General Certification Policy

Notarial Certification Agency

ancert

Agencia Notarial de Certificación

General Information

Document control

Project:	**General certification policy**
Target entity:	**Notarial Certification Agency, S.L.U.**
Reference code:	
Version:	**2.9**
Date of publication:	
File:	**PG_Certificacion_ANCERT_EN.docx**
Format:	**Word 2007**

Versioning

Version	Parties change	Description	Modification Date	Publication Date
2.0	Original	Creation of document	27/03/2010	
2.1	All	Document Review	05/05/2010	
2.2	Logo ANCERT	Change of logo	30/11/2010	
2.3	All	Final legal review	21/12/2010	01/01/2011
2.4	Section 1.1.2	Addition of CGN title certificates and corporate secure server certificates. Error fixing.	01/02/2011	01/03/2011
2.5	Sections 4.9.6, 5.7.4 and 9.2	AICPA/CICA WebTrust Program for CA v 2 compliance.	01/06/2012	01/10/2012
2.6	Sections 6.1 and 6.2	Private key protection controls in accordance with AICPA/CICA WebTrust Program for CA v 2.	29/09/2014	03/11/2014
2.7	All	EU 910/2014 (EIDAS) compliance	04/05/2017	15/05/2017
2.8	Section 9.4	EU 2016/679 compliance		25/05/2018
2.9	Sections 3.3, 4.6 and 6.2 Section 1.1.4 Section 5.3.2 and 9.4	Certificate renewal is optional as specified in the CPS. Electronic seals. LOPDP 3/2019	01/04/2019	03/05/2019

Index

1. Introduction

This document contains the general certification policy of the Notarial Certification Agency.

1.1. Presentation

1.1.1. Certification model

1. This section describes the certification services model of the Notarial Certification Agency.

The model is constructed from abstract types of certificates, from whom specific certificates profiles are defined.

The certificates are defined by the following criteria:

- Status of the recipient of the certificate.
    - Infrastructure.
    - End entities.
- Service target community
    - Own.
    - The general public.
- Registration and delivery procedures.
    - College.
    - Notary.
    - Corporate.
- Use of the end entity certificates.
    - Electronic signature.
    - Authentication.
    - Encryption.
    - Systems.
- Legal level of end entities electronic signature
    - Advanced electronic signature.
    - Qualified electronic signature.
- Person identified as the signer.
    - Natural person.
    - Legal person.
    - Entity without legal personality.

- Person identified as the subscriber.
  - Individual.
  - Community.
- Legal action range of the natural person
  - Acting on his own behalf.
  - Representation.

1.1.1.1. Infrastructure and end-entity certificates

Regarding the condition of the recipient of the certificate, there are two types of certificates:

1) Certificates of infrastructure owned by the Notarial Certification Agency which are used to produce certification authority certificates, time stamping and other infrastructure services of the certification services provider.
2) End entity certificates, owned by the corresponding subscribers, which are used for end uses other than infrastructure management.

1.1.1.2. Private and public certificates

As for the community addressing the service, there are two types of certificates:

1) Own certificates, issued to the close community of users consisting of Colleges of Notaries, Notaries and employees of Notaries, and not issued to the public.
2) Certificates for the general public, issued in the free market, to end entities interested in them.

1.1.1.3. College, notarial and corporate certificates

In terms of the procedure for registration and delivery, there are three types of certificates:

1) College certificates: issued to notaries and college employees by Notarial Colleges., and to employees of notaries by notaries themselves.
2) Notarial certificates: issued by notaries to natural persons, legal persons or entities without legal personality.
3) Corporate Certificates[1]: issued by private corporations to end entities.

1.1.1.4. Signature certificates and system certificates.

As for the use of the end-entity certificates, there are two types of certificates:

[1] Also called “private networks certificates"

1) Electronic signature, authentication and encryption certificates: used primarily by individuals to produce signatures, to authenticate electronically on computer systems and to encrypt documents and messages.

2) System certificates: used primarily by computer systems for purposes other than the production of qualified signatures.

