Declaration of Certification Practices

Corporate Certificates

Versión: 1.6

Vigencia: 01/03/2011

ancert

Agencia Notarial de Certificación

1. Overview

1.1. Document control

Project:	**Declaration of Certification Practices class Corporate Certificates**
Target entity:	**Notarial Certification Agency, S.L.U.**
Reference code:	
Version:	**1.6**
Date of publication:	
File:	**DPC-ANCERT-Cert-CORP-v1r6.doc**
Format:	**Word 2007**

1.2. Versioning

Version	Changes	Description of Change	Date of change	Publication Date
1.1	Original	Creation of document	27/03/2010	
1.2		Document Review	05/05/2010	
1.3	1.3.1	Incorporation of the fingerprints of CA certificates	02/06/2010	
1.4	Logo ANCERT	New logo ANCERT	30/11/2010	
1.5		Review of legal issues and format	21/12/2010	01/01/2011
1.6	Section 4.9.6 Section 1.1.2 Sections 1, 2, 3 y 4	CRL 60 days of historical information.More detailed description of certifícate uses. Addition of Corporate Certificates of Secure Server.	30/01/2011	01/03/2011

2. Table of Contents

3. Introduction

This document contains the Declaration of Certification Practices for certificates of class "Corporate Certificates" issued by the Notarial Certification Agency.

3.1. Presentation

3.1.1. Corporate Certificate class

The Class Public Law Corporation Personal certificates groups certificates issued to private Corporations that act as Registration Authorities.

3.1.2. Issued certificates

The following certificates are issued within the class "Notarial Certificate":

3.1.2.1. Personal Corporate Certificate

Personal Corporate certificates are qualified certificates, under the terms of Article 11 of Law 59/2003 on Electronic Signatures. They are electronic certificates issued by the Notarial Certification Agency fulfilling the requirements regarding the verification of the identity and other circumstances of the requestors and ensuring the reliability of the certification services they provide.

There are two types of Personal Corporate Certificates

- Hardware personal corporate certificates.
- Software personal corporate certificates.

Hardware personal corporate certificate can be used for three functionalities, each one with a different certificate:

- Generation of qualified electronic signature, which is the advanced electronic signature based on a qualified certificate and generated with a secure signature creation device, having the same legal value as the handwritten signature
- Personal authentication in electronic information systems, in the physical presence or remotely. The certificate of authentication can also be used for creating advanced electronic signature of electronic documents under the conditions agreed by the parties to interact with each other, or when applicable administrative regulations expressly permits it.
- Encryption and decryption of electronic documents, with key recovery.
- Software personal corporate certificate can be used for three functionalities, all in a single certificate:Generation of advanced electronic signature based on a qualified certificate
- Personal authentication in electronic information systems, in physical presence or distance
- Encryption and decryption of electronic documents, with key recovery.

3.1.2.2. Systems corporate certificates

Systems corporate certificates provide security for software applications. These certificates are not qualified certificates according to Law 59/2003 on Electronic Signatures.

There is only one type of Systems Corporate Certificates

- Corporate certificates of secure server are issued to private corporations, as owners of SSL servers, in order to establish secure communications between the server and SSL/TLS client
- Corporate certificates of secure application are issued to private corporations, as owners of software applications requiring authentication, digital signature or encryption features.

Todas las funcionalidades del Certificado Corporativo de Aplicación Segura se contienen en un único certificado.

3.2. Document name and identification

This document is the Declaration of Certification Practices of the class "CGN" of the Notarial Certification Agency and has been assigned the following OID: ANCERT.0.1.0.3

The OID of ANCERT is 1.3.6.1.4.1.18920.

The Notarial Certification Agency has assigned the following object identifiers (OID) to the set of certificates, in order to be identified by the applications:

Certificate	Identifier
Hardware Personal Corporate Certificates (qualified signature)	ANCERT 2.1.1.2.1
Hardware Personal Corporate Certificates (authentication)	ANCERT 2.1.1.2.2
Hardware Personal Corporate Certificates (encryption)	ANCERT 2.1.1.2.3
Software Personal Corporate Certificates	ANCERT 2.1.1.2.4
Software Corporate Certificates of Secure Application	ANCERT 2.2.1.1.2
Software Corporate Certificates of Secure Server	ANCERT.2.2.2.1.2

The Notarial Certification Agency publishes, in its repository, a document containing the OIDs for certification practices and current certificates.

3.3. Participants in the certification services

This Declaration of certification practices regulates the provision of certification services to the general public. The Registration Authority identifies and verifies the requestor's personal circumstances, and ensures their sufficient capacity and legitimacy and that the consent was freely given, and according to the law and the will duly informed.

The participants in the certification services are:

3.3.1. Certification Services Provider

The Notarial Certification Agency acts as a provider of certification services, commissioned by the General Council of Notaries of Spain.

For this class "Corporate Certificates" the Notarial Certification Agency has the following Certification Entities:

3.3.1.1. ANCERT Private Networks Certificates V2

ANCERT Private Networks Certificates V2 is the root certification authority, based on a self-signed root certificate whose fingerprint algorithm based on SHA-1 is:

A49D 9A8A 21B5 C3D8 D59B 1B1D 5653 03DB 5A2B 45E8

ANCERTCGN Certificates issues the following root certificates for subordinate CAs:

- ANCERT Personal Corporate Certificates V2
- ANCERT Systems Corporate Certificates V2

3.3.1.2. ANCERT Personal Corporate Certificates V2

This subordinate Certification Authority issues electronic certificates called Personal Corporate Certificates.

The fingerprint of this subordinate CA algorithm based on SHA-1 is:

55D4 F862 B735 F945 7C3F 6D36 B259 719F 8FFA D728

3.3.1.3. ANCERT Systems Corporate Certificates V2

This subordinate Certification Authority issues electronic certificates called Systems Corporate Certificates.

The fingerprint of this subordinate CA algorithm based on SHA-1 is:

6B2A 3E14 B64E 2FE7 5DD3 0F60 7A21 AF6E E198 22A4

3.3.2. Registration Entities

The registration authorities will be the natural or legal persons assisting the Notarial Certification Agency in the task of issuing and managing certificates, and specifically in the following tasks:

- Legal binding of end entities to certification services.
- Identification and authentication of the identity and personal circumstances of individuals receiving certificates.
- Certificate generation and delivery of secure signature creation devices to subscribers.
- Storing of documents related to certification services.

For certificates issued by ANCERT Personal Corporate Certificates V2 and ANCERT Systems Corporate Certificates V2, the Registration Authority is the private corporation that acts also as the subscriber.

3.3.3. End entities

End entities will be persons and organizations recipients of the services of issuing, management and use of digital certificates, for signing, authentication and encryption, and including the following:

1) Certificate requestors, who request certificates for themselves or others.
2) Subscribers of certificates, which retain the ownership of certificates.
3) Key holders, who use them for the purposes and uses provided on the certificates.
4) Third parties who trust the certificates.

3.3.3.1. Certificate requestors

Corporate certificates must be requested by a natural person on behalf of an organization.

For personal corporate certificates, this natural person, even without being a subscriber, is the key holder.

For corporate certificates of secure application, this natural person acts as the legal representative of the organization.

For corporate certificates of secure server, this natural person acts as the legal representative of the organization.

3.3.3.2. Certificate subscribers

Subscribers are organizations holders of the certificate.

For certificates of class “Corporate Certificates ", the subscriber is the person identified in the certificate.

3.3.3.3. Key Holders

Key holders are natural persons owning, in a exclusive way, the cryptographic keys. The key holder matches the concept of signer used in electronic signature legislation, but is named more generically as he can also use the certificate for other functions such as authentication and decryption.

Key holders are properly identified in the certificate, by their names, surnames, or, in certain cases, by using pseudonyms.

For corporate certificates of secure server and secure application, there is no role of key holder.

3.3.3.4. Third parties who trust the certificates

Third parties who trust the certificates are individuals and organizations that receive digital signatures and digital certificates.

As a previous step to trust certificates, third parties must verify them, as set out in this policy and the other relevant legal documents.

3.4. 3.4. Use of certificates

This section lists the applications for which you can use each type of certificate issued by the class “Corporate Certificates ", and sets limits on certain uses and prohibit certain uses of certificates.

3.4.1. Permitted uses for certificates

Certificates of class Corporative can be used for the uses described in this Declaration of Certification Practices.

Regarding the use, it should be taken into account the following:

- Authenticity of the issuer: the document or electronic communication comes from the signature creation device of the person or entity who claims to be from. This feature is accomplished by the use of electronic signature. The recipient of a digitally signed message can verify the signature using the certificate.
- Server authentication: the electronic communication comes from the server that claims to be from Users can verify server authenticity by verify the certificate of secure server.
- Acceptance of content by the issuer : Prevents that the sender of a message can deny, the issuance. This is accomplished by using electronic signatures. The recipient of a digitally signed message can verify the signature using the certificate. This way it can proved the identity of the sender and the acceptance of its contents, without the posssibility of refutation.

- Integrity: allows the verification that an electronic document for which it has been generated an electronic signature, has not been modified by any external agent. To ensure integrity, cryptographical methods use mathematical summary functions (hash functions) in combination with the digital signature This method is based on a single summary of the electronic document, digitally signed with the subscriber's private key so that any alteration of the document causes a modification of its summary
- Transmitted data can not be read by non authorized third parties (data is encrypted)

3.4.2. Limits and prohibitions on use of certificates

3.4.2.1. Limits of Use

All certificates must be used for their proper function and purpose as set out in this document, and may not be used in other functions and for other purposes.

Also, certificates should be used only in accordance with applicable law, taking into account the restrictions on imports and exports in each moment.

The certificates may contain additional limits within the field *Subject Directory Attributes* , as described in this Certification Practice Statement, as well as the general conditions of use of the certificates. The verifier must take into account these limits before trusting the certificates:

Although end-entity certificates can be used, with some exceptions, for encryption or decryption of electronic documents, it is noted that such uses are conducted under the responsibility of the Subscriber.

A continuación se describen las informaciones adicionales que se encuentran contenidas en los certificados y que suponen o pueden suponer limitaciones en el uso de los certificados.

The verifier must take into account these limits before trusting the certificates:

3.4.2.1.1. Limit on the amount of financial transactions.

Personal corporate certificates are issued without limits on the amount of financial transactions.

3.4.2.2. Prohibited uses

Corporate certificates can not be used to sign public key certificates of any kind, or sign revocation lists (CRLs) or certificate status information (OCSP or similar), except where expressly permitted.

Certificates are not designed; neither can be used or resold for control equipment in dangerous situations or for uses requiring fail-safe performance, such as operation of nuclears, air navigation and communication systems, or weapon control systems, where failure could lead directly to death, personal injury or severe environmental damage.

All legal liabilities, contractual or extra contractual, direct or indirect damages derived from limited and/or prohibited uses fall under the responsibility of the subscriber. Under no circumstances may the subscriber, the key holder or injured third parties claim the Notarial

Certification Agency or the General Council of Notaries any compensation for damages or liabilities derived from the use of keys or certificates for limited and/or prohibited uses.

3.5. Document Management

3.5.1. Organization that manages the document

Notarial Certification Agency S.L.U.

Paseo General Martinez Campos, number 46. 6th floor, Building Elcano

28010 Madrid (Spain)

NIF number B-83395988

3.5.2. Contact the organization

Any contact with the Notarial Certification Agency regarding this Declaration of Certification Practices may be accomplished by the following means:

- Via e-mail to the email address ancert@ancert.com
- By phone at 902 348 347.
- Directly at the headquarters of the Notarial Certification Agency: Notarial Certification Agency, S.L.U., Paseo General Martinez Campos, number 46. 6th floor, Building Elcano (Spain)

Changes occurring on the above data as Web, mail, address or phone will be notified in the website www.ancert.com.

3.5.3. Document management procedures

The Notarial Certification Agency determines the suitability of this Declaration of Certification Practices, and should be approved by its Board.

This Declaration of Certification Practices can be modified at any time by the Notarial Certification Agency. Those subscribers who do not accept the changes may ask for the revocation of their certificates.

This revocation does not give rise to any claim or compensation, or even partial refund of the price of the certificate, unless the correction or amendment of this Declaration of Certification Practices involve a limitation of rights of use or restrictions on the scope of application of the certificate.

4. Publication of the information and certificate repository

4.1. Certificate repository

The Notarial Certification Agency has a certificate repository.

This repository should be available 24 hours 7 days a week and in case of system failure beyond the control of the certification service provider, best efforts should be made to restore the availability of the service according to this Declaration of Certification Practices.

4.2. Publication of the information of the certification service provider

The Notarial Certification Agency must publish the following information in its repository:

- Issued certificates,includingCertification Entities certificates.
- Certificate revocation lists and other revocation information.
- The general policy of certification of the General Council of Notaries, and any specific policies for certificates issued by the Notarial Certification Agency to develop further requirements within the framework of this policy.
- Declaration of Certification Practices.
- The documents of general conditions for the subscribers and third parties trusting the certificates.

4.3. Frequency of publication

The above information, including policies and Declarations of Certification Practices, will be published as soon as available.

Changes in policy documents and the Declarations of Certification Practices shall be governed by the provisions of this document.

The revocation status information will be published in accordance with the provisions this document.

4.4. Access Control

The Notarial Certification Agency does not limit read access to the information but will establish controls to prevent unauthorized persons from adding, modifying or deleting records from the repository in order to protect the integrity and authenticity of the revocation status information.

The Notarial Certification Agency will use trustworthy systems for the management of the repository, so that:

- Only authorized persons can make entries and changes.
- Authenticity of the information can be verified.
- The certificates may only be available for consultation if the subscriber has given his consent.

