulfils the requirements laid down in Article 24;
r) “Certificate holder” means a legal or natural person identified in a certificate as the owner of a signature creation device;
s) "Electronic signature product" means hardware or software, or relevant components thereof, which are intended to be used by a certifying entity for the provision of qualified electronic signature services or are intended to be used for the creation or verification of qualified electronic signatures;
t) “Certification body” shall mean the public or private entity responsible for the assessment and certification of the compliance of electronic signature processes, systems and products with the requirements referred to in point c) of paragraph 1 of article 12;
u) [Former point j)].
v) [Former point l)].

Article 3
[…]

1. …

2. Where an electronic document with the contents referred to in the preceding paragraph bears a qualified electronic signature certified by an accredited certifying entity, it shall be of an equivalent evidential value to that of a private signed document, pursuant to article 376 of the Civil Code.

3. Where an electronic document, the contents of which may not be represented in the form of a written statement, bears a qualified electronic signature certified by an accredited certifying entity, it shall be of an equivalent evidential value to that provided for in article 368 of the Civil Code and article 167 of the Criminal Procedure Code.

4. The provisions of the preceding paragraphs shall not prevent the use of further means of authorship and integrity evidence as regards electronic documents, including other types of electronic signature, provided that the said means are adopted by the parties pursuant to a valid evidence agreement or that they are accepted by the person against whom the document is presented.

5. Without prejudice to the provision of the preceding paragraph, the evidential value of electronic documents which do not bear a qualified electronic signature certified by an accredited certifying entity shall be assessed under the general terms of the law.

Article 5
[…]

1. Public bodies may issue electronic documents bearing a qualified electronic signature placed pursuant to the provisions of this statutory instrument.

2. …

Article 6
[…]

1. …

2. …

3. The transmission of an electronic document which bears a qualified electronic signature, by a means of telecommunications which ensure an effective reception, is equivalent to a delivery sent by registered letter service and, if the reception thereof is confirmed through a delivery certification message in the same form, addressed to the sender by the addressee, it is equivalent to a delivery by registered post with acknowledgement of receipt.

4. …

5. …

Article 7
Qualified electronic signature

1. The placing of a qualified electronic signature on an electronic document shall be equivalent to a handwritten signature on a printed document, the following presumptions being established:

a) The person who placed the qualified electronic signature is the holder thereof or the entitled representative of the legal person holder of the qualified electronic signature;
b) The qualified electronic signature was placed with the intention of signing the electronic document;
c) The electronic document has not been altered since the qualified electronic signature was placed therein.

2. The qualified electronic signature shall be uniquely linked to a single natural or legal person and to the document whereon it is placed.

3. The placing of a qualified electronic signature shall replace, in all the situations laid down by law, the affixing of seals, stamps, markings or further particulars identifying the holder thereof.

4. The placing of a qualified electronic signature on a certificate which is revoked, expired or suspended at the time of the signature or which does not comply with the conditions provided for therein shall be deemed to be equivalent to a lack of signature.

Article 8
Obtaining signature data and certificate

Whoever intends to use a qualified electronic signature shall generate or obtain the signature creation or verification data pursuant to paragraph 1 of article 28, and obtain the

respective certificate issued by a certifying entity, pursuant to the provisions of this statutory instrument.

Article 9
[…]

1. The activity of the certifying entity shall be freely exercised, being optional the accreditation request governed by articles 11 et seq.

2. Without prejudice to the provision of the preceding paragraph, the certifying entities issuing qualified certificates shall carry out the register thereof pursuant to the provisions to be determined through an administrative rule of the Minister for Justice.

3. The accreditation and register shall be subject to the payment of fees according to the costs linked to the correspondent administrative, technical, operational and supervising work, pursuant to the provisions to be determined through a joint order of the Ministers for Justice and for Finance, which shall be deemed as a revenue of the accrediting authority.

Article 11
[…]

The accreditation of certifying entities shall be incumbent upon the accrediting authority, for the purposes of this statutory instrument.

Article 12
[…]

1. Entities certifying qualified electronic signatures shall be granted accreditation, on presentation of a request to the accrediting authority, where they fulfill the following requirements:

a) …
b) to provide assurances of absolute integrity and independence in the pursuit of the certification activity of qualified electronic signatures;
c) to be provided with technical and human resources which meet the security and effectiveness standards provided for in the regulation referred to in article 39;
d) …

2. The accreditation shall be valid for a three-year period and it may be renewed for similar periods.

Article 13
[…]

1. The accreditation request of certifying entities shall attach the following particulars:

a) …
b) …
c) …

d) …
e) …
f) Evidence of the technical and human means required pursuant to the regulatory instrument referred to in point c) of paragraph 1 of article 12, including compliance certificates of the electronic signature products issued by an acknowledged certifying body accredited pursuant to article 37;
g) …
h) …
i) …
j) …

2. …

3. …

4. …

5. The accreditation renewal request shall attach the following particulars:

a) General activity program planned for the following three years;
b) General description of the activities performed for the last three years, as well as the financial statements of the corresponding financial years;
c) Declaration that all the particulars referred to in paragraph 1 of this article and in paragraphs 2 and 3 of article 32 have not been altered since the presentation thereof to the accrediting authority.

Article 14
[…]

1. Private certifying entities which are legal persons shall be provided with a share capital that must not be less than (Euro) 20000, or with an equivalent estate net worth, where such private entities are not companies.
2. …
3. …

Article 15
[…]

1. …
2. Amongst additional circumstances worthy of notice, the following shall be deemed to be indicative of unsuitability where the person concerned:

a) …
b) …
c) has been subject to penalties within the country or abroad, for failure to comply with legal or regulatory provisions that govern the activities regarding document issuing, authenticating, registering and storing, namely the activities associated to notary services, public registers, judicial administration, public libraries and certification of qualified electronic signatures.

3. The lack of suitability requirements provided for in this article shall constitute grounds for refusing or revoking the accreditation, pursuant to point c) of paragraph 1of article 18 and point f) of paragraph 1 of article 20.

Article 16
Compulsory civil liability insurance

(Former article 17).

Article 17
Decision

1. (Former paragraph 1 of article 18).

2. The decision on the accreditation request or the renewal thereof shall be notified to the interested parties within three months of receipt of the request or, where appropriate, of receipt of the solicited additional information or the completion of the arrangements deemed necessary; in no circumstances shall the decision exceed a six-month time limit after the date on which the request was received.