1.1.1.5. Certificates for advanced and qualified electronic signature

As for the legal type of electronic signature produced by end entities, there are two types of certificates:

1) Advanced electronic signature certificates: qualified certificates working on applications and programs for the generation of electronic signatures.

2) Qualified electronic signature certificates: qualified certificates operating in conjunction with a secure signature creation device.

Additionally, both types of certificates can be used to sign authentication messages (confirmation of identity), and other types of messages, offering as well encryption features which can be used to produce or receive encrypted documents and messages, but without the possibility of recovering the private key.

1.1.1.6. Certificates for natural persons, legal persons and entities without legal personality

As for the person identified as the signer in the certificate, there are three types of certificates:

1) Certificates for a natural person acting as the signer, in its own name or on behalf of another person.

2) Certificates for a legal person responsible, as a signer, of the signed documents in the cases expressly provided by law and without the need to take into account any power of attorney or acting capabilities of the person who keeps the electronic signature certificate.

3) Certificates for entities without legal personality responsible, as a signer, of the signed documents in the cases expressly provided by law and without the need to take into account any power of attorney or acting capabilities of the person who keeps the electronic signature certificate.

1.1.1.7. Certificates for individuals and communities

As for the person identified as the subscriber in the certificate, there are two types of certificates:

1) Individual certificates, where the subscriber is the natural person.

2) Certificates for communities, where the subscriber is a legal person or an entity without legal personality identified in the certificate, while the natural person simply acts as the key holder or authorized signer[2].

1.1.1.8. Certificates for acting on one's own behalf or in representation

As for the acting legal range, there are two types of natural person certificates:

1) Certificates for acting on one's own behalf, according to the general rules of legal capacity.
2) Certificates of representation, for which it must be taken into account powers of attorney and the acting legal range of the person, indicated or not in the certificate, before trusting the signature.

1.1.2. An array of classes and definitions of certificates

The above criteria serve also for the grouping of certificates in classes or groups of common definitions of certificates.

The classes of certificates used by the Notarial Certification Agency include:

- **Infrastructure class,** which includes all self-issued certificates that serve to give support to the certification operations. These certificates are not issued to the general public in any case.
- **Council of Notaries class,** which includes all certificates for professional use by Notaries and their employees, including Colleges, offices of the notarial organization and Notaries. These certificates are not issued to the general public in any case.
- **Public Law Corporations class,** which includes all certificates issued to the general public, for professional use in the context of public law corporations (other than the Notarial corporation).
- **Notarial Class,** which includes all certificates issued to the general public with notarial intervention, providing the highest level of legal guarantee**.**
- **Corporate class,** which includes all certificates issued to the general public where companies act as registration entities instead of Notaries.

The Notarial Certification Agency shall issue, at least, the following type of certificates:

- Infrastructure clas.
  - Certification Authority.
  - Time Stamping Authority.

[2] For example, a certificate for an employee of a company: while the company is the subscriber of the certificate, the employee is the key holder authorized to sign.

- Council of Notaries class.
    - Notary (FEREN certificate).
    - Title certificates.
    - Employees.
- Public Law Corporations class.
    - Natural person belonging to a Public Law Corporation.
    - Secure application.
- Notarial class.
    - Natural person.
        - In representation of a natural person .
    - Corporate.
        - In representation of a Corporation.
        - Electronic invoicing.
    - Systems.
        - Secure server.
        - Time Stamping.
        - OCSP responder.
        - Code signing.
        - Secure application.
- Corporate Class.
    - Personal.
    - Secure application.
    - Secure server.

1.1.3. Definition of new certificates

The definition of new certificates and their incorporation into the array above should be done following the next procedure:

- The certificate should be described as a particular combination of features and conditions set out in Section 1.1.1 of this policy.
- When the resulting description differs from the previously existing certificate definitions, it should be named and incorporated into the array.
- When a certificate has already been defined with a definition equivalent to the description of the new certificate, the definition of the existing certificate will be

expanded instead of incorporating the new certificate to the array. When a certificate has already been defined with a definition similar to the description of the new certificate, the new certificate will be treated as a subtype of the previously existing certificate.

