

***Royal Decree 1671/2009, of 6 November, which partially develops Law 11/2007 of 22 June, regarding citizens' electronic access to public services***

© Gobierno de España. Ministerio de Política Territorial y Administración Pública  
Marzo de 2011

*This document is a translation of the Royal Decree 1671/2009, of 6 November, which partially develops Law 11/2007 of 22 June, regarding citizens' electronic access to public services, published in the Spanish Official State Gazette. It is not an official translation and therefore has no legal validity. The original version can be found at [http://www.boe.es/aeboe/consultas/bases\\_datos/doc.php?id=BOE-A-2009-18358](http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-2009-18358)*

eI. GENERAL PROVISIONS

MINISTRY OF THE PRESIDENCY

**18358** *Royal Decree 1671/2009, of 6 November, which partially develops Law 11/2007 of 22 June, regarding citizens' electronic access to public services.*

Law 11/2007 of 22 June, regarding citizens' electronic access to public services, marks an important milestone in the construction of an information-society based government in Spain. This law rested on the experience acquired through the application of Law 30/1992 of 26 November, regarding the legal regime for Government bodies and the common administrative procedure, particularly in articles 38, 45, 46 and 59, in which it offered a general legal framework of reference for systematically incorporating information and communications technologies into administrative functions. Ratification of Law 58/2007 of 17 December, the General Taxation Law, was also a significant step forward as it was the first to address automating administrative processes and generating electronic images of documents with the same legal status and validity as the originals. However, Law 11/2007 of 22 June goes beyond serving to strengthen or consolidate the previous law by truly reorganising the relationship between the Government and citizens.

Law 11/2007 of 22 June introduced a new concept; the regulation is framed on the basis of the citizens' right to use electronic means of communication in their dealings with the Government and in exercising their rights. This novel starting point, with the citizen and his or her rights at the centre, means that there is now a legal commitment to incorporating information technology into all administrative functions. In addition, it implies that the citizen has the right to receive service, and the administration must effectively satisfy those rights. To that end, the law establishes a series of rights relating specifically to electronic communication with the Government and to citizen status: the right to obtain means of electronic identity, the right to choose the communication channel or authentication method that guarantees accessibility, and effective equality between the sexes, between groups with special needs and other groups, and between citizens living in different geographical areas.

This ambitious strategy was undertaken decisively. The third and final disposition of Law 11/2007 of 22 June sets 31 December 2009 as the date after which citizens may exercise their rights fully and by electronic means for any procedure or activity under the Government's responsibility.

In order to fulfil the legal objectives set forth by Law 22/2007 of 22 June and comply with its effective dates, it will be necessary to develop the provisions of the law, for the following reasons:

a) Law 22/2007 of 22 June does not fully regulate electronic access to public services as a result of the criteria for distributing competencies and the way they affect the capacities of self-organisation pertaining to other public administrations.

b) On the other hand, the diagonal nature of this regulation would suggest operations to adapt different procedures and activities. This need can only be met by providing a regulatory system characterised by the simultaneous presence of different legislative levels which cooperate amongst each other in order to form a general, objective, stable and predictable framework compatible with functional adaptation and with the state of technological development in this area.

This royal decree is intended to provide the complementary measure necessary in order for the Government of Spain to ensure the effective exercise of those rights recognised by Law 11/2007 of 22 June.

This royal decree was elaborated based on the following strategic principles:

a) Firstly, to attain full effectiveness of those rights recognised in Law 11/2007 of 22 June and habilitate them as far as the state of technology will permit, and to guarantee that other constitutionally protected rights, such as the rights to personal data protection, access to administrative information or preserving third-party interests, will not be affected.

b) Secondly, to establish the most flexible framework possible for implementing means of communication, with careful attention to security levels and protection of the rights and interests listed in both Law 11/2007 of 22 June and in general administrative legislation. This is done with a three-fold objective in mind: one, to prevent the new legislation from changing solutions for communicating with citizens to such an extent that it would eliminate well-established, existing techniques; two, to facilitate the process of implementation and adaptation for the different organisations, functions and procedures to which the royal decree applies; and three, to ensure that the option determined by certain solutions does not make it difficult to incorporate new solutions and services in the future.

Nevertheless, following through with these objectives requires another two instruments of a technical and complementary nature: the Spanish National Interoperability Framework, which is responsible for establishing the common criteria for information management in order to permit information and solution sharing, and the Spanish National Security Framework which establishes the necessary security criteria and levels for the information handling processes which the royal decree describes.

In keeping with this overview, the royal decree opens with a specific regulation aimed at effectively establishing the right not to provide documents which are already in the Government's keeping, and the rules necessary in order to obtain the required data and documents, with guarantees sufficient to prevent this function from becoming, in practice, a reason for delaying the resolution of administrative procedures.

In this way, the law regulates the form and the effects of citizens' exercising their rights, lists the different circumstances that may exist with respect to obtaining data or documents, and establishes the mandatory time frames for responding to applications. It also regulates the duty of informing the interested party of any delays in handling applications so that the party may remedy the lack of activity on the part of the responsible institution or entity, without prejudice of taking any legal action which may be in order.

One key component in legal communication with citizens by electronic means is the concept of the virtual office. On this matter, the royal decree aims to reinforce the reliability of these communication centres by applying three types of measures: 1) ensuring that these addresses are properly identified and distinguished as sites providing communication services to interested parties, 2) establishing the list of characteristic services and the scope of the site's effectiveness and responsibility, and 3) implementing a common regime so that the citizen is not confused by an excessive array of different sites. The office regime, which must be compatible with the necessary decentralisation arising from the current complexity of Government endeavours and activities, shall nevertheless be compatible with the creation of a common point of access to the entire administrative structure. This shall constitute a general gateway to Government services which citizens may use to transmit generic electronic communications or obtain the information necessary in order to visit other virtual offices where they may initiate or participate in procedures requiring access to specific applications or forms because they are presented in an electronic format.

With regard to identification and authentication, the Royal Decree aims to establish the minimum measures necessary in order to uphold the criterion of flexibility promoted by Law 11/2007 of 22 June. In addition to admitting the devices for identity confirmation and electronic signature associated with the Spanish national ID card as universal means of authentication, this law permits the use of other authentication means that meet the safety and security standards necessary for administrative functions to be carried out.

A specific regime has therefore been implemented to facilitate acting in the name of a third party by means of two fundamental mechanisms. The first takes the form of the general and specific adaptations which are basically designed for the continuous, professional performance of activities related to performing management and representation functions before Government bodies, in addition to voluntary registration for representatives. This is also set up in order to facilitate exercising the representative function through the establishment an online accreditation mechanism for a previously-registered title.

The royal decree also specifies the provisions contained within the law regarding the possibility of properly capacitated civil servants being able to undertake certain operations by electronic means by using their own identification and authentication systems for cases in which citizens do not have their own.

The legal relevance of the administrative activity requires that special attention be paid to the administration's use of electronic identification and authentication methods, establishing the need to add time stamps or references to accredit the effective date of the acts and documents which it issues. Special attention has also been paid to authentication in the area of automated processes.

Lastly, the law incorporates provisions intended to guarantee the interoperability and effectiveness of the legal system. These include express recognition of the signature policies which will be the instruments responsible for specifying the technical and organisational solutions necessary for the rights recognised by law to be fully operable, and a national certificate verification system intended to simplify and speed up operations to verify certificate validity.

With regard to electronic records, an important new step is to be found in the legal provisions: the creation of a common electronic register permitting the use of electronic means for any procedure which citizens undertake with the Government and its dependent or related public entities.

The same necessary line of development for the legal provisions has also been followed for electronic communications and messages, through establishing the proper guarantees ensuring that options included in Law 11/2007 of 22 June do not come to represent a disadvantage for citizens' interests and the public interest in general.

Lastly, one of the essential points in the legal discipline is its regulation of how electronic information provided by private citizens is managed, with stipulations of the minimum conditions so that its use does not interfere with the execution of administrative functions. A particularly novel change is that our schema provides for a regime for managing and changing formats. This will serve to facilitate file management by allowing the entity processing the file to choose the format in which the procedure is to be processed. The royal decree also takes stock of the importance of integrating information permitting document management, filing and recovery as soon as documents are received. Likewise, by regulating the processes by which paper documents being copied electronically may be destroyed, the royal decree establishes a stronger system of guarantees, paying particular attention to the conservation of documents with historical value.