3. (Former paragraph 3 of article 18).

4. The accreditation shall be entered in the register referred to in paragraph 2 of article 9 and published in the Diário da República, II Series.

5. The accreditation decision shall be notified to the European Commission and other Member States of the European Union.

Article 18
Accreditation refusal

1. The accreditation may be refused where:

a) [Former point a) of article 19].
b) [(Former point b) of article 19].
c) The accrediting authority deems unfulfilled any of the requirements listed in articles 12 et seq.

2. (Former paragraph 2 of article 19).

Article 19
Accreditation expiry

1. The accreditation shall expire in the following cases:

a) Where the certification activity has commenced within 12 months of receipt of the accreditation notification;

b) As regards a legal person, where the dissolution thereof has occurred, without prejudice to the necessary proceedings involved in the respective winding-up;
c) As regards a natural person, upon death or declaration of interdiction or disability thereof;
d) Upon expiry of the validity period, where the accreditation renewal has not taken place.

2. The accreditation expiry shall be entered in the register referred to in paragraph 2 of article 9 and published in the Diário da República, II Series.

3. The accreditation expiry shall be notified to the European Commission and other Member States of the European Union.

Article 20
Revocation of Accreditation

1. Without prejudice to further penalties applicable under the law, the accreditation shall be revoked in the following cases:

a) [Former point a) of paragraph 1 of article 21].
b) [Former point b) of paragraph 1 of article 21].
c) [Former point c) of paragraph 1 of article 21].
d) [Former point d) of paragraph 1 of article 21].
e) [Former point e) of paragraph 1 of article 21].
f) [Former point f) of paragraph 1 of article 21].
g) Where the certificates issued by the certification body referred to in point f) of paragraph 1 of article 13 have been revoked.

2. (Former paragraph 2 of article 21).

3. The revocation decision shall be entered in the register referred to in paragraph 2 of article 9 and published in the Diário da República, II Series.

4. The revocation decision shall be notified to the European Commission and other Member States of the European Union.

Article 21
Irregularities of managing and supervising bodies

(Former article 22.)

Article 22
Notification of alterations

(Former article 23.)

Article 23
Registry of alterations

1. (Former paragraph 1 of article 24).

2. (Former paragraph 2 of article 24).

3. (Former paragraph 3 of article 24).

4. The registry shall be refused in case of unsuitability, pursuant to paragraph 15, the refusal being notified to the interested parties and to the certifying entity, which shall take the appropriate steps towards their immediate termination of service or the cessation of the relationship thereof, provided for in that article, with the legal person.

5. (Former paragraph 5 of article 24).

Article 24
Duties of the certifying entity issuing qualified certificates

It is incumbent upon the certifying entity issuing qualified certificates:

a) to fulfill the estate requirements established in article 14;
b) to provide assurances of absolute integrity and independence in the pursuit of the certification activity;
c) to demonstrate the reliability necessary for providing certification services;
d) to retain a valid insurance contract, for the appropriate coverage of the liability risks arising from the certification activity;
e) to be provided with technical and human resources which meet the security and effectiveness standards provided for in the regulatory instrument;
f) to use trustworthy systems and products which are protected against modification and ensure the technical security of the process supported by them;
g) to take measures against forgery or alteration of certificate data, and, in cases where the certifying entity generates signature creation data, to guarantee confidentiality during the generating process of such data;
h) to use trustworthy systems to store certificates so that:

i) certificates are publicly available for retrieval in only those cases for which the certificate holder's consent has been obtained;
ii) only authorized persons can make data entries and changes;
iii) information can be checked for authenticity;
iv) any technical changes compromising the security requirements are immediately apparent to the operator.

i) to strictly verify the identity of applicants holding certificates and, as regards the representatives of legal persons, the respective power of representation, as well as, if applicable, the specific attributes referred to in point i) of paragraph 1 of article 29;
j) to retain the particulars that prove the true identity of applicants with certificates bearing a pseudonym.
l) to inform the applicants in writing, accurately and clearly, of the qualified certificate issue process, as well as of the precise terms and conditions regarding the use of the qualified certificate, including any limitations on its use;
m) [Former point e) of article 25.]

n) not to store or copy signature creation data of the certificate holder to whom the certifying entity provided key management services;
o) to ensure the operation of a service that:

i) provides a prompt and secure directory of computerized entries of issued, revoked, suspended or expired certificates;
ii) ensures a secure and immediate certificate revocation, suspension or expiry service;

p) [Former point h) of article 25.]
q) [Former point j) of article 25.]
r) [Former point i) of article 25.]

Article 25
Data protection

1. Certifying entities may collect personal data only insofar as it is necessary for the purposes of the performance of the activities thereof, directly from the parties interested in holding the signature creation and verification data and respective certificates, or from authorized third parties.

2. (Former paragraph 2 of article 26.)

3. (Former paragraph 3 of article 26.)

4. (Former paragraph 4 of article 26.)

Article 26
Civil liability

1. The certifying entity shall be is subject to liability for injury or loss caused to certificate holders and third parties, as a result of non-compliance with the obligations arising under this statutory instrument and the regulations thereof, save if it is proved that such damages were not deliberately or negligently committed.

2. (Former paragraph 2 of article 27.)

Article 27
Termination of activity

1. If the certifying entity issuing qualified certificates contemplates terminating its activity on a voluntary basis, it shall so inform the accrediting authority and the persons who have been issued certificates remaining in force, at least three months in advance, indicating furthermore the certifying entity whereto the documentation or certificate revocation is to be transferred at the end of that period, and, in the latter case, where the certifying entity is accredited, it shall place the documentation under custody of the accrediting authority.

2. The certifying entity issuing qualified certificates being at risk of going bankrupt, of entering an undertaking rescue process or of terminating its activity, owing to

circumstances beyond its control, shall immediately notify the accrediting authority thereof.

3. (Former paragraph 3 of article 28.)

4. The termination of activity of the certifying entity issuing qualified certificates shall be entered in the register referred to in paragraph 2 of article 9 and published in the Diário da República, II Series.

5. The termination of activity of the certifying entity shall be notified to the European Commission and other Member States of the European Union.

Article 28
Issue of qualified certificates

1. At the request of an interested natural or legal person and in favour thereof, the certifying entity shall issue the signature creation and verification data, or where solicited, shall make available the necessary technical means for the creation thereof, having first checked, through a legally suitable and secure means, the identity and, where it exists, the power of representation of the applicant.