- Any technical change affecting the security requirements can be traced.

5. Identification and authentication

5.1. Name management

5.1.1. Types of names

All certificates shall contain a distinguished name of the person and/or organization identified in the certificate, defined in accordance with Recommendation ITU-T X.501 and included in the Subject field, including also a Common Name component.

Certificates may contain alternative names for persons and organizations identified in the certificates, mainly in the field SubjectAlternativeName such as e-mail.

Personal circumstances and attributes of individuals and organizations identified in the certificate must be included in predefined attributes according to the technical standards and specifications widely used in the sector or sectors where the certificates are used.

5.1.2. Meaning of names

The names of the certificates will be understandable and interpreted in accordance with applicable law to the names of individuals and legal persons holders of the certificates, as indicated in the Country part of the name.

Names included on the certificates will be treated according the following norms:

- The name will be codified as it appears in the documentation.
- Accents can be eliminated to ensure the highest possible technical compatibility.
- Names can be adapted and reduced in order to ensure compliance with length limits applying to each certificate field.

5.1.3. Use of anonymous and pseudonymous

For CGN certificates, anonymous and pseudonymous are not permitted.

5.1.4. Interpreting names formats

The Notarial Certification Agency uses the following naming scheme:

Hardware Personal Corporate Certificate:

SUBJECT NAME	
FIELD	**CONTENT**
Country (C)	Country (nationality of the person identified, indicating the two-letter code specified in ISO 3166)

Organization (O)	Name of the subscriber entity
Organizational Unit(OU)	Free field
Organizational Unit(OU)	"Certificado Corporativo Personal (" + "Firma" o "Autentica" o "Cifrado" + ")"
Title	Rol or title of the key holder
Surname (SU)	Surname of the key holder
Given Name (GN)	Name of the key holder
Serial Number	Key holder's NIF (NIF of the natural person identified, in order to be accepted by Public Administration)
Common Name (CN)	Name and surname of the key holder.
SUBJECT ALTERNATIVE NAME	
rfc822Name	Email.
SUBJECT DIRECTORY ATTRIBUTES	
ANCERT.10.1.1	"Sin garantía de poderes"
ANCERT.10.1.4	Additional attributes of the key holder

Software Personal Corporate Certificate:

SUBJECT NAME	
FIELD	**CONTENT**
Country (C)	Country (nationality of the person identified, indicating the two-letter code specified in ISO 3166)
Organization (O)	Name of the subscriber entity
Organizational Unit(OU)	Free field
Organizational Unit(OU)	"Certificado Corporativo Personal"
Title	Rol or title of the key holder
Surname (SU)	Surname of the key holder
Given Name (GN)	Name of the key holder
Serial Number	Key holder's NIF (NIF of the natural person identified, in order to be accepted by Public Administration)
Common Name (CN)	Name and surname of the key holder.
SUBJECT ALTERNATIVE NAME	
rfc822Name	Email.
SUBJECT DIRECTORY ATTRIBUTES	
ANCERT.10.1.1	"Sin garantía de poderes"

ANCERT.10.1.4	Additional attributes of the key holder

Corporate Certificate of Secure Application:

SUBJECT NAME	
FIELD	**CONTENT**
Country (C)	Country (nationality of the person identified, indicating the two-letter code specified in ISO 3166)
Organization (O)	Name of the subscriber entity
Organizational Unit(OU)	"Certificado Corporativo de Aplicación Segura"
Serial Number	CIF of the subscriber entity
Common Name (CN)	ID of the secure application
SUBJECT ALTERNATIVE NAME	
rfc822Name	Email

Corporate Certificate of Secure Server:

SUBJECT NAME	
FIELD	**CONTENT**
Country (C)	Country (nationality of the person identified, indicating the two-letter code specified in ISO 3166)
Organization (O)	Name of the subscriber entity
Organizational Unit(OU)	"Certificado Corporativo de Servidor Seguro"
Serial Number	CIF of the subscriber entity
Common Name (CN)	Server and domain name.
SUBJECT ALTERNATIVE NAME	
rfc822Name	Email
dnsName	Other names for Server and domain

5.1.4.1. Usage limits

5.1.4.1.1. Power of attorney

This usage limit is contained in the attribute ANCERT.10.1.1 within the field *Subject Directory Attributes* of Corporate Certificates. This usage limit also indicates the absence of guarantee regarding the power of attorney of a natural person, with the following possibilities:

- "Sin garantía de *poderes",* which is used to indicate that the certificate is issued without verifying if the person has any power to act.

5.1.4.2. Additional attributes of the natural person

Corporate Certificates may incorporate additional attributes of the requestor, including: membership in a corporation, honorary positions, etc ...), in the attribute ANCERT.10.1.4 of the field *Subject Directory Attributes*.

5.1.4.3. Publication in the repository

The Notarial Certification Agency shall publish in the repository information on the syntax and semantics required for the treatment by third parties of such extensions and private attributes.

5.1.5. Uniqueness of names

The names of the subscribers of certificates will be unique for each Certification Authority operated by the Notarial Certification Agency. A person may have more than one certificate with the same name at a time during the renewal of certificates, to ensure the continuity of his operations.

In no case shall be assigned a subscriber name that has already been used by a different subscriber.

5.1.6. Name conflict resolution

Name conflicts are solved by the inclusion, in the distinguished name of the certificate, of key holder's identity card number, or equivalent, or the tax identification number for legal persons, as appropriate.

Requestors of certificates must not include names in their requests that may involve a violation, by the prospective subscriber, of third party rights.

The Notarial Certification Agency is not obliged to determine in advance that a requestor of certificate has rights on a trademark or domain included in a certificate request.

Also, the Notarial Certification Agency shall not act as an arbitrator or mediator, or in any other way to resolve any dispute concerning the ownership of the names of individuals or organizations, domain names, trademarks or trade names.

However, in case of reception of a notification of a name conflict, according to Spanish law, may engage in the appropriate legal actions in order to block or withdraw the certificate issued.

In any case, the Notarial Certification Agency reserves the right to refuse a certificate request because of name conflict.

5.2. Initial validation of the identity

This section establishes requirements for identification and authentication procedures to be used for the registration of subscribers, including communities and individuals, to be conducted prior to the issuance and delivery of certificates.

5.2.1. Proof of possession of the private key

This section describes the methods used to prove the possession of the private key corresponding to the public key being certified.

The method of proof of possession of private key shall be PKCS#10, another cryptographically equivalent test or any other reliable method approved by the Notarial Certification Agency.

This requirement does not apply when the key pair is generated by the registration authority, delegated by the subscriber during the personalization process or delivery to the subscriber or key holder.

In this case, the possession of the private key is proved by the existence of a reliable method of delivery and acceptance of the secure device and the corresponding certificate and key pair stored in it.

5.2.2. Authentication of the identity of a natural person

The process of identification and authentication of a natural person is performed exclusively by physical presence in front of the organization to which he belongs.

5.2.2.1. Required identification elements

- The types of documents that are needed to confirm the identity of an individual are only the national identity card, residence card, passport or other lawful means, provided it contains at least the following information: - Name and surname
- Date of birth
- Legally recognized identity number

5.2.2.2. Validation of the identification elements

Validation of the elements required for the identification is performed exclusively by the representative of the organization.

5.2.2.3. Need for personal presence

For corporative certificates is required the presence of the natural person identified in the certificate except when:

Se puede obviar esta presencia cuando:

- the organization has already identified to the natural person, and the period of time since this identification is less than five years,
- when for requesting a new certificate is used another valid certificate, which had been issued to the natural person once identified by his presence in front of the Registration Authority.

5.2.2.4. Binding of the natural person to the organization

For corporate certificates, the natural person has a link with the organization subscriber of the certificate.

the legal representative of the organization should ensure that this relationship still exists, making the necessary checks with the personnel responsible for staff contracts.

5.2.3. Unchecked subscriber's information

Subscriber's unverified information must not be included in the certificate.

5.3. Identification and authentication of renewal requests with change of key

5.3.1. Validation for the regular renewal of certificates

It can be renewed Corporate Certificates during their lifetime or within three months after its expiration.

Before renewing a certificate, the Notarial Certification Agency or the relevant registration authorities shall verify that the information used to verify the identity (and other related information) of the subscriber and the key holder, is still valid.

It may be used electronic signatures based on a certificate to request its renewal, always before its expiration. Subsequently other mechanisms may be used, provided they are sufficiently reliable.

If any subscriber or key holder information has changed, these changes will be properly recorded in accordance with the provisions of this document.

5.3.2. Validation for certificate renewal after revocation

Not applicable, because the Notarial Certification Agency in any case should renew certificates that have been revoked.

5.4. Identification and authentication for a suspension request

The legitimate requestor must call the number 902 348 347 of the Notarial Certification Agency.

5.5. Identification and authentication for a suspension request

The Notarial Certification Agency shall authenticate requests and reports relating to the revocation of a certificate, in order to verify that they come from an authorized person.

The revocation could be requested:

- the request of the Registration Entity. Ésta puede solicitar la suspensión de los certificados emitidos.
- At the request of the Notarial Certification Agency which may proceed to revoke the certificate when has had certain knowledge of the occurrence of one of the revocation causes listed in this document.

In all cases, once the certificate has been revoked, the revocation will be published in the Directory of Certificates of the Notarial Certification Agency producing effects on third parties from this very moment, and included in the Certificate Revocation List in a maximum time of twenty-four (24) hours.

6. Operational requirements for the life cycle of certificates

6.1. Certificate request

Prior to the issuance and delivery of a certificate, it must be a certificate request, at the request of an interested party.

There may be the following types of requests:

1) Pre-request, consisting of an application request, electronic or in person, of a certificate (the request does not contain a public key and is not signed).
2) Request is made in person, producing a technical and electronic request using either a public key provided by the applicant (PKCS # 10 or consistent mechanism, with user's public key and digital signature in order to prove possession of private key in accordance with this document).

6.1.1. Legitimation of issuance requests

Are entitled to request the issuance of a certificate:

- The person designated by the organization.

6.1.2. Registration procedure: responsibilities

The registration process should include the physical presence in fron of the Registration Entity.

The corresponding registration entity (of the Notarial Certification Agency) must ensure that certificate requests are complete, accurate and properly authorized.

Prior to the issuance and delivery of the certificate, the registration entity shall inform the key holder of the applicable terms and conditions.

Such information shall be communicated in a durable medium, on paper or electronically, and in easily understandable language.

The application shall be accompanied by supporting documentation of the identity and other circumstances of the requestor, the future subscriber and the key holder, as appropriate, in accordance with the provisions of this document.

Also, it must be provided a physical address or other equivalent data, which allows to make contact with the requestor, the future subscriber and the key holder, as appropriate.

For Corporative Certificates, the corresponding Registration Authority is committed to the fulfillment of these obligations on equal terms that the Notarial Certification Agency.

6.2. Processing the information request

6.2.1. Identification and authentication

Upon receipt of a certificate request, the certification service provider must verify the information provided according to this document, by following the procedure below:

- It should be create a new record, in paper or electronic format.
- The key holder should be physically in person in the Registration Entity.
- The key holder should be identified with original documents identification

6.2.2. Approval or rejection of the request

If verification has not been successful, the registration entity must reject the request or stop the approval until proper verifications had been carried out.

If data are verified correctly, the Registration Entity must approve the request of the certificate and inform of such approval to the requestor.

Also, the Registration Entity requests to the Certification Entity "Corporate Certificates" the generation of the certificate.

If this procedure failed to complete, a form should be filled and sent to the Certification Entity.

6.2.3. Resolution term

Not defined.

6.3. Issuance of certificate

6.3.1. Actions during the process of issuing

Following the approval of the request, the operator proceeds to the issuance of the certificate. The actions to be taken to issue the keys and the certificate are different, depending on whether the support for storage is a cryptographic card or software.

In any case, the Notarial Certification Agency shall:

- Use a procedure to generate certificates that securely bind the certificate with the registration information, including the certified public key.
- Protect the confidentiality and integrity of registration data, especially if they are exchanged electronically with the requestor during the pre-request.
- Include on the certificate the information provided by Article 11 of Law 59/2003 of December 19th, in accordance with the provisions of this policy.
- Indicate the date and time of issuance.
- In cases where the Notarial Certification Agency provides the secure signature creation device, follow a procedure for the management of secure devices to ensure that the device is delivered in a secure way to the key holder.
- Use trustworthy systems and products that are protected against modification and ensure technical and cryptographic security.
- It must also be ensured that the certificate is issued by systems protected against forgery and, if the certification service provider generates the private keys, the confidentiality of the keys in the generation process.

6.3.1.1. Issuance using a cryptographic card

For hardware corporate certificates:

1. The Responsible for Registration Entity assigned to this task inserts his cryptographic card (containing the certificate which identifies him as a registration authority) into the card reader and accesses the registration application.

2. Once authenticated, the responsible for the Registration Entity inserts into the card reader the cryptographic card of key holder. Prior to this, ANCERT Corporate Certificates has provided the Registration Entity with blank cards and the corresponding PIN and PUK, in a sealed envelope.

The responsible for Registration Entity complete the registration form with the data provided by the requestor, and requests the issuance of the certificate.

4. At this time, the registration application requests the PIN corresponding to the applicant's cryptographic card, to activate the key generation procedure.

5. At that time the key pair is generated in the subscriber's cryptographic card and a request is sent to the Notarial Certification Agency, which generates the certificate and sends it via SSL to the computer of the Registration Entity, being automatically stored in the subscriber's cryptographic card.

6. The system automatically generates an invoice according to the amount published in the web of the Notarial Certification Agency: www.ancert.com

6.3.1.2. Issuance for software certificates

Para los Certificados emitidos en software se utilizan como soporte los sistemas operativos o aplicaciones informáticas de los usuarios finales.