The present royal decree is issued by virtue of the Government's express capacity to do so as per the seventh and final disposition of Law 11/2007 of 22 June. It was published

by the Spanish Data Protection Agency, the High Council on eGovernment, and the Consumers and Users Council.

In this capacity, following the proposal of the Ministers of the Presidency, of the Economy, of the Treasury, and of Industry, Tourism and Commerce, and in accordance with the Council of State, and having been deliberated by the Council of Ministers in their meeting dated 6 November 2009,

IT IS HEREBY STATED:

## TITLE I

### General Dispositions

#### Article 1. *Purpose and scope of application.*

1. The purpose of this royal decree is to develop Law 11/2007 of 22 June, regarding citizens' electronic access to public services in the sphere of the Government of Spain and the public institutions related to or dependent upon it. It refers to data transmission and general points of access, identification and authentication, electronic registers, communication and notices, and electronic documents and copies.

2. Its dispositions apply to:

- a) Activity by the Government of Spain and the public institutions related to or dependent upon it.
- b) Citizens in their dealings with the entities listed in the previous paragraph.
- c) Dealings between the entities and institutions referred to in paragraph a).

#### Article 2. *Transmitting data and documents, including certificates, between Government entities and institutions for the purpose of the activity recognised by article 6.2.b) of Law 11/2007 of 22 June.*

1. When citizens exercise their right not to provide data and documents that are already in the public administration's keeping, as established in article 6.2.b) in Law 11/2007 of 22 June, before the administrative bodies included in the sphere of application of article 1 of that royal decree, the following rules will apply:

a) The Administration will enable the parties concerned by the administrative procedures to exercise their right, which may be done by electronic means.

In any case, the concerned parties will be informed expressly that the exercise of that right implies their consent, in the terms set forth by article 6.2.b) of Law 11/2007 of 22 June, for the entity or institution in question to obtain the data or documents involved in exercising that right from the entities or institutions in which they are to be found.

The right shall be exercised specifically and individually for each specific procedure. Exercising the right before an entity or institution shall not imply general consent for all procedures that may be carried out in relation to the concerned party.

b) At any moment, the concerned parties may provide the necessary data, documents or certificates, or revoke their consent for the entity to access their personal data.

c) If the government entity entrusted with handling the procedure is in possession of the necessary data, documents or certificates in any format, or has electronic access to the same, it shall add them to the corresponding administrative procedure with no need for further measures. In any case, this shall be reflected in the files pertaining to the entity or institution ceding access to the data or documents to the entity or institution requesting them.

d) When the government body in charge of handling the procedure does not have access to the necessary data, documents or certificates, it shall request them from the government entity which does have access. If the government body is included under the sphere of application of article 1.2.a), it must use electronic means to transmit the necessary data, documents and certificates within the maximum time frame allowed by specific legislation, which may not exceed ten days. That time frame will also apply if there is none specified in the legislation.

e) Should it be impossible for the government entity handling the procedure to obtain the necessary data, documents or certificates, the concerned party will be instructed to provide them in the time span and for the purposes set forth in the legislation regulating the procedure in question, in a message which also indicates the motive or cause. In this case, the concerned party may lodge a complaint in accordance with Royal Decree 951/2005 of 29 July, which establishes the general framework for improving service quality within the Government of Spain.

f) The entities or institutions before which the right is exercised shall retain the documentation accrediting the effective exercise of the right and add it to the file in question.

That documentation shall be available to the entity providing the data and to any authorities which may be responsible for supervising and monitoring the legality of the transfers that occur.

2. The Spanish National Interoperability Framework and the National Security Framework shall establish such provisions as are necessary to enable citizens to exercise this right.

3. In order to comply with the requirement in article 9 of Law 11/2007 of 22 June, regarding data transmission between Public Administrations for effective exercise of the right recognised in article 6.2.b) of the same, the Government of Spain and its public institutions shall promote the signing of agreements with other Public Administrations in order to enable citizens to exercise that right. These agreements shall specifically establish the procedures enabling entities or institutions which transfer data to verify that the right has been effectively exercised with respect to the data or documents to which access was requested.

## TITLE II

### **Virtual offices and the general access point for the Government of Spain**

#### *Article 3. Creation of the virtual office.*

1. Government entities and public institutions connected with or dependent upon the government shall create their virtual offices according to the requirements established in this royal decree.

2. Virtual offices shall be created by order of the corresponding Ministry or by resolution of the public institution's governing body. Such orders must be published in Spain's Official State Gazette and contain the following minimum information:

a) Scope of application for the office. This may be the entire Ministry or public institution, or one or more of its entities, at General Directorate level at the very least.

b) Identification of the office's website of reference.

c) Identification of the governing body, and of the entity or entities responsible for website management and its services at the citizens' disposal.

d) Identification of the channels to access the services available on the site, listing, where applicable, the telephone numbers and offices which can be used as points of access.

e) Means available for submitting suggestions and lodging complaints.

f) Any other information considered to be useful to correctly identify the office and its responsibilities.

3. Shared offices may also be created by order of the Ministry of the Presidency, at the request of the Ministries in question, by grouping several ministerial departments. They may also be set up by a collaborative agreement in the case of grouping public institutions or local or Autonomous Community governments. This must be published in the Official State Gazette. Collaborative agreements may also determine an entity's or institution's inclusion in a pre-existing virtual office.

Article 4. *Characteristics of virtual offices.*

1. Virtual offices will be used to carry out all actions, procedures and services requiring authentication by the Administration or by citizens, using electronic means.

2. One or more virtual offices may be created as subsidiaries of a virtual office. Subsidiary virtual offices, or sub-offices, must be accessible through the main office's website, regardless of whether another direct electronic access is available.

Subsidiary virtual offices must meet the same requirements as the main virtual offices, excepting for being required to publish the order or resolution creating them; this will be done through the main office on which they depend. Their scope of application covers entities at General Subdirectorate level at the least.

Article 5. *Conditions for virtual office identification and secure communications.*

1. The websites pertaining to the Government of Spain and the public entities related to or dependent on it, and which function as virtual offices, should make this function known in a visible, clearly recognisable manner.

2. The instrument permitting the constitution of the virtual office should be accessible either directly or through a link showing its publication in the Official State Gazette.

3. The conditions for virtual office identification and secure communications shall be established by the third title of this royal decree, and in title VIII of the Regulations developing Organic Law 15/1999 of 13 December, ratified by Royal Decree 1720/2007 of 21 December.

4. Information systems supporting virtual offices must guarantee the confidentiality, availability and integrity of the information they manage. The National Interoperability Framework for and the National Security Framework shall establish the provisions necessary for doing so.

Article 6. *Content and services offered by virtual offices.*

1. All virtual offices shall post the following minimum content:

a) Identification of the office and governing body bodies and a list of those responsible for the management and services made available on the site and for any subsidiary offices, where applicable.

b) Information necessary for proper use of the office, including the virtual office map or equivalent information, specifying the website structure and the different sections available and the information regarding intellectual property.

c) Electronic assessment services to assist the customer in using the office correctly.

d) A system to verify the office's certificates, which shall be free and directly accessible.

e) List of the electronic signature systems which, in accordance with that stated in this royal decree, shall be permitted or used in the office.

f) Standards for creating the electronic register or registers to which the office has access.

g) Information related to personal data protection, including a link to the virtual office of the Spanish Agency for Data Protection.

2. Virtual offices shall place the following at their users' disposal:

- a) A list of services available through the virtual office.
- b) A charter of services and a charter of electronic services.
- c) A list of the electronic means referred to in article 27.4 of Law 11/2007 of 22 June.
- d) A link for formulating suggestions and complaints before the entities responsible for each particular case.
- e) Access to the file's processing status, where applicable.
- f) Publication of official notices or gazettes, where applicable.
- g) Where applicable, electronic publication of acts and notices that must appear on the notice board, indicating whether each substitutes or complements a regulation.
- h) Verification of the electronic identities of the public institutions or entities hosted by the website.
- i) Verification of the authenticity and integrity of documents issued by public organisations or entities hosted by the website, where those documents have been authenticated using a secure verification code.
- j) A marker showing the official date and time to those effects stated in article 26.1 of Law 11/2007, of 22 June.

3. Titular entities responsible for the site may also include other services or content, provided that the content complies with that stated in article 10 of Law 11/2007 of 22 June, and in this royal decree.

4. Subsidiary offices shall not be required to include the information and services referred to in the previous sections, as they will already be shown on the website for the parent institution.