2. The certifying entity shall issue, at the request of the certificate holder, one or more duplicates of the certificate and of the complementary certificate.

3. (Former paragraph 3 of article 29.)

4. The certifying entity shall provide the certificate holders with the necessary informations for the correct and secure use of the signatures, namely the ones concerning:

a) [Former point a) of paragraph 4 of article 29.]
b) the procedure regarding signature placing and verification;
c) the desirability of documents bearing a signature being resigned in justified technical circumstances.

5. (Former paragraph 5 of article 29.)

Article 29
Contents of qualified certificates

1. Qualified certificates must contain at the least the following particulars:

a) [Former point a) of paragraph 1 of article 30.]
b) the identification of the certifying entity and the State in which it is established;
c) signature verification data which correspond to signature creation data under the control of the certificate holder;
d) [Former point d) of paragraph 1 of article 30.]
e) [Former point e) of paragraph 1 of article 30.]
f) Identification of algorithms used for the verification of the certificate holder's and certifying entity's signatures;

g) [Former point g) of paragraph 1 of article 30.]
h) Conventional limitations to the certifying entity's liability, without prejudice to the provision of paragraph 2 of article 26;
i) [Former point i) of paragraph 1 of article 30.]
j) an indication that the certificate is issued as a qualified certificate.

2. (Former paragraph 2 of article 30.)

Article 30
Suspension and revocation of qualified certificates

1. The certifying entity shall suspend the certificate:

a) At the request of the certificate holder, duly identified for the purpose;
b) Where there are reasonable grounds to believe that the certificate was issued based on false or misleading information, that it has ceased to conform to reality or that the confidentiality of signature creation data is not guaranteed.

2. (Former paragraph 2 of article 31.)

3. (Former main body of paragraph 3 of article 31.)

a) At the request of the certificate holder, duly identified for the purpose;
b) Where, upon the certificate suspension, it is confirmed that the certificate was issued based on false or misleading information, that it has ceased to conform to reality or that the confidentiality of signature creation data is not guaranteed;
c) [Former point c) of paragraph 3 of article 31].
d) [Former point d) of paragraph 3 of article 31].
e) [Former point l) of paragraph 3 of article 31].

1. The revocation decision based on the grounds established in points b), c) and d) of paragraph 3 shall be duly substantiated and immediately entered in the register, the certificate holder being notified thereof.

4. (Former paragraph 5 of article 31).

5. (Former paragraph 6 of article 31).

6. (Former paragraph 7 of article 31).

7. As from the suspension or revocation of a certificate or upon expiry of its validity period, the issue of a certificate concerning the same signature creation data by the same certifying entity or another is hereby prohibited.

Article 31
Obligations of the certificate holder

1. (Former paragraph 1 of article 32).

2. In cases of doubt as to the loss of confidentiality of signature creation data, the certificate holder shall request the certificate suspension, and upon confirmation of loss of confidentiality, the revocation thereof.

3. As from the suspension or revocation of a certificate or upon expiry of its validity period, the use by the certificate holder of the respective signature creation data to generate an electronic signature is hereby prohibited.

4. (Former paragraph 4 of article 32).

Article 32
Information duties of certifying entities

1. Certifying entities shall promptly and thoroughly provide the accrediting authority with the information requested for purposes of its activity supervision, granting permission for the inspection of its facilities and a local assessment of documents, objects, hardware and software equipment and operational procedures, in the course of which the accrediting authority may perform the necessary copies and registries.

2. Accredited certifying entities shall notify the accrediting authority, as soon as possible, of the relevant alterations that supervene upon the requirements and particulars referred to in articles 13 and 15.

3. By the last working day of each six-month period, certifying entities must have forwarded the accrediting authority an updated version of the schedules referred to in point b) of paragraph 1 of article 13.

Article 33
Security auditor

1. Certifying entities issuing qualified certificates shall be audited by a security auditor who complies with the requirements established in the regulatory instrument referred to in article 39.

2. The security auditor shall elaborate a security annual report that shall be submitted to the accrediting entity up to 31 March of each calendar year.

Article 37
Certification bodies

The compliance of electronic signature products with the technical requirements referred to in point c) of paragraph 1of article 12 shall be assessed and certified by:

a) Certification body accredited within the Portuguese Quality System;
b) Certification body accredited within the UE (European Cooperation for Accreditation), the respective acknowledgement being established by the competent entity of the Portuguese Quality System for Accreditation;

c) Certification body appointed by other Member States and notified to the European Commission pursuant to point b) of paragraph 1 of article 11 of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999.

Article 38
Certificates issued in other States

1. Qualified electronic signatures certified by a certifying entity accredited in another Member State of the European Union shall be recognized as legally equivalent to qualified electronic signatures certified by a certifying entity accredited pursuant to this statutory instrument.

2. Qualified certificates issued by a certifying entity which is subject to a supervision system under another Member State of the European Union shall be recognized as legally equivalent to qualified certificates issued by a certifying entity established in Portugal.

3. Qualified certificates which are issued by certifying entities established in third countries shall be recognized as legally equivalent to qualified certificates issued by a certifying entity established in Portugal, to the extent that one of the following circumstances occurs:

a) The certifying entity fulfils the requirements laid down in Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 and has been accredited under an accreditation scheme established in a Member State of the European Union;
b) The certificate is guaranteed by a certifying entity established within the European Union which fulfils the requirements laid down in this Directive;
c) the certificate or the certifying entity is recognized under an international agreement that binds the Portuguese State.

4. (Former paragraph 2 of article 37.)

Article 39
Regulatory provisions

(Former article 38.)»

Article 3
Amendment of the epigraph of chapter II of
Decree-Law no. 290-D/99, of 2 August

The epigraph of chapter II of Decree-Law no. 290-D/99, of 2 August, is hereby amended to read as follows:

«CHAPTER II
Qualified electronic signatures»

Article 4
Repealing provision

Article 39 of Decree-Law no. 290-D/99, of 2 August, is hereby repealed.

Article 5
Republication

Decree-Law no. 290-D/99, of 2 August, with the amendments introduced hereto, is hereby republished in annex to this decree-law, of which it is deemed to be an integral part.

Article 6
Entry into force

This statutory instrument shall enter into force on the day following its publication.
Checked and approved in the Council of Ministers of 29 January 2003. – José Manuel Durão Barroso – Maria Manuela Dias Ferreira Leite – António Manuel de Mendonça Martins da Cruz – Maria Celeste Ferreira Lopes Cardona – Nuno Albuquerque Morais Sarmento – Pedro Lynce de Faria.

