DISCLAIMER - Automatic translation: This document is an unofficial translation to facilitate the understanding of the university regulatory framework in Spain. The University is not responsible for it. The official version of this document is available in Spanish at the following link: BOE-A-2003-23399 Ley 59/2003, de 19 de diciembre, de firma electrónica.

NOTA ACLARATORIA – Traducción automática: *El presente documento es una traducción no oficial para facilitar a los interesados la comprensión del marco regulatorio universitario en España. La Universidad no se hace responsable de la misma. Puede consultar en castellano la versión oficial del presente documento en el siguiente enlace: BOE-A-2003-23399 Ley 59/2003, de 19 de diciembre, de firma electrónica.*

Law 59/2003, of December 19, 2003, on electronic signature.

Head of State
"BOE" No. 304, of December 20, 2003
Reference: BOE-A-2003-23399

INDEX

CONSOLIDATED TEXT
Last modification: November 12, 2020

Rule repealed, effective November 13, 2020, by the repealing provision.a) of Law 6/2020, of November 11, 2020.
Ref. BOE-A-2020-14046

JOHN CHARLES I

KING OF SPAIN

To all who see and understand this document.

Be it known: That the Cortes Generales have approved and I have come to sanction the following ley.

EXPLANATORY MEMORANDUM

Royal Decree Law 14/1999, of September 17, 1999, on electronic signatures, was approved with the aim of promoting the rapid incorporation of new security technologies for electronic communications in the activities of companies, citizens and public administrations. In this way, it helped to boost the growth and competitiveness of the Spanish economy through the rapid establishment of a legal framework for the use of a tool that provides confidence in the performance of electronic transactions in open networks such as the Internet. The aforementioned Royal Decree ley incorporated Directive 1999/93/EC of the European Parliament and of the Council of December 13, 1999, establishing a Community framework for electronic signatures into Spanish public law, even before its enactment and publication in the Official Journal of the European Communities.

After its ratification by the Congress of Deputies, it was agreed to process Royal Decree Law 14/1999 as a draft Law, in order to submit it to wider public consultation and subsequent parliamentary debate to perfect its text. However, this initiative lapsed when the mandate of the Chambers expired in March 2000. This Law, therefore, is the result of the commitment assumed in the VI Legislature, updating at the same time the framework established in Royal Decree Law 14/1999 by incorporating the modifications that the experience accumulated since its entry into force both in our country and in the international sphere advises.

The development of the information society and the dissemination of the positive effects derived from it require the generalization of public confidence in telematic communications. However, the most recent data indicate that there is still a lack of confidence on the part of those involved in telematic transactions and, in general, in the communications that the new technologies allow when transmitting information, and this lack of confidence constitutes a brake on the development of the information society, in particular, electronic administration and commerce.

In response to this need to confer security to communications over the Internet, the electronic signature, among others, has arisen. The electronic signature is an instrument capable of allowing verification of the origin and integrity of messages exchanged over telecommunication networks, providing the basis for avoiding repudiation, if appropriate measures are taken on the basis of electronic dates.

The parties that make the use of electronic signatures possible are the so-called certification service providers. For this purpose, they issue electronic certificates, which are

electronic documents that link the electronic signature tools held by each user with his or her personal identity, thus making him or her known in the telematic environment as a signatory.

The ley obliges certification service providers to carry out a permanent guardianship and management of the electronic certificates they issue. The details of this management must be included in the so-called certification practices statement, which specifies the conditions applicable to the request, issuance, use, suspension and termination of the validity of electronic certificates. In addition, these providers are obliged to maintain accessible a consultation service on the status of validity of the certificates in which it must be indicated in an updated way if they are in force or if their validity has been suspended or terminated.

It should also be noted that the ley defines a particular class of electronic certificates called qualified certificates, which are those electronic certificates that have been issued in compliance with qualified requirements as regards their content, the procedures for verifying the identity of the signatory and the reliability and guarantees of the electronic certification activity.

Qualified certificates are a fundamental part of the so-called qualified electronic signature, which is defined according to the guidelines imposed by Directive 1999/93/EC as the advanced electronic signature based on a qualified certificate and generated by means of a secure signature creation device. The ley grants to the qualified electronic signature the functional equivalence with the handwritten signature with respect to the data recorded in electronic form.

On the other hand, the ley contains the guarantees that must be complied with by signature creation devices in order to be considered as secure devices and thus form a recognized electronic signature.

The technical certification of secure electronic signature creation devices is based on the framework established by Law 21/1992, of July 16, 1992, on Industry and its implementing provisions. For this certification, the technical standards published for such purposes in the "Official Journal of the European Communities" or, exceptionally, those approved by the Ministry of Science and Technology will be used.

Additionally, the Law establishes a framework of obligations applicable to certification service providers, depending on whether they issue qualified certificates or not, and determines their liability regime, taking into account the duties of diligence incumbent on signatories and third parties to whom electronically signed documents are addressed.

This Law is enacted to reinforce the existing legal framework by incorporating into its text some new features with respect to Royal Decree Law 14/1999 that will contribute to boosting the market for the provision of certification services.

Thus, the terminology has been revised, the systematics have been modified and the text has been simplified, making it easier to understand and giving it a structure more in line with our legislative technique.

One of the novelties offered by the Law with respect to Royal Decree-Law 14/1999 is the denomination of the electronic signature as a recognized electronic signature, which is functionally equivalent to the handwritten signature. It is simply the creation of a new concept demanded by the sector, without implying any modification of the substantive requirements that both Directive 1999/93/EC and Royal Decree Law 14/1999 itself had been demanding. This clarifies that the advanced electronic signature is not enough to be equated with the handwritten signature; the advanced electronic signature must be based on a qualified certificate and must have been created by a secure creation device.

It is also worth mentioning the elimination of the registry of certification service providers, which has given way to the establishment of a mere service for the dissemination of information on the providers operating in the market, their quality certifications and the characteristics of the products and services they have for the development of their activity.

On the other hand, the Iey modifies the concept of certification of certification service providers to grant it a greater degree of freedom and give a greater role to the participation of the private sector in the certification systems and eliminating the legal presumptions associated with it, adapting it more precisely to the provisions of the directive. Thus, the self-regulation of the industry is favored, so that it can design and manage, according to its own needs, voluntary accreditation systems aimed at improving the technical and quality levels in the provision of certification services.

The new regime is based on the conviction that quality seals are an effective tool for convincing users of the advantages of electronic certification products and services, and that it is essential to facilitate and speed up the process of obtaining these external symbols for those who offer them to the public.

Although the concepts of "accreditation" of certification service providers and "conformity" of secure electronic signature creation devices contained in the Directive are faithfully reflected in the Law, the terminology has been adapted to the most commonly used and well-known terminology contained in Law 21/1992, of July 16, 1992, on Industry.

Another relevant modification is that the Law clarifies the obligation for certification service providers issuing recognized certificates to provide a financial guarantee, establishing a single minimum amount of three million euros, making the combination of the different instruments to provide the guarantee more flexible.

On the other hand, since the provision of certification services is not subject to prior authorization, it is important to note that the IEA strengthens the inspection and control capacities of the Ministry of Science and Technology, stating that this department may be assisted by independent and technically qualified entities to carry out supervision and control tasks on certification service providers.

Also noteworthy is the regulation contained in the Law with respect to the electronic national identity document, which is a recognized electronic certificate called to generalize the use of secure electronic communication instruments capable of conferring the same integrity and authenticity as that which currently surrounds communications by physical means. The Law limits itself to establishing the basic regulatory framework of the new electronic ID, highlighting its two most characteristic features - it accredits the identity of its holder in any administrative procedure and allows the electronic signature of documents - referring to the specific regulations regarding the particularities of its legal regime.

Another novelty is the establishment in the Law of the regime applicable to legal persons as signatories, for the purpose of integrating these entities in telematic traffic. This goes beyond the 1999 Royal Decree Law, which only allowed legal entities to be holders of electronic certificates in the field of tax management.

Precisely, the enormous expansion of these certificates in this area in recent years, without any increase in litigation or legal uncertainty in transactions, makes it advisable to generalize the ownership of certificates by legal entities.