1.1.4. Information and Validation services

The Notarial Certification Agency shall provide information and validation services for the certificates, both issued in accordance with this policy or by other providers of certification services.

1.2. Document name and identification

This document is the "Certification General Policy" of the Notarial Certification Agency.

The Notarial Certification Agency must assign to each type of certificate an object identifier (OID) for its identification by the applications, which must be also described in the corresponding Declaration of Certification Practices.

Additionally, the Notarial Certification Agency will publish a document describing the OIDs for the current certificate policies.

1.3. Participants in the certification services

This certification policy regulates the provision of certification services to closed communities of users and to the general public. Certificates issued to closed communities are not issued to the public.

Closed communities of users may be:

- The community of Spanish notaries, to whom certificates are issued for various uses and for their use by professional applications related to its member entities.
- Public Law Corporations, to whom certificates are issued for their own uses.

Secondly, this policy governs the provision of certification services by the Notarial Certification Agency to the public, mainly with the collaboration of notaries, as well as other private entities.

The participants in the certification are described below.

1.3.1. Certification Services Provider

The Notarial Certification Agency will act as the sole provider of certification services, commissioned by the General Council of Notaries of Spain.

The Notarial Certification Agency may have one or more Certification Authorities for the provision of services, according to the following criteria:

- Different Root Certification Authorities can be created, grouping the certificate policies in classes. In any case, there should be at least one root entity for each certificate class, with the exception of infrastructure class.
- Depending on the above entities, various Subordinate Certification Authorities can be created, and there must be only one Certification Authority for each certification policy and its subtypes.

1.3.2. 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.

1.3.3. 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) Represented persons or organizations.
5) Third parties who trust the certificates.

1.3.3.1. Certificate requestors

A certificate must be requested by a person in his own name (natural person) or on behalf of an organization (legal person or entity without legal personality).

A requestor can be:

1) The person who will be the subscriber (natural person certificates), and therefore, the key holder.
2) The person who, without being the subscriber of for the requested certificate, will be the key holder (mandatory in the case of certificates of legal person or entity without legal personality, and optional in the case of certificates for communities).

3) A person who, without being the subscriber or key holder of the certificate, will request the certificate for another natural person by delegation.

1.3.3.2. Certificate subscribers

Subscribers are individuals and organizations holders of the certificate.

In the case of certificates for individuals, the subscriber matches the key holder while for certificates for communities, the subscriber is an entity and the key holder, a person authorized or empowered to receive and use the certificate.

The key holder's legal capacity to act on behalf of the subscriber of the certificate shall be established in the certificate itself, in accordance with the requirements of this policy.

1.3.3.3. 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.

The key holder's legal capacity to act on behalf of the subscriber of the certificate for shall be established in the certificate itself, in accordance with the requirements of this policy.

1.3.3.4. Represented persons or organizations

Represented persons or organizations shall be considered as the natural or legal persons on whose behalf the requestors request certificates of representation, without prejudice to their status as a subscriber, in the case of certificates for communities.

1.3.3.5. 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.

1.4. Use of certificates

This section lists the applications for which you can use each type of certificate, according to the classification described in section 1.1.1, sets limits on certain uses and prohibits certain uses of certificates.

The Declaration of Certification Services shall determine the specific uses for each certificate, in accordance with those established in this section.

1.4.1. Permitted uses for certificates

1.4.1.1. Infrastructure and end-entity certificates

Infrastructure certificates are used exclusively by the Notarial Certification Agency for the provision of certification services and related services.

End entity certificates are used according to what is described in each Declaration of Certification Practices, excluding the possibility of using them as infrastructure certificates.

1.4.1.2. Electronic signature certificates and system certificates

Electronic signature certificates are used for authentication, signature and, where appropriate, cryptographic protection of electronic documents.

System certificate, in turn, are used for purposes other than personal signature, as the protection of electronic communications networks and their corresponding servers and agents, or for the protection of the code transmitted through them.