Promulgated on 20 March 2003.
Let it be published.
The President of the Republic, JORGE SAMPAIO.
Counter-signed on 24 March 2003.
The Prime Minister, José Manuel Durão Barroso.

ANNEX
Decree-Law no. 290-D/99, of 2 August
(legal regime for electronic documents and electronic signatures)

CHAPTER I
Electronic documents and legal acts

Article 1
Scope

This statutory instrument governs the validity, effectiveness and evidential value of electronic documents, electronic signatures and the certification activity of certifying entities resident in Portugal.

Article 2
Definitions

For the purpose of this statutory instrument:
a) “Electronic document” means a document created through electronic data processing;
b) "Electronic signature" means the result of electronic data processing likely to be subject of an exclusive and individual right and to be used to make the author of the electronic document known;
c) "Advanced electronic signature" means an electronic signature which meets the following requirements:

i) It clearly identifies the signatory as the author of the document;
ii) The placing thereof on the document depends solely on the will of the author;
iii) It is created using means that the signatory can maintain under his exclusive control;
iv) It is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

d) “Digital signature” means a type of advanced electronic signature, based on an asymmetric cryptographic system, comprising an algorithm or series of algorithms, such that a pair of asymmetric, exclusive and interdependent keys is created, one of which is private while the other is public, allowing the author, on the one hand, to use the private key in order to claim authorship of the electronic document on which the signature is placed and to agree with the contents thereof, and the recipient, on the other hand, to use the public key to verify whether the signature was created through the corresponding private key and whether the initial electronic record has been altered since the signature was placed thereon;
e) “Private key” means one the elements of the pair of asymmetric keys intended to be known to the holder thereof alone, through which the digital signature is placed upon the electronic document, or an electronic document previously encrypted with the corresponding public key is decrypted;
f) “Public key” means the other element of the pair of asymmetric keys intended to be disclosed to the public, through which the digital signature placed on the electronic document by the holder of the asymmetric pair of keys is verified, or an electronic document to be forwarded to the mentioned pair of keys holder is encrypted;
g) “Qualified electronic signature” means a digital signature or another type of advanced electronic signature that meets the security requirements similar to those of the digital signature, based on a qualified certificate and created by means of a secure signature creation device;
h) "Signature creation data" means unique data, such as private keys, which are used by the signatory to create an electronic signature;
i) "Signature creation device" means configured software or hardware used to implement the signature creation data;
j) "Secure signature creation device" means a signature creation device which, by appropriate technical and procedural means, ensures that:

i) the signature creation data used for signature generation shall practically occur only once, and that their secrecy shall be reasonably assured;
ii) the signature creation data used for signature generation shall not, with reasonable assurance, be derived from other data and the signature shall be protected against forgery using currently available technology;
iii) the signature creation data used for signature generation shall be reliably protected by the legitimate signatory against the use of others;
iv) the data to be signed shall not be altered nor shall it be prevented from being presented to the signatory prior to the signature.

l) "Signature verification data" means data, such as public keys, which are used for the purpose of verifying an electronic signature;

m) “Accreditation” means the act through which the entity requesting it, entitled to provide certification services, is acknowledged to meet the requirements defined in this statutory instrument for the purposes provided for herein;
n) “Accrediting authority” means the entity responsible for the accreditation and supervision of certifying entities;
o) “Certifying entity” means an entity or a legal or natural person who creates or provides the means to create and verify signatures, issues certificates, ensures the publicity thereof or provides other services related to electronic signatures;
p) "Certificate" means an electronic attestation which links signature-verification data to the holder thereof and confirms the identity of that holder;
q) "Qualified certificate" means a certificate which meets the requirements laid down in Article 29 and is provided by a certifying entity who fulfils the requirements laid down in Article 24;
r) “Certificate holder” means a legal or natural person identified in a certificate as the owner of a signature creation device;
s) "Electronic signature product" means hardware or software, or relevant components thereof, which are intended to be used by a certifying entity for the provision of qualified electronic signature services or are intended to be used for the creation or verification of qualified electronic signatures;
t) “Certification body” shall mean the public or private entity responsible for the assessment and certification of the compliance of electronic signature processes, systems and products with the requirements referred to in point c) of paragraph 1 of article 12;
u) “Chronological validation” means a statement of assurance on the part of the certifying entity as to the date and hour of the creation, sending or receiving of an electronic document;
v) “E-mail address” means the identification of the appropriate computer equipment to receive and store electronic documents.

Article 3
Form and evidential value

1. The electronic document shall fulfill the legal written form requirement where its contents are liable to be provided in a written statement.

2. Where an electronic document with the contents referred to in the preceding paragraph bears a qualified electronic signature certified by an accredited certifying entity, it shall be of an equivalent evidential value to that of a private signed document, pursuant to article 376 of the Civil Code.

3. Where an electronic document, the contents of which may not be represented in the form of a written statement, bears a qualified electronic signature certified by an accredited certifying entity, it shall be of an equivalent evidential value to that provided for in article 368 of the Civil Code and article 167 of the Criminal Procedure Code.

4. The provisions of the preceding paragraphs shall not prevent the use of further means of authorship and integrity evidence as regards electronic documents, including other types of electronic signature, provided that the said means are adopted by the parties

pursuant to a valid evidence agreement or that they are accepted by the person against whom the document is presented.

5. Without prejudice to the provision of the preceding paragraph, the evidential value of electronic documents which do not bear a qualified electronic signature certified by an accredited certifying entity shall be assessed under the general terms of the law.

Article 4
Copies of documents

Copies of electronic documents, whether in the same medium or not, shall be valid and effective pursuant to general law, and enjoy the same evidential value as photocopies, pursuant to paragraph 2 of article 387 of the Civil Code and to article 168 of the Criminal Procedure Code, where the requirements provided therein are complied with.

Article 5
Electronic documents issued by public bodies

1. Public bodies may issue electronic documents bearing a qualified electronic signature placed pursuant to the provisions of this statutory instrument.

2. Regarding operations that concern the creation, issue, storage, storage, reproduction, copying and transmission of electronic documents, which formalize administrative acts through computer systems, including the transmission thereof by telecommunications means, the data relating to the interested body and the person who practiced each administrative act shall be indicated in readily identifiable language and in such a manner that it may confirm the functions or position of each document's signatory.