In any case, the electronic certificates of legal entities do not alter the civil and mercantile legislation regarding the figure of the organic or voluntary representative and do not replace the electronic certificates issued to natural persons in which such representation relationships are reflected.

As a means of legal security, the Law requires, on the one hand, a special legitimacy for individuals to request the issuance of certificates; on the other hand, it obliges applicants to be responsible for the custody of the electronic signature creation data associated with such certificates, without prejudice to their use by other individuals linked to the entity. Finally, with regard to third parties, the use of these certificates is limited to the acts that are part of the relationship between the legal entity and the Public Administrations and to the things or services that constitute the ordinary business or traffic of the entity, without prejudice to the possible quantitative or qualitative limits that may be added. It is a matter of combining the dynamism that must preside over the use of these

The balance between one and the other principle has been established with respect to the things and services that constitute the ordinary course of business, parallel to how our more than century-old Code of Commerce regulates the binding of acts and services to third parties in the ordinary course of business. The balance between one and the other principle has been established on the things and services that constitute the ordinary line of business or traffic of the company in a parallel way to how our more than centenary Code of Commerce regulates the binding before third parties of the acts of commerce carried out by the factor of the establishment.

The expression "ordinary course of business" of an entity updates to a vocabulary more in line with our times what in Spanish mercantile legislation is called "manufacturing or mercantile establishment". This includes transactions carried out directly or immediately for the performance of the core business of the entity and the management or administrative activities necessary for the development of the same, such as the contracting of tangible and intangible supplies or auxiliary services. Finally, it should be emphasized that, although "ordinary business" is a term coined by commercial law, the regulation on certificates of legal persons applies not only to commercial companies, but to any type of legal person wishing to make use of electronic signatures in its activity.

Additionally, a special regime is added for the issuance of electronic certificates to unincorporated entities referred to in Article 33 of the General Tax Law, for the sole purpose of their use in the tax field, under the terms established by the Ministry of Finance.

On the other hand, following the guidelines established by Law 34/2002, of July 11, 2002, on information society services and electronic commerce, the support on which the electronically signed data are contained is included within the modality of documentary evidence, giving greater legal certainty to the use of the electronic signature by subjecting it to the rules of effectiveness in court of documentary evidence.

In addition, it should be noted that another novel aspect of the Law is the explicit acceptance of the representation relationships that may underlie the use of electronic signatures. There can be no doubt that the concept of representation is widely used in business transactions, hence the advisability of giving legal certainty to the imputation to the legal sphere of the principal of the declarations made by the representative by means of the electronic signature.

For this purpose, it is established as a novelty that in the issuance of recognized certificates that admit among their attributes representation relationships, the latter must be supported by a public document that reliably proves such representation relationship as well as the sufficiency and suitability of the powers conferred to the representative. Likewise, mechanisms are foreseen to ensure the maintenance of the powers of representation during the entire term of the recognized certificate.

Finally, it should be noted that the Law allows certification service providers, with the aim of improving confidence in their services, to establish coordination mechanisms with the data that must be kept in the public registries, in particular, by means of telematic connections, for the purpose of verifying the data contained in the certificates at the time they are issued.

Such coordination mechanisms may also include the telematic notification by the registries to the certification service providers of subsequent registry changes.

IV

The Law consists of 36 articles grouped in six titles, 10 additional provisions, two transitory provisions, one derogatory provision and three final provisions.

Title I contains the general principles that delimit the subjective and objective scope of application of the Law, the effects of the electronic signature and the regime of use before the Public Administrations and access to the activity of providing certification services.

The regime applicable to electronic certificates is contained in Title II, which devotes its first chapter to determining who may be their holders and to regulating the vicissitudes affecting their validity. Chapter II regulates the recognized certificates and the third chapter regulates the electronic national identity document.

Title III regulates the activity of providing certification services, establishing the obligations to which providers are subject - clearly distinguishing those that only affect those issuing recognized certificates - and the applicable liability regime.

Title IV establishes the requirements to be met by electronic signature creation and verification devices and the procedure to be followed to obtain quality seals in the activity of providing certification services.

Titles V and VI are devoted, respectively, to establishing the supervision and sanction regimes for certification service providers.

Finally, the text closes with the additional provisions, which refer to the special regimes that are preferentially applicable, the transitory provisions, which provide legal certainty to the activity carried out under the previous legislation, the derogatory provision and the final provisions relating to the constitutional basis, the authorization for regulatory development and the entry into force.

This provision has been subject to the information procedure on technical standards and regulations provided for in Directive 98/34/EC, of the European Parliament and of the Council, of June 22, 1998, laying down a procedure for the provision of information in the field of technical standards and regulations, as amended by Directive 98/48/EC, of the European Parliament and of the Council, of July 20, 1998, and in Royal Decree 1337/1999, of July 31, 1999, which regulates the provision of information on technical standards and regulations and regulations relating to information society services.

TITLE I

General Provisions

Article 1. *Object.*

1. This Law regulates electronic signatures, their legal effectiveness and the provision of certification services.

2. The provisions contained in this Law do not alter the rules relating to the conclusion, formalization, validity and effectiveness of contracts and any other legal acts, nor those relating to the documents in which they are recorded.

Article 2. *Certification service providers subject to the law.*

1. This Law shall apply to certification service providers established in Spain and to certification services that providers resident or domiciled in another State offer through a permanent establishment located in Spain.

2. A certification service provider is a natural or legal person that issues electronic certificates or provides other services related to electronic signatures.

3. It shall be understood that a certification service provider is established in Spain when its residence or registered office is located in Spanish territory, provided that these coincide with the place where the administrative management and direction of its business is effectively centralized. Otherwise, the place where such management or direction is carried out shall be taken into account.

4. A supplier will be considered to operate through a permanent establishment located in Spanish territory when he has there, on a continuous or habitual basis, installations or workplaces where he carries out all or part of his activity.

5. A certification service provider shall be presumed to be established in Spain when such certification service provider or any of its branches has been registered in the Commercial Registry or in any other Spanish public registry in which registration is required for the acquisition of legal personality.

The mere use of technological means located in Spain for the provision of or access to the service does not imply, by itself, the establishment of the provider in Spain.

Electronic signature and electronically signed documents.

1. The electronic signature is the set of data in electronic form, consigned together or associated with others, which can be used as a means of identification of the signatory.

2. An advanced electronic signature is an electronic signature that makes it possible to identify the signatory and to detect any subsequent changes to the signed data, that is uniquely linked to the signatory and to the data to which it refers, and that has been created by means that the signatory can use, with a high level of confidence, under his exclusive control.

3. A qualified electronic signature is an advanced electronic signature based on a qualified certificate and generated by means of a secure signature creation device.

4. A qualified electronic signature shall have the same value with respect to data recorded in electronic form as a handwritten signature has with respect to data recorded on paper.

5. An electronic document is information of any nature in electronic form, filed in an electronic support according to a specific format and susceptible of identification and differentiated treatment.

Without prejudice to the provisions of the preceding paragraph, for an electronic document to be considered a public document or an administrative document, it must comply, respectively, with the provisions of letters a) or b) of the following paragraph and, if applicable, with the specific applicable regulations.

6. The electronic document will be support of:

a) Public documents, because they are electronically signed by officials who have legally attributed the power to give public, judicial, notarial or administrative faith, provided that they act within the scope of their powers with the requirements of the ley in each case.

b) Documents issued and signed electronically by civil servants or public employees in the exercise of their public functions, in accordance with their specific legislation.

c) Private documents.

7. The documents referred to in the preceding paragraph shall have the value and legal effectiveness corresponding to their respective nature, in accordance with the applicable legislation.

8. The support on which the electronically signed data are contained shall be admissible as documentary evidence in court. If the authenticity of the qualified electronic signature with which the data included in the electronic document has been signed is challenged, it shall be verified that it is an advanced electronic signature based on a qualified certificate, which meets all the requirements and conditions established in this Law for this type of certificates, as well as that the signature has been generated by means of a secure electronic signature creation device.