For software corporate certificates:

1. The requestor must present the certificate request (in PKCS10 format) to the Registration Entity.

2. The Responsible for Registration Entity inserts his cryptographic card (containing the certificate which identifies him as a registration authority) into the card reader and accesses the registration application

The responsible checks, using the tools provided by the Notarial Certification Agency, that the file provided by the requestor matches the information in the certificate profile.

4. If all the data is correct, the responsible completes the registration form and requests the issuance of the certificate.

5. Within 48 hours the requestor may obtain his Corporate Certificate, downloading it from the address: www.ancert.com

6. The system automatically generates an invoice according to the amount published in the web of the Notarial Certification Agency: www.ancert.com

For the issuance of corporate certificates of application, the process is the same as for software personal corporate certificates.

6.3.2. Notification to the subscriber

The Notarial Certification Agency shall, in the act of issuing or after, notify the issuance to the subscriber or, where appropriate, the key holder.

Within 48 hours the requestor may obtain his certificate, downloading it from the address: www.ancert.com

6.4. Delivery and acceptance of the certificate

6.4.1. Responsibilities of the Notarial Certification Agency

The Notarial Certification Agency:

- Gives access to the subscriber or the key holder to the certificate, delivering also, where appropriate, the secure device.
- Delivers to the key holder a delivery sheet for the certificate and, where appropriate, for the device, with the following minimum contents:

    a) Basic information about the policy and uses of the certificate, including information on the Notarial Certification Agency and the Declaration of Certification Practices, their duties, faculties and responsibilities.
    b) Information about the certificate and the secure device, as appropriate.

    c) Acknowledgement by the subscriber or the key holder, as appropriate, of the receiving of the certificate and, where appropriate, the secure device, and the acceptance of these elements.

    d) Obligations of the subscriber and, where appropriate, the key holder.

    e) Responsibilities of the Subscriber and, where appropriate, the key holder.

    f) Method for the secure delivery to the subscriber and the holder of the private key, activation data and, where appropriate, secure device in accordance with the provisions of this policy.

    g) The date of the act of delivering and receiving.

6.4.2. Acceptance of the certificate

The acceptance by the subscriber should be understood from the time of issuance and delivery by the Notarial Certification Agency, and the signing of the corresponding delivery sheet.

By accepting the Certificate, the subscriber further agrees terms and conditions contained in this Declaration of Certification Practices.

In any case, by accepting a certificate issued by the Notarial Certification Agency, the subscriber declares:

- That all information submitted during the requesting procedure of the Certificate is true.
- That the certificate is used exclusively for authorized and legal uses, according to this Declaration of Certification Practices and within the scope determined by the Certification Policy.
- That ensures its exclusive control over the signature creation data that correspond to the signature verification data included in the Certificate issued by the Notarial Certification Agency and linked to their personal identity, which in any case and without limitation,

include the actions and measures necessary to prevent its loss, disclosure, modification, or use by someone other than the Subscriber.

The Notarial Certification Agency will consider as valid all certificate accepted by the Subscriber and published in its repository, provided it has not expired and not affected by any cause for revocation.

6.4.3. Publication of the certificate

Once issued the certificate, the Notarial Certification Agency automatically publishes a copy in the repository referred to in this document, with appropriate access controls.

6.4.4. Notification to a third party

The Notarial Certification Agency does not notify the issuing of certificates to third parties.

6.5. Key pair and certificate usage

6.5.1. Use by the subscriber and, where appropriate, the key holder

6.5.1.1. Obligations of the subscriber and, where appropriate, the key holder.

By the general conditions of issuance, the Notarial Certification Agency must require the subscriber to:

- If the subscriber generates his own keys, it shall be required to:

  Generate subscriber keys using an algorithm recognized as acceptable for qualified electronic signature.

  Create the keys within the secure signature creation device.

  Use key lengths and algorithms recognized as acceptable for qualified electronic signature.

- Provide the Notarial Certification Agency and their registration entities with a complete and proper information, in accordance with the requirements of this certificate policy and specific policies, especially regarding the registration procedure.
- Give the consent prior to the issuance and delivery of a certificate, for the publication in the repository and when appropriate, for the notification of the issue to third parties.
- Fulfill the obligations provided for the subscriber in this Declaration of Certification Practices.
- Use the certificate in accordance with the provisions of this Declaration of Certification Practices.

- Be diligent in keeping the private key to prevent unauthorized use, in accordance with the provisions of this Declaration of Certification Practices, not allowing the use of the private key to anyone else.
- Communicate to the Notarial Certification Agency and any person that the subscriber or the key holder believes may trust the certificate, without unjustifiable delays:

  The loss, theft or potential compromise of the private key or the secure device.

  Loss of control over the private key or the security device, due to the potential compromise of activation data (eg PIN of the secure signature creation device) or any other cause.

  Inaccuracies or changes to the content of the certificate that might be known by the subscriber or the key holder.
- Cease in the use of the private key after the period specified in this document.
- Transfer, to the key holders, specific obligations.
- Do not monitor, manipulate or reverse-engineer on the technical implementation of the certification services of the Notarial Certification Agency or the General Council of Notaries, without prior written permission.
- Do not intentionally compromise the security of certification services of the Notarial Certification Agency or the General Council of Notaries, without prior written permission.

Subscribers generating digital signatures using the private key corresponding to their public key included in the certificate, shall recognize, in due legal document that such signatures are electronic signatures equivalent to handwritten signatures, as provided in Article 3 of Law 59/2003 of December, 19th.Civil liability of the subscriber Notarial Certification Agency requires the subscriber and, if applicable, the holder of keys, to ensure:

6.5.1.2. Civil liability of the subscriber

By the general conditions of issuance, the Notarial Certification Agency must require the subscriber and, where appropriate, the key holder to:

- If the subscriber was the requestor for the certificate, that all statements made in the request are correct.
- That all information supplied by the subscriber and contained in the certificate is correct.
- That the certificate is used exclusively for authorized and legal uses, according to the corresponding Declaration of Certification Practices.
- That each digital signature generated using the public key included in the certificate is the digital signature of the subscriber, and the certificate has been accepted and is operational (not expired or been revoked) at the time of signature creation.
- That the subscriber is an end entity and not a certification service provider, and will not use the private key corresponding to the public key included in the certificate to sign any

certificate (or any other certified public key format) or Certificate Revocation List, or for acting on behalf of other certification service provider or any other case.

- Those digital signatures will only be generated while having the certainty that no unauthorized person has ever had access to the private key.
- That the subscriber is solely responsible for damage caused by its breach of duty to protect the private key.

6.5.2. Use by third parties who trust the certificates

6.5.2.1. Obligations of third parties who trust the certificates

By the terms of use, the Notarial Certification Agency must require the third parties who trust the certificates, to:

- Get external advice about the fact that the certificate is appropriate for the intended use.
- Check the validity, suspension or revocation of issued certificates using information on the status of certificates.
- Check all certificates in the certification hierarchy, before relying on digital signatures or in any certificate in the hierarchy.
- Keep in mind any limitations on the use of the certificate, regardless of whether these limitations are included in the certificate or in a contract, or not.
- Keep in mind any precautions established in a contract or other instrument, regardless of their legal form.
- Do not monitor, manipulate or reverse-engineer on the technical implementation of the certification services of the Notarial Certification Agency or the General Council of Notaries, without prior written permission.
- Do not intentionally compromise the security of certification services of the Notarial Certification Agency or the General Council of Notaries, without prior written permission.
- The Notarial Certification Agency shall require the third party, by the conditions of use, to recognize that electronic signatures properly verified are electronic signatures equivalent to handwritten signatures, in accordance with Article 3 of Law 59/2003 of December, 19th.

6.5.2.2. Civil liability of third parties who trust the certificates

By the conditions of use, the certification services provider shall require third parties who trust the certificates, to recognize that:

- have enough information to make an informed decision in order to trust the certificate or not.
- are solely responsible for trusting or not the information contained in the certificate.

- will be solely responsible for the violation of its obligations as a third party who trust the certificate.

6.6. Renewal of certificates

Valid certificates may be renewed by a specific and simplified renewal procedure in order to maintain the continuity of the certification service.

The renewal of certificates can be done with or without the renewal of the keys, in this case in accordance with the provisions of this document.

The certificates can be renewed during their lifetime or within three months after its expiration.

6.7. Renewing keys and certificates

6.7.1. Causes for the renewal of keys and certificates

The certificates must be renewed together with the keys when they reach the end of their lifetime, or the lifetime of the secure device that contains them.

6.7.2. Legitimation of renewal requests

Prior to the issuance and delivery of a certificate, it must be a certificate request, at the request of the subscriber or the key holder.

6.7.3. 6.6.2. Processing the renewal application

The request for renewal is performed by the subscriber or the key holder, with his current certificate as proof of possession of private key, provided that it's been no more than five years from the issuance of the certificate to renew.

In case the information to be included in the renewed certificate has not changed, including contact information, a new certificate is issued and automatically delivered.

In case of renewal of certificates that have expired or been revoked it is not allowed to perform an automatic renewal, and it should be requested a new certificate.

6.7.4. Notification of new certificate issuance

The Notarial Certification Agency notifies the issuance to the subscriber and the key holder, as appropriate.

6.7.5. Acceptance of the certificate

Not defined.

6.7.6. Publication of the certificate

The Notarial Certification Agency automatically publishes a copy in the repository referred to in this document, with appropriate access controls.

6.7.7. Notification of the issue to a third party

The Notarial Certification Agency does not notify the renewal of certificates to third parties.

6.8. Modification of certificates

The modification of certificates, except modification of the certified public key, which will be considered renovation and will be treated as a new issuance , according to the corresponding section of this policy.

6.9. Revocation and suspension of certificates

6.9.1. Causes for the revocation of certificates

The Notarial Certification Agency may revoke a certificate due, at least, to the following reasons:

Circumstances affecting the information contained in the certificate:

Modification of any of the information contained in the certificate.

Any of the information contained in the certificate request is known to be incorrect.

Any of the information contained in the certificate is known to be incorrect.

Circumstances affecting the security of the key or certificate:

Compromise of the private key or the infrastructure and systems of the certification services provider that issued the certificate, provided that affects the reliability of certificates issued from that incident.

Violation, by the certification services provider, of the requirements for certificate management established in the corresponding Declaration of Certification Practices.

Compromise or suspicion of compromise of subscriber's (or key holder) key or certificate.

Unauthorized access or use by a third party, of subscriber's (or key holder) private key.

Irregular use of the certificate by the subscriber or the key holder, or lack of diligence in keeping the private key.

Circumstances affecting the security of the cryptographic device:

Compromise or suspicion of compromise of the security of the cryptographic device.

Loss or damaging of the cryptographic device.

Unauthorized access, by a third party, to subscriber (or key holder) activation data.

Circumstances affecting the subscriber or the key holder:

Ending of the legal relationship between the certification services provider and the subscriber or the key holder.

Modification or ending of the underlying legal relationship or what caused the issuance of the certificate to the subscriber or the key holder.

Violation, by the certificate requestor, of pre-established requirements for performing the request.

Violation, by the subscriber or the key holder, of their obligations, liabilities and guarantees established in the general conditions for issuance or the corresponding Declaration of Certification Practices.

Incapacity or death of the subscriber or the key holder.

In case of certificates for communities, the extinction of the legal person subscribing the certificate, the ending of the authorization by the subscriber to the key holder or the termination of the relationship between subscriber and key holder.

Revocation request by the subscriber, in accordance with the provisions of this document.

Other circumstances:

The suspension of the digital certificate for a period exceeding that provided in this document.

Termination of the service provided by the Notarial Certification Agency, in accordance with the provisions of this document.

If the entity to which the request for revocation is addressed does not have all the information necessary to determine the revocation of a certificate, but has evidence of its compromise, this entity can suspend it.

In this case it shall be considered that actions taken during the suspension period will not be valid as long as the certificate was finally revoked. On the contrary, these actions will be valid if the suspension is revoked and the certificate becomes valid again.

The general conditions of issuance sets the obligation to request the revocation of the certificate in case of any of the circumstances mentioned above.

6.9.2. Legitimation of revocation requests

Are authorized to request the revocation of a certificate:

- In any event, the Subscriber on whose behalf the certificate was issued. The organization, as the subscriber of the certificate, must act through a natural person with sufficient legal powers to revoke the certificate.

6.9.3. Procedures for request the revocation

The entity intending to revoke a certificate should request it to the Notarial Certification Agency or to any authorized entity for each specific policy, and should provide the following information:

- Date of the revocation request.
- Subscriber's identity.
- Detailed reason for the revocation request.
- Name and title of the person requesting the revocation.
- Contact details of the person requesting the revocation.

Where immediate revocation of the certificate is required, it shall be made a call, asking for the suspension, or send an email to the Notarial Certification Agency to the email address revocacion@ancert.com.

Prior to revocation the request is authenticated in accordance with the requirements of this document.

In case the request is addressed to a registration entity, once authenticated, this entity can revoke the certificate directly or send a request to that effect to the Notarial Certification Agency, through telematics application for revocation.

The revocation request is processed upon receipt.

The subscriber and, where appropriate, the key holder are informed of the revocation.

The Notarial Certification Agency can not reactivate the certificate once revoked.

6.9.4. Time period of the revocation request

Requests for revocation shall be sent reasonably diligently once the causes for revocation are known.

6.9.5. Obligation to obtain the certificate revocation information

Third parties who trust the certificates must check the status of those certificates.

A method by which the certificate status can be checked is by consulting the latest Certificate Revocation List issued by the Certification Authority that issued the certificate.