5. Virtual offices whose governing body is active in territories having co-official languages shall provide access to their content and services in the appropriate languages.

#### *Article 7. Specific rules for responsibility.*

1. Establishing a virtual office means that the governing body shall be responsible for ensuring that the information and services to which it provides access shall be complete, truthful and updated. The governing body of a virtual office containing a link to another office under the responsibility of a different government body or public administration shall not be responsible for that site's providing complete, truthful and updated information.

The office shall establish the means that are necessary in order for a citizen to know whether the information or service he/she is accessing belongs to the office itself, an access link that does not serve as an office, or a third-party site.

2. Public organisations or entities responsible for the shared virtual offices described in article 3.3 of this royal decree shall in any case be answerable for their own content, with shared responsibility for common content.

#### *Article 8. Virtual office directory.*

1. The Ministry of the Presidency shall manage a directory of the virtual offices pertaining to the Government of Spain and its public entities. This directory shall be public and accessible



through the general access point referred to in article 9 of this royal decree.

2. This directory shall list each of the virtual offices by name, scope of application, governing body and website.

*Article 9. General point of access to the Government of Spain.*

1. The general point of access to the Government of Spain shall contain the virtual office which, in this sphere, shall facilitate access to the available services, procedures, and information offered by the government and its related or dependent public entities. It may also provide access to services or information corresponding to other public administrations if the appropriate agreements are signed.

2. Access shall be organised with attention to the different criteria permitting citizens to have easy, intuitive access to the services they wish to use.

3. The general point of access shall be managed by the Ministry of the Presidency, with the participation of all of the Ministries, and, if applicable, the public entities empowered by law to have a special independent regime, in order to guarantee that the site will contain complete and exact information and access links.

4. The general point of access may include additional services, and distribute information regarding electronic access to public services in such a way to enable its use by other ministry departments, administrations or the private sector.

## TITLE III

### Identification and authentication

#### CHAPTER I

#### Identification and authentication in citizens' electronic access to the Administration and its related or dependent public entities

*Article 10. Electronic signatures for citizens.*

1. Physical persons may use the electronic signature systems built into the Spanish National ID card in all cases, and such advanced electronic signature systems as are permitted by article 13.2.b) of Law 11/2007 of 22 June, for undertaking electronic procedures with the Government of Spain and its related or dependent public organisations.

2. Legal persons and entities without legal personhood may use electronic signature systems for legal persons or entities without legal personhood in all procedures and dealings with the government that permit electronic processes.

3. If a virtual office does not permit electronic signatures, it must provide alternative systems enabling legal persons and entities without legal personhood to exercise their right to undertake procedures with the government by electronic means.

*Article 11. Other electronic signature systems.*

1. The admission of other electronic signature systems as contemplated by article 13.2.c) of Law 11/2007 of 22 June must be approved by a Ministry order, or resolution by the governing body in the case of public entities, following a report by the High Council on eGovernment.

2. When the system refers to the entire Government of Spain, an agreement of the Council of Ministers will be necessary following a proposal by the Ministry of the Presidency and the Ministry of Industry, Tourism and Commerce, subject to report by the High Council on eGovernment.

3. The ratification act shall contain the name and general description of the identification system and the public body or institution responsible for its application and performance guarantees. It shall be published at the appropriate virtual offices, which shall inform the public of what procedures permit these methods of identification and authentication.

*Article 12. Common dispositions for the use of the electronic signature.*

1. The use of the electronic signature does not exclude the obligation of including, within the document or electronic message, the identification data which may be necessary under applicable legislation.

2. Citizens' use of electronic signature systems implies that Government bodies or other dependent or related public entities may examine the enclosed personal data in order to verify the signature.

*Article 13. Provisions for representing third parties.*

1. According to that stated in article 23 of Law 11/2007 of 22 June, the Government of Spain and its related or dependent entities may grant physical or legal persons the authority to present documents electronically in order to represent concerned parties, whether in general or specific cases.

Providing this power entails applying the representation regime regulated in the following article.

2. Granting such authority shall require the prior signing of an agreement between the competent Ministry or public entity and the concerned corporation, association or institution. The agreement must specify, at the very least, the procedures and processes in which representation is possible, and the conditions and obligations which apply to both the legal person or entity signing the contract and the physical or legal persons representing them.

In each case, a Ministerial Order from the department in charge of management shall determine the requirements and conditions for signing the Conventions referred to in this section. This order shall guarantee, in all cases, respect for the principles of objectivity, proportionality and non-discrimination as defined in the conditions for enabling representation.

3. Representation agreements shall exert effects on both the signing corporation, association or institution and on the physical or legal persons who are members or associates of those institutions. For the power of representation to become active, such members or associates must sign a personalised membership document that expressly states acceptance of its full content.

4. Failure to comply with the obligations assumed by the corporations, associations or institutions which sign the agreement will render it and the representation enabled by it null and void, following a review of the dossier in question in the presence of the concerned entity.

Failure to comply on the part of the person signing the personalised membership document shall entail his/her exclusion from the agreement, following the procedure and guarantees explained in the previous paragraph.

In both cases, consequences are described without prejudice to the liabilities that may be established.

*Article 14. Regime for granting power of representation before the Administration.*

1. Persons or entities invested with the power to present documents electronically in representation of third parties must have the necessary power of representation for each action, under the terms established in article 32 of Law 30/1992 of 26 November, or under the terms resulting from the legislation applying in the specific case.

2. The administration may require enabled persons to produce proof of their representative status at any time. Representation accredited by standard documents approved by the Administration for each procedure shall be considered to be valid.

Lack of demonstrable power of representation on the part of those persons in whose name documents were presented shall give rise to the appropriate penalties.

3. Enabling representation only grants the authorised person the status of representative for acts that are expressly authorised. It does not authorise said person to receive notifications from the Administration in the concerned party's name, even if they were issued as a result of the document presented by the representative.

4. Power of representation only enables the delivery of applications, letters or messages through the electronic registers corresponding to the sphere for which representation is effective.

*Article 15. Electronic register of instruments conferring consent for representatives to engage in electronic dealings with the Government of Spain and its related or dependent public organisations.*

1. The electronic register of instruments conferring consent shall be created for the sphere and exclusive purpose of electronic undertakings with the Government and its related or dependent public organisations, and not to serve as a public register. This register may be used to justify the certificates of representation which concerned parties grant to third parties who may then act in the former's name in electronic undertakings with the Government and/or its related or dependent public entities.

2. The Ministry of the Presidency shall create the files containing the necessary personal data and manage the register. The register must be coordinated with any other similar, more specific registries pertaining to the Government.

3. The instrument register allows subscribing Ministries and public institutions related to or dependent on the Government to verify the certificates of representation of those undertaking electronic actions in the name of a third party.

4. Each Ministerial Department and public institution shall specify the procedures and actions within its sphere of influence for which the certificates of representation listed in the registers shall be valid. In addition, should the certificates of representation formally incorporated into the instrument register be lacking or insufficient, the concerned party may claim the appropriate damages under the terms of article 32.4 of Law 30/1992 of 26 November, or in the terms of the specific legislation in question.

5. An order by the Ministry of the Presidency shall be given to specify the regime by which certificates of representation may be drawn up, the means of accrediting them, their scope of application, and the means to revoke the certificate, as well as the location and procedure for presenting documents accrediting representation. This shall be done to incorporate certificates into the electronic instruments register and organise other relative aspects.

*Article 16. Identification and authentication of citizens by civil servants.*

1. In order for civil servants to identify and authenticate citizens in accordance with that stated in article 22 of Law 11/2007 of 22 June, for those services for which such actions are taken, and which require the use of electronic signature systems but lack them, the civil servant capacitated for this task must have an electronic signature system recognised by the public entity or institution receiving the petition which requires identification or authentication. Likewise, the citizen must identify himself or herself before the civil servant and provide express consent, which must be duly documented in cases of discrepancy or legal action.

2. The Ministry of the Presidency will maintain an updated registry of the civil servants empowered by the Government and its public institutions to perform the identification and authentication processes regulated in this article. The appropriate cooperative agreement may be used to extend its effects to relationships with other Administrations.

3. Orders of the Ministry of the Presidency shall regulate the functioning of the registry of empowered civil servants, including the system for determining which civil servants may be so empowered and the scope of the empowerment.

4. In addition, the Ministerial Departments and public institutions may capacitate the civil servants they employ to identify and authenticate citizens before that Ministerial Department or institution.