The burden of carrying out the aforementioned verifications will correspond to the person who has presented the electronic document signed with a recognized electronic signature. If said verifications obtain a positive result, the authenticity of the recognized electronic signature with which said electronic document has been signed shall be presumed, and the costs, expenses and fees arising from the verification shall be borne exclusively by the person who has filed the challenge. If, in the opinion of the court, the challenge was reckless, it may also impose a fine of 120 to 600 euros.

If the authenticity of the advanced electronic signature, with which the data incorporated in the electronic document has been signed, is challenged, the provisions of Article 326(2) of the Civil Procedure Act shall apply.

9. An electronic signature that does not meet the requirements of a qualified electronic signature in relation to the data to which it is associated shall not be denied legal effect merely because it is in electronic form.

10. For the purposes of the provisions of this article, when an electronic signature is used in accordance with the terms agreed upon by the parties to relate to each other, the stipulations between them shall be taken into account.

11. All electronic identification and signature systems provided for in the Law on Common Administrative Procedure of Public Administrations and in the Law on the Legal Regime of the Public Sector shall have full legal effect.

Use of the electronic signature in the scope of the Public Administrations.

1. This Law shall apply to the use of the electronic signature within the Public Administrations, their public bodies and the entities dependent or linked to them and in the relations that they maintain among themselves or with individuals.

The public administrations, in order to safeguard the guarantees of each procedure, may establish additional conditions for the use of electronic signatures in the procedures. Such conditions may include, among others, the imposition of electronic dates on the electronic documents included in an administrative file. An electronic date is understood to be the set of data in electronic form used as a means of establishing the time at which an action has been carried out on other electronic data with which it is associated.

2. The additional conditions referred to in the previous paragraph may only refer to the specific characteristics of the application in question and must guarantee compliance with the provisions of Article 45 of Law 30/1992, of 26 November, on the Legal Regime of Public Administrations and Common Administrative Procedure. These conditions shall be objective, proportionate, transparent and non-discriminatory and shall not hinder the provision of certification services to the citizen when different national or European Economic Area public administrations are involved.

3. The rules establishing additional general conditions for the use of the electronic signature before the General State Administration, its public bodies and the entities dependent or linked to the same shall be issued at the joint proposal of the Ministries of Public Administrations and of Science and Technology and after a report from the Higher Council of Informatics and for the promotion of Electronic Administration.

4. The use of electronic signatures in communications involving classified information, public security or national defense shall be governed by their specific regulations.

Article 5. *Regime for the rendering of certification services.*

1. The provision of certification services is not subject to prior authorization and shall be carried out under free competition. No restrictions may be established for certification services coming from another Member State of the European Economic Area.

2. The competition authorities shall ensure the maintenance of conditions of effective competition in the provision of certification services to the public through the exercise of the functions legally attributed to them.

3. The provision of certification services to the public by public administrations, their public bodies or entities dependent or linked to them shall be carried out in accordance with the principles of objectivity, transparency and non-discrimination.

TITLE II

Electronic certificates

CHAPTER I

General Provisions

Article 6. *Concept of electronic certificate and signatory.*

1. An electronic certificate is a document signed electronically by a certification service provider that links signature verification data to a signatory and confirms the signatory's identity.

2. The signatory is the person who uses a signature creation device and who acts on his own behalf or on behalf of a natural or legal person he represents.

Article 7. *Electronic certificates of legal entities.*

1. The electronic certificates of legal entities may be requested by their administrators, legal representatives and volunteers with sufficient power of attorney for this purpose.

The electronic certificates of legal entities may not affect the organic or voluntary representation regime regulated by the civil or mercantile legislation applicable to each legal entity.

2. The custody of the signature creation data associated with each electronic certificate of a legal entity or, if applicable, of the means of access to them shall be the responsibility of the natural person requesting them, whose identification shall be included in the electronic certificate.

3. The signature creation data may only be used when it is admitted in the relations that the legal entity maintains with the public administrations or in the contracting of goods or services that are proper or concerning its ordinary line of business or traffic.

Likewise, the legal entity may impose additional limits, by reason of the amount or subject matter, for the use of such data, which, in any case, must appear in the electronic certificate.

4. Acts or contracts in which the signature of the legal entity has been used within the limits set forth in the preceding paragraph shall be deemed to have been performed by the legal entity.

If the signature is used in breach of the aforementioned limits, the legal entity shall be bound vis-à-vis third parties only if it assumes them as its own or if they have been concluded in its interest. Otherwise, the effects of such acts shall be borne by the natural person responsible for the custody of the signature creation data, who may, where appropriate, take action against the person who has used them.

5. The provisions of this article shall not apply to certificates used to verify the electronic signature of the certification service provider with which it signs the electronic certificates it issues.

6. The provisions of this article shall not apply to certificates issued in favor of public administrations, which shall be subject to their specific regulations.

Article 8. *Termination of the validity of the electronic certificates.*

1. These are causes for the termination of the validity of an electronic certificate:

a) Expiration of the validity period stated on the certificate.

b) Revocation formulated by the signatory, the natural or legal person represented by the signatory, an authorized third party or the natural person requesting an electronic certificate of a legal person.

c) Violation or compromise of the secrecy of the signature creation data of the signatory or the certification service provider or misuse of such data by a third party.

d) Judicial or administrative resolution ordering it.

e) Death or termination of the legal personality of the signatory; death or termination of the legal personality of the principal; total or partial incapacity of the signatory or of the principal; termination of the representation; dissolution of the represented legal entity or alteration of the conditions of custody or use of the signature creation data that are reflected in the certificates issued to a legal entity.

f} Cessation of the certification service provider's activity unless, with the signatory's express consent, the management of the electronic certificates issued by the certification service provider is transferred to another certification service provider.

g) Alteration of the data provided to obtain the certificate or modification of the circumstances verified for the issuance of the certificate, such as those related to the position or powers of representation, in such a way that the certificate no longer conforms to reality.

h) Any other lawful cause provided for in the certification practice statement.

2. The period of validity of the electronic certificates will be appropriate to the characteristics and technology used to generate the signature creation data. In the case of qualified certificates, this period shall not exceed five years.

3. The termination of the validity of an electronic certificate shall be effective against third parties, in the event of expiration of its validity period, from the time this circumstance occurs and, in other cases, from the time the indication of such termination is included in the consultation service on the validity of the certificates of the certification service provider.

Suspension of the validity of the electronic certificates.

1. The certification service providers shall suspend the validity of the electronic certificates issued if any of the following causes occur:

a) Application by the signatory, the natural or legal person represented by the signatory, an authorized third party or the natural person applying for a legal person's electronic certificate.

b) Judicial or administrative resolution ordering it.

c) The existence of well-founded doubts about the concurrence of the causes for termination of the validity of the certificates contemplated in paragraphs c) and g) of Article 8.1.

d) Any other lawful cause provided for in the certification practice statement.

2. The suspension of the validity of an electronic certificate shall take effect as soon as it is included in the certificate validity query service of the certification service provider.

Provisions common to the termination and suspension of the validity of electronic certificates.

1. The certification service provider shall immediately state, in a clear and unequivocal manner, the termination or suspension of the validity of the electronic certificates in the certificate validity query service as soon as it becomes aware of any of the facts determining the termination or suspension of their validity.

2. The certification service provider shall inform the signatory of this circumstance prior to or simultaneously with the termination or suspension of the validity of the electronic certificate, specifying the reasons and the date and time at which the certificate will be terminated. In cases of suspension, it shall also indicate its maximum duration, the validity of the certificate being extinguished if the suspension has not been lifted after this period has elapsed.

3. The termination or suspension of the validity of an electronic certificate shall not have retroactive effects.

4. The expiration or suspension of the validity of an electronic certificate shall remain accessible in the certificate validity query service at least until the date on which its initial period of validity has expired.

CHAPTER II

Recognized certificates

Article 11. *Concept and content of the recognized assignees.*

1. Qualified certificates are those electronic certificates issued by a certification services provider that meets the requirements established in this Law regarding the verification of the identity and other circumstances of the applicants and the reliability and guarantees of the certification services they provide.