The Notarial Certification Agency provides information to third parties who trust certificates on how and where to find the corresponding Certificate Revocation List, among other methods, by including the Web address of publication of the lists within the certificates.

6.9.6. Frequency of issue for certificate revocation lists (CRLs)

The Notarial Certification Agency issues a new CRL at least every 24 hours.

The CRL includes the scheduled time for the issuance of a new CRL, although it may be issued a CRL before the deadline stated in the previous CRL.

Expired certificates will be removed from the CRL.

6.9.7. Availability of certificate status information services

Alternatively, third parties who trust certificates may check their status in the repository of the Notarial Certification Agency, which is available 24 hours 7 days a week, at the web address http://www.ancert.com.

In case of failure of systems for status checking due to reasons beyond the control of the Notarial Certification Agency, it will be made every effort to ensure that this service remains idle the shortest possible time.

6.9.8. Obligation to use the certificate revocation information services

Third parties that do not use CRLs to check the validity must use the repository.

6.9.9. Other forms of certificate revocation information

The Notarial Certification Agency has a public OCSP service to provide status information about certificates, available at the web address indicated on the certificates.

6.9.10. Special requirements if case of private key compromise

The compromise of the private key of a Certification Entity will be notified, as far as possible, to all participants in the certification services of the General Council of Notaries and the Notarial Certification Agency.

This notification occurs at least through the publication of information in the Repository of the Notarial Certification Agency.

6.9.11. Causes for suspension of certificates

The Notarial Certification Agency may suspend certificates in the following cases:

- By receiving the corresponding request.
- The existence of a judicial or administrative resolution, or the existence of an investigation, or judicial or administrative proceeding that could determine that the certificate is affected by a cause for revocation.
- The existence of serious doubts about the concurrence of causes for revocation.

It must be ensured that the certificate is not suspended for longer than necessary to confirm the above causes.

6.9.12. Legitimation of suspension requests

The suspension of a certificate may be requested by the subscriber, the natural or legal person represented by him or an authorized third party.

It can also be requested the suspension to the Notarial Certification Agency when it became known by reliable means of the occurrence of any of the causes for suspension.

6.9.13. Procedures for suspension request

In order to request a suspension electronically, the subscriber or the key holder should make a phone call to the Notarial Certification Agency (902 348 347, Customer Services Center), which will record and store the request For proof purposes, the conversation between the operator and the applicant can be recorded.

In any case it may be requested the suspension of a certificate by sending an email.

6.9.14. Maximum period of suspension

The maximum period of suspension is sixty (60) calendar days from the date the Notarial Certification Agency becomes aware of any causes for suspension, and makes this explicit in the Repository of Certificates and Certificate Revocation List.

6.9.15. Lifting of the suspension

Subscribers can request the lifting of the suspension during the sixty (60) days following the suspension by making a phone call to the number 902 348 347 (Customer Services Centre) of the Notarial Certification Agency. For proof purposes, the conversation between the operator and the applicant can be recorded.

The requestor should respond with the password provided in the certificate requesting process. In the event that the response matches the password the operator will proceed to lift the suspension of the certificate.

In all cases, once lifted the suspension of the Certificate, it will be published immediately in the Repository the Notarial Certification Agency and included in the Certificate Revocation List (CRL) in a maximum time allowed of twenty-four (24) hours.

In the event that the suspension has come the Notarial Certification Agency, the lift of the suspension can only be performed under certain knowledge of the disappearance of the cause that led to suspension. In this case, it shall be immediately updated the Certificate Revocation List.

6.9.16. Notice of revocation or suspension

The subscriber whose certificate is suspended or revoked shall be informed of that fact and, where appropriate, the lifting of the suspension. The Notarial Certification Agency shall notify

this information by email or postal letter, or even by phone if it was not possible by any of the two previous forms.

Notwithstanding the preceding paragraph, the notice shall be deemed duly completed when it is done by email to the address included on the certificate and, therefore, accepted by the user of the certificate.

However, if the system would produce an error message or reject the communication, it should be understood that the Notarial Certification Agency has sufficiently fulfilled with its obligation when the notification has been sealed. To justify further the fulfillment of due diligence, the Notarial Certification Agency will retain for fifteen years, the electronic proof of the communication for the revocation or suspension.

Termination or suspension of the validity of an electronic certificate will remain accessible in the directory of Certificate Revocation Lists at least until the date of completion of its initial period of validity.

6.10. Services for certificate status checking

6.10.1. Operational features of the services

The services for certificate status checking are provided through a web query interface, through the repository, and through the OCSP service.

6.10.2. Availability of services

The services for certificate status checking are available 24 hours a day, 7 days a week, throughout the year, except for scheduled stops.

6.10.3. Optional Features

Not defined.

6.11. Ending of the subscription

The subscription ends after the period of validity of the certificate, expiring the certificate consequently.

As an exception, the subscriber may maintain the existing service by requesting the renewal of the certificate, in the cases and terms determined by this Declaration of Certification Practices.

6.12. Deposit and Key Recovery

6.12.1. Deposit and key recovery policy and practices

The Notarial Certification Agency does not store or retrieve keys from subscribers or key holders, except the encryption keys.

Encryption keys can be recovered only at the request of the individual identified in the certificate, and using the corresponding procedure implemented by the Notarial Certification Agency.

6.12.2. Policies and practices of encapsulation and recovery of session keys

Not defined.

7. Management, operations and physical security controls

We distinguish in this section the following domains:

- Certificate creation domain.

  Physical, management and operations controls in the domain of creation of certificates are operated directly by the Notarial Certification Agency and conducted in accordance with the corresponding policy and this document.

- User registration and card management domain.

  Physical, management and operations controls in the domain of user registration and management of cryptographic cards are operated by a legal representative of the Organization.

7.1. Physical security controls

Certificate creation domain.

The Notarial Certification Agency has physical facilities to protect, at least, the services for certificate generation, cryptographic devices, revocation infrastructure, and compromises caused by unauthorized access to systems or data.

Physical protection is achieved through the establishment of clearly defined security perimeters around the certificate generation services, cryptographic devices and revocation infrastructure. The part of the facilities shared with other organizations must be outside of these perimeters.

The Notarial Certification Agency establishes physical and environmental security controls to protect the systems and the equipment used for operations.

The environmental and physical security policies applicable to certificate generation services, cryptographic devices and revocation infrastructure establish requirements for the following contingencies:

- Physical access controls.
- Protection against natural disasters.
- Protective measures against fire.
- Failure of support systems (power electronics, telecommunications, etc.).
- Collapse of the structure.

- Flooding.
- Burglar protection.
- Burglary and unauthorized entry.
- Disaster recovery.
- Unauthorized departure of equipment, information, media and applications used for the services of the certification service provider.

User registration and card management domain.

The Notarial Certification Agency establishes physical and environmental security controls to protect the systems and the equipment used for operations.

The environmental and physical security policies applicable to certificate registration and generation services and cryptographic devices, establish requirements for the following contingencies:

- Physical access controls.
- Burglar protection.
- Burglary and unauthorized entry.
- Disaster recovery.
- Unauthorized departure of equipment, information, media and applications used for the services of the certification service provider.

These measures are applicable to the facilities of the Organization where the managing and the approval of certificate requests is performed, under the full responsibility of the Notarial Certification Agency.

The Notarial Certification Agency has established in the facilities of the organization, physical and environmental security controls to protect the systems and the equipment used for operations.

7.1.1. Location and construction of facilities

For all domains

Physical protection is achieved through the establishment of clearly defined security perimeters. The quality and strength of materials of construction of the facility ensure adequate levels of protection against intrusion by brute force.

Certificate creation domain.

The Notarial Certification Agency has physical facilities to protect, at least, the services for certificate generation, cryptographic devices, revocation infrastructure, and compromises caused by unauthorized access to systems or data.

The location of the facilities allows the presence of security forces in a reasonably time since an incident was notified (in the case of not having a permanent physical presence of security personnel working for the certification service provider).

The Notarial Certification Agency maintains disaster recovery facilities for its operations, with comparable security perimeters to the main facility.

User registration and card management domain.

The Notarial Certification Agency has physical facilities to protect, at least, the services for certificate generation, cryptographic devices, revocation infrastructure, and compromises caused by unauthorized access to systems or data.

7.1.2. Physical Access

Certificate creation domain.

The Notarial Certification Agency establishes at least four (4) levels of security with restricted access to perimeters and physical barriers.

In order to access to locations where services related to the lifecycle of certificates are managed, it is required the prior identification, including closed-circuit TV filming and archiving.

This identification is performed by recognition of a biometric parameter of the individual (two-factor methods and proximity card protected by PIN) except for escorted visits

Cryptographic key generation and storage for Certification Entities are made in specific units for these purposes which will require dual access.

Access to keys is subject to a strict policy of segregation of duties, and the opening and closing of these cabins and safes are registered for subsequent audit.

User registration and card management domain.

The Notarial Certification Agency has established in the facilities of the organization, enough physical and environmental security controls as to protect the systems and the equipment used for operations.

7.1.3. Power and air conditioning

For all domains

Computer equipments of the certification services provider are adequately protected against fluctuations or power outages that could damage or disrupt the service.

Facilities include a system of stabilization of the electric current, as well as self-generation system with sufficient autonomy to maintain the supply during the time required to complete an orderly shutdown of all systems.

The equipment is located in an environment that ensures a climate (temperature and humidity) appropriate to their optimum working conditions.

7.1.4. Exposure to water

For all domains

The Notarial Certification Agency has flood warning systems in place to protect equipment and assets for this eventuality, if the conditions of location of facilities make this necessary.

7.1.5. Fire prevention and protection

Certificate creation domain.

All facilities and assets of the Notarial Certification Agency have automatic fire detection and extinction.

In particular, cryptographic devices and media for the storage of keys have a specific and additional fire protection system.

User registration and card management domain.

All facilities and assets of the Notarial Certification Agency have automatic fire detection and extinction.

7.1.6. Media storage

For all domains

Media storage is made so as to guarantee both their integrity and confidentiality, according to the established classification of information.

Fireproof locations or cabinets are used for this purpose.

Access to these supports, including their removal, is restricted to authorized persons.

7.1.7. Waste treatment

For all domains

The removal of media, both in paper and magnetic, is done by ensuring the impossibility of recovering the information.

In the case of magnetic media, a full formatting, permanent erasure or physical destruction of the support is performed.

For paper documents, they undergo a physical treatment of destruction.

7.1.8. Backup off-site

For all domains

Periodically, the Notarial Certification Agency stores backup information in a location, other than where computers are installed, and physically separated.

7.2. Management procedures

For all domains

The Notarial Certification Agency ensures that its systems are operating safely, for which it establishes and implements procedures for the functions that affect the provision of their services.

The staff of the Notarial Certification Agency perform administrative and management procedures in accordance with the current security policy.

7.2.1. Reliable functions

Certificate creation domain.

The Notarial Certification Agency identifies, in its security policy, reliable functions or roles.

Persons required to hold such responsibilities are formally designated by the senior management of the certification service provider.

Reliable functions include:

- Personnel responsible for security.
- System administrators.
- System operators.
- System auditors.
- Individuals on the previous roles are subject to specific control procedures.

User registration and card management domain.

The Notarial Certification Agency identifies, in its security policy, reliable functions or roles.

Persons required to hold such responsibilities are formally designated by a legal representative of the organization.

Reliable functions include:

- Personnel responsible for security.
- Personnel for customer services.
- Personnel for management of cryptographic operations

Individuals on the previous roles are subject to specific control procedures.

7.2.2. Number of people per task

Certificate creation domain.

Reliable functions identified in the previous section and the security policy, and its associated responsibilities, are documented in job descriptions.

These descriptions are made taking into account that there are a separation of sensitive functions, and a minimum grant of privilege, when possible.

To determine the sensitivity of the function, it is considered the following elements:

- Duties associated with the function.
- Access level.
- Function monitoring.
- Training and awareness.
- Required skills.

The most sensitive tasks, including access and management of cryptographic hardware, requires multiple reliable people. Specifically, the internal control procedures are designed to ensure that at least two people are required for reliable access to sensitive devices (physically or logically).

Access to cryptographic hardware is strictly controlled throughout the entire lifecycle, from receipt and inspection until its final (physical or logical) destruction.

User registration and card management domain.

Reliable functions identified in the previous section and the security policy, and its associated responsibilities, are documented in job descriptions.

The Notarial Certification Agency maintains and implements control procedures that ensure segregation of duties and reliable people to perform sensitive tasks.

7.2.3. Identification and authentication for each function

For all domains

The Notarial Certification Agency identifies and authenticates the staff before granting access to the corresponding reliable function.

7.2.4. Roles requiring separation of duties

Certificate creation domain.

The following tasks are performed at least by two people:

- Physical Access management.
- Software management.
- Configuration management and change control.
- Archive management.
- Management of cryptographic equipment.
- Generation, issuance and destruction of certificates for Certification Authorities.

- Issuance and revocation of certificates, and access to te repository.

User registration and card management domain.

- The certificate request is made by the customer and its approval should be given by the responsible of the service in the organization.
- The responsible of the service in the organization will be in charge of the secure printing of the card.

7.3. Personnel controls

7.3.1. History, qualifications, experience and authorization requirements

For all domains

The Notarial Certification Agency employs, for the provision of services, qualified and experienced personnel in the field of electronic signature and information security.

The Notarial Certification Agency employs, for the provision of services, qualified and experienced personnel in the field of electronic signature and information security.

The qualification and experience may be substituted by an appropriate education and training.

The staff occupying reliable roles is free of personal interests that may be in conflict with the development of the function that has been entrusted.