## CHAPTER II

### **Identification and authentication of virtual offices and of the communications sent out by institutions or public entities within the Government of Spain, or those related to or dependent on the Government**

*Article 17. Identifying virtual Government offices and offices pertaining to its related or dependent public entities.*

1. Virtual offices shall be identified through electronic signature systems based on secure device certificates or equivalent means. In addition, for purposes of instant identification, citizens will possess the general mandatory information that must be shown in those signatures in accordance with that stated in the present royal decree.

2. For purposes of easy identification, virtual offices shall follow the general dispositions established for the Government's institutional image and their website name shall include the third-level dominion name ".gob.es".

*Article 18. Certificates for virtual offices of the Government of Spain and offices pertaining to its related or dependent public entities.*

1. Electronic certificates for virtual offices shall have the following minimum content:

- a) Description of the certificate type, bearing the name "virtual office".
- b) Descriptive name of the virtual office.
- c) Dominion name.
- d) Subscribing entity's VAT number.
- e) Administrative unit subscribing to the certificate.

2. The use of virtual office certificates is limited to identifying the office. Their use for signing documents and procedures electronically is excluded.

3. The National Security Framework referred to in article 42 of Law 11/2007 of 22 June shall determine the characteristics and requirements with which electronic signature systems shall comply, and the certificates and equivalent methods established in virtual offices in order to identify and guarantee secure communications.

*Article 19. Electronic signature systems using electronic stamp certificates.*

1. Electronic stamp certificates shall be created by resolution of the appropriate Undersecretary of the Ministry or the governing body of the public entity. It shall be published in the corresponding virtual office, showing the following:

- a) Organisation or entity holding the title to the electronic stamp certificate and responsible for its use, and proof of its registration with the Government or a public entity dependent on the Government.

- b) General technical characteristics of the applicable signature and certificate system.
- c) Validation service for verifying the certificate.
- d) Actions and procedures for which it may be used.

2. Electronic stamp certificates shall have the following minimum content:

- a) Description of the certificate type, bearing the name "electronic stamp certificate".
- b) Name of subscriber.
- c) Subscriber's VAT number.

3. The means of issuing electronic stamp certificates shall be defined in the National Security Framework.

#### Article 20. *Secure verification code systems.*

1. The Government of Spain and its related or dependent public entities may use secure code systems for verifying documents when carrying out automated processes. That code shall be linked to the entity or institution, and, where applicable, to the signer of the document. It shall in any case enable verifying the document's integrity through access to the corresponding virtual office.

2. The secure verification code system must guarantee, in all cases:

- a) The unique nature of the code generated for each document.
- b) Its connection with the document created and with the signer.
- c) It must also guarantee the possibility of verifying the document according to the time established in the resolution authorising use of this procedure.

3. Application of this system shall require an order from the appropriate Ministry or a resolution from the public organisation's governing body, following a report by the High Council on Electronic Administration, which shall be published at the corresponding virtual office. In addition to describing the function of the system, the said order or resolution by the public organisation's governing body must necessarily address the following:

- a) Automated processes to which the system applies.
- b) Entities responsible for applying the system.
- c) Dispositions that arise from applying the procedure.
- d) A list of mechanisms used in order to generate the code.
- e) Virtual office which concerned parties may access in order to verify the action or document content.
- f) Available time frame for the verification system as regards documents authorised by that system.

4. The Administration responsible for applying this system shall provide a direct and free channel for the use of concerned parties. Access to original documents shall be granted in accordance with the conditions and limits established by personal data protection laws or other specific legislation, as well as the general regime for access to administrative information established in article 37 of Law 30/1992 of 26 November.

5. The necessary measures shall be adopted to guarantee consistency in authenticating documents and checking for integrity once they are no longer available in the verification system, so that they may then be filed.

6. In order to improve electronic interoperability and make it possible to authenticate electronic documents with no need to access the virtual office in order to check the secure verification code, that code may be marked with the electronic stamp certificate described in the previous article.

7. Article 21. *Electronic signatures using personal authentication means.*

Employees of the Government of Spain and its related or dependant public institutions shall use the electronic signature systems determined for each case. These may include:

- a) Signature based on Spain's electronic ID card.
- b) Signature based on the certificate of a public employee in the service of the Government of Spain where expressly permitted for this purpose.
- c) Secure verification codes. In this case, that stated in Article 20 shall apply, with the appropriate adaptations.

Article 22. *Characteristics of electronic signature systems based on certificates provided to personnel employed by the Government of Spain or its public institutions.*

1. Electronic signature systems based on certificates which the Government of Spain or its related or dependant public organisations specifically provide to employees may only be used to execute functions pertaining to the position they occupy, or for dealings with Public Administrations when so permitted.

2. The electronic signature regulated in this article must comply with the guarantees established in applicable signature policies.

3. Certificates issued as signatures shall be known as "public employees' electronic certificates" and have the following minimum content:

- a) Description of the type of certificate to be referred to as a "public employee's electronic certificate".
- b) Certificate holder's name and surname(s).
- c) Certificate holder's National ID number or Foreign Resident number.
- d) Public institution or entity which provides services to the certificate holder.
- e) VAT number of the public institution or entity which provides services to the certificate holder.

## CHAPTER III

### **Common identification and authentication dispositions and interoperability conditions**

Article 23. *Obligations for certification service providers.*

1. Recognised certification service providers must comply with the obligations set forth in Law 59/2003 of 19 December on electronic signatures, as well as the additional general conditions referred to in section 3.

2. Certification service providers must provide the public validation platforms set up in accordance with this royal decree with free electronic access in order to verify the validity of certificates associated with systems used by citizens, the Government of Spain and its public entities.

3. The additional general conditions referred to in article 4.3 of Law 59/2003 of 19 December shall be passed by a royal decree approved by the Spanish Council of Ministers and drawn up jointly between the Ministry of the Presidency and the Ministry of Industry, Tourism and Commerce, following a report by the High Council on eGovernment.

Publishing the list of the recognised certification service providers and verifying that the established additional general conditions are met shall be the task of the Ministry of the Presidency and the Ministry of Industry, Tourism and Commerce.

Article 24. *Electronic signature and certificate policy.*

1. The electronic signature and certificate policy for the Government of Spain and its public institutions is made up of the directives and technical standards for the use of certificates and electronic signatures within their scope of application.

2. Without prejudice to that set forth in article 23, the electronic signature and certificate policy must contain in all cases:

- a) The requirements for electronic signatures presented before Government entities and public institutions.
- b) The technical and operational specifications for defining and providing the certificate services associated with the new identification and authentication methods used by the Government and listed in the present royal decree.
- c) The definition of its scope of application.

3. The electronic signature and certificate policy shall be approved by the High Council on eGovernment. An extract of the agreement approving the electronic signature and certificate policy shall be published in the Official State Gazette as a resolution by the Secretary of State for Civil Service. It shall be published in full on the virtual office offering general access to the Government of Spain.

Article 25. *Platforms for verifying certificates and the national verification system.*

1. The Ministry of the Presidency shall manage a platform for verifying the revocation status of certificates whose use is permitted by the Government of Spain and its related or dependent institutions, as stated in article 21.3 of Law 11/2007 of 22 June. This platform shall enable verification of certificates' revocation status and content and provide free and accessible service to all public administrations, whether Spanish or European.

2. Within the scope of their responsibilities, ministerial departments and public entities may use their own platforms to verify certificates' revocation status.

3. In order to improve the quality, reliability and availability of verification services offered to all public administrations, a national certificate verification system shall be created. It shall consist of the platform described in section one and additional platforms which shall comply with that stated in section four. The platforms within the national system may delegate specific verification operations to any of the other platforms. In particular, the platform operated by the Ministry of the Presidency shall provide the rest of the platforms with services for the validation of European-level certificates.

4. The validation service platforms that form part of the national certificate verification system must meet the following requirements:

- a) They must be able to automatically obtain and process the lists of recognised certificates issued as per this royal decree and which meet the terms established in the applicable electronic signature and certificate policy.
- b) They must be accessible through, and provide their services over, the Spanish Government communications network, in keeping with the security and availability conditions appropriate to the volume and criticality of the services using them. However, other access channels may exist as back-up methods.
- c) They must include service documentation and operating procedures.
- d) They must guarantee a service level ensuring the availability of status information and certificate validation under the conditions established in the electronic signature and certificate policy.
- e) They must include a declaration of validation practices with a list of the verification service obligations to which the institution commits. The declaration must be accessible to the public for free and by electronic means.

f) They must set up the calling and synchronisation mechanisms and protocols which are necessary in order to create the national certificate verification system and access the universal validation systems offered by the Ministry of the Presidency's platform. Their operability shall be based on the directives defined in the electronic certificate and signature policy within the scope of the Government of Spain.

g) They shall comply with that established in the National Interoperability and Security Frameworks with regard to the general conditions which regulate certificate validation services and platforms.