2. The recognized certificates shall include, at least, the following data:

a) The indication that they are issued as such.

b) The unique identification code of the certificate.

c) The identification of the certification service provider issuing the certificate and its address.

d) The advanced electronic signature of the certification service provider issuing the certificate.

e) The identification of the signatory, in the case of natural persons, by their name and surname and their national identity card number or by means of a pseudonym that is unequivocally identified as such and, in the case of legal persons, by their name or company name and their tax identification code.

f) Signature verification data corresponding to the signature creation data under the signatory's control.

g) The beginning and end of the period of validity of the certificate.

h) The limits of use of the certificate, if established.

i) The limits on the value of transactions for which the certificate may be used, if established.

3. Qualified certificates may also contain any other circumstance or attribute specific to the signatory if it is significant in terms of the purpose of the certificate and provided that the signatory so requests.

4. If the recognized certificates admit a relation of representation, they shall include an indication of the public document that reliably certifies the signatory's powers to act on behalf of the person or entity he/she represents and, if registration is mandatory, the registration data, in accordance with Article 13.2.

Article 12. *Obligations prior to the issuance of recognized certificates.*

Prior to the issuance of a qualified certificate, certification service providers shall comply with the following obligations:

a) Verify the identity and personal circumstances of certificate applicants in accordance with the provisions of the following article.

b) Verify that the information contained in the certificate is accurate and that it includes all the information prescribed for a qualified certificate.

c) Ensure that the signatory has sole control over the use of the signature creation data corresponding to the verification data contained in the certificate.

d) Ensure the complementarity of signature creation and verification data, provided that both are generated by the certification service provider.

Verification of the identity and other personal circumstances of the applicants for a recognized certificate.

1. The identification of the natural person requesting a qualified certificate shall require his/her appearance in person before those in charge of verifying it and shall be proven by means of the national identity card, passport or other legally accepted means. The appearance in person may be dispensed with if the signature on the application for the issuance of a qualified certificate has been notarized.

The system of personal appearance in the application for certificates issued after identification of the applicant before the Public Administrations shall be governed by the provisions of the administrative regulations.

2. In the case of recognized certificates of legal persons, the certification service providers shall also verify the data relating to the incorporation and legal personality and the extent and validity of the powers of representation of the applicant by means of the public documents that serve to accredit the aforementioned points in an irrefutable manner and their registration in the corresponding public registry, if required. The aforementioned verification may also be carried out by means of consultation in the public registry in which the incorporation and power of attorney documents are registered, using the telematic means provided by the aforementioned public registries.

3. If the recognized certificates reflect a voluntary representation relationship, the certification service providers shall verify the data relating to the legal personality of the principal and the extent and validity of the powers of the representative by means of the public documents that serve to prove the aforementioned points in an irrefutable manner and their registration in the corresponding public registry, if required. The aforementioned verification may also be carried out by means of consultation in the public registry at

where the aforementioned data are registered, and may use the telematic means provided by the aforementioned public registries.

If the recognized certificates admit other cases of representation, the certification service providers must require the accreditation of the circumstances on which they are based, in the same way as previously foreseen.

When the recognized certificate contains other personal circumstances or attributes of the applicant, such as his or her status as holder of a public office, membership in a professional association or qualifications, these must be verified by means of the official documents that accredit them, in accordance with their specific regulations.

4. The provisions of the preceding paragraphs may be waived in the following cases:

a) When the identity or other permanent circumstances of the applicants for the certificates were already known to the certification service provider by virtue of a pre-existing relationship, in which, for the identification of the interested party, the means indicated in this article had been used and the period of time elapsed since the identification is less than five years.

b) When, in order to request a certificate, another certificate in force is used for the issuance of which the signatory had been identified in the manner prescribed in this article and the certification service provider is satisfied that the period of time elapsed since the identification is less than five years.

5. The certification service providers may carry out the verification actions provided for in this article by themselves or through other natural or legal persons, public or private, being responsible, in any case, the certification service provider.

6. By Order of the Minister of Economic Affairs and Digital Transformation, the conditions and technical requirements applicable to the verification of the identity and, if applicable, other specific attributes of the person requesting a qualified certificate, by means of other identification methods that provide equivalent security in terms of reliability to physical presence, shall be determined.

Article 14. *International equivalence of recognized certificates.*

The electronic certificates that certification service providers established in a State that is not a member of the European Economic Area issue to the public as qualified certificates in accordance with the legislation applicable in that State shall be considered equivalent to those issued by those established in Spain, provided that any of the following conditions are met:

a) That the certification service provider meets the requirements established in the Community regulations on electronic signatures for the issuance of qualified certificates and has been certified in accordance with a voluntary certification system established in a Member State of the European Economic Area.

b) That the certificate is guaranteed by a certification service provider established in the European Economic Area that complies with the requirements established in the Community regulations on electronic signatures for the issuance of recognized certificates.

c) That the certificate or certification service provider is recognized by virtue of a bilateral or multilateral agreement between the European Community and third countries or international organizations.

CHAPTER III

The electronic national identity card

Article 15. *Electronic National Identity Card.*

1. The electronic national identity card is the national identity document that electronically accredits the personal identity of its holder, in the terms established in article 8 of Organic Law 4/2015, of March 30, on the protection of citizen security, and allows the electronic signature of documents.

2. All natural or legal persons, public or private, shall recognize the effectiveness of the electronic national identity document to prove the identity and other personal data of the holder contained therein, and to prove the identity of the signatory and the integrity of the documents signed with the electronic signature devices included therein.

Article 16. *Requirements and characteristics of the electronic national identity card.*

1. The competent bodies of the Ministry of the Interior for the issuance of the electronic national identity document shall comply with the obligations imposed by this Law on certification service providers issuing recognized certificates, with the exception of that relating to the provision of the guarantee referred to in paragraph 2 of Article 20.

2. The General State Administration will use, as far as possible, systems that guarantee the compatibility of the electronic signature instruments included in the national electronic identity document with the different generally accepted electronic signature devices and products.

TITLE III

Provision of certification services

CHAPTER I

Obligations

Article 17. *Protection of personal data.*

1. The processing of personal data required by certification service providers for the development of their activity and by administrative bodies for the exercise of the functions attributed by this Law shall be subject to the provisions of Organic Law 15/1999, of December 13, on the Protection of Personal Data and its implementing regulations.

2. For the issuance of electronic certificates to the public, certification service providers may only collect personal data directly from the signatories or with their express consent.

The required data will be exclusively those necessary for the issuance and maintenance of the electronic certificate and the provision of other services in connection with the electronic signature, and may not be processed for other purposes without the express consent of the signatory.

3. Certification service providers that include a pseudonym in the electronic certificate at the signatory's request must verify the signatory's true identity and keep the documentation that proves it.

Said certification service providers shall be obliged to disclose the identity of the signatories when requested to do so by the judicial bodies in the exercise of the functions attributed to them and in the other cases provided for in Article 11.2 of the Organic Law on Personal Data Protection in which this is required.

4. In any case, certification service providers shall not include in the electronic certificates they issue, the data referred to in article 7 of Organic Law 15/1999, of December 13, 1999, on Personal Data Protection.

Article 18. *Obligations of certification service providers issuing electronic certificates.*

Certification service providers issuing electronic certificates shall comply with the following obligations:

a) Not to store or copy, by themselves or through a third party, the signature creation data of the person to whom they have rendered their services, except in the case of their management on behalf of

of the signatory. In this case, appropriate technical and organizational procedures and mechanisms shall be implemented to ensure that the signatory has exclusive control over the use of his signature creation data.

Only certification service providers issuing qualified certificates may manage the electronic signature creation data on behalf of the signatory. For this purpose, they may make a backup copy of the signature creation data provided that the security of the duplicated data is of the same level as that of the original data and that the number of duplicated data does not exceed the minimum necessary to ensure continuity of service. Signature creation data may not be duplicated for any other purpose.

b) Provide the applicant with the following minimum information prior to the issuance of the certificate, which must be transmitted free of charge, in writing or electronically:

1. The signatory's obligations, the manner in which the signature creation data must be kept, the procedure to be followed to report the loss or possible misuse of such data or, as the case may be, of the means protecting them, as well as information on the electronic signature creation and verification devices that are compatible with the signature data and the certificate issued.