It is not assigned to a reliable or management position a person who is not qualified, especially for having been convicted of crime or offense concerning their suitability for the position. For this reason, an investigation is conducted in accordance with the provisions in the next section on the following:

- Academic history, including the alleged degree.
- Previous work, up to five years, including professional references and claimed work.
- Delinquency
- To the extent allowed by applicable law, criminal records.

7.3.2. Procedures for history research

Certificate creation domain.

The Notarial Certification Agency conducts the investigation before the person is hired and/or has access to the workplace.

In the application for the job is informed about the need to undergo a preliminary investigation.

He is also advised that a refusal to accept the investigation will result in rejection of the application.

It is obtained the consent from the candidate for conducting this previous research, protecting all his personal information in accordance with the LOPD and related regulation.

The following checks are performed:

- Past work references.
- Professional references
- Academic history, including the alleged degree.

The research is repeated every three years.

User registration and card management domain.

The Notarial Certification Agency must check the existence of the organization and the authorized representative.

7.3.3. Training requirements

For all domains

The Notarial Certification Agency trains staff in reliable positions and management until they reach the necessary qualifications in accordance with the provisions of this document.

The training includes the following contents:

- Principles and security mechanisms of the certification hierarchy and the workplace.
- Current versions of hardware and software.
- Tasks to be performed by the person.
- Management and handling of incidents and security problems.
- Business continuity and emergency procedures.

7.3.4. Requirements and frequency of training update

For all domains

The Notarial Certification Agency schedules a training update for the staff at least every two years.

7.3.5. Sequence and frequency of job rotation

Certificate creation domain.

The Notarial Certification Agency defines job turns in order to meet the needs of the service 24x7.

User registration and card management domain.

Not applicable.

7.3.6. Sanctions for unauthorized actions

Certificate creation domain.

The Notarial Certification Agency has a penalty system for potential liabilities arising from unauthorized actions, which is appropriate to the applicable labor legislation and, in particular, is coordinated with the disciplinary system of the collective agreement applicable to the staff.

Disciplinary actions include suspension and dismissal of the person responsible for the harmful action.

User registration and card management domain.

Not applicable.

7.3.6.1. Disciplinary proceedings

The staff of the Notarial Certification Agency is bound by the following:

- Use the material means of the Notarial Certification Agency without engaging in activities that would be considered unlawful or which infringe the rights of the entity or third parties, or that might violate the moral or ethical rules and etiquette of such networks.
- Do not send confidential information to outside by hardware or by any means of communication, including simple visualization or access, except when expressly authorized by the Notarial Certification Agency.
- Save, indefinitely, the utmost discretion and not disclose or use directly or indirectly or through third parties or companies, data, documents, methodologies, key, analysis, software and other information to which they have access during their employment in the Notarial Certification Agency or related institutions, both software and physical supports. This obligation will remain even if the employment relationship has been extinguished.
- Not to misuse material or information property of the Notarial Certification Agency, both now and in the future.
- In the case that, for reasons directly related to the job, is required the possession of confidential information in any medium, such possession shall be construed as strictly temporary, with the obligation of secrecy and without any ownership or copyright granted regarding such information. The previously mentioned materials should be immediately returned to the Notarial Certification Agency after completion of the tasks and, in any case, after the termination of employment.
- Transfer to the Notarial Certification Agency patent rights over inventions or other intellectual property that they originate and/or develop. All programs and documents generated by employees in their working time and/or with the means and/or materials of the Notarial Certification Agency are considered property of the latter, which assumes all legal ownership of the contents of all computer systems under their control.

In order to ensure compliance with internal regulations the Notarial Certification Agency has the right to revise, without notice, computer systems (e-mail files, files on the hard disk of personal computers, voice mail files, print queues, etc ...). Inspections are performed after approval by the Security Department, according to the procedure established in the applicable regulations.

The Notarial Certification Agency can remove from its computer systems, any material that it deems offensive or potentially illegal.

7.3.6.2. Unauthorized activities

The following activities are not authorized for employees of the Notarial Certification Agency:

- Share or provide user IDs and/or password provided by the Notarial Certification Agency with other third party, including the staff. In case of violation of this prohibition, the employee shall be solely responsible for the acts of the third person using these user IDs.
- Trying to distort or falsify system LOG records.
- Trying to decipher keys, encryption algorithms and other security elements involved in telematic processes of the Notarial Certification Agency.
- Destroy, alter, disable or otherwise damage data, programs or electronic documents the Notarial Certification Agency or third parties.
- Willfully hinder other employees access to the network through mass consumption of computing resources and telematic the Notarial Certification Agency, as well as actions that damage, interrupt or generate errors in the system.
- Send emails in bulk or commercial or advertising purposes without the consent of the recipient (spam).
- Read, delete, copy or modify e-mail messages or files of other employees.
- Use the system to attempt to access restricted areas of computer systems of the Notarial Certification Agency or third parties.
- Try to increase the privilege level of an employee in the system.
- Voluntarily introduce programs, viruses, macros, applets, ActiveX controls or any other logic device or sequence of characters that are causing or are likely to cause any alteration in the computer system the Notarial Certification Agency or third parties. The employee will be required to use antivirus software and updates to prevent entry into the system from any element intended to destroy or corrupt computer data.
- Enter, download from Internet, reproduce, and use or distribute software unless expressly authorized by the Notarial Certification Agency.
- Install illegal copies of any program, including standardized copies.
- Remove any programs installed illegally.
- Using telematic resources of the Notarial Certification Agency including the Internet, for activities unrelated to the work of the employee.
- Transfer to the corporate network of the Notarial Certification Agency obscene, immoral or offensive, and in general, superfluous contents.

- Use information and/or log in as natural or legal persons identified or identifiable in the network without the necessary legitimacy for use.
- Create files containing personal data without authorization the Notarial Certification Agency.
- Crossing information concerning personal data from different files or services with the aim of establishing personality profiles, buying habits or any kind of preferences, without the express permission of the Notarial Certification Agency.
- Any other activity specifically prohibited in the security policy the Notarial Certification Agency and current legislation on protection of personal data.
- Treat personal data, in writing or orally, without the proper authorization by the Notarial Certification Agency.
- The use of bypass systems, designed to avoid protective measures, and other files that could compromise protection systems or resources.

7.3.7. Requirements for hiring professionals

Certificate creation domain.

The Notarial Certification Agency can hire professionals for any function, even for a reliable place in which case should be referred to the same controls mentioned above.

In the case that the professional does not need to undergo such controls, he must be constantly accompanied by a reliable employee while he is present in the installations of the Notarial Certification Agency.

User registration and card management domain.

Not applicable.

7.3.8. Providing documentation to staff

Certificate creation domain.

The Notarial Certification Agency provides the documentation strictly required by the staff at any time, in order to be competent enough as set out in this document.

User registration and card management domain.

Not applicable.

7.4. Security Audit Procedures

7.4.1. Types of recorded events

Certificate creation domain.

The Notarial Certification Agency keeps records for, at least, the following events:

- Turning on/off of the systems.
- Starting and ending of the software for the certification authority or the registration authority.
- Attempts to create, delete, change passwords or user permissions within the system.
- Generation and changes in the keys of the Certification Entity.
- Changes in the policies for issuing certificates.
- System login/logout attempts.
- Unauthorized access attempts to the network of the Certification Entity.
- Unauthorized attempts to the file system.
- Failed attempts to read a certificate, and reading and writing in the repository of certificates.
- Events related to the lifecycle of the certificate, such as request, issuance, revocation and renewal of a certificate.
- Events related to the lifecycle of the cryptographic module, such as reception, use and uninstallation.

The Notarial Certification Agency should also keep, either manually or electronically, the following information:

- The key generation ceremony and databases for key management.
- Physical access logs.
- Maintenance and system configuration changes.
- Staff changes.
- Incidental reports.
- Records of destruction of material containing information of keys, activation data or personal information of the subscriber or the key holder.
- Possession of activation data, for operations using the private key of the Certification Entity.

User registration and card management domain.

The Notarial Certification Agency (through the organization) will store the following information:

- Turning on/off of the system hosting the registration entity.
- Start and ending of the registration entity application.
- Correct and incorrect requests processing.
- Issuance, renewal and revocation requests.

7.4.2. Review period for audit logs

For all domains

Audit logs are reviewed for suspicious or unusual activity at least once a month.

The processing of audit logs consists of a review of records (including verification that these records have not been tampered), a brief inspection of all log entries and further investigations of any alerts or irregularities in records.

Actions taken during the audit review are also documented.

7.4.3. Retention period for audit logs

For all domains

Audit logs must be retained on site for at least two months after processing and, thereafter, shall be archived in accordance with this document.

7.4.4. Protection of audit logs

For all domains

Audit logs, either manual or electronic are protected from reading, modification, deletion or any other unauthorized manipulation using logical and physical access controls.

7.4.5. Backup procedures

For all domains

It is generated, at least, incremental backup copies of audit logs daily, and full backups weekly.

7.4.6. Log aggregation systems

For all domains

The log aggregation system is, at least, an internal system consisting of application logs, network logs and operating system logs, in addition to data generated manually, which will be stored by authorized personnel.

7.4.7. Notification of audit event

For all domains

When the log aggregation system records an event, it is not necessary to send a notification to the individual, organization, device or application that caused the event.

It may be communicated if the result of his action was successful or not, but not that this action has been audited.

7.4.8. Vulnerability Scan

For all domains

Events in the audit process are saved, in part, to monitor system vulnerabilities.

The vulnerability analysis is performed, reviewed and revised through an examination of these monitored events.

These analyzes are performed daily, monthly and annually in accordance with the audit plan or document replacing it.

7.5. Archiving of information

For all domains

The Notarial Certification Agency must ensure that all information relating to certificates is stored for an appropriate period, as provided in this document.

7.5.1. Types of recorded events

Certificate creation domain.

The Notarial Certification Agency keeps all events that occur during the life cycle of a certificate, including renewal.

It is stored a record of the following:

- Identity of the entity processing the certificate request.
- Certificate lifecycle information
- Audit data

User registration and card management domain.

The Notarial Certification Agency (through the organization) will store the following information:

- Type of document presented at the request of the certificate.
- Unique identification number provided by the previous document.
- The location of copies of certificate requests and the document signed by the subscriber or the key holder, as appropriate.

7.5.2. Record retention period

For all domains

The Notarial Certification Agency keeps the records specified in the previous section a minimum of fifteen (15) years.

7.5.3. 7.5.3. Archive Protection

For all domains

The Notarial Certification Agency:

- Maintains the integrity and confidentiality of the archive containing the data of issued certificates.
- Archives the above information assuring completion and confidentiality.
- Maintains the privacy of subscriber's (or key holder) registration data.

7.5.4. Backup procedures

For all domains

The Notarial Certification Agency performs daily incremental backups and weekly full backups of all its electronic documents, according to this document. It is also performed weekly full backups for data recovery cases, in accordance with this document.

Certificate creation domain.

According to this document, it is also kept paper documents in a location outside the Notarial Certification Agency for cases of data recovery.

User registration and card management domain.

En este dominio se utilizarán las mismas medidas que las usadas en los procedimientos de la Organización

7.5.5. Timestamping requirements

Certificate creation domain.

The Notarial Certification Agency issues certificates and CRLs using reliable date and time. It is not necessary that this information is digitally signed.

User registration and card management domain.

The databases of the Registration Entity employ reliable records of date and time.

It is not necessary that this information is digitally signed.

7.5.6. Location of the archive

For all domains

The Notarial Certification Agency must have a management system for the archive located outside its own facilities as specified in this document.

7.5.7. Procedures for obtaining and verifying archived information

For all domains

Only persons authorized by the Notarial Certification Agency have access to archived data, either in the same facilities of the Notarial Certification Agency or an outdoor location.

7.6. Key Renewal

Certificate creation domain.

The Notarial Certification Agency establishes a scheduled renovation plan for infrastructure keys, in order to ensure continuity of services.

User registration and card management domain.

Not applicable

7.7. Key compromise and disaster recovery

7.7.1. Procedures of incident management.

Certificate creation domain.

Backups are saved in external storage facilities of the following information, which are made available in the event of compromise or disaster: technical data of certificate requests, audit data and records of issued certificates.

Backups of private keys of the Notarial Certification Agency are generated and maintained in accordance with this document.

User registration and card management domain.

Same measures as for the incident management system.

7.7.2. Corruption of resources, applications or data

Certificate creation domain.

Where there is an event of corruption of resources, applications or data, the Notarial Certification Agency initiates the necessary steps, in accordance with the security plan, the emergency plan and the audit plan or equivalent documents, to bring the system back to normal operation.

User registration and card management domain.

The incident should be communicated to the Security Manager and the procedures for the management of the incident should be initiated.

7.7.3. Revocation of the public key of the entity

Certificate creation domain.

In case that the Notarial Certification Agency must revoke the public key of a Certification Authority belonging to its hierarchy, it is performed the following actions:

- Report this fact, when it may happen,, to the General Council of Notaries.
- Report the matter by issuing a CRL, as provided in this document..
- Make every effort to report the revocation to all subscribers to which the Notarial Certification Agency has issued certificates, as well as to third parties who trust certificates.
- Perform a key renewal, if the revocation was not due to termination of service by the Notarial Certification Agency as provided in this document..

User registration and card management domain.

- Not applicable.

7.7.4. Compromise of the private key of the entity

Certificate creation domain.

The business continuity plan of the Notarial Certification Agency (or disaster recovery plan) considers the compromise or suspected compromise of the private key of the Certification Entity as a disaster.

In case of compromise, the Notarial Certification Agency does at least the following:

- Inform all subscribers and third parties.
- Inform that the certificates and revocation status information that have been delivered using this key are no longer valid.