1.4.1.3. Advanced and qualified electronic signature certificates

Electronic signature certificates - and other uses - are qualified certificates, in accordance with Law 59/2003 of December 19th, (Article 11), and issued in accordance with Articles 12, 13 and 17 to 21 of the same law, in accordance also with technical specification TS 101 456 v1.4.1 of the European Telecommunications Standards Institute.

Qualified electronic signature certificates work in conjunction with secure signature creation device that meets the requirements of Article 24.3 of Law 59/2003 and this policy, while the advanced electronic signature certificates do not offer this guarantee.

Qualified electronic signature certificates can be used to perform any legal act electronically documented, especially when the same document in paper form requires a handwritten signature, and assuming that the certificate does not incorporate any limit preventing it.

Meanwhile, advanced electronic signature certificates can be used under the conditions agreed by the parties to interact with each other, or when applicable administrative regulations expressly permit it.

Certificates may also be used for additional functions, such as authentication, or encryption and decryption of messages and documents by the subscriber or the key holder.

1.4.1.4. Certificates for natural persons, legal persons and entities without legal personality

Natural person certificates must be used for acts performed by their individual subscribers, on its own behalf or on behalf of a third party, subject to the requirements of their acting legal range and guaranteeing the authenticity of the sender, non-repudiation of origin and content integrity.

The certificates of legal person must be employed in accordance with the provisions of Article 7 of Law 59/2003 of December 19th, of electronic signature, in the context of public administration and procurement of goods or services concerning his own or ordinary business, meaning activities necessary for the development of his core bussiness, such as the hiring of supplies or services guaranteeing the authenticity of the sender, the non-repudiation of origin and content integrity.

Certificates for entities without legal personality must be used exclusively in the area of taxation, according to the provisions of the law.

1.4.1.5. Certificates for individual and communities

Certificates for communities must always be used according to the policies of the subscriber community.

1.4.1.6. Certificates for acting on your own behalf and certificates for representation.

Certificates for acting on your own behalf must be used exclusively for the performance of personal acts, subject to the requirements of the corresponding acting legal range.

Certificates for representation must be employed only according to the corresponding power of attorney.

1.4.2. Limits and prohibitions on use of certificates

1.4.2.1. Limits of Use

Certificates should be used for their proper function and purpose, and may not be used in other functions and for other purposes.

Certificates can incorporate limits on the amount or general subject, which should be coded in an extension of the certificate registered by the Notarial Certification Agency.

In the case of certificates for representation, such limits should be consistent, where appropriate, with the public, administrative or judicial document in which the representation is based.

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

Although the end-entity certificates may be used, with some exceptions, for encryption or decryption of electronic documents, such uses fall under the responsibility of the subscriber or the key holder, as appropriate.

1.4.2.2. Prohibited uses

End-entity certificates must not be used to sign public key certificates of any kind, or sign certificate 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.

1.5. Policy management

1.5.1. Organization that manages the document

Notarial Certification Agency S.L.U.

1.5.2. Contact

Notarial Certification Agency S.L.U.
Paseo del General Martinez Campos 46, 6th floor
28010 Madrid

Phone: 902 104 045
ancert@ancert.com

1.5.3. Document management procedures

There should be procedures for the creation, review and formal approval of this document andother documents of the service.

2. Publication of the information and certificate repository.

2.1. Certificate repository

The Notarial Certification Agency must have a repository of certificates. 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 the section 6.7.4 and the Declaration of Certification Practices.

2.2. Publication of the information of the certification service provider

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

- Issued certificates, including Certification 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.

The repository should contain current versions and the historical legacy.

2.3. 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 section 1.5 .

The revocation status information will be published in accordance with the provisions of sections 4.9.6 and 4.9.7 of this policy.

2.4. Access Control

The Notarial Certification Agency does not limit read access to the information set out in Section 2.2 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 certification service provider 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.

3. Identification and authentication

3.1. Name management

3.1.1. 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.

When some personal circumstances are not easily represented following the technical standards and specifications outlined above, the Notarial Certification Agency shall establish certificate private extensions and private attributes to include this information in the certificates.

3.1.2. 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.

3.1.3. Use of anonymous and pseudonymous

Anonymous certificates must not be issued in any case.