2.° The mechanisms to ensure the reliability of the electronic signature of a document over time.

3.° The method used by the provider to verify the identity of the signatory or other information contained in the certificate.

4.° The precise conditions of use of the certificate, its possible limits of use and the way in which the provider guarantees his patrimonial responsibility.

5.° The certifications obtained, if any, by the certification service provider and the applicable procedures for the extrajudicial resolution of conflicts that may arise from the exercise of its activity.

6.° The other information contained in the certification practice statement.

The aforementioned information that is relevant to third parties affected by the certificates must be available upon request.

c) Maintain an updated directory of certificates, indicating which certificates have been issued and whether they are valid or whether their validity has been suspended or terminated. The integrity of the directory shall be protected through the use of appropriate security mechanisms.

d) Ensure the availability of a fast and secure certificate validity query service.

Article 19. *Declaration of certification practices.*

1. All certification service providers shall formulate a certification practices statement in which they shall detail, within the framework of this Law and its implementing provisions, the obligations they undertake to comply with in relation to the management of signature creation and verification data and electronic certificates, the conditions applicable to the request, issue, use, suspension and termination of the validity of the certificates, the technical and organizational security measures, the profiles and the information mechanisms on the validity of the certificates and, where appropriate, the existence of coordination procedures with the public registries, suspension and extinction of the validity of the certificates, the technical and organizational security measures, the profiles and the information mechanisms on the validity of the certificates and, if applicable, the existence of coordination procedures with the corresponding public registries that allow the immediate exchange of information on the validity of the powers of attorney indicated in the certificates and that must be included in the said registries.

2. The certification practice statement of each provider shall be available to the public in an easily accessible manner, at least electronically and free of charge.

3. The certification practice statement shall be considered as a security document for the purposes set forth in the legislation on the protection of personal data and shall contain all the requirements required for such document in the aforementioned legislation.

Article 20. *Obligations of certification service providers issuing qualified certificates.*

1. In addition to the obligations established in this chapter, certification service providers issuing qualified certificates shall comply with the following obligations:

a) Demonstrate the necessary reliability to provide certification services.

b) Ensure that the date and time at which a certificate was issued, terminated or suspended can be accurately determined.

c) Employ personnel with the necessary qualifications, knowledge and experience to provide the certification services offered and the appropriate security and management procedures in the field of electronic signatures.

d) Use reliable systems and products that are protected against any alteration and that guarantee the technical and, where appropriate, cryptographic security of the certification processes they support.

e) Take measures against certificate forgery and, in the event that the certification service provider generates signature creation data, ensure its confidentiality during the generation process and its delivery by a secure procedure to the signatory. If the service provider manages the signature creation data on behalf of the signatory, it must safeguard and protect them against any alteration, destruction or unauthorized access, as well as ensure their continued availability to the signatory.

f) Keep recorded by any secure means all information and documentation relating to a qualified certificate and the certification practice statements in force at any time, for at least 15 years from the time of issue, so that the signatures made with it can be verified.

g) Use reliable systems for storing recognized certificates that make it possible to verify their authenticity and prevent unauthorized persons from altering the data, restrict their accessibility in the cases or to the persons indicated by the signatory, and make it possible to detect any change that affects these security conditions.

2. Certification service providers issuing qualified certificates must take out liability insurance for at least 3,000,000 euros to cover the risk of liability for damages that may be caused by the use of the certificates they issue.

The aforementioned guarantee may be totally or partially replaced by a guarantee by means of a bank guarantee or surety insurance, so that the sum of the insured amounts is at least 3,000,000 Euros.

The amounts and the means of insurance and guarantee established in the two preceding paragraphs may be modified by Royal Decree.

Article 21. *Termination of the activity of a certification service provider.*

1. The certification services provider that is going to cease its activity must inform the signatories using the electronic certificates it has issued as well as the applicants of certificates issued in favor of legal persons ; and may transfer, with their express consent, the management of those that are still valid on the date on which the cessation occurs to another certification services provider that assumes them or, otherwise, terminate their validity.

Said communication shall be made at least two months prior to the effective termination of the activity and shall inform, where appropriate, on the characteristics of the provider to whom it is proposed to transfer the management of the certificates.

2. The certification service provider that issues electronic certificates to the public must notify the Ministry of Science and Technology, with the advance notice indicated in the previous section, of the cessation of its activity and the destination it will give to the certificates, specifying, if applicable, if it will transfer the management and to whom or if it will terminate its validity.

Likewise, it shall communicate any other relevant circumstance that may prevent the continuation of its activity. In particular, it must notify, as soon as it becomes aware of it, the opening of any bankruptcy proceedings against it.

3. The certification service providers shall send to the Ministry of Science and Technology, prior to the definitive cessation of their activity, the information related to the electronic certificates whose validity has been terminated so that the Ministry can take custody of them for the purposes of the provisions of Article 20.1.f). This ministry shall maintain accessible to the public a specific consultation service containing an indication of the aforementioned certificates for a period of time that it considers sufficient according to the queries made to it.

CHAPTER II

Responsibility

Article 22. *Liability of cedification service providers.*

1. Certification service providers shall be liable for damages caused to any person in the exercise of their activity when they fail to comply with the obligations imposed by this Law.

The liability of the certification service provider regulated in this Law shall be enforceable in accordance with the general rules on contractual or non-contractual fault, as appropriate, although it shall be up to the certification service provider to prove that he acted with the professional diligence required of him.

2. If the certification service provider does not comply with the obligations set forth in paragraphs b) to d) of Article 12 when guaranteeing an electronic certificate issued by a certification service provider established in a State not belonging to the European Economic Area, it shall be liable for damages caused by the use of such certificate.

3. In particular, the certification service provider shall be liable for the damages caused to the signatory or to third parties in good faith due to the lack or delay in the inclusion in the certificate validity query service of the termination or suspension of the validity of the electronic certificate.

4. Certification service providers shall assume all liability to third parties for the performance of persons to whom they delegate the execution of any or some of the functions necessary for the provision of certification services.

5. The regulation contained in this Law on the liability of the certification service provider is without prejudice to the provisions of the legislation on unfair terms in consumer contracts.

Article 23. *Limitations of liability of cedification service providers.*

1. The certification service provider shall not be liable for damages caused to the signatory or third parties in good faith, if the signatory incurs in any of the following cases:

a) Failure to provide the certification service provider with truthful, complete and accurate information about the data that must be included in the electronic certificate or that are necessary for its issuance or for the termination or suspension of its validity, when its inaccuracy could not be detected by the certification service provider.

b) Failure to promptly notify the certification service provider of any change in the circumstances reflected in the electronic certificate.

c) Negligence in the conservation of your signature creation data, in the assurance of their confidentiality and in the protection of any access or disclosure of them or, as the case may be, of the means giving access to them.

d) Not to request the suspension or revocation of the electronic certificate in case of doubt as to the maintenance of the confidentiality of its signature creation data or, as the case may be, of the means that give access to them.

e) Use the signature creation data when the validity period of the electronic certificate has expired or the certification service provider notifies the expiration or suspension of its validity.

f} Exceeding the limits that appear in the electronic certificate in terms of its possible uses and the individualized amount of the transactions that may be carried out with it or not using it in accordance with the conditions established and communicated to the signatory by the certification service provider.

2. In the case of electronic certificates that include a power of attorney of the signatory, both the signatory and the person or entity represented, when the latter becomes aware of the existence of the certificate, are obliged to request the revocation or suspension of the validity of the certificate under the terms set forth in this Law.

3. When the signatory is a legal entity, the applicant for the electronic certificate shall assume the obligations indicated in paragraph 1.