User registration and card management domain.

- Not applicable.

7.7.5. Disaster on the facilities

Certificate creation domain.

The Notarial Certification Agency develops, maintains, tests and, if necessary, implements an emergency plan in case a natural or manmade disaster should occur on its facilities. This plan describes how to restore the information systems services.

The location of the disaster recovery systems has adequate physical security safeguards as detailed in the security plan.

The database used by the Notarial Certification Agency for disaster recovery is synchronized with the production database, within the time limits specified in the security plan.

The disaster recovery equipment implements the physical security measures specified in the security plan, and is equivalent to those of the main equipment.

User registration and card management domain.

- Not applicable.

7.8. Termination of Service

Certificate creation domain.

ANCERT shall communicate , where appropriate, the cessation of its activity, to Subscribers and Requestors for Certificates on behalf of legal persons, and may transfer, with their explicit consent, the management of the ones that remain valid on the date on which the cessation occurs to another certification service provider that assumes or otherwise terminates their validity.

This communication shall take place with a minimum of two months in advance to the effective end of the activity and shall inform, where appropriate, about the characteristics of the provider to whom is proposed to transfer the management of the Certificates.

ANCERT will also publish on the web and on a national newspaper this circumstance with a minimum of two months in advance. ANCERT will inform the Ministry of Science and Technology, with the time indicated in the above paragraph , the cessation of its activity and the destination that will give to the Certificates, specifying, where appropriate, whether to transfer the management and to whom or if it will terminate its validity.

It will notify any other relevant circumstances that may prevent the continuation of its activity. In particular, it shall communicate, on becoming aware of this, the opening of any insolvency proceedings taken against him.

ANCERT will forward to the Ministry of Industry, Trade and Tourism, prior to the termination of its activities, the information concerning to the Electronic certificates whose validity has expired so the Ministry can take over its custody based on the provisions of Article 20.1.f) of the Law on Electronic Signature. The Ministry will maintain a specific consultation service, publicly available, which contains an indication of the above Certificates for a period deemed sufficient in terms of the consultations made to it.

User registration and card management domain.

The Notarial Certification Agency, through the Organization, ensures that potential disruptions affecting subscribers and third parties would be minimal due to the termination of the services and, in particular, ensure maintenance of records required to provide evidence of certification for civil or criminal investigation, by transferring these records to a notarial deposit.

Before termination of service, the Notarial Certification Agency, through the organization, develops a plan of termination, with the following provisions:

- Execution of the tasks required to transfer the obligations of maintaining the registration information and event log files for the periods indicated to the subscriber and third parties who trus the certificates.

8. Technical security controls

The Notarial Certification Agency uses trustworthy systems and products protected against modification, and also ensure technical and cryptographic security of the certification process.

8.1. Generation and Installation of the key pair Generation of the key pair

8.1.1. Generation of the key pair

The Notarial Certification Agency, when acting as root Certification Authority, generates and signs its own key pair and proceeds to the generation of the keys for each subordinate Certification Authority, all in accordance with the key ceremony within the high security perimeter specifically for this task.

The key pairs of end entities are generated by the Notarial Certification Agency or end entities, either in secure devices such as cryptographic cards or USB tokens, or in softwar.e

- Cryptographic card The creation of public and private keys (2048 bit RSA) is performed internally by the card itself so that it guarantees both the robustness of the keys as the impossibility of a compromise in the generation process.
- For software certificates, the generation of the keys is performed in the operating systems or applications of end users.

8.1.2. Delivery of the private key to the subscriber

The subscriber's (or key holder) private key is delivered properly protected by the cryptographic device, except when the key is generated by the end entity (organization), in which case this section is not applicable.

8.1.3. Delivery of the public key to certificate issuer

The method for delivering the public key to the Certification Entity is PKCS # 10, another cryptographically equivalent proof or any other method approved by the Notarial Certification Agency.

8.1.4. Distribution of the public key

The keys of the Certification Entities are communicated to third parties who trust the certificates, ensuring the integrity of the key and authenticating its origin.

The public key of each Certification Entity is published in the repository, as a self-signed certificate or signed by another Certification Authority, along with a statement regarding the fact that this key authenticates the Certification Entity.

Additional measures are established to trust self-signed certificates, such as checking the fingerprint of the certificate.

Users can access the repository in order to obtain the public keys of the Certification Authorities.

Additionally, for S/MIME applications the message may contain the certificate chain, which can be used to communicate keys to users.

8.1.5. Key sizes

The length of the keys of the Certification Entities shall be at least 4096 bits, while for the remaining types of certificates shall be at least 2048 bits.

8.1.6. Public key parameters generation

Not defined.

8.1.7. Quality checking for public key parameters

The Notarial Certification Agency may provide methods for verifying the quality of the public key parameters.

8.1.8. Key generation in software or hardware

The keys of the Certification Entities are generated in cryptographic hardware that meets FIPS 140-2 Level 3.

The keys for electronic signature of end users are generated in cryptographic devices that meet the functional security measures in the protection profile described in the technical specification CEN CWA 14169, and can be certified in accordance with this profile or other equivalent protection profiles, both Common Criteria and other internationally recognized certification schemes, except for software certificates where the generation of the keys is performed in the operating systems or applications of end users.

8.1.9. Key Usage

The Notarial Certification Agency includes the extension KeyUsage in all certificates, indicating the permitted uses of the corresponding private key.

8.2. Protection of private key

8.2.1. Cryptographic Module Standards

For modules that manage keys of Certification Entities or used by subscribers to generate qualified electronic signature, it is ensured the level required by the standards stated in the previous sections.

8.2.2. Control by more than one person (n of m) on the private key

Access to private keys of Certification Entities will necessarily require simultaneous operation of two (2) cryptographic devices protected by password, from a set of four (4) devices.

The password is only known by one person responsible for that device. No person knows more than one password. Ninguna de ellas conoce más que una de las claves de acceso.

Cryptographic devices are stored on the facilities of the certification service provider, and require an additional person in order to gain access to them.

8.2.3. Deposit of the private key

The private keys of Certification Entities should be stored in fireproof locations and protected by dual physical access controls.

No other private keys should be stored.

8.2.4. Backing up the private key

Private keys of the Certification Entities are backed up, stored in a separate location where it is usually stored and retrieved if necessary, by personnel subject to the trust policy for the staff. These personnel are expressly authorized for such purposes, and are restricted to the minimum necessary.

The security controls applied to backups of Certification Entities are of equal or higher level than those usually applied to the keys in use.

When the keys are stored in a hardware module, appropriate controls are provided so that they can never leave the device.

8.2.5. Archive of the private key

The private keys of Certification Entities are archived permanently at the end of its period of operation.

End user's private keys for the generation of signature are not archived.

8.2.6. Importing the private key in the cryptographic module

Private keys can be generated in the cryptographic modules, or in external cryptographic modules from where they are encrypted and exported, in order to import them later in the production modules.

Private keys of Certification Entities are stored on encrypted files with fragmented keys in cryptographic devices (from where they could not be removed)

These devices are used to import the private key in the cryptographic module.

8.2.7. Private key activation method

The private key of each Certification Authority will be activated by running the startup procedure for secure cryptographic modules.

The subscriber's private key will be activated by entering the PIN on the cryptographic device or in the signature application.

8.2.8. Private key deactivating method

For qualified electronic signature certificates, when the cryptographic device is removed from the reader or disconnected from the computer, or the session of the application using it has expired, it shall be required the introduction of the PIN again.

8.2.9. Private key destruction method

Private keys shall be destroyed in a manner to prevent theft, modification, unauthorized disclosure or unauthorized use.

8.3. Other aspects of key pair management

8.3.1. Public key archive

Certification Entities shall archive their public keys in a permanent way, in accordance with the provisions of this document.

8.3.2. Periods of use of public and private keys

Periods of use of the keys are determined by the duration of the certificate. They are not used after the expiration of the certificate.

As an exception, the private key can continue to be employed for decryption of documents, even after the expiration of the certificate.

8.4. Activation data

8.4.1. Generating and installing activation data

In cases where the Notarial Certification Agency provides the subscriber a secure signature creation device, then the device activation data is securely generated by the certification service provider.

To make a signature or activate the card is needed to enter the secret activation code (PIN) that is only known by the key holder of the card. Three consecutive erroneous attempts in the entry of the PIN cause a blockage of the card. To unlock the card, the cardholder must enter the PUK code (three consecutive attempts at the introduction of wrong PUK cause irreversible blocking of the card).

8.4.2. Protection of activation data

The Notarial Certification Agency generates and provides the subscriber activation data for the device using safe procedures such as delivery in person, or distance, in which case the activation data is distributed separately from the secure signature creation device (at different times, or by different routes, for example).

8.4.3. Other aspects of the activation data

Not defined.

8.5. Computer security controls

8.5.1. Specific technical requirements for computer security

Access to the systems is limited to the authorized persons. In particular:

- Effective management of the access level of users (operators, administrators and anyone with direct access to the system) is ensured in order to maintain system security, including user account management, auditing and modifications or denial of access privileges.
- Access to information systems and applications is restricted in accordance with the provisions of the access control policy, and that the systems provide adequate security controls to implement segregation of duties identified in the practices, including separation of functions between the management of security systems and operators. In particular, the use of system utility programs should be restricted and controlled.
- Personnel are identified before using critical applications related to the lifecycle of the certificate.
- The staff is responsible and can justify their activities, for example by using an event log file.
- It is avoided the possibility of disclosure of sensitive data by reusing storage resources (eg deleted files) that are accessible to unauthorized users.
- Security and monitoring systems allows rapid detection, recording and acting against irregular or unauthorized access attempts to sensitive resources (for example, by using an intrusion detection, monitoring and alarm system)
- Access to public repositories of information (eg certificates or revocation status information) has access control for changes or deletion of data.

8.5.2. Assessing the level of computer security

Software for Certification and Registration Authorities used by the Notarial Certification Agency is trustworthy. This condition must be credited, for example, by a product certification against a profile of protection, according to ISO 15408, with level EAL4 +.

8.6. Lifecycle technical controls

8.6.1. System development controls

It is conducted an analysis of security requirements during the phases of specification and design of any application used by certification and registration authorities, in order to ensure that systems are secure.

Procedures have also been defined for updates, change control for new releases and emergency patches of these components.

8.6.2. Security Management Controls

The Notarial Certification Agency maintains an inventory of all information assets and defines a classification of them according to their protection needs and consistent with the current risk analysis.

The configuration of the systems is regularly audited, in accordance with the provisions of this document.

Capacity requirements are monitored and procedures are planned to ensure sufficient availability of storage for electronic and information assets.

8.6.3. Assessing the security level of the life cycle

The General Council of Notaries may require that the Notarial Certification Agency undergo independent evaluations, audits and, where appropriate, security certifications for the lifecycle of its products.

8.7. Network Security Controls

Access to different networks of the Notarial Certification Agency is restricted to authorized persons. In particular:

- Controls are implemented to protect the internal network from external domains accessible by third parties. Firewalls are configured so as to prevent access and protocols that are not necessary for the operation of the Certification Entity.
- Sensitive data is protected when exchanged over insecure networks (including data such as subscriber registering information)
- Local network components are located in secure environments, and scheduling regular audits of their configurations are also performed.

8.8. Engineering controls for cryptographic modules

The keys of the Certification Entities are generated in cryptographic equipment, operated by trusted staff and in a secure environment under dual control.

This equipment meets the security cryptography standards, which have been indicated in previous sections.

Key generation algorithms are accepted and appropriate to the intended key usage (for each type of certificate).

9. Certificate and certificate revocation list profiles

9.1. Certificate profile

Certificates have the content and fields described in this section including at least the following:

- Serial number, it will be a unique code with respect to the issuer's distinguished name.
- Signature algorithm.
- Distinguished name of the issuer.
- Beginning of the validity period, in Coordinated Universal Time, according to RFC 3280.
- End of validity period, in Coordinated Universal Time, according to RFC 3280.
- Distinguished name of the subject.
- Subject's public key, according to RFC 3280.
- Signature, generated and encoded according to RFC 3280.

Certificates are compliant with the following standards:

- RFC 3280: Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, April 2002.
- ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997, with updates and corrections.

Additionally, certificates for electronic signature shall comply with the following standards:

- ETSI TS 101 862 v1.3.3 (2006-01): Qualified Certificate Profile, 2006.
- RFC 3739: Internet X.509 Public Key Infrastructure - Qualified Certificate Profile, March 2004 (unless they conflict with TS 101 862).

The Notarial Certification Agency publishes their certificate profiles in the repository.

9.2. Certificate revocation list profile

The Notarial Certification Agency publishes their certificate revocation list profiles in the repository.

10. Compliance audit

The Notarial Certification Agency periodically conducts a compliance audit to prove compliance with the security and operational requirements needed to meet the certification services policy of the General Council of Notaries.

10.1.1. Frequency of compliance audit

A compliance audit is conducted annually, in addition to internal audits that can be carried out at their own discretion or at any time because of a suspected break of any security measure or a key commitment.

10.1.2. Identification and qualification of auditors

If the Notarial Certification Agency has an internal audit department, it may undertake to perform the compliance audit.

In the case of not having that department, or if considered appropriate, it is required the services from an independent auditor, which must demonstrate experience in security of information and auditing public key infrastructure services.

10.1.3. Relationship between the auditor and the auditee

Compliance audits performed by third parties are conducted by an independent entity. The Notarial Certification Agency does not have any conflict of interest with this independent auditor affecting his ability to perform audit services.

10.1.4. List of audited items

The audited items are:

- Processes of public key certification.
- Information systems.
- Protection of the processing center.
- Documentation of service.