Article 6
Transmission of electronic documents

1. The electronic document transmitted through a telecommunications means shall be deemed as sent and received by the recipient where it is forwarded to the e-mail address agreed between the parties and received therein.

2. The date and hour of creation, sending and receiving of an electronic document bearing a chronological validation issued by a certifying entity are enforceable between the parties and may be relied upon against third parties.

3. The transmission of an electronic document which bears a qualified electronic signature, by a means of telecommunications which ensure an effective reception, is equivalent to a delivery sent by registered letter service and, if the reception thereof is confirmed through a delivery certification message in the same form, addressed to the sender by the recipient, it is equivalent to a delivery by registered post with acknowledgement of receipt.

4. Data and documents transmitted through telecommunication means are deemed to be in the possession of the sender up to the reception thereof by the recipient.

5. Operators ensuring the transmission of electronic documents through telecommunication means shall not have access to the contents thereof, not shall they duplicate them by any means or transfer to third parties any information, even in summary or excerpts, on the existence or contents of those documents, save where the information, given their nature or by an explicit indication on the part of the sender, is intended to be disclosed.

CHAPTER II
Qualified electronic signatures

Article 7
Qualified electronic signature

1. The placing of a qualified electronic signature on an electronic document shall be equivalent to a handwritten signature on a printed document, the following presumptions being established:

a) The person who placed the qualified electronic signature is the holder thereof or the entitled representative of the legal person holder of the qualified electronic signature;
b) The qualified electronic signature was placed with the intention of signing the electronic document;
c) The electronic document has not been altered since the qualified electronic signature was placed therein.

2. The qualified electronic signature shall be uniquely linked to a single natural or legal person and to the document whereon it is placed.

3. The placing of a qualified electronic signature shall replace, in all the situations laid down by law, the affixing of seals, stamps, markings or further particulars identifying the holder thereof.

4. The placing of a qualified electronic signature on a certificate which is revoked, expired or suspended at the time of the signature or which does not comply with the conditions provided for therein shall be deemed to be equivalent to a lack of signature.

Article 8
Obtaining signature data and certificate

Whoever intends to use a qualified electronic signature shall generate or obtain the signature creation or verification data pursuant to paragraph 1 of article 28, and obtain the respective certificate issued by a certifying entity, pursuant to the provisions of this statutory instrument.

CHAPTER III
Certification

SECTION I
Pursuit of the certification activity

Article 9
Free pursuit of the certification activity

1. The activity of the certifying entity shall be freely pursued, being optional the accreditation request governed by articles 11 et seq.

2. Without prejudice to the provision of the preceding paragraph, the certifying entities issuing qualified certificates shall carry out the register thereof pursuant to the provisions to be determined through an administrative rule of the Minister for Justice.

3. The accreditation and register shall be subject to the payment of fees according to the costs linked to the correspondent administrative, technical, operational and supervising work, pursuant to the provisions to be determined through a joint order of the Ministers for Justice and for Finance, which shall be deemed as a revenue of the accrediting authority.

Article 10
Free choice of the certifying entity

1. The choice of a certifying entity shall be free.

2. The choice of a specific entity shall not be a condition for the offer or conclusion of any legal commitment.

Article 11
Competent entity on accreditation

The accreditation of certifying entities shall be incumbent upon the accrediting authority, for the purposes of this statutory instrument.

Article 12
Accreditation of the certifying entity

1. Entities certifying qualified electronic signatures shall be granted accreditation, upon a request submitted to the accrediting authority, where they fulfill the following requirements:

a) to be provided with adequate capital and financial resources;
b) to provide assurances of absolute integrity and independence in the pursuit of the certification activity of qualified electronic signatures;
c) to be provided with technical and human resources which meet the security and effectiveness standards provided for in the regulation referred to in article 39;
d) to retain a valid insurance contract, for the appropriate coverage of the liability risks arising from the certification activity.

2. The accreditation shall be valid for a three-year period and it may be renewed for similar periods.

Article 13
Accreditation request

1. The accreditation request of certifying entities shall attach the following particulars:

a) Bylaws of the legal person, and as regards a company, the respective statutes, or as regards a natural person, the respective identification and address;
b) As regards a company, a list of all partners, specifying the respective shares, as well as of the members of managing and supervising bodies, and as regards a limited company, a list of all shareholders with significant shares, whether direct or indirect;
c) Declarations signed by all natural and legal persons referred to in paragraph 1 of article 15 stating that they are not in any of the situations indicative of unsuitability described in paragraph 2 thereof;
d) Evidence of the available estate net worth and financial resources, and namely, as regards companies, of the fully paid-up capital;
e) Description of the internal organization and security plan;
f) Evidence of the technical and human means required pursuant to the regulatory instrument referred to in point c) of paragraph 1 of article 12, including compliance certificates of the electronic signature products issued by an acknowledged certifying body accredited pursuant to article 37;
g) Appointment of the security auditor;
h) General activity program planned for the first three years;
i) General description of the activities performed for the last three years, or in the course of the time elapsed since the establishment thereof, if less, as well as the financial statements of the corresponding financial years;
j) Evidence of a valid insurance contract, for the appropriate coverage of the liability risks arising from the certification activity.

2. Where, at the date of the request, the legal person is not yet established, the request shall attach the following particulars, replacing the provision of point a) of the preceding paragraph:

a) the minute of the meeting at which the establishment of the legal person was deliberated;
b) Draft of the bylaws or statutes;
c) Statement of commitment, signed by all founding members, indicating that at the act of establishment, and as a condition thereof, the estate required by law shall be fully paid-up.

3. The statements provided for in point c) of paragraph 1 may be submitted subsequently to the request, in compliance with the determinations and time limit to be settled by the accrediting authority.

4. For the purposes of this statutory instrument, significant shares shall mean those which reach or exceed 10% of the limited company's capital.

5. The accreditation renewal request shall attach the following particulars:

a) General activity program planned for the following three years;
b) General description of the activities performed for the last three years, as well as the financial statements of the corresponding financial years;

c) Declaration that all the particulars referred to in paragraph 1 of this article and in paragraphs 2 and 3 of article 32 have not been altered since the presentation thereof to the accrediting authority.

Article 14
Estate requirements

1. Private certifying entities which are legal persons shall be provided with a share capital that must not be less than (Euro) 20000, or with an equivalent estate net worth, where such private entities are not companies.