4. The certification service provider shall also not be liable for damages caused to the signatory or to bona fide third parties if the recipient of the electronically signed documents acts negligently. It shall be understood, in particular, that the recipient acts negligently in the following cases:

a) When it does not check and take into account the restrictions contained in the electronic certificate regarding its possible uses and the individualized amount of the transactions that may be carried out with it.

b) When it does not take into account the suspension or loss of validity of the electronic certificate published in the consultation service on the validity of the certificates or when it does not verify the electronic signature.

5. The certification service provider shall not be liable for damages caused to the signatory or third parties in good faith by the inaccuracy of the data contained in the electronic certificate if they have been accredited by a public document, recorded in a public registry if required. In the event that such data must be recorded in a public registry, the certification service provider may, where appropriate, check them in that registry before issuing the certificate, and may use the telematic means provided by the aforementioned public registries.

6. The exemption from liability towards third parties obliges the certification service provider to prove that it acted in any case with due diligence.

TITLE IV

Electronic signature devices and certification systems for electronic signature providers

certification services and electronic signature devices

CHAPTER I

Electronic signature devices

Article 24. *Electronic signature creation devices.*

1. Signature creation data is the unique data, such as codes or private cryptographic keys, that the signer uses to create the electronic signature.

2. A signature creation device is a computer program or system used to apply signature creation data.

3. A secure signature creation device is a signature creation device that offers at least the following guarantees:

a) That the data used for signature generation can be produced only once and reasonably ensures its secrecy.

b) That there is reasonable assurance that the data used for signature generation cannot be derived from the signature verification data or the signature itself and that the signature is protected against forgery with the technology available at the time.

c) That the signature creation data can be reliably protected by the signatory against use by third parties.

d) That the device used does not alter the data or the document to be signed or prevent it from being shown to the signatory prior to the signing process.

Article 25. *Electronic signature verification devices.*

1. Signature verification data is the data, such as codes or public cryptographic keys, used to verify the electronic signature.

2. A signature verification device is a computer program or system used to apply signature verification data.

3. Electronic signature verification devices shall ensure, whenever technically feasible, that the verification process of an electronic signature satisfies at least the following requirements:

a) That the data used to verify the signature corresponds to the data shown to the person verifying the signature.

b) That the signature is reliably verified and the result of that verification is correctly presented.

c) That the person verifying the electronic signature can, if necessary, reliably establish the content of the signed data and detect whether it has been modified.

d) The identity of the signatory or, if applicable, the use of a pseudonym, as well as the result of the verification, must be correctly shown.

e) That the authenticity and validity of the corresponding electronic certificate are reliably verified.

f) That any change related to its security can be detected.

4. Likewise, data relating to the verification of the signature, such as the time at which the signature occurs or a verification of the validity of the electronic certificate at that time, may be stored by the person verifying the electronic signature or by trusted third parties.

CHAPTER II

Certification of certification service providers and certification devices creation of electronic signature

*Cedification of certification service providers***.**

1. Certification of a certification service provider is the voluntary procedure by which a public or private qualified entity issues a declaration in favor of a certification service provider, which implies an acknowledgement of compliance with specific requirements in the provision of services offered to the public.

2. The certification of a certification service provider may be requested by the latter and may be carried out, among others, by certification entities recognized by an accreditation entity designated in accordance with the provisions of Law 21/1992, of July 16, 1992, on Industry, and its implementing provisions.

3. Technical standards or other appropriate certification criteria may be used in the certification procedures. If technical standards are used, preference shall be given to those that are widely recognized and approved by European standardization bodies and, failing that, to other international or Spanish standards.

4. The certification of a certification service provider shall not be necessary to recognize the legal effectiveness of an electronic signature.

Cedification of secure devices for the creation of electronic signatures.

1. The certification of secure electronic signature creation devices is the procedure by which it is verified that a device meets the requirements established in this ley for its consideration as a secure signature creation device.

2. Certification may be requested by manufacturers or importers of signature creation devices and shall be carried out by certification entities recognized by an accreditation entity designated in accordance with the provisions of Law 21/1992, of July 16, 1992, on Industry and its implementing provisions.

3. In the certification procedures, the technical standards whose reference numbers have been published in the "Official Journal of the European Union" shall be used and,

exceptionally, those approved by the Ministry of Science and Technology, which will be published on the Internet address of this Ministry.

4. The certificates of conformity of secure signature creation devices shall be modified or, as the case may be, revoked when the conditions established for obtaining them are no longer met.

Certification bodies shall ensure the dissemination of decisions on revocation of signature creation device certificates.

Article 28. *Acknowledgement of conformity with the regulations applicable to electronic signature products.*

1. Electronic signature products referred to in Articles 20(1)(d) and 24(3) shall be presumed to be in conformity with the requirements of those Articles if they comply with the corresponding technical standards whose reference numbers have been published in the "Official Journal of the European Union".

2. Certificates of conformity on secure signature creation devices that have been granted by the bodies designated for this purpose in any Member State of the European Economic Area shall be recognized as effective.

TITLE V

Supervision and control

Article 29. *Supervision and control.*

1. The Ministry of Science and Technology will control the compliance by the certification service providers that issue electronic certificates to the public of the obligations established in this Law and in its development provisions. Likewise, it will supervise the operation of the system and of the certification bodies of secure devices for the creation of electronic signatures.

2. The Ministry of Science and Technology will carry out the inspection actions that are necessary for the exercise of its control function.

The civil servants assigned to the Ministry of Science and Technology who carry out the inspection referred to in the previous section shall be considered public authorities in the performance of their duties.

3. The Ministry of Science and Technology may agree on the appropriate measures for compliance with this Law and its implementing provisions.

4. The Ministry of Science and Technology may resort to independent and technically qualified entities to assist it in the tasks of supervision and control over the certification service providers assigned to it by this Law.

5. Tests by laboratories or specialized entities may be required to certify compliance with certain requirements. In this case, the service providers shall bear the costs of this evaluation.

Article 30. *Duty of information and collaboration.*

1. The certification service providers, the independent accreditation entity and the certification bodies have the obligation to provide the Ministry of Science and Technology with all the information and collaboration necessary for the exercise of its functions.

In particular, they must allow their agents or inspection personnel access to their facilities and the consultation of any documentation relevant to the inspection in question, being applicable, where appropriate, the provisions of Article 8.5 of Law 29/1998, of July 13, 1998, regulating the Contentious-Administrative Jurisdiction. In their inspections they may be accompanied by experts or experts in the matters to which they refer.

2. Certification service providers must inform the Ministry of Science and Technology of the start of their activity, their identification data, including tax and registry identification, if applicable, the data that allow establishing communication with the provider, including the Internet domain name, customer service data, the characteristics of the services to be provided, the certifications obtained for

their services and the certifications of the devices they use. This information must be conveniently updated by the providers and will be published on the Internet address of the aforementioned ministry in order to provide maximum dissemination and knowledge.

3. When, as a result of an inspection activity, facts become known that could constitute infractions typified in other laws, they shall be reported to the competent bodies or agencies for their supervision and sanction.

TITLE VI

Violations and penalties

Article 31. *Infringements.*

1. Violations of the provisions of this Law are classified as very serious, serious and minor.

2. These are very serious infractions:

a) Failure to comply with any of the obligations set forth in Articles 18 and 20 in the issuance of qualified certificates, provided that serious damage has been caused to users or the security of the certification services has been seriously affected.

The provisions of this paragraph shall not apply with respect to non-compliance with the obligation to provide the financial guarantee provided for in Article 20.2.

b) The issuance of recognized certificates without carrying out all the prior verifications indicated in article 12, when this affects the majority of the recognized certificates issued in the three years prior to the start of the sanctioning procedure or since the start of the provider's activity if this period is shorter.