When the electronic relationship with public administrations is not one of the potential uses , there may be a special policy supporting the use of pseudonyms.

It must not be issued, under the same policy, certificates with pseudonyms and certificates indicating the real identity. This should be done using different policies or a specific policy under another existing policy.

3.1.4. Interpreting format names

The Notarial Certification Agency may use the naming scheme it considers most appropriate, according to the following standards:

- When any of the potential uses, among the ones permitted by the certificate, is to establish electronic relationships with public administrations, should be a name format acceptable by public administrations and in particular, compatible with the constraints set by the AEAT.
- All certificates for electronic signature shall include the following information:
    - Country, contained in the Country component, which is used to identify the nationality of the subscriber or the key holder, as appropriate.
    - Name and last name of the natural person identified in the certificate, and the number of identity card or equivalent, as a combination of the following components: Common Name, Given Name, Last Name, Serial Number, and when the certificate has to be admitted by the AEAT, the specific component defined by the AEAT for the number of identity card or equivalent of the custodian of the certificates of legal person and entities without legal personality.
- The certificates of class General Council of Notaries should include the following additional information:
    - Locality corresponding to the notary or the Notarial College, contained in the component Locality Name.
    - Province corresponding to the notary or Notarial College contained in the component State or Province Name.
    - Notarial College, contained in a component Organizational Unit Name.
    - Notary or title code, if any, contained in a component Organizational Unit Name.
- Certificates of class Public Law Corporations should include the following additional information:
    - Corporation, contained in the component Organization
- Certificates of Notarial class should include the following additional information:
    - Type of certificate, contained in the Organizational Unit Name component.
    - The authorizing notary , contained in a component Organizational Unit Name
    - When the representation is included, name, surname and tax identification number of the represented, or the address and tax identification number of the represented, as appropriate.
    - System certificates will have their own rules, adapted to the specific needs of each type of certificate, indicating in any case the person or entity holder of the certificate and the appropriate technical information such as the domain or application.

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.

3.1.5. 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.

3.1.6. Name conflict resolution

In certificates of General Council of Notaries class and Public Law Corporations class, besides the number of National Identity Card or equivalent, it can also be included the collegiate or administrative staff number, where they exist.

In all other certificates for electronic signature, conflict of names of key holders identified in the certificates with his real name are resolved 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.

3.2. 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.

3.2.1. 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.

3.2.2. Authenticating the identity of an organization

This section contains requirements for verifying the identity of an organization included in the certificate or taking part in digital certification processes.

The Notarial Certification Agency must authenticate, prior to the issuance and delivery of a certificate for a community, the identity of the subscriber and other data, in accordance with the provisions of section 3.1.

The certification service provider may use registration authorities for this task, and may employ the following methods:

1) Obtaining information about the organization from an external provider, at the discretion of the Notarial Certification Agency which must approve the previously mentioned external provider.
2) Checking the documentation provided by the requestor, on the following:
    - Full legal name of the organization.
    - Legal status of the organization.
    - Tax identification number.
    - Registry information.

The Declaration of Certification Practices shall determine, for each case, the methods to be used and the appropriate authentication procedures.

It will not be required to authenticate the identity of professional colleges and other organizations acting as registration entities, because that identity has been duly authenticated previously in establishing the legal relationship with the Notarial Certification Agency.

3.2.3. Authentication of the identity of a natural person

This section contains requirements for the verification of the identity of a natural person included in a certificate.

3.2.3.1. Required identification elements

The Notarial Certification Agency shall establish the number and types of documents that are needed to confirm the identity of the key holder, and may employ the following:

1) National Identity Card.
2) Foreigner Identification Card.
3) Passport.

These documents must contain the following information:

1) Name and surname.
2) Date of birth.
3) Identity number legally recognized.
4) Other attributes required in accordance with the applicable policy.

3.2.3.2. Validation of the identification elements

The identification information of subscribers of individual certificates, as well as key holders for certificates for communities is done by matching the information of the request with the documentation provided, electronically or on physical media, by the corresponding registry entity.

3.2.3.3. Need for personal presence

In general, direct physical presence is required for certificate requesters and, where appropriate, the natural person identified in the certificate in order to obtain the certificate.