2. The estate, and namely the company's minimum share capital shall be fully paid up at the date of accreditation, where the legal person is already established, or at the establishment of the legal person, where it takes place subsequently to the accreditation.

3. Certifying entities which are natural persons shall possess and maintain, in the course of their activity, an estate net worth equivalent to that provided for in paragraph 1, free of any liabilities.

Article 15
Suitability requirements

4. The natural person, or where a legal person is concerned, the members of the managing and supervising bodies, employees, agents and representatives of certifying entities with access to certifying acts or instruments, the partners of companies and, as regards limited companies, the shareholders thereof with significant shares, shall be persons of acknowledged suitability.

5. Amongst additional circumstances worthy of notice, the following shall be deemed to be indicative of unsuitability where the person concerned:

a) Has been convicted, in Portugal or abroad, of theft, robbery, swindling, computer or communication swindling, extortion, breach of public trust, infidelity, forgery, supply of false statements, deliberate bankruptcy, negligent bankruptcy, unduly favourable treatment of creditors, bounced cheques issue, misuse of guarantee or credit card, illegitimate appropriation of assets of public or cooperative sectors, harmful mismanagement of an economic unit of public or cooperative sectors, usury, bribery, corruption, unauthorized receiving of deposits and other repayable funds, unlawful acts or operations concerning insurance or pension funds related activities, money laundering, insider trading, manipulation of securities markets or crime provided for in the Code of Commercial Companies;
b) Has been declared insolvent or bankrupt by national or foreign court decision, or deemed liable for the bankruptcy or insolvency of companies under his control, or whose managing or supervising bodies he was a member of;
c) has been subject to penalties, in Portugal or abroad, for failure to comply with legal or regulatory provisions that govern the activities regarding document issuing, authenticating, registering and storing, namely the activities associated to notary services, public registers, judicial administration, public libraries and certification of qualified electronic signatures.

6. The lack of suitability requirements provided for in this article shall constitute grounds for refusing or revoking the accreditation, pursuant to point c) of paragraph 1of article 18 and point f) of paragraph 1 of article 20.

Article 16
Compulsory civil liability insurance

The Minister for Finances shall determine, through an administrative order, the features of the civil liability insurance contract referred to in point d) of article 12.

Article 17
Decision

1. The accrediting authority may request from applicants the necessary additional informations and perform or order any checks, questioning and inspections which are deemed necessary for the assessment of the request.

2. The decision on the accreditation request or the renewal thereof shall be notified to the interested parties within three months of receipt of the request or, where appropriate, of receipt of the solicited additional information or the completion of the arrangements deemed necessary; in no circumstances shall the decision exceed a six-month time limit after the date on which the request was received.

3. The accrediting authority may include additional conditions on the accreditation, to the extent that they are deemed necessary to ensure compliance with legal or regulatory provisions applicable to the pursuit of the activity of the certifying entity.

4. The accreditation shall be entered in the register referred to in paragraph 2 of article 9 and published in the Diário da República, II Series.

5. The accreditation decision shall be notified to the European Commission and other Member States of the European Union.

Article 18
Accreditation refusal

1. The accreditation may be refused where:

a) The request has not attached all necessary information and documents;
b) The particulars attached to the request are misleading or false;
c) The accrediting authority deems unfulfilled any of the requirements listed in articles 12 et seq.

2. Where the particulars attached are defective, the accrediting authority, prior to the refusal of accreditation, shall notify the applicant to correct the defects, granting for the purpose a reasonable time in which to do so.

Article 19

Accreditation expiry

1. The accreditation shall expire in the following cases:

a) Where the certification activity has commenced within 12 months of receipt of the accreditation notification;
b) As regards a legal person, where the dissolution thereof has occurred, without prejudice to the necessary proceedings involved in the respective winding-up;
c) As regards a natural person, upon death or declaration of interdiction or disability thereof;
d) Upon expiry of the validity period, where the accreditation renewal has not taken place.

2. The accreditation expiry shall be entered in the register referred to in paragraph 2 of article 9 and published in the Diário da República, II Series.

3. The accreditation expiry shall be notified to the European Commission and other Member States of the European Union.

Article 20
Revocation of Accreditation

1. Without prejudice to further penalties applicable under the law, the accreditation shall be revoked in the following cases:

a) Where it is granted through the supply of false declarations or other unlawful means;
b) Where any of the requirements listed in article 12 have ceased to be fulfilled;
c) Where the entity has terminated the certification activity or reduced it to an insignificant level for more than 12 months;
d) Where serious irregularities are detected as to the entity's management, organization or internal supervision;
e) Where, in the pursuit of the certification activity or of other social activity, unlawful acts are performed which harm or jeopardize public trust in the accreditation;
f) Where any of the unsuitability circumstances referred to in article 15 supervenes regarding any of the persons mentioned in paragraph 1 thereof;
g) Where the certificates issued by the certification body referred to in point f) of paragraph 1 of article 13 have been revoked.

2. The revocation of the accreditation is incumbent upon the accrediting authority, through a reasoned decision which shall be notified to the entity within eight working days.

3. The revocation decision shall be entered in the register referred to in paragraph 2 of article 9 and published in the Diário da República, II Series.

4. The revocation decision shall be notified to the European Commission and other Member States of the European Union.

Article 21
Irregularities of managing and supervising bodies

1. Where, for any reason, cease to be fulfilled the requirements imposed by law and bylaws as to the normal functioning of managing and supervising bodies, the accrediting authority shall determine a period of time within which the situation is to be rectified.

2. The accreditation shall be revoked where the situation is not rectified within the determined period of time, pursuant to the preceding paragraph.

Article 22
Notification of alterations

The accrediting authority shall be notified, within 30 days, of alterations of certifying entities issuing qualified certificates, regarding:

a) Legal form or name;
b) Scope;
c) Head office address, save if the change takes place within the same or to a neighbouring municipality;
d) Estate or property, provided it is a significant alteration;
e) Management and supervisory structure;
f) Restriction of the powers of managing and supervising bodies;
g) Demerger, merger and dissolution.

Article 23
Registry of alterations

1. The register of the persons referred to in paragraph 1 of article 15 shall be solicited of the accrediting authority within 15 days after the positions referred therein have been undertaken, through a request of the certifying entity or of the interested parties, attaching thereto the evidence as to the fulfilled requirements determined therein, failing which the accreditation shall be revoked.