3. These are serious infractions:

a) Failure to comply with any of the obligations established in Articles 18 and 20 in the issuance of recognized certificates, except for the obligation to provide the guarantee established in paragraph 2 of Article 20, when it does not constitute a very serious infringement.

b) Failure by providers issuing recognized certificates to lodge the financial guarantee referred to in Article 20, paragraph 2.

c) The issuance of recognized certificates without carrying out all the prior verifications indicated in article 12, in those cases in which it does not constitute a very serious infraction.

d) Non-compliance by certification service providers who do not issue qualified certificates with the obligations set forth in Article 18, if serious damage has been caused to users or the security of the certification services has been seriously affected.

e) Non-compliance by certification service providers of the obligations established in article 21 regarding the cessation of their activity or the occurrence of circumstances that prevent the continuation of their activity, when these are not punishable in accordance with the provisions of Organic Law 15/1999, of December 13, on the Protection of Personal Data.

f) The resistance, obstruction, excuse or unjustified refusal to the inspection activities of the bodies empowered to carry them out in accordance with this Law and the lack or deficient presentation of the information requested by the Ministry of Science and Technology in its inspection and control function.

g) Failure to comply with the resolutions issued by the Ministry of Science and Technology to ensure that the certification service provider complies with this ley.

4. They constitute minor infractions:

Non-compliance by certification service providers that do not issue qualified certificates with the obligations set forth in Article 18; and non-compliance by certification service providers with the remaining obligations.

established in this Law, when it does not constitute a serious or very serious infringement, with the exception of the obligations contained in paragraph 2 of Article 30.

Article 32. *Sanctions.*

1. The following penalties shall be imposed for the commission of the infractions set forth in the preceding article:

a) For the commission of very serious infringements, the offender shall be fined from 150,001 to 600,000 euros.

The commission of two or more very serious infringements within a period of three years may give rise, depending on the graduation criteria of the following article, to the sanction of prohibition to act in Spain for a maximum period of two years.

b) For the commission of serious infractions, the offender shall be fined from 30,001 to 150,000 euros.

c) For minor offenses, a fine of up to 30,000 euros shall be imposed on the offender.

2. Serious and very serious infringements may entail, at the expense of the sanctioned party, the publication of the sanctioning resolution in the "Official State Gazette" and in two national newspapers or on the home page of the provider's website and, if applicable, on the website of the Ministry of Science and Technology, once the resolution has become final.

For the imposition of this sanction, the social repercussion of the infraction committed, the number of users affected and the seriousness of the offense shall be considered.

Article 33. *Graduation of the amount of the sanctions.*

The amount of the fines to be imposed, within the limits indicated above, will be graduated taking into account the following:

a) The existence of intentionality or repetition.

b) Recidivism, for committing infractions of the same nature, sanctioned by means of a firm resolution.

c) The nature and amount of the damages caused.

d) The period of time during which the infringement has been committed e) The benefit the infringer has derived from the commission of the infringement.

f) Volume of the turnover affected by the infraction committed.

Article 34. *Provisional measures.*

1. In disciplinary proceedings for serious or very serious infringements, the Ministry of Science and Technology may adopt, in accordance with Law 30/1992, of November 26, 1992, on the Legal Regime of the Public Administrations and Common Administrative Procedure, and its implementing regulations, the provisional measures deemed necessary to ensure the effectiveness of the final decision issued, the proper outcome of the proceedings, to avoid the continuation of the effects of the infringement and the requirements of the general interest.

In particular, the following may be agreed upon:

a) Temporary suspension of the activity of the certification service provider and, where appropriate, temporary closure of its establishments.

b) Sealing, deposit or seizure of records, supports and computer files and documents in general, as well as computer devices and equipment of all kinds.

c) Warning the public of the existence of possible infringing conduct and of the initiation of the sanctioning proceedings in question, as well as of the measures adopted for the cessation of such conduct.

In the adoption and enforcement of the restriction measures referred to in this section, the guarantees, rules and procedures provided for in the legal system to protect the rights to personal privacy and the protection of personal data, when these could be affected, shall be respected in all cases.

2. In cases of exceptionally serious damage to the security of the systems used by the certification service provider that seriously undermine the confidence of users in the services offered, the Ministry of Science and Technology may agree to the suspension or loss of validity of the certificates affected, even permanently.

3. In any case, the principle of proportionality of the measure to be adopted with the objectives to be achieved in each case shall be respected.

4. In cases of urgency and for the immediate protection of the interests involved, the provisional measures provided for in this article may be agreed upon prior to the initiation of the sanctioning proceedings.

The measures must be confirmed, modified or lifted in the agreement to initiate the procedure, which must be made within 15 days of their adoption, and may be subject to the appropriate appeal.

In any case, such measures shall be null and void if the sanctioning procedure is not initiated within said term or when the initiation agreement does not contain an express pronouncement on the same.

Article 35. *Coercive fine.*

The administrative body competent to resolve the sanctioning procedure may impose coercive fines for an amount not exceeding 6,000 euros for each day that elapses without complying with the provisional measures that have been agreed.

Article 36. *Jurisdiction and sanctioning procedure.*

1. The imposition of sanctions for non-compliance with the provisions of this Law shall correspond, in the case of very serious infringements, to the Minister of Science and Technology, and in the case of serious and minor infringements, to the Secretary of State for Telecommunications and the Information Society.

However, failure to comply with the obligations set forth in Article 17 shall be sanctioned by the Data Protection Agency in accordance with the provisions of Organic Law 15/1999, of December 13, 1999, on the Protection of Personal Data.

2. The sanctioning power regulated in this Law shall be exercised in accordance with the provisions of the Law on the Legal Regime of Public Administrations and Common Administrative Procedure and its implementing regulations.

First additional provision. *Public faith and use of electronic signature.*

1. The provisions of this Law do not replace or modify the rules that regulate the functions that correspond to the officials who legally have the power to attest documents in the scope of their competences, provided that they act with the requirements demanded in the Law.

2. In the field of electronic documentation, certification service providers shall be responsible for certifying the existence of the services provided in the exercise of their electronic certification activity, at the request of the user, or of a judicial or administrative authority.

Second additional provision. *Exercise of the sanctioning power over the accreditation entity and the certification bodies of electronic signature creation devices.*

1. In the field of the certification of signature creation devices, the Secretary of State for Telecommunications and for the Information Society of the Ministry of Science and Technology shall be responsible for the imposition of sanctions for the commission, by the certification bodies of secure electronic signature creation devices or by the entity that accredits them, of the serious infringements provided for in paragraphs e), f) and g) of the second paragraph of article 31 of Law 21/1992, of July 16, 1992, of Industry, of the serious infractions foreseen in paragraphs e), f) and g) of the second section of article 31 of Law 21/1992, of July 16, 1992, of Industry, and of the slight infractions indicated in paragraph a) of section 3 of article 31 of the mentioned Law that they commit in the exercise of activities related to the certification of electronic signature.

2. When such infringements are classified as very serious infringements, they shall be sanctioned by the Minister of Science and Technology.

Third additional provision. *Issuance of electronic certificates to unincorporated entities for the fulfillment of tax obligations.*

Electronic certificates may be issued to the unincorporated entities referred to in Article 33 of the General Tax Law for the sole purpose of their use in the tax field, under the terms established by the Minister of Finance.

Fourth Additional Provision. *Provision of services by the Fabrica Nacional de Moneda y Timbre-Real Casa de la Moneda.*

The provisions of this Law are without prejudice to the provisions of Article 81 of Law 66/1997, of December 30, 1997, on fiscal, administrative and social measures.

Fifth additional provision. *Modification of addendum 81 of Law 66/1997, of December 30, 1997, on fiscal, administrative and social measures.*

Section twelve is added to Article 81 of Law 66/1997, of December 30, 1997, on fiscal, administrative and social measures, with the following wording.

> "Twelve. In the exercise of the functions attributed to it by this article, the National Mint-Royal Mint shall be exempt from the constitution of the guarantee referred to in section 2 of article 20 of Law 59/2003, on Electronic Signatures."

Sixth additional provision. *Legal regime of the electronic national identity document.*

1. Without prejudice to the application of the regulations in force regarding the national identity card in all matters that are appropriate to its particular characteristics, the electronic national identity card shall be governed by its specific regulations.
2. The Ministry of Science and Technology may contact the Ministry of the Interior so that the latter may adopt the necessary measures to ensure compliance with the obligations incumbent upon it as a certification service provider in relation to the national electronic identity card.