The details of how to conduct the audit of each of these items is detailed in the audit plan of the Notarial Certification Agency.

10.1.5. Actions to be taken as a result of a lack of conformity

Upon the reception of the audit compliance report, the Notarial Certification Agency discusses with the entity that performed the audit and, where appropriate, with the General Council of Notaries, the deficiencies found, and defines and implements a plan in order to solve these deficiencies.

If the Notarial Certification Agency is unable to develop and/or implement such plan, or if the deficiencies pose an immediate threat to the security or integrity of the system, it is taken one of the following actions:

- Revocation of the key of the Certification Entities as described in this document.
- Ending the certification services, as described in this document.

10.1.6. Treatment of audit reports

The Notarial Certification Agency submits the audit results to the General Council of Notaries, within 15 days after completion of the audit.

11. Business and legal requirements

11.1. Fees

11.1.1. Fee for the issuance or renewal of certificates

The Notarial Certification Agency establishes a fee for the issuance or renewal of certificates, which is approved by the General Council of Notaries.

11.1.2. Fee for certificate access

The Notarial Certification Agency does not establish a fee for access to the certificates.

11.1.3. Certificate status information fee

The Notarial Certification Agency does not establish a fee for access to status information of certificates.

11.1.4. Fees for other services

Not defined.

11.1.5. Refund policy

The Notarial Certification Agency has the following refund policy:

When a correction or amendment of the Declaration of Certification Practices implies a limitation of rights of use or restriction on the scope of an existing certificate, the subscriber may claim a refund, limited to the value of the certificate.

In other cases, the Subscriber shall have no right to refund the cost of the certificate.

11.2. Financial Capacity

The Notarial Certification Agency has sufficient financial resources to maintain operations and meet its obligations, and to address the risk of liability for damages.

11.2.1. Insurance Coverage

The Notarial Certification Agency has civil liability coverage, by professional civil liability insurance or through a bond or guarantee.

The guaranteed amount is, at least, 3,000,000 euros or higher.

11.2.2. Other assets

Not defined.

11.2.3. Insurance coverage for subscribers and third partied who trust the certificates

Not defined.

11.3. Confidentiality

11.3.1. Confidential information

The following information, at least, is kept confidential by the Notarial Certification Agency:

- Certificate requests approved or denied, and any other personal information collected for issuing and maintaining certificates, except the information specified in the following section.
- Private keys generated and/or stored by the Notarial Certification Agency.
- Transaction records, including audit records of transactions.
- Internal and external audit records, created and/or maintained by the Notarial Certification Agency and their auditors.
- Business continuity and emergency plans.
- Security plans and policy.
- Documentation of operations and other operational plans, as archiving, monitoring and the like.
- Any other information marked "Confidential."

11.3.2. Non-confidential information

The following information is considered non-confidential:

- Certificates issued, or in process of issuance.

- Relationship between a subscriber and a certificate issued by a Certification Entity.
- First and last name of the certificate subscriber or the key holder, as appropriate, and any other circumstance or personal data that may be meaningful in terms of the purpose of the certificate.
- Email address of the subscriber or the key holder, as appropriate or any other proper email.
- Uses and amount limits defined in the certificate.
- Period of validity of the certificate, and date of certificate issuance and expiration date.
- Serial number.
- States of the certificate, and their associated starting date, namely: generation and/or delivery, valid, revoked, suspended or expired and the reason that caused the status change.
- Certificate revocation lists (CRLs) and the other revocation status information.
- Information of the repository.
- Any other information not contained in the previous section of this policy.

11.3.3. Disclosure of suspension and revocation information

See the previous section.

11.3.4. Legal Disclosure of information

The Notarial Certification Agency will disclose confidential information in cases provided by law.

Specifically, records that support the reliability of data contained in the certificate will be disclosed if they are required to provide evidence of certification in case of legal proceedings, even without consent of the certificate subscriber.

These circumstances shall be indicated in the privacy policy under this document.

11.3.5. Disclosure by request of the holder

The Notarial Certification Agency includes requirements to permit the disclosure of subscriber information and, where appropriate, the key holder, directly to them or others.

11.3.6. Other circumstances for information disclosure

Not defined.

11.4. Privacy Policy

In order to provide certification services, the Notarial Certification Agency needs to collect and store certain information, including personal information.

The Notarial Certification Agency develops a privacy policy in accordance with Organic Law 15/99 of December 13th on the Protection of Personal Data, and describes it in its Declaration of Certification Practices, together with aspects and security procedures corresponding to the Security Document, as described by law. This Declaration of Certification Practices will be considered as the Security Document.

11.4.1. Scope of Data Protection

The Notarial Certification Agency will protect the files with personal data collected in the course of his business as Certification Service Provider (hereinafter Files) in accordance with the provisions of Law 15/1999 of December 13, on Personal Data Protection,(LOPD), the Regulation of security measures approved by Royal Decree 994/1999 of June 6 (RD 994/1999) and other regulations. These files are privately owned and its creation, modification or deletion shall be notified to the General Registry of Data Protection of the Spanish Agency for Data Protection.

To perform its certification activity, Registration Authorities will access these files. The Notarial Certification Agency will have the status of Responsible of the File, being the decision maker on the content and use of the processing of personal data, and the Registration Authorities shall be deemed responsible for the processing, which must use the data contained in those files only and exclusively for the purposes listed in its Certification Practice Statement.

The Registration Authorities, in compliance with the provisions of Article 12 of the Personal Data Protection Law undertake:

1. Process personal data according to the instructions of the Responsible of the File.
2. To ensure and protect civil liberties and fundamental rights of individuals, and especially their honor and personal and family privacy.
3. A professional secrecy regarding personal data, not disclosing to third parties information collected during this contractual relationship, This obligation shall continue even after the end of relations with the Responsible of the File.
4. To comply with all appropriate technical and organizational measures to ensure the security of the Files, processing centers, facilities, equipment, systems, programs and people involved in the processing of personal data, all reflected in the security document that is required by the RD 994/1999.
5. To implement appropriate technical and organizational measures to ensure the security and integrity of personal data and avoid its alteration, loss, or unauthorized access, given the state of technology, the nature of the data stored and the risks they are exposed to, whether they come from human action or natural.
6. To submit to the Notarial Certification Agency the personal data of the Requestors and/or Subscribers of Certificates through secure communications.
7. To process data as stipulated in the contract with the Notarial Certification Agency, and not apply or use it for different purposes, nor communicate it, even for its preservation, to others.

8. To only access Files of the Notarial Certification Agency Files when necessary to perform the contracted services.
9. To destroy or return all personal data processed once completed for any reason the relationship with the Notarial Certification Agency, except the information required by law to be kept for a minimum of 15 years.

The Registration Authorities shall verify that the Subscriber and/or Requestor are informed and give consent to the processing of their data, for the purposes established in the relevant documents of consent.

The Notarial Certification Agency is released from any liability that may be generated by the failure of those responsible for the processing of their described obligations. In such events, they will be considered as responsible and liable for the infringements they have incurred personally.

In accordance with the provisions of Article 5 of the Personal Data Protection Law, it should be notified to the Requestor/Subscriber that personal data included in the forms, contracts or documents that are filled in during the requesting process for the issuance of a Certificate shall be recorded in a file created for that purpose. The Notarial Certification Agency will only provide certification services if the forms are filled in entirely with real information. In any case, the Requestor/Subscriber that by any means communicates personal data to the Notarial Certification Agency is consenting to the processing of his data for the uses and purposes of providing certification services under the terms established in the Law and this Certification Practice Statement.

In accordance with the provisions of Article 11 of the Personal Data Protection Law , the Requestor/Subscriber or any user of the Certificates, is consenting to the communication to third parties who trust the electronic certificates of their personal data contained in the Certificate through the Directory of Certificates contained in the website www.ancert.com, only for the purpose of allowing consultation of the Certificates issued by the Notarial Certification Agency and their validity period, and in the Directory of Certificates and Certificate Revocation Lists to query certificates revoked by the Notarial Certification Agency.

Third Parties who trust the Certificates may only use information in accordance with the purposes described. Nevertheless, and in general, any treatment, record or use for other purposes than the above necessarily requires the prior consent of the holders of the data. It is noted that the Personal Data Protection Law punishes with fines that can reach up to SIX HUNDRED THOUSAND EUROS (600,000 €) for each of the offenses or breaches of that law, regardless of any criminal proceedings that can be derived from the Criminal Code as well as civil claims from the damaged .

The Requestor/Subscriber may exercise rights of access, rectification, cancellation and opposition according to the Personal Data Protection Law by sending the request to the address listed in this document.

11.4.2. Security document

11.4.2.1. Purpose of the Security Document

By this document, the Notarial Certification Agency ANCERT establishes the security measures to be implemented to protect the personal data contained in its files according to the current legislation on Protection of Personal Data.

As mentioned, the Notarial Certification Agency, directly or through Registration Authorities, collects personal information from Requestors/Subscribers, in order to identify them and provide the requested certification services. Given the nature of such data, according to Royal Decree 994/1999, the Notarial Certification Agency must adopt security measures of basic level.

The validity of the Security Document starts from its implementation and management of security measures until amended, if necessary.

This document ensures implementing the necessary technical and organizational measures to ensure the security of personal data processed in the Files that are responsibility of the Notarial Certification Agency to prevent its modification, loss, or unauthorized access and so they are used for a legitimate purpose.

With the Security Document, the Notarial Certification Agency implements security regulations to the computers and machines responsible for the processing of files, or local treatment centers, network, personnel, users, jobs, programs or applications and storage hardware or devices.

All staff that is directly or indirectly involved in the processing of personal data is obliged to observe and respect the provisions established in Royal Decree 994/1999 and, in particular, what is established in this document.

All personnel authorized to access the data is informed of their obligations and responsibilities.

11.4.2.2. Functions and responsibilities of the staff

ANCERT staff, as users that process Files, knows and performs its duties and obligations under the ANCERT Security Document. The use and processing of personal data involves personnel with different functions assigned, distinguishing:

the File Manager

the Security Manager

Systems Manager

The roles of those responsible are defined below:

The File Manager

His functions may be delegated to the Head of Security, stating such delegation in writing and expressly signed by both.

Are functions of the File Manager:

1. Managing the System of Protection of Personal Data.

2. Manage the treatment, quality and security controls of personal data.
3. Control the manner and procedure requirements for inscriptions and cancellations.
4. Control of security hardware.
5. Manage and direct the procedures of access, rectification, cancellation and opposition of those affected.
6. Implement, manage and maintain the security policy and provide the appropriate resources to ensure compliance with current regulations regarding the treatment of information on people.
7. Manage the notification and registration of the file.
8. Assure the compliance of the rules referred to in the Security Document.

Security Manager

Person formally designated by the File Manager for the coordination and control of the actions defined in the security document.

His functions are:

Within the scope of the file legalization:

1. Legalize the system of personal information and take care that the necessary notifications to the competent supervisory authority are made. Also perform or supervise where appropriate, that registration of the file and its modification or cancellation is made in an appropriate way.

Within the scope of legitimacy:

1. Ensure that personal data incorporated into the information system is properly entitled.
2. Supervise that application of data conforms to the following principles:
    a. Principle of Consent: The processing of personal data will require the express consent of the owner precisely and unequivocally.
    b. Information principle: it is required to inform the holder of personal data explicitly, precisely and unequivocally:
        i. The existence of a file or processing of personal data.
        ii. The identity and address of the File Manager.
        iii. The purpose of the collection.
        iv. The recipients of information.
        v. Mandatory or optional character of his response to the questions demanded.

vi. The consequences of obtaining personal data and the consequences of the refusal to supply it.

vii. The possibility of exercising rights of access, rectification, cancellation and opposition.

c. Principle of exercise: it must be ensured that the holder of personal data can exercise his rights of: access, rectification, cancellation and opposition

d. Quality Principle: Personal data may be collected for treatment only when it is adequate, relevant and not excessive in relation to the scope and specific, explicit and legitimate purposes for which they were obtained. Furthermore, the data must be accurate and updated so that they respond truthfully to the current situation of the holder.

e. Principle of shielding: The information system must be shielded by perimeter contracts, against third parties who, within the framework of a legal relationship of service provision, access or can access the personal data of which the Notarial Certification Agency is responsible.

3. Is responsible for the development and maintenance of the Security Document information system that collects the security measures in the different areas of the entity.

4. Supervise the correct implementation of the Security Document and the register of incidences protocol.

Within the technology scope:

1. Plan, implement and monitor the security of hardware devices, software applications and the various communications, and so it will manage:

    a) The identification and authentication of users.

    b) The backup and recovery procedure of personal data.

    c) The automated organization of supports.

    d) Perform audits or reviews.

    e) Incidental management

Within the physical domain:

1. Plan, implement and monitor the security of the centers, units, physical storage devices and hardware:

    f) The identification and authentication of users.

    g) The backup and recovery procedure of personal data.

    h) Organization of hardware.

    i) Perform audits or reviews.

j) Incidental management

System Administrator

This person is responsible for managing and maintaining the operating environment of the files. To this end, he may have the ability to access protected data, prior authorization of the File Manager.

Are functions of the Information System Manager:

1. Plan, implement and monitor the security of hardware devices, software applications and the various communications, and so it will manage:
    a) The identification and authentication of users.
    b) The backup and recovery procedure of personal data.
    c) The automated organization of supports.
    d) Perform audits or reviews.
    e) Incidental management

11.4.2.3. Measures, standards, procedures and rules aimed at ensuring the security level required in the RD 1720/2007.

Processing areas

ANCERT has an inventory of physical accesses which refers to the existing entrances to access the facilities where personal information is processed. Access is limited to authorized personnel only.