2. The certifying entity or the interested parties may solicit a provisional register, prior to their undertaking of the positions referred to in paragraph 1 of article 15, the definite conversion being requested within 30 days from appointment, failing which the provisional register shall expire.

3. Where a reappointment takes place, it shall be endorsed in the register, at the request of the certifying entity or interested parties.

4. The registry shall be refused in case of unsuitability, pursuant to paragraph 15, the refusal being notified to the interested parties and to the certifying entity, which shall take the appropriate steps towards their immediate termination of service or the cessation of the relationship thereof, provided for in that article, with the legal person.

5. Without prejudice to other legal provisions, the absence of register shall not determine in itself the voidness of legal acts performed by the person concerned in the exercise of his duties.

SECTION II

Pursuit of activity

Article 24
Duties of the certifying entity issuing qualified certificates

It is incumbent upon the certifying entity issuing qualified certificates:

a) to fulfill the estate requirements established in article 14;
b) to provide assurances of absolute integrity and independence in the pursuit of the certification activity;
c) to demonstrate the reliability necessary for providing certification services;
d) to retain a valid insurance contract, for the appropriate coverage of the liability risks arising from the certification activity;
e) to be provided with technical and human resources which meet the security and effectiveness standards provided for in the regulatory instrument;
f) to use trustworthy systems and products which are protected against modification and ensure the technical security of the process supported by them;
g) to take measures against forgery or alteration of certificate data, and, in cases where the certifying entity generates signature creation data, to guarantee confidentiality during the generating process of such data;
h) to use trustworthy systems to store certificates so that:

i) certificates are publicly available for retrieval in only those cases for which the certificate holder's consent has been obtained;
ii) only authorized persons can make data entries and changes;
iii) information can be checked for authenticity;
iv) any technical changes compromising the security requirements are immediately apparent to the operator.

i) to strictly verify the identity of applicants holding certificates and, as regards the representatives of legal persons, the respective power of representation, as well as, if applicable, the specific attributes referred to in point i) of paragraph 1 of article 29;
j) to retain the particulars that prove the true identity of applicants with certificates bearing a pseudonym;
l) to inform the applicants in writing, accurately and clearly, of the qualified certificate issue process, as well as of the precise terms and conditions regarding the use of the qualified certificate, including any limitations on its use;
m) to comply with security standards for the processing of personal data established in the respective legislation;
n) not to store or copy signature creation data of the certificate holder to whom the certifying entity provided key management services;
o) to ensure the operation of a service that:

i) provides a prompt and secure directory of computerized entries of issued, revoked, suspended or expired certificates;
ii) ensures a secure and immediate certificate revocation, suspension or expiry service;

p) to stake steps for the immediate publication of the revocation or suspension of certificates, in the cases provided for in this statutory instrument;

q) to ensure that the date and hour of certificate issue, suspension and revocation may be determined through chronological validation;
r) to store issued certificates for no less than 20 years.

Article 25
Data protection

1. Certifying entities may collect personal data only insofar as it is necessary for the purposes of the performance of the activities thereof, directly from the parties interested in holding the signature creation and verification data and respective certificates, or from authorized third parties.

2. Personal data collected by the certifying entity shall nor be used for other purposes than the certification, save if the law or the interested person provides an explicit consent thereto.

3. Certifying entities and the accrediting authority shall comply with the legal standards in force on the protection, processing and free flow of personal data and on the protection of privacy in the telecommunications sector.
4. Certifying entities shall notify the judicial authority, upon a legal order thereof, as to data relating to holders of certificates bearing a pseudonym, complying with the provision of article 182 of the Criminal Procedure Code, where applicable.

Article 26
Civil liability

1. The certifying entity shall be is subject to liability for injury or loss caused to certificate holders and third parties, as a result of non-compliance with the obligations arising under this statutory instrument and the regulations thereof, save if it is proved that such damages were not deliberately or negligently committed.

2. Conventions which provide for the exoneration or limitation of liability shall be void.

Article 27
Termination of activity

1. If the certifying entity issuing qualified certificates contemplates terminating its activity on a voluntary basis, it shall so inform the accrediting authority and the persons who have been issued certificates remaining in force, at least three months in advance, indicating furthermore the certifying entity whereto the documentation or certificate revocation is to be transferred at the end of that period, and, in the latter case, where the certifying entity is accredited, it shall place the documentation under custody of the accrediting authority.

2. The certifying entity issuing qualified certificates being at risk of going bankrupt, of entering an undertaking rescue process or of terminating its activity, owing to circumstances beyond its control, shall immediately notify the accrediting authority thereof.

3. In the case provided for in the preceding paragraph, where the certifying entity terminates its activity, the accrediting authority shall transfer the documentation thereof to another certifying entity, or, where such transfer is not possible, shall revoke issued certificates and store particulars of such certificates for the period of time to which the certifying entity was bound.

4. The termination of activity of the certifying entity issuing qualified certificates shall be entered in the register referred to in paragraph 2 of article 9 and published in the Diário da República, II Series.

5. The termination of activity of the certifying entity shall be notified to the European Commission and other Member States of the European Union.

SECTION III
Certificates

Article 28
Issue of qualified certificates

1. At the request of an interested natural or legal person and in favour thereof, the certifying entity shall issue the signature creation and verification data, or where solicited, shall make available the necessary technical means for the creation thereof, having first checked, through a legally suitable and secure means, the identity and, where it exists, the power of representation of the applicant.

2. The certifying entity shall issue, at the request of the certificate holder, one or more duplicates of the certificate and of the complementary certificate.

3. The certifying entity shall take adequate measures against forgery or alteration of certificates and ensure compliance with applicable legal and regulatory provisions, employing duly qualified staff for the purpose.

4. The certifying entity shall provide the certificate holders with the necessary informations for the correct and secure use of the signatures, namely the ones concerning:

a) The duties upon the certificate holder and the certifying entity;
b) the procedure regarding signature placing and verification;
c) the desirability of documents bearing a signature being resigned in justified technical circumstances.

5. The certifying entity shall organize and permanently update a computer register of issued, suspended and revoked certificates, which shall be publicly available for retrieval, including by telecommunication means, protected against unauthorized alterations.