Seventh additional provision. *Issuance of invoices by electronic means.*

The provisions of this Law are without prejudice to the requirements derived from the tax regulations regarding the issuance of invoices by electronic means.

Eighth additional provision: *Amendments to Law 34/2002, of July 11, 2002, on information society services and electronic commerce.*

One. Addition of a new paragraph 3 to Article 10 of Law 34/2002, of July 11, 2002, on information society services and electronic commerce.

A paragraph 3 is added with the following text:

> "3. When a telephone numbering range has been allocated to premium rate services in which access to information society services is allowed and its use is required by the service provider, such use and the downloading of software that performs dialing functions shall be made with the prior, informed and express consent of the user.
>
> For this purpose, the service provider shall provide at least the following information:
>
> a) The characteristics of the service to be provided.
>
> b) The functions to be performed by the software to be downloaded, including the telephone number to be dialed.

c) The procedure for terminating the premium rate connection, including an explanation of the specific time at which such termination will occur, and d) The procedure necessary to reestablish the connection number prior to the premium rate connection.

The above information shall be available in a clearly visible and identifiable manner.

The provisions of this paragraph are without prejudice to the provisions of telecommunications regulations, especially in relation to the applicable requirements for access by users to telephone numbering ranges, if any, allocated to premium rate services."

Sections 2, 3 and 4 of Article 38 of Law 34/2002, of July 11, 2002, on information society services and electronic commerce shall be worded as follows:

"2. The following are very serious infringements:

a) Failure to comply with orders issued pursuant to Article 8 in those cases in which they have been issued by an administrative body.

b) Failure to comply with the obligation to suspend transmission, data hosting, network access or the provision of any other equivalent intermediation service, when ordered to do so by a competent administrative body, pursuant to the provisions of Article 11.

c) Significant non-compliance with the obligation to retain traffic data generated by communications established during the provision of an information society service, as provided for in Article 12.

d) The use of data retained, in compliance with article 12, for purposes other than those indicated therein.

3. These are serious infractions:

a) Failure to comply with the obligation to retain traffic data generated by communications established during the provision of an information society service, as provided for in Article 12, unless it should be considered a very serious infringement.

b) Significant non-compliance with paragraphs a) and f) of Article 10.1.

c) The mass sending of commercial communications by electronic mail or other equivalent means of electronic communication or the sending, within a period of one year, of more than three commercial communications by the aforementioned means to the same addressee, when such mailings do not comply with the requirements established in article 21.

d) Significant non-compliance with the service provider's obligation set forth in Article 22(1), in relation to the procedures for revoking the consent given by the recipients.

e) Failure to make available to the recipient of the service the general conditions to which, if any, the contract is subject, in the manner provided for in article 27.

f) Habitual non-compliance with the obligation to confirm receipt of an acceptance, when its exclusion has not been agreed or the contract has been concluded with a consumer.

g) Resistance, excuse or refusal to the inspection activities of the bodies empowered to carry them out in accordance with this Law.

h) Significant noncompliance with the provisions of paragraph 3 of Article 10.

i) Significant non-compliance with reporting or disclosure obligations or with establishment of a procedure for refusal of data processing, as provided for in Article 22(2).

4. These are minor infractions:

a) Failure to notify the public registry in which they are registered, in accordance with the provisions of Article 9, of the domain name or names or Internet addresses used for the provision of information society services.

b) Failure to report in the manner prescribed by article 10.1 on the aspects indicated in paragraphs b), c), d), e) and g) thereof, or in paragraphs a) and f) when this does not constitute a serious infringement.

c) Failure to comply with the provisions of Article 20 for commercial communications, promotional offers and contests.

d) The sending of commercial communications by electronic mail or other equivalent means of electronic communication when such mailings do not comply with the requirements set forth in Article 21 and do not constitute a serious infringement.

e) Failure to provide the information referred to in Article 27.1, when the parties have not agreed on its exclusion or the recipient is a consumer.

f) Failure to comply with the obligation to confirm receipt of a request under the terms set forth in Article 28, when its exclusion has not been agreed or the contract has been concluded with a consumer, unless it constitutes a serious infringement.

g) Failure to comply with the obligations to provide information or to establish a procedure for refusal of data processing, as set forth in Article 22(2), when this does not constitute a serious infringement.

h) Failure to comply with the obligation of the service provider established in paragraph 1 of Article 22, in relation to the procedures to revoke the consent given by the recipients when it does not constitute a serious infringement.

i) Failure to comply with the provisions of paragraph 3 of Article 10, when it does not constitute a serious infringement."

Three. Amendment of Article 43, paragraph 1, second subparagraph of Law 34/2002, of July 11, 2002, on information society services and electronic commerce.

Article 43, paragraph 1, second subparagraph, shall read as follows:

"Notwithstanding the foregoing, the imposition of sanctions for non-compliance with the resolutions issued by the competent bodies depending on the matter or entity in question referred to in paragraphs a) and b) of Article 38.2 of this Law will correspond to the body that issued the non-compliant resolution. Likewise, the Data Protection Agency shall be responsible for the imposition of sanctions for the commission of the infringements set out in Articles 38.3 c), d) and i) and 38.4 d), g) and
h) of this Law".

Four. Amendment of Article 43, paragraph 2 of Law 34/2002, of July 11, 2002, on information society services and electronic commerce.

Paragraph 2 of Article 43 shall read as follows:

"The sanctioning power regulated in this Law shall be exercised in accordance with the provisions of Law 30/1992, of November 26, 1992, on the Legal Regime of the Public Administrations and the Common Administrative Procedure, and its implementing regulations. However, the maximum duration of the simplified procedure shall be three months."

Ninth additional provision. *Guarantee of accessibility for persons with disabilities and senior citizens.*

The services, processes, procedures and electronic signature devices must be fully accessible to persons with disabilities and senior citizens, who may in no case be discriminated against in the exercise of the rights and faculties recognized in this Law for reasons based on disability or advanced age.

Tenth additional provision. *Modification of the Civil Procedure Law.*

A new paragraph three is added to article 326 of the Civil Procedure Law with the following wording:

> "When the party to whom the effectiveness of an electronic document is of interest requests it or its authenticity is challenged, it shall proceed in accordance with the provisions of Article 3 of the Electronic Signature Law."

Eleventh additional provision. *Resolution of conflicts.*

Users and certification service providers may submit disputes arising in their relations to arbitration.

When the user is a consumer or user, under the terms established by consumer protection legislation, the provider and the user may submit their disputes to consumer arbitration, by means of their adhesion to the competent Consumer Arbitration System.

First transitory **provision.** *Validity of electronic certificates issued prior to the entry into force of this law.*

Electronic certificates that have been issued by certification service providers within the framework of Royal Decree Law 14/1999, of September 17, 1999, on electronic signature, shall remain valid.

Second Transitory Provision. *Cedification service providers established in Spain prior to the entry into force of this law.*

Certification service providers established in Spain prior to the entry into force of this Law must notify the Ministry of Science and Technology of their activity and the characteristics of the services they provide within one month of the entry into force of this Law. This information will be published in the Internet address of the aforementioned Ministry in order to provide it with the maximum dissemination and knowledge.

Sole derogatory provision. *Repeal of regulations.*

Royal Decree Law 14/1999, of September 17, 1999, on electronic signatures and any other provisions of equal or lower rank that oppose the provisions of this Law are hereby repealed.

First final provision. *Constitutional basis.*

This Law is issued under Article 149.1.8.ª , 18.ª , 21.ª and 29.ª of the Constitution.

Second final provision. *Regulatory development.*

1. The Government shall adapt the regulations governing the national identity card to the provisions of this Law.

2. Likewise, the Government is empowered to issue such other regulatory provisions as may be necessary for the development and application of this Law.

Third Final Provision. *Entry into force.*

This Law shall enter into force three months after its publication in the "Official Gazette of the State".

Therefore, I command all Spaniards, individuals and authorities, to keep and enforce the observance of this Law.

Madrid, December 19, 2003.

JUAN CARLOS R.

President of the
Government, JOSÉ MARÍA
AZNAR LÓPEZ