In the case of certificates of Corporate and Public Law Corporations classes, it may be used methods based on indirect physical presence when the validation of identity has been previously performed personally, and corporate records are kept constantly updated.

It shall, in any case, be guaranteed the delivery and acceptance of the certificate by the subscriber or the key holder, as appropriate.

3.2.3.4. Relationship of an individual with an organization

In certificates for communities or for representation it must be identified and authenticated the connection of the individual to the organization, by procedures appropriate to each certification policy.

3.2.4. Unchecked subscriber information

Subscriber unverified information must not be included in the certificate.

3.3. Identification and authentication of renewal requests

3.3.1. Validation for the regular renewal of certificates

Certificates may be renewed during its 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 section 3.2.

3.3.2. Validation for certificate renewal after revocation

Revoked certificates cannot be renewed. In this case, it would be necessary a new request and validation of identity, in accordance with the provisions of section 3.2.

3.4. Identification and authentication for a revocation 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.

Such petitions and reports will be verified according to the procedures established in the corresponding Declaration of Certification Practices, and may consist of authentication mechanisms based on knowledge of information previously provided or agreed with the Notarial Certification Agency during the process of issuing certificates.

4. Operational requirements for the life cycle of certificates

4.1. Certificate request

4.1.1. Legitimation of issuance requests

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

Requests can be addressed to three types of registration authorities:

1) Requests for college certificates, corresponding to "General Council of Notaries" and "Corporations of Public Law" classes, can only be made to registration authorities belonging to the corporations concerned.

2) Requests for certificates of class "Notarials" can only be made in the presence of a Spanish Notary.

3) Requests for certificates of class "Corporate" can only be addressed to private organizations that have signed a contract, as a registration authority, with the Notarial Certification Agency.

Should applicant and subscriber be different entities, such as certificates for communities, the requester must have a legal authorization from the subscriber in order to make the request.

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 section 3.2.1 of this certificate policy) or generating new keys.

Certificate requests must be documented, either in paper or electronic format, including the requestor´s acceptance to the general conditions of the issuance.

4.1.2. Registration procedure: responsibilities

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 subscriber or the key holder, as appropriate, 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 sections 3.2.2 and 3.2.3 of this policy.

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.

4.2. Processing the information request

4.2.1. Identification and authentication

Upon receipt of a certificate request, the certification service provider must verify the information provided, according to section 3.2 of this policy and complying with the specific requirements established for each certificate in the corresponding specific policy.

4.2.2. 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 Notarial Certification Agency must approve the certificate request.

The Notarial Certification Agency shall notify the approval or denial of the request to the requestor.

4.2.3. Resolution term

There is no maximum term to resolve a certification request.

4.3. Issuance of the certificate

4.3.1. Actions during the process of issuing

Following the approval of the certification request shall be the issuance of the certificate, storing on the secure device, and its delivery to the requestor, in accordance with the provisions of section 4.3.2.

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 sections 3.1 and 8.1 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 requestor, subscriber or key holder, as appropriate.
- 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.

4.3.2. 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.

For system certificates or certificates generated on secure devices with keys that were previously generated and held by the applicant, it shall be notified that the certificate is available and how to get it.

4.4. Delivery and acceptance of the certificate

4.4.1. Responsibilities of the Notarial Certification Agency

- Give access to the subscriber or the key holder to the certificate, delivering also, where appropriate, the secure device.
- Deliver 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 sections 7.2 and 7.4 of this policy.

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

4.4.2. Conduct constitutive of the acceptance of the certificate

The Notarial Certification Agency shall document in its Declaration of Certification Practices and its legal documentation, the conduct constitutive of the acceptance of the certificate.

4.4.3. Publication of the certificate

The Notarial Certification Agency shall publish the certificate in the repository referred to in this policy, with appropriate access controls.

4.4.4. Notification to third parties

The Notarial Certification Agency may establish cases and methods for the notification of the issuance to third parties.