## TITLE IV

### Electronic Registers

#### Article 26. *Electronic registers.*

All Ministerial Departments within the Government of Spain, as well as its public entities, must include an electronic registry service for receiving and issuing applications, statements and messages corresponding to the procedures and actions under its jurisdiction. The registry service may be its own or provided by another entity or organisation.

#### Article 27. *Creation of electronic registers.*

1. Electronic registers shall be created by order of the respective Ministry or resolution of the governing body of the public entity after receiving the approval of the Ministry of the Presidency, except for public institutions that do not require one, in accordance with the institution's specific legislation. Public entities may use the electronic register belonging to their corresponding ministerial department. To this end, they will sign the appropriate agreement.

2. Dispositions which create electronic registers will contain the following minimum elements:

- a) Organisation or unit responsible for managing the register.
- b) Official date and time of reference and calendar of non-working days as applicable.
- c) Identification of the organisation(s) responsible for approving and modifying the list of standard electronic documents under that register's jurisdiction, and a list of the processes and procedures in which they are used.
- d) Means of presenting additional documentation to accompany a message, statement or application which was previously entered in the electronic register.

3. The official e-mail addresses assigned to civil servants or to various units and organisations shall under no circumstances be considered electronic registers.

4. Likewise, devices for receiving fax communication shall not be considered electronic registers, except in those cases where such is expressly stated by legal decree.

#### Article 28. *Functions of electronic registers.*

Electronic registers shall perform the following functions:

a) Receiving and issuing applications, statements and messages under the organisation's jurisdiction in accordance with its statutes of creation and the attached documents, in addition to issuing the receipts necessary for confirming reception under the terms set forth by Article 25 of Law 11/2007 of 22 June.

b) Issuing statements, applications and messages to concerned individuals, entities or units under the terms of this royal decree and Article 24.2.b of Law 11/2007 of 22 June.



- c) Recording the corresponding entry and issue numbers.
- d) Providing proofs and certification in the case of lawsuits, discrepancies or questions regarding the receipt or issue of applications, statements and messages.

Article 29. *Applications, statements and messages that may be refused by electronic registers.*

1. Electronic registers may refuse electronic documents presented under the following circumstances:

- a) The documents are addressed to organisations or entities which are outside the jurisdiction of the Government of Spain.
- b) Documents contain malicious code or devices that may affect system integrity or security.
- c) For standard documents, when fields listed as required in the resolution approving that document are left blank, or when they contain incongruences or omissions that prevent them from being processed.
- d) Documents which, in accordance with that established in articles 14 and 32, must be presented in certain specific electronic registers.

2. In those cases listed in the previous section, the sender of the document will be informed of the refusal and of the reasons for it. In addition, whenever possible, the sender will be advised as to how to remedy the situation and the address to which documents should be sent. When the concerned party so requests, he/she shall receive proof of attempted delivery, including the reasons for refusal.

3. When one or more of the circumstances listed in section 1 are present but the application was not automatically rejected by the electronic register, the competent administrative body shall demand that the appropriate corrective measures be taken, informing the concerned party that if the requirements are not fulfilled, the presentation will not be valid or recognised.

Article 30. *Receipt of applications, statements and messages.*

1. Applications, statements and messages may be presented by electronic register 24 hours a day on any day of the year.

2. Receipt of applications, statements and messages may be interrupted during only such time as is necessary for documented reasons of technical or operational maintenance work. Potential users of the electronic register must be notified regarding service interruptions as early as possible in each case.

In cases of unplanned interruptions in the operation of the electronic register, where possible, there shall be means available in order to inform users of this situation and of the effects of suspending service. Express mention shall be made of any extensions to immediate deadlines, where applicable. As an alternative, a re-routing system may be set up allowing users to employ a different electronic register from the one that was interrupted.

3. The electronic register shall use the same format to automatically issue an electronically signed receipt, using one of the signing systems mentioned in article 18 of Law 12/2007 of 22 June with the following content:

- a) Copy of the presented statement, message or application. A literal transcription of the data that was entered in the form is valid for these purposes.
- b) Date and time of presentation and register entry number.
- c) Where applicable, a list of the documents attached to the electronic form or presented document, followed by the electronic identifier for each document.
- d) Information regarding the maximum time frame established by law for resolving the procedure and notifying the concerned party, including the implications of receiving no

This document is a translation of the Royal Decree 1671/2009, of 6 November, which partially develops Law 11/2007 of 22 June, regarding citizens' electronic access to public services, published in the Spanish Official State Gazette. It is not an official translation and therefore has no legal validity. The original version can be found at [http://www.boe.es/aeboe/consultas/bases\\_datos/doc.php?id=BOE-A-2009-18358](http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-2009-18358)

answer from the administration, when this may be determined automatically.

Article 31. *Creation, nature and workings of the Common Electronic Register.*

1. The Common Electronic Register for the Government of Spain shall be created and made accessible through the general access point established in Article 9.
2. The Common Electronic Register shall be managed by the Ministry of the Presidency.
3. The Common Electronic Register shall make it possible to present any type of applications, statements and messages addressed to the Government of Spain and its public organisations.
4. The Common Electronic Register shall inform citizens and redirect them, where applicable, to the registers set up to receive documents requiring specific computer applications in order to be processed.
5. An order of the Ministry of the Presidency shall establish the requirements and conditions for the workings of the Common Electronic Register, including the creation of a dossier that meets the conditions of the legislation on personal data protection, as well as other requirements stated in Article 27.2.

TITLE V

**Regarding messages and notifications**

CHAPTER I

**Electronic communications**

Article 32. *Communication by electronic means as a mandatory action.*

1. Communicating with institutions within the Government of Spain or its related or dependent public entities by electronic means, under those circumstances listed in Article 27.6 of Law 11/2007 of 22 June, may be made mandatory by a ministerial order. This obligation may extend to include sending administrative notifications by electronic means, and the necessary use of such electronic registers as may be called for.
2. The order establishing such an obligation shall specify the communications to which it applies, the electronic format in question, and the individuals bound to the obligation. This order must be published in the Official State Gazette and posted at the virtual office of the relevant public institution or organisation.
3. If communication by electronic means is mandatory and those means are not used, the competent administrative institution shall notify the subject of the need to remedy the situation, stating that if the requirement is not met, presentation of the document will not be valid.

Article 33. Modification of the initially chosen means of communication.

With the exception of the cases listed in the previous article, citizens may modify their means of communication with the public institutions or organisations related to or dependent on the Government of Spain and use a channel other than that initially chosen. This shall begin to produce effects with respect to the communications that are issued beginning the day after receiving the request through the competent institution's register.

Article 34. *Communications between the institutions and public entities of the Government of Spain.*

1. Institutions and public entities of the Government of Spain shall use electronic means to communicate with each other. Use of other means of communication shall be

This document is a translation of the Royal Decree 1671/2009, of 6 November, which partially develops Law 11/2007 of 22 June, regarding citizens' electronic access to public services, published in the Spanish Official State Gazette. It is not an official translation and therefore has no legal validity. The original version can be found at [http://www.boe.es/aeboe/consultas/bases\\_datos/doc.php?id=BOE-A-2009-18358](http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-2009-18358)

permitted in exceptional cases when electronic means cannot be used due to documented technical reasons.

2. Institutions and public entities of the Government of Spain shall use electronic means to communicate with other administrations. However, other means of communication may also be used depending on the technical workings of the other administrations.

The necessary agreements shall be signed in order to guarantee the conditions for this communication, except when those conditions are already stated in specific legislation.

## CHAPTER II

### Electronic notifications

Article 35. Sending notifications by electronic means.

1. Institutions and public organisations within the Government of Spain shall provide electronic notification systems as per that stated in this chapter.

2. Electronic notifications may be sent by means of the following methods:

a) By using the website set up according to regulations stated in Article 38 of this royal decree.

b) By using e-mail systems with a delivery confirmation function that furnishes proof that messages have been received, according to that stated in Article 39 of this royal decree.

c) By making an electronic appearance at the virtual office as regulated by Article 40 of this royal decree.

d) By other means of electronic notification that may be established, provided that there is proof of the concerned party's having received the notice within the time frame and under the conditions established by specific legislation.