Assets are rearranged and relocated rationally in order of criticality, trying as far as possible to house them in cabinets equipped with locks.

In no case, unauthorized persons can stay in units that require authorization or qualification, without the presence of authorized persons.

Network, operating system and communications

The Notarial Certification Agency regulates the use and access to the operating system, tools or programs, or communications environment, so as to prevent unauthorized access to personal information.

Only authorized personnel may grant, modify or cancel the authorized access to personal data and resources, in accordance with criteria established by the Security Manager.

The operating system and communications is under the supervision of the System Administrator.

The Security Manager must keep the backups in a protected place so that no unauthorized person has access to them.

Applications of access to personal information

The computer systems of access to personal information must have their access restricted through a username and password.

All authorized users to access personal information must have a user code that is unique, and that will be associated to a password, that will only be known by the user.

If the application that allows access to personal information has no access control, should be the operating system that runs the application, the one preventing unauthorized access through the control of codes and passwords.

Applications for processing the personal data needed to generate an electronic certificate must produce temporary files (log files) which are properly guarded to ensure that such personal data is not later accessible by unauthorized personnel.

Procedure for Identification and Authentication.

Access to the office server (domain server) of the Notarial Certification Agency where personal information is located is restricted by a user code and password.

The System Administrator ensures that there is an updated list of users who have authorized access to the information system and to establish procedures for identification and authentication for access.

During the validity period, passwords are stored unintelligibly.

Personal passwords are one of the basic components of personal data security, and must therefore be specially protected.

As keys to access the system, passwords should be strictly confidential and personal, and any incident that compromises their confidentiality will be immediately reported to the Security Manager and remedied in the shortest time possible.

Distribution and storage of passwords

There is a default procedure of allocation, distribution and storage of passwords. Only those persons indicated by the Security Manager may have access to personal information of the system. The passwords are assigned and will change through the mechanism and timing determined in that procedure.

The identification numbers and passwords assigned to each user will be personal and not transferable; the user is the solely responsible for any consequences resulting from misuse, disclosure or loss.

Each user is responsible for the confidentiality of his password and, if it is disclosed accidentally or fraudulently by unauthorized persons, he must register it as incidence and proceed immediately to change it.

The file where the passwords are stored must be protected and under the responsibility of the Security Manager.

11.4.2.4. Structure of files with personal data

The structure of the personal data file used by the Notarial Certification Agency for the purpose of providing the certification activity is that which is contained in the File notified to the Spanish Agency for Data Protection. This structure is as follows:

Personal Data:

ID / Passport No.

Name and surname

Email Address

Phone

Home Address

Electronic signature

Workplace

Attributes

11.4.2.5. Procedure for reporting, managing and responding to incidents

Staff with knowledge of an incident shall be responsible for its notification in an express and writing form to the area manager affected by such incident, being either the physical, technological or human resources.

An Incidence is considered any event that may occur sporadically and can be a danger to the security of the Files, understood in its three aspects of confidentiality, integrity and availability of data.

The Security Manager enables an incident record book in which each area manager, prior express written notification to be made by any user who detected an incident, records this incidence. The Security Manager will also report that incidence with each and every one of the detailed data in the preceding paragraph, in the event log book.

The knowledge and no notification of an incident by a user shall be considered as an offense against the security of files.

The notification of an incident shall include at least the following information: type of incident, date and time of occurrence, person making the notification, a person to whom is communicated, possible effects and detailed description.

11.4.2.6. Procedures for backup and data recovery

The security of the personal data of the File involves not only their confidentiality but also the integrity and availability of such data.

To ensure these two aspects of security it is necessary the existence of some backup and recovery processes allowing recovering and rebuilding the data files in case of failure of the system.

The Security Manager will be responsible for obtaining a daily backup of files in order to recover them in case of failure and to safeguard it properly offsite.

In case of system failure with total or partial loss of personal data, there is an emergency plan which establishes a procedure that, starting from the last backup and transactions logged from the time of the backup, rebuilds the personal data to the state it was at the time of failure.

It will be required a written authorization from the Security Manager to implement the recovery procedures of personal data and shall be recorded in the record book of incidents all the operations performed for such recoveries, including the person who performed the process, the restored data and data that has been recorded manually in the recovery process.

11.4.2.7. Media handling

The hardware containing the files, either as a result of their processing or due to periodic backup, must be clearly identified with an external label to indicate which file it is, type of data contained, process that has originated it and date of creation.

Each area manager will create a detailed account (updated regularly) of the material containing personal data and the status of each hardware.

Hardware containing the files should be stored in places that no unauthorized persons have access for their use.

The removal of hardware containing the files off the premises where the information system is located must be expressly authorized by the Security Manager using an authorization document.

11.5. Intellectual Property Rights

11.5.1. Ownership of certificates and revocation information

The Notarial Certification Agency is the only entity that will benefit from the intellectual property rights of issued certificates, and shall grant non-exclusive license to reproduce and distribute certificates, without charge, provided that the reproduction is complete and does not alter any element of the certificate, and also is necessary regarding the authorized and legitimate uses in accordance with this policy and in accordance with the corresponding conditions of use.

The same rules will be applicable to the use of certificate revocation information.

The OID property of the Notarial Certification Agency has been registered with the IANA (Internet Assigned Number Authority) under the branch 1.3.6.1.4.1., having assigned the number 18920 (the Notarial Certification Agency), whose information is public:

http://www.iana.org/assignments/enterprise-numbers

It is further prohibited the use in full or partial of any of the OID assigned to the Notarial Certification Agency except for the applications described in the Certificates or Directory of Certificates.

It is forbidden all unauthorized extraction and/or reuse of all or a substantial part of the contents or databases that the Notarial Certification Agency makes available to the Subscribers of Certificates.

11.5.2. Ownership of policies and Declaration of Certification Practices

The General Council of Notaries is the only entity that will benefit from the intellectual property rights of policies of certificates.

The Notarial Certification Agency will also own the Declaration of Certification Practices.

11.5.3. Ownership of information concerning names

The subscriber and, where appropriate, the key holder, shall preserve any right (in case it does exist) on the brand, product or trade name contained in the certificate.

The subscriber will own the certificate distinguished name consisting of the information specified in this document.

11.5.4. Key property

The key pairs will be owned by subscribers of certificates.

When a key is divided into parts, all parts of the key are owned by the key owner.

11.6. Obligations and Liability

11.6.1. Model of obligations of the provider certification

The Notarial Certification Agency ensures, under its own responsibility, that meets all requirements for each certificate policy for issuing certificates.

It is the only entity responsible for compliance with the procedures described in this policy.

The Notarial Certification Agency provides its certification services in accordance with its current Declaration of Certification Practices, in which it is detailed their functions, operating procedures and security measures.

Prior to the issuance and delivery of the certificate to the subscriber, he is informed of the terms and conditions of use of the certificate, its price - when established - and its limitations of use.

This requirement is fulfilled through a "Text informative about the certificate policy", which may be transmitted electronically, using a medium long lasting, and in understandable language.

Subscribers, key holders and third parties who trust the certificates must comply with general conditions of issue and use of certificates, which must be in understandable language, and must have the following minimum contents:

- Requirements to comply with the provisions of this certification policy.
- Indication of applicable policy, including statements about the need of secure device and whether the certificates are issued to the public or not.
- Statement that the information contained in the certificate is correct, unless otherwise notified by the subscriber.
- Consent for the publication of the certificate in the repository and for granting access to third parties.
- Consent for the storage of information about the subscriber registration and the delivery of secure signature creation device, and for the provision of such information to third parties in case of termination of operations of the Certification Entity without revocation of valid certificates.
- Limits on the use of the certificate, including those set out in this policy.
- Information on how to validate a certificate, including the requirement to check the status of the certificate, and the conditions under which one can reasonably trust the certificate, which applies when the subscriber acts as a trusting party.
- Liability guarantees of the Notarial Certification Agency.
- Limitations of liability, including uses for which the Notarial Certification Agency accepts or excludes its liability.
- Archive period for certificate request information.
- Period of audit log file.
- Procedures for dispute resolution.
- Applicable law and jurisdiction.
- If the Certification Entity has been declared in conformity with the certification policy and, where appropriate, according to which system.

The Notarial Certification Agency must assume other duties directly incorporated in the certificate or incorporated by reference.

11.6.2. Guarantees offered to subscribers and third parties who trust the certificates

The Notarial Certification Agency, under the general conditions of issue and use of certificates, establishes and rejects warranties and applicable limitations of liability.

The Notarial Certification Agency ensures, at least, the subscriber:

- That there are no factual errors in the information contained in the certificates known by the Notarial Certification Agency and, where applicable, by the registration entity.
- That there is no factual errors in the information contained in the certificates due to lack of due diligence in the management of the certificate request or the generation.

- That certificates meet all requirements established in the Declaration of Certification Practices.
- That revocation services and the repository meet all requirements established in the Declaration of Certification Practices.

The Notarial Certification Agency guarantees, at least, to third parties trusting the certificates:

- That the information contained or incorporated by reference in the certificate is correct, except where otherwise indicated.
- In case of certificates published in the repository, that the certificate has been issued to the subscriber identified in it and that the certificate has been accepted in accordance with this certification policy.
- That the approval of the certificate request and the issuance has met the requirements established in the Declaration Certification Practices.
- The speed and security in the provision of services, especially revocation and repository services.

In addition, when issuing a certificate of electronic signature it is ensured the subscriber and third parties who trust the certificates:

- That the certificate contains the information that must contain a qualified certificate, in accordance with Article 11 of Law 59/2003 of December 19th.
- Liability of the Notarial Certification Agency, with the legal limits established.

11.6.3. Rejection of other warranties

The Notarial Certification Agency may reject any other warranty not legally enforceable, except as provided in this document.

Specifically, the Notarial Certification Agency neither guarantees the used cryptographic algorithms nor is liable for damage caused by external attacks against these algorithms, provided that due diligence has been applied in the context of current state of the art, and it has acted in accordance with this Declaration of Certification Practices and the Law 59/2003 and its implementing regulations.

11.6.4. Disclaimer

The Notarial Certification Agency will limit its liability to the issuing and managing of certificates and, where appropriate, managing of subscriber's key pairs and cryptographic devices (for signing and signature verification, and encryption or decryption) supplied by the Notarial Certification Agency.

The Notarial Certification Agency limits its liability by including usage limits, and limits of the value of transactions for which the certificate can be used in accordance with the provisions of this document.

All legal liabilities, contractual or extra contractual, direct or indirect damages derived from such uses fall under the responsibility of the subscriber. Under no circumstances may the subscriber, the key holder or injured third parties claim the Notarial Certification Agency or the General Council of Notaries any compensation for damages or liabilities derived from the use of keys or certificates for limited and/or prohibited uses.

11.6.5. Indemnity clauses

11.6.5.1. Indemnity clause for the subscriber

The Notarial Certification Agency includes, in the general conditions of issuance of certificates, a clause by which the third parties who trust the certificates agree to exclude liability of the Notarial Certification Agency for any damage arising from any act or omission resulting in liability, damage or loss, expense of any kind, including judicial and legal representation, for the publication and use of the certificate, in the following cases:

- Falsehood or misrepresentation made by the user of the certificate.
- Mistake made by the user when providing information during the certificate request.
- Negligence in protecting the private key, in the use of a trustworthy system or the maintenance of the necessary precautions to prevent the compromise, loss, disclosure, alteration or unauthorized use of that key.
- Use by the subscriber of a name (including common names, email and domain names), or other information in the certificate, that infringes intellectual property of others.

11.6.5.2. Indemnity clause for third parties who trust the certificates

The Notarial Certification Agency includes, in the general conditions of issuance of certificates, a clause by which the third parties who trust the certificates agree to exclude liability of the Notarial Certification Agency for any damage arising from any act or omission resulting in liability, damage or loss, expense of any kind, including judicial and legal representation, for the publication and use of the certificate, in the following cases:

- Breach of the obligations of third parties who trust certificates.
- Unreasonable confidence in a certificate.
- Negligence in the verification of the status of a certificate, to determine if it is suspended or revoked.

11.6.6. Fortuitous event or force majeure

The Notarial Certification Agency includes provisions in the general conditions of issue and use of certificates, to limit its liability for fortuitous events or force majeure.

11.6.7. Applicable Law

The Notarial Certification Agency specifies, in the conditions of issue and use of certificates, that the law applicable to the provision of services, including policy and certification practices, is the Spanish law.

11.6.8. Severability clause, survival, entire agreement and notification

The Notarial Certification Agency specifies, in the conditions of issue and use of certificates, severability clauses, survival, entire agreement and notification:

- Under the severability clause, the invalidity of a clause does not affect the remainder of the contract.
- Under the survival clause, certain rules, certain rules will survive the termination of the regulatory legal services between the parties. For this purpose, it shall be ensured that, at least the requirements contained in sections: Obligations and responsibility, Audit of compliance and Confidentiality, continue in force after termination of services.
- Under the entire agreement clause, it should be understood that the legal document regulating the service contains the complete will and all agreements between the parties.
- Under the notification clause, it shall be established the procedure by which the parties will notify each other acts.

11.6.9. Jurisdiction clause

The Notarial Certification Agency specifies, in the conditions of issue and use of certificates, a jurisdiction clause stating that international jurisdiction is for the Spanish judges.

The territorial and functional jurisdiction is determined under the rules of international private law rules that may apply.

11.6.10. Conflict Resolution

The Notarial Certification Agency specifies, in the conditions of issue and use of certificates, procedures for mediation and conflict resolution.

The situations of dispute arising from use of the certificates are resolved by applying the same criteria of competence that in case of signed handwritten documents.