4.5. Key pair and certificate usage

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

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

The Notarial Certification Agency shall oblige the subscriber by the general conditions of issue to:

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

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

b) Create the keys within the secure signature creation device.

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

- Provide the Notarial Certification Agency and their registration entitites 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 the present certification policy and specific policies.
- Use the certificate in accordance with the provisions of section 1.4 of this policy and specific policies.
- Be diligent in keeping the private key to prevent unauthorized use, in accordance with the provisions of sections 7.1,7.2 and 7.4 of this certification policy and specific policies, 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:

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

  b) 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.

  c) 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 section 7.3.2 of this policy and specific policies.
- 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.

4.5.1.2. Civil liability of the subscriber

4.5.1.2.1. Guarantees given by the subscriber

The Notarial Certification Agency shall require , by the general conditions of issue, the subscriber and (if applicable) the key holder, to ensure:

- 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.
- That digital signatures will only be generated while having the certainty that no unauthorized person has ever had access to the private key.

4.5.1.2.2. Protection of the private key

The Notarial Certification Agency shall require the subscriber, by the general conditions of issue, to ensure that the subscriber is solely responsible for damage caused by its breach of duty to protect the private key.

4.5.2. Use by third parties who trust the certificates

4.5.2.1. Obligations of third parties who trust the certificates

4.5.2.1.1. General context

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 this 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.
- Not intentionally compromise the security of certification services of the Notarial Certification Agency or the General Council of Notaries, without prior written permission.

4.5.2.1.2. Electronic signature certificate

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.

4.5.2.2. 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.

4.6. 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 made with or without renewal of the keys, according to the provisions of section 4.7 of this policy.

Certificates may be renewed during the period of validity or within three months after its expiration.

4.7. Renewing keys and certificates

4.7.1. Causes of key and certificate renewal

The certificates must be renewed in conjunction with the keys when the end of their lifetime or the lifetime of the secure device in which they are contained has been reached

4.7.2. Legitimation of renewal requests

Prior to the issuance and delivery of a renewed certificate, it must exists a renewal request, which must occur at the request of the subscriber or the key holder, as appropriate.

4.7.3. Processing the renewal request

The renewal request shall be made and sent by the subscriber or the key holder, with its current certificate as proof of possession of the private key.

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

The Notarial Certification Agency must conduct a further confirmation of the identity of the key holder, according to the procedures for initial validation of identity.

In case of renewal of certificates that have been expired or revoked, there shall be no automatic renewal, and it must be followed the procedure as for the case of a new issuance.

4.7.4. Notification of new certificate issuance

The Notarial Certification Agency shall notify the certificate issuance to the subscriber and the key holder, as appropriate.

4.7.5. Acceptance of the certificate

Acceptance of the certificate will occur as set out in Section 4.4.2 of this policy.

4.7.6. Publication of the certificate

The Notarial Certification Agency shall publish (with the appropriate security controls) the renewed certificate in the repository according to this policy.

4.7.7. Notification of the issuance to a third party

The Notarial Certification Agency may establish cases and methods for the notification of the issuance to third parties.

4.8. 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.

4.9. Revocation and suspension of certificates

The Notarial Certification Agency shall detail in the corresponding Declaration of Certification Practices, the following aspects:

- Who can request for a revocation.
- How to send the request.
- The requirements for the confirmation of revocation requests.
- When certificates can be suspended and the causes of suspension.
- The mechanisms used to distribute revocation status information.
- The maximum delay between the receiving of the request and providing the revocation status change to the other parties who trust the certificate, which may not exceed in any case one day.

4.9.1. Causes for the revocation of certificates

A certification services provider may revoke a certificate due, at least, to the following reasons:

1) Circumstances affecting the information contained in the certificate:

a) Modification of any of the information contained in the certificate.

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

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

2) Circumstances affecting the security of the key or certificate:

a) 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.

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

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

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

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

3) Circumstances affecting the security of the cryptographic device:

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

b) Loss or damaging of the cryptographic device.

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

4) Circumstances affecting the subscriber or the key holder:

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

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

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

d) 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.

e) Incapacity or death of the subscriber or the key holder.

f) 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.

g) Revocation request by the subscriber, in accordance with the provisions of section 3.4 of this policy.