Article 36. *Choosing the notification method.*

1. Notifications shall be issued by electronic means upon the request or express consent of the third party, or when electronic means are made mandatory in accordance with that stated in Articles 27.6 and 28.1 of Law 11/2007 of 22 June.

2. The request should express that party's wish to receive notification through one of the recognised electronic means, and indicate a valid address for electronic notifications in accordance with that stated in the present royal decree.

3. Both the statement of preference for use of electronic means and the statement of consent may be issued and procured by electronic means, in all cases.

4. When the notification must necessarily be received by electronic means, the concerned party may choose among the different available methods, unless the regulation establishing the mandatory nature of electronic notifications should indicate a specific method.

5. When several notifications are generated with regard to the same administrative act, due to using different electronic or non-electronic means, it shall be understood that all legal effects deriving from notification shall be in force when the first of the properly issued notifications is received. This shall also apply to the time span allowed for appealing a decision. Government entities may include this statement in the content of the notification itself.

6. When notification is issued by one of the valid and recognised methods, if the concerned party should undertake actions that would require knowledge of the content and scope of the resolution or act regarding which the notification was sent, then that party is considered to have consented to the use of electronic means of notification for that specific administrative action. The notification shall be effective beginning on the date when the concerned party undertakes such actions.

In the case described in the preceding paragraph, all other resolutions or acts related to that procedure must be notified by the applicable means and format in accordance with that

stated in Law 11/2007 of 22 June, and in the present royal decree.

*Article 37. Modifying the notification method.*

1. While the procedure is being carried out, the concerned party may request that the public entity in question not use electronic means for subsequent notifications. In this case, other means permitted by Article 59 of Law 30/1992 of 26 November may be used, except in those cases in which notification by electronic means shall be mandatory in accordance with that stated in Articles 27.6 and 28.1 of Law 11/2007 of 22 June.

2. The request to modify the preferred means of communication must include the method and address for receiving subsequent notifications.

3. Changing the means of notification shall be effective for those notifications issued beginning on the day after the request for modification is received at the register of the responsible public organisation or entity.

*Article 38. Notification by making the electronic document available through the website set up for that purpose.*

1. Electronic notification systems using a properly configured website shall be valid as long as they meet the following minimum requirements:

- a) Indication of the date and time when the act requiring notification was made available to the concerned party.
- b) Possibility for concerned parties to have permanent access to the corresponding website by using a virtual office or other means.
- c) Indication of the date and time when the concerned party accessed the content.
- d) Inclusion of authentication mechanisms to determine the user's identity and guarantee his or her exclusive access to the content.

2. A website shall be set up in order to provide these notifications, and it shall be available to all public institutions and entities related to or dependent on the Government of Spain which do not possess their own notification systems. This website shall be the responsibility of the Ministry of the Presidency. Here, citizens may request an electronic address, which shall be valid during an indefinite period except in cases of closure by the address holder, death of the physical person or dissolution of the legal entity, order by an administrative or judicial order, or when three years pass without the address being used for notifications. In this case, the e-mail address shall be discontinued, and the concerned party informed of that action.

3. In cases in which the use of electronic notifications is mandatory, the electronic address referred to in the previous paragraph shall be officially assigned and may be valid indefinitely, in accordance with the framework established by the Ministry of the Presidency and referred to in the first final disposition. The framework for all other valid electronic addresses shall be established by order of the governing body for the corresponding Department.

*Article 39. Receiving notification through an e-mail address.*

It shall be possible to issue notifications to the e-mail addresses of an individual's choosing provided that the e-mail service issues a delivery confirmation slip at such time as the content of the notification is accessed. Confirmation must be issued automatically and without intervention by the recipient.

*Article 40. Notification by making an electronic appearance.*

1. Notification by means of an electronic appearance refers to duly identifying the concerned party and granting him or her access to the content for the corresponding administrative action through the virtual office of the responsible public entity or organisation.

2. In order for electronic citation to give rise to the effects of notification in accordance with Article 28.5 of Law 11/2007 of 22 June, the following conditions must be met:

- a) Prior to gaining access to the content, the concerned party must view a message stating that accessing the administrative procedure in this way will have the legal effects of receiving notification.
- b) The corresponding information system shall record that the access took place and indicate the date and time.

## TITLE VI

### Electronic documents and copies

#### CHAPTER I

#### Common dispositions regarding electronic documents

Article 41. *Characteristics of electronic documents.*

1. Electronic documents must meet the following requirements in order to be valid:

- a) Contain information of any type.
- b) Store information in electronic form and in a certain format which enables individual identification and processing.
- c) Be provided with identifying data allowing them to be handled individually even if they are included in an electronic file.

2. In addition to meeting the previous conditions, electronic administrative documents must have been electronically issued and signed using one of the signature systems listed in Articles 18 and 19 of Law 11/2007 of 22 June. They must also comply with the validity requirements set forth in Law 30/1992 of 26 November.

Article 42. *Adding metadata to electronic documents.*

1. To the effects of this royal decree, metadata shall be understood as any type of information in electronic format that is associated with electronic documents, instrumental in nature and independent from content, and intended to make a certain characteristic known in an immediate and automatable way. Its purpose is to guarantee availability, accessibility, preservation and interoperability for that document.

2. Electronic documents subject to being included within an electronic file must have associated metadata which allow them to be sorted by their corresponding entity or institution, function, and the administrative procedure in question.

In addition, information regarding the document signature and time stamp shall be associated with them in the manner regulated by this royal decree.

3. For all cases, the acting entity or institution shall be the one to associate metadata with the electronic documents submitted by citizens or issued by the Government of Spain or its public organisations, in the manner determined for each case.

4. The minimum mandatory metadata associated with electronic documents, as well as the association of signature or time stamp data, shall be specified in the National Interoperability Framework.

5. Once the metadata are associated with an electronic document, they may not be modified in any subsequent phase of the administrative process, except in the following cases:

- a) When errors or omissions are found in the initially assigned metadata.

b) When the metadata require updating, if such is indicated in the National Interoperability Framework.

Metadata modification must be performed by the competent entity according to the specific legislation for each institution, or automatically according to the standards established to that effect.

6. Apart from the minimum mandatory metadata referred to in section 4, different entities or organisations may also associate complementary metadata with electronic documents to meet the specific classification needs for each management environment. These metadata shall be added according to the specifications established by the National Interoperability Framework for that purpose. Complementary metadata are not subject to the modification prohibitions set forth in the previous section.

*Article 43. Electronic documents copied electronically by the Government of Spain and its public institutions.*

1. Since the electronic copies are identical to the original electronic document, with no changes in format or content, they shall have the same legal effects as the original electronic document.

2. If there is a change in the original format, the following conditions must be met in order for an electronic document to be considered an authentic copy:

- a) The original electronic document must still exist and be in the keeping of the Administration.
- b) The copy must be made in accordance with the competency and procedure regulations which apply in each case, including those concerning automatic retrieval.
- c) The associated metadata must indicate that the document is a copy.
- d) The copy must be authorised by an electronic signature proceeding from the systems listed in Articles 18 and 19 of Law 11/2007 of 22 June.

3. Authentic electronic copies may be made from other authentic electronic copies provided that the requirements established in the previous sections are met.

4. The entities issuing administrative electronic documents or receiving private electronic documents or files shall be bound to keep the original documents, even if the documents have been copied in accordance with that stated in the present article, without prejudice to that stated in article 52.

5. Electronic copies of electronic documents presented using standardised systems or forms shall be considered authentic in the following cases:

- a) When obtained according to that stated in the sections preceding this article.
- b) When the electronic document, authenticated with the electronic signature of the receiving institution or entity, contains all of the variable information which the citizen filled out and endorsed on the corresponding form used to present the individual content.

*Article 44. Electronic copies of documents in non-electronic format.*

1. Electronic copies of documents in paper format or another format which may be digitalised, including documents issued by the administration and private documents delivered by citizens, shall be prepared by the Government of Spain and its related or dependent public organisations in accordance with that regulated in this Article.

2. To the effects of that regulated by this royal decree, an electronic copy is defined as an "electronic image resulting from applying a digitisation process to a document in paper or another format permitting extraction of a faithful copy".

"Digitisation" is understood to mean the technological process by which a document in paper or another non-electronic format is converted into an electronic file containing a complete, faithful encoded image of the document.