Article 29
Contents of qualified certificates

1. Qualified certificates must contain at the least the following particulars:

a) name or designation of the signatory, and other particulars necessary for an unequivocal identification and, where there are powers of representation, the name of the qualified representative or representatives, or a pseudonym, which shall be clearly identified as such;
b) the identification of the certifying entity and the State in which it is established;
c) signature verification data which correspond to signature creation data under the control of the certificate holder;
d) identity code of the certificate;
e) indication of the beginning and end of the period of validity of the certificate;
f) identification of algorithms used for the verification of the certificate holder's and certifying entity's signatures;
g) indication as to possible limitations on the scope of use of the certificate, as well on the value of transactions for which the certificate can be used;
h) Conventional limitations to the certifying entity's liability, without prejudice to the provision of paragraph 2 of article 26;
i) provision for a specific attribute of the signatory, regarding the intended use of the certificate;
j) an indication that the certificate is issued as a qualified certificate.

2. At the request of the certificate holder, additional information may be included in the certificate or complementary certificate relating to the powers of representation granted by the certificate holder to third parties, to the professional qualifications thereof or other attributes, through the supply of the respective evidence, or by declaring these informations to be unconfirmed.

Article 30
Suspension and revocation of qualified certificates

1. The certifying entity shall suspend the certificate:

a) At the request of the certificate holder, duly identified for the purpose;
b) Where there are reasonable grounds to believe that the certificate was issued based on false or misleading information, that it has ceased to conform to reality or that the confidentiality of signature creation data is not guaranteed.

2. The suspension on the grounds provided for in point b) of the preceding paragraph shall be reasoned and promptly notified to the certificate holder, as well as entered in the certificate register, and shall be lifted where such grounds prove not to correspond to reality.

3. The certifying entity shall revoke the certificate:

a) At the request of the certificate holder, duly identified for the purpose;
b) Where, upon the certificate suspension, it is confirmed that the certificate was issued based on false or misleading information, that it has ceased to conform to reality or that the confidentiality of signature creation data is not guaranteed.
c) Where the certifying entity terminates its activities without first transferring the documentation thereof to another certifying entity;
d) Where the accrediting authority order the revocation of the certificate on legal grounds;

e) Where records were brought to the its attention demonstrating the death, interdiction or disability of the natural person or the extinction of the legal person.

4. The revocation decision based on the grounds established in points b), c) and d) of paragraph 3 shall be duly substantiated and immediately entered in the register, the certificate holder being notified thereof.

5. The certificate's suspension and revocation may be relied upon against third parties as from the entering on the respective register, save if it is proved that the grounds thereof were known thereto.

6. The certifying entity shall store the information concerning the certificates for no less than 20 years from the suspension or revocation of each certificate, making it available to any interested party.

7. The certificate's suspension and revocation shall state the date and hour from which they take effect; this may not be earlier than the date and hour where the information is disclosed to the public.

8. As from the suspension or revocation of a certificate or upon expiry of its validity period, the issue of a certificate concerning the same signature creation data by the same certifying entity or another is hereby prohibited.

Article 31
Obligations of the certificate holder

1. Certificate holders shall take all the technical and organizing steps deemed necessary to prevent injury to third parties and to protect the confidentiality of all transmitted information.

2. In cases of doubt as to the loss of confidentiality of signature creation data, the certificate holder shall request the certificate suspension, and upon confirmation of loss of confidentiality, the revocation thereof.

3. As from the suspension or revocation of a certificate or upon expiry of its validity period, the use by the certificate holder of the respective signature creation data to generate an electronic signature is hereby prohibited.

4. Where grounds exist for the certificate's revocation or suspension, the holder thereof shall request of the certifying entity the respective revocation or suspension, acting swiftly and with due care.

Article 32
Information duties of certifying entities

1. Certifying entities shall promptly and thoroughly provide the accrediting authority with the information requested for purposes of its activity supervision, granting permission for the inspection of its facilities and a local assessment of documents, objects, hardware

and software equipment and operational procedures, in the course of which the accrediting authority may perform the necessary copies and registries.

2. Accredited certifying entities shall notify the accrediting authority, as soon as possible, of the relevant alterations that supervene upon the requirements and particulars referred to in articles 13 and 15.

3. By the last working day of each six-month period, certifying entities must have forwarded the accrediting authority an updated version of the schedules referred to in point b) of paragraph 1 of article 13.

Article 33
Security auditor

1. Certifying entities issuing qualified certificates shall be audited by a security auditor who complies with the requirements established in the regulatory instrument referred to in article 39.

2. The security auditor shall elaborate a security annual report that shall be submitted to the accrediting entity up to 31 March of each calendar year.

Article 37
Certification bodies

The compliance of electronic signature products with the technical requirements referred to in point c) of paragraph 1of article 12 shall be assessed and certified by:

a) Certification body accredited within the Portuguese Quality System;
b) Certification body accredited within the UE (European Cooperation for Accreditation), the respective acknowledgement being established by the competent entity of the Portuguese Quality System for Accreditation;
c) Certification body appointed by other Member States and notified to the European Commission pursuant to point b) of paragraph 1 of article 11 of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999.

Article 38
Certificates issued in other States

1. Qualified electronic signatures certified by a certifying entity accredited in another Member State of the European Union shall be recognized as legally equivalent to qualified electronic signatures certified by a certifying entity accredited pursuant to this statutory instrument.

2. Qualified certificates issued by a certifying entity which is subject to a supervision system under another Member State of the European Union shall be recognized as legally equivalent to qualified certificates issued by a certifying entity established in Portugal.

3. Qualified certificates which are issued by certifying entities established in third countries shall be recognized as legally equivalent to qualified certificates issued by a certifying entity established in Portugal, to the extent that one of the following circumstances occurs:

a) The certifying entity fulfils the requirements laid down in Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 and has been accredited under an accreditation scheme established in a Member State of the European Union;
b) The certificate is guaranteed by a certifying entity established within the European Union which fulfils the requirements laid down in this Directive;
c) the certificate or the certifying entity is recognized under an international agreement that binds the Portuguese State.

4. The accrediting authority shall make known, where possible and through the publicity means deemed adequate, the information at its disposal regarding accredited certifying entities in foreign States, making them available for all interested parties.

Article 39
Regulatory provisions

1. The regulation of this statutory instrument, namely as regards technical and security standards, shall be provided for in a regulatory decree, to be adopted within 150 days.

2. Public Administration bodies and services may issue regulatory provisions as to requirements for documents received through electronic means.

Article 40
Appointment of accrediting authority

The appointment of the entity referred to in article 11 will be the subject of a separate statutory instrument, to be issued within 150 days.

Article 41
Entry into force

This statutory instrument shall enter into force on the day following its publication.