3. When they are made by the Administration, electronic images are considered authentic electronic copies. They shall have the scope and legal effects set forth in Article 46 of Law 30/1992 of 26 November, provided that they meet the following requirements:

- a) The document being copied must be an original or an authentic copy.
- b) The electronic copy must be authorised by an electronic signature proceeding from the systems listed in Articles 18 and 19 of Law 11/2007 of 22 June.
- c) The electronic images must be encoded according using the formats, quality levels and technical conditions specified in the National Interoperability Framework.
- d) The associated metadata must indicate that the document is a copy.
- e) The copy must be made in accordance with the regulations regarding competency and procedure which apply in each case, including those on automatic retrieval.

4. The administrative entity delivering the original administrative document will not have to intervene in order for authentic electronic copies to be made, provided that the electronic images are obtained from authentic paper copies that meet the requirements listed in Article 46 of Law 30/1992 of 26 November.

Article 45. *Paper copies of official administrative electronic documents made by the Government of Spain and its public institutions.*

The following requirements must be met in order for paper copies of official administrative electronic documents to be considered authentic copies:

- a) The copied electronic document must be an original or an authentic electronic copy of the original electronic or paper document, and original/authentic copies must be issued according to that stated in the present royal decree.
- b) The document must bear an electronically generated code or another verification system indicating that the code permits verification of the copy's authenticity through access to the electronic archives of the issuing public organisation or institution.
- c) The copy must be made in accordance with the regulations referring to competency and procedure which apply in each case, including those on automatic retrieval.

Article 46. *Destroying documents in non-electronic format.*

1. Original documents and authentic paper or other non-electronic copies admitted as proof for legal purposes may be destroyed under the terms and conditions determined in the corresponding resolutions if authentic electronic copies have been made and the following requirements are met:

a) Destroying documents shall require the adoption of a resolution by the organisation responsible for the procedure, or where applicable, by the entity responsible for keeping the documents. The appropriate elimination process file must first be opened, and it must list the specific nature of the documents to be destroyed, the administrative procedures in question, the conditions and guarantees of the destruction process, and a list of the persons or entities responsible for the process.

The resolutions approving the elimination processes regulated by Article 30.4 of Law 11/2007 of 22 June shall require a preliminary report from the respective Commission for the Classification of Administrative Documents, followed by a favourable sentence from the

High Commission on the Classification of Administrative Documents. As a whole, the reporting period may not exceed three months. Once this time period has passed and if neither entity has issued an express response, the elimination process file shall be resolved and the documents destroyed.

b) Documents may not have any historical, artistic or any other relevant value that would justify their being preserved or protected, and they may not contain signatures or any other handwritten or mechanical marks that would lend them exceptional value.

2. An analysis of the risks involved in destroying the documents in question must be included in the elimination process file. The analysis must make explicit mention of the guarantees in place for preserving electronic copies and complying with security conditions established by the National Security Framework for the preservation and safekeeping of electronic documents.

3. The destruction of any type of document other than those listed in the previous sections shall be subject to that stated in Royal Decree 1164/2002 of 8 November. That decree regulates the preservation of documents with historical value, management of the elimination of other documents pertaining to the Government of Spain and its public entities, and the preservation of administrative documents in formats other than the originals.

## CHAPTER II

### **Specific regulations regarding administrative electronic documents**

Article 47. *Time references for administrative electronic documents.*

1. The Government of Spain and its dependent or related public entities shall, under the terms of Article 29.3 of Law 11/2007 of 22 June, associate one of the following types of time reference, in accordance with that stated in the code regulating each different procedure:

a) "Time reference", understood to mean use of electronic means to imprint the date, and where applicable, the time, on an electronic document. The time reference shall be used in all cases in which regulations do not call for the use of a time stamp.

b) "Time stamp" is understood to mean electronically assigning a date and time to an electronic document with the intervention of a certification services provider which guarantees the exact, integral nature of the document's time reference.

Information regarding time references and stamps shall be associated with electronic documents in the manner determined by the National Interoperability Framework.

2. The list of electronic certification service providers which lend time stamp services to the Government of Spain, in accordance with that stated in article 29.3 of Law 11/2007 of 22 June, as well as the requirements which they must meet in order to be listed, shall be regulated by the royal decree referred to in article 23.3.

## CHAPTER III

### **Specific regulations regarding electronic documents delivered by citizens**

Article 48. *Electronic images delivered by citizens.*

1. In accordance with Article 35.2 of Law 11/2007 of 22 June, concerned parties may, at any stage of a procedure, deliver digital copies of documents bearing an advanced electronic



signature proving that they are faithful copies of the original. The public administration may have the content of copies provided in a file checked against the originals. If checking the originals is not possible, the administration may, as an exception, require the citizen to present the original document or information. Providing such copies implies authorising the administration to access and handle the personal information contained in these documents. The abovementioned electronic images shall not be considered authentic copies.

2. Electronic images presented by citizens must meet the format and standard requirements approved in the National Interoperability Framework for such processes. Should this requirement not be met, the concerned party shall be bound to remedy the situation according to the terms established in article 71 of Law 30/1992 of 26 November.

3. In addition to concerned parties presenting documents in any of the appropriate locations established by Article 2.1.a), b), and d) of Royal Decree 772/1999 of 7 May, they may also present formats containing electronic documents to the effects established in Article 35.2 of Law 11/2007 of 22 June.

4. Requests to check delivered copies, which are described by Article 35.2 of Law 11/2007 of June 22, shall be regulated by the data transmission standards set forth in Article 2 of the present royal decree.

#### CHAPTER IV

##### **Standards relating to citizens' obtaining electronic copies**

###### *Article 49. Obtaining electronic copies of electronic documents.*

Citizens may exercise their right to obtain electronic copies of electronic documents used in procedures that are of concern to them, in accordance with the regulations for the procedure in question.

A copy may be issued in the form of an extract of the document, or using other electronic methods that permit any data that do not concern the individual in question to be kept confidential.

###### *Article 50. Obtaining electronic copies for certification purposes.*

When concerned parties wish to exercise the right regulated in Article 8.1 of Royal Decree 772/1999 of 7 May regarding delivering certified copies for a procedure, and where the originals are not necessary for that procedure, the office receiving the document should proceed to obtain the electronic copy of the documents to be certified, if it possesses the proper means to do so. This must be done using the procedure regulated in Article 44 of this royal decree, and the office must be one of the locations for presenting documents listed in Article 2.1.a), b) and d) of the royal decree mentioned above.

These digitised copies shall be signed electronically using one of the procedures listed in Articles 18 and 19 of Law 11/2007 of 22 June. They shall be considered certified or verified copies as per Article 8 of Royal Decree 772/1999 of 7 May, with no need to accredit the authenticity of the original document, as they are exempt from the verification procedure set forth in Article 35.2 of said law.

#### CHAPTER V

##### **Electronic archiving of documents**

###### *Article 51. Electronic archiving of documents.*

1. The Government of Spain and its related or dependent public institutions must use electronic formats for archiving all electronic documents used in administrative procedures,

and which form part of an administrative archive. This also applies to all other documents which justify the dealings between citizens and the Administration.

2. Preservation of electronic documents may be done on a document-by-document basis, or by compiling information which they contain in data bases. In the latter case, it will be necessary to have the criteria for reconstructing the electronic forms or applications used to create the documents, and for checking the electronic signature for those data.

Article 52. *Preserving electronic documents.*

1. The minimum periods for archiving electronic documents will be determined by each government entity depending on the administrative procedure in question. In any case, the general regulations on preserving historical documents and eliminating documents belonging to the Government of Spain and its public entities shall apply in all cases, except in the case of destroying paper documents which have electronic copies.

2. In order to preserve the maintenance, access and legibility of archived electronic documents, conversion operations may be carried out in accordance with the regulations on copying such documents set forth in this royal decree.

3. Those responsible for electronic archiving shall promote the creation of authentic copies, changing document and file formats in the archives as soon as those formats are dropped from the list of formats permitted for administrative purposes under the National Interoperability Framework.

## Chapter VI

### Electronic files

Article 53. *Creation of electronic files.*

1. Creating electronic files is the responsibility of the entity assigned by the specific organisation's regulations. If no such assignment exists, it shall fall to the entity's process supervisor.

2. Electronic files which may be forwarded or made available shall be created according to the following rules:

a) Electronic files shall have a unique code permitting them to be identified by any entity within the Administration in an environment permitting exchange between different entities.

b) Electronic files shall be paginated by means of an electronic index signed electronically using one of the systems listed in Articles 18 and 19 of Law 11/2007 of 22 June, and according to the terms of article 32.2 of that law.

c) In order to guarantee the interoperability of the files, referring to both their structure and format and to the specifications for forwarding and reference use will follow the regulations established for that purpose by the National Interoperability Framework.

d) Electronic files shall contain electronic documents which may be included in different files; files may contain other electronic files if the procedure so requires. Exceptionally, when a document's nature or volume does not permit it to be included in the file, or when it would make doing so extremely difficult in light of the established standards and procedures, documents must be listed in the file index regardless of being added separately.

e) Documents included in the electronic file shall be in a long-duration format or formats, and accessible under the terms determined by the National Interoperability Framework.

Additional provision one. *Special procedures.*

1. That stated in this royal decree shall be applicable without prejudice to the special regulation contained in Law 30/2007 of 30 October, on Public Sector Contracts and their operational regulations with regard to the contractor profile, the State Hiring Platform and the use of electronic media for procedures related to public hiring.

2. The dispositions in this royal decree on the electronic management of procedures having to do with taxation, social security and unemployment, and the legal regime for foreign nationals in Spain shall be applied in accordance with that established in the fifth, sixth, seventh and nineteenth additional dispositions of Law 30/1992 of 26 November.

3. That stated in the present royal decree shall also apply to the special regime outlined in Royal Decree 1496/2003 of 28 November which approves the regulations on invoicing obligations. It also modifies the Regulation on Value Added Tax and Order EHA/962/2007 of 10 April which develops certain dispositions on electronic invoicing and the electronic storage of invoices mentioned in the above royal decree. This special legal regime shall apply to any electronic copies of invoices to be submitted to entities and organisations within the Government of Spain.

4. That stated in this royal decree shall not affect the regulation contained in royal decrees 181/2008 of 8 February regarding the ordinance for the administrative journal known as the "Official State Gazette" and 1979/2008 of 28 November, regulating the electronic edition of the "Official Gazette of the Companies Register".

Additional provision two. *Statistical function.*

That stated in Article 2 shall not apply to data gathering activities covered by Chapter II of Law 12/1989 of 9 May on the Public Statistical Function.

Additional provision three. *Directory of virtual offices.*

Within six months of the date on which this royal decree enters into force, the Ministry of the Presidency shall post the Directory of virtual offices referred to in Article 8 on its website.

Additional provision four. *Preserving the identities of electronic addresses.*

Without prejudice to that established as a general standard in Article 17.2, existing and well-known e-mail addresses for public entities may be maintained with the same electronic identification.

Additional provision five. *Certificate verification platform pertaining to the Fabrica Nacional de Moneda y Timbre-Real Casa de la Moneda.*

In accordance with the capacities bestowed on the *Fabrica Nacional de Moneda y Timbre-Real Casa de la Moneda* (National Mint and Stamp Factory – Royal Mint) by Article 81 of Law 66/1997 of 30 December on Fiscal, Administrative and Social measures relating to additional disposition four in Law 59/2003 of 19 December on electronic signatures, the certificate verification platform developed by that entity shall be integrated into the national certificate verification system regulated by article 25.3 in the present royal decree, in compliance with that specified in Article 25.4.

The Ministry of the Presidency and the National Mint and Stamp Factory shall adopt the measures necessary in order to attain permanent and perfect functional coordination and technical compatibility between both verification platforms. This shall serve to guarantee their interoperability and ensure better service to administrations and citizens.

Additional disposition six. *Absence of budgetary impact.*

The implementation of the provisions contained in this royal decree should not lead to any increases in public spending or decreases in public revenue. Involved ministerial departments must therefore develop the measures needed in order to comply with a view to their ordinary budgetary resources. Under no circumstances should this lead to the contemplation of additional financing needs.

Transitory provision one. *Electronic signature systems.*

1. Until such time as the National Interoperability and Security Frameworks shall be ratified, the currently admitted identification and authentication methods may be used. These frameworks establish the time frames for approving the lists of permitted methods, as well as the maximum time frames for employing those methods which were used at one point, but which do not conform to the list of permitted methods.

2. In particular, they may still be employed for the purposes listed in this royal decree and with the same legal effects as the electronic stamp and the electronic signature belonging to a legal person or the governing body of an administrative entity, observing that stated in the corresponding legislation.

Transitory provision two. *Security conditions for verification platforms.*

Until such time as the National Interoperability and Security Frameworks shall be ratified, the existing verification services that are operating at the time when this royal decree enters into force shall continue to be valid. Certificates linked to these systems or services may be used in the procedures that indicate them expressly.

Transitory provision three. *Electronic notification system regulated in Article 38.2.*

Until such time as legislation for the electronic notification system regulated in article 38.2 shall be approved, in accordance with the first final disposition, the operations planned for the notification system shall be carried out using authorised services, in accordance with Order PRE 1551/2003 of 10 June which develops the first final disposition of Royal Decree 209/2003 of 21 February, regulating electronic registers and notifications and the use of electronic means to substitute the presentation of certificates by citizens.

Transitory provision four. *Adapting virtual offices.*

Until such time as the National Interoperability and Security Frameworks shall be ratified, the creation of virtual offices must be accompanied by a report attesting to compliance with the confidentiality, availability and completeness conditions for the information and communications relayed through those offices.

Transitory provision five. *Adapting the Foreign Offices of the Government of Spain.*

For Foreign Offices of the Government of Spain, that stated in this royal decree to shall be applied depending on the means for identifying and authenticating citizens, the electronic channels and the operating conditions that are available at a given time.

Sole derogatory provision. *Revoked provisions.*

The dispositions of equal or lower rank which contradict that stated in this royal decree are hereby null and void, particularly:

- a) Royal Decree 263/1996 of 16 February regulating the use of electronic, computing and automated techniques by the Government of Spain.

b) Articles 14 to 18 of Royal Decree 772/1999 of 7 May, regulating the presentation of applications, statements and messages to the Government of Spain, the issuing of document copies and return of originals, and the regime for register offices.

First final disposition. *Electronic notification system regulated in Article 38.2.*

The regime for the official electronic address system outlined in article 38.2, which must conform to the provisions of that article, is hereby established by order of the Ministry of the Presidency.

Second final disposition. *General access point.*

Within three months of the date on which this royal decree enters into force, the Minister of the Presidency shall adopt such dispositions as are necessary in order to constitute the general access point for the Government of Spain as regulated in Article 9.

Third final disposition. *Electronic registers.*

Electronic registers which already existed when Law 11/2007 of 22 June entered into force, and which are regulated by Section 2 of the Single Transitory Disposition of that law, shall adapt their operations to those established by this royal decree within the six months following its entry into force.

Adapting measures to those described in the present royal decree shall be done by means of a ministerial order, or where applicable, a resolution by the governing body of the corresponding public organisation; the latter case must be in accordance with that described in Article 27.

Fourth final disposition. *Virtual offices.*

Electronic access points belonging to the Government of Spain or to its dependent or related public entities through which communications peculiar to the virtual office currently take place must adapt to that stated in this royal decree for virtual offices or sub-offices, where applicable. This must be done within four months beginning on the date on which this royal decree enters into force, without prejudice to that stated in transitory dispositions one and two of this royal decree and in the third final disposition of Law 11/2007 of 22 June.

Fifth final disposition. *Capacitation for legislative development.*

The Ministers of the Presidency, Economy, the Treasury and Industry, Tourism and Commerce are hereby capacitated to formulate the dispositions necessary to execute this royal decree within the scope of their respective jurisdictions.

Sixth final disposition. *Entry into force.*

The present royal decree shall enter into force on the day following its publication in the Official State Gazette.

Ordered in Madrid on 6 November 2009.

JUAN CARLOS I.

First Vice-President of the Government  
and Minister of the Presidency,  
MARIA TERESA FERNÁNDEZ DE LA VEGA SANZ

*This document is a translation of the Royal Decree 1671/2009, of 6 November, which partially develops Law 11/2007 of 22 June, regarding citizens' electronic access to public services, published in the Spanish Official State Gazette. It is not an official translation and therefore has no legal validity. The original version can be found at [http://www.boe.es/aeboe/consultas/bases\\_datos/doc.php?id=BOE-A-2009-18358](http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-2009-18358)*

evc. BOE-A-2009-18358