5) Other circumstances:

a) The suspension of the digital certificate for a period exceeding that provided in section 4.9.13 of this policy.

b) Termination of the service provided by the Notarial Certification Agency, in accordance with the provisions of section 6.8 of this policy.

The Notarial Certification Agency may establish other causes of revocation in specific policies, provided they are compatible with the legal system and, specifically, with Law 59/2003 of December 19th, of electronic signature.

Also, each Declaration of Certification Practices shall adapt the above causes to each particular case.

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 issue must establish the obligation to request the revocation of the certificate in case of knowledge of any of the circumstances mentioned above.

4.9.2. Legitimation of revocation requests

The revocation of a certificate can be requested by:

- The subscriber on whose behalf the certificate was issued.
- For corporate certificates and certificates for communities, an authorized representative of the subscriber or even the key holder.
- In case of certificates of representation, the represented person.
- The registration entity who requested the issuance of the certificate or any other that receives a revocation request.

4.9.3. Procedures for request the revocation

Any 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 identity.
- Detailed reason for the revocation request.
- Name and title of the person requesting the revocation.
- Contact details of the person requesting the revocation.

Immediate revocation can be requested by sending an email or making a phone call to the Notarial Certification Agency.

The request must be authenticated by the receiver prior to revocation, in accordance with the requirements of section 3.4 of this policy.

If the recipient of the request is a registration entity, once authenticated, revocation can be performed directly, or a request can be send to that effect to the Notarial Certification Agency, depending on the provisions of the specific policy for the certificate.

The revocation request will be processed upon reception.

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

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

4.9.4. Time period of the revocation request

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

4.9.5. 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 shall provide information to third parties who trust certificates on how and where to find the corresponding Certificate Revocation List.

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

The Notarial Certification Agency shall issue a new CRL at least every 24 hours. Additionally, a new CRL must be issued in a reasonable period after the revocation of a certificate.

It must be included in the CRL 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.

4.9.7. 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 must be available 24 hours 7 days a week.

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

The Declaration of Certification Practices should provide information to third parties who trust the certificates about the status information service.

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

4.9.8. Other forms of certificate revocation information

The Notarial Certification Agency may implement other ways of providing status information and should describe them in its Declaration of Certification Practices.

More specifically, it must have a public OCSP service.

4.9.9. Special requirements in 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.

The way this requirement will be fulfilled will be detailed in the Declaration of Certification Practices.

4.9.10. 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.

4.9.11. Legitimation of suspensión 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.

4.9.12. 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, which will record and store the request.

The requestor of the suspension should respond with the password or shared secret specified during the process of the certification request. If the response matches the password the suspension will take place.

The mechanisms and procedures for managing the suspension systems will be identified in the Declaration of Certification Practices.

4.9.13. Maximum period of suspension

The maximum period of suspension shall be sixty (60) calendar days.

4.10. Services for certificate status checking

4.10.1. Operational features of the services

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

4.10.2. Availability of services

The services for certificate status checking will be available 24 hours a day, 7 days a week, year round, except for scheduled downtime.

4.10.3. Optional Features

Not defined.

4.11. 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 policy and the corresponding Declaration of Certification Practices.

4.12. Deposit and key recovery

4.12.1. Deposit and key recovery policy and practices

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

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

Not defined.

5. Operational requirements for the life cycle of certificates of subordinate Certification Entities

5.1. Legitimation of issuance requests

The signing of subordinate certification entities can only be requested by the Notarial Certification Agency or the General Council of Notaries.

The Declaration of Certification Practices of the new entity must be aligned with this General Certification Policy.

5.2. Processing the certification request

Key generation for the subordinate CA, the generation of the certificate request and its processing by a root certification authority must be performed in a Key Generation Ceremony as described in paragraph 7.1.1

Only requests that meet the requirements described in paragraph 5.1 will be accepted.

5.3. Issuance of certificate

The issuance of the certificate will take place in the key generation ceremony, in accordance with paragraph 5.2

Certificates of subordinate entities must be aligned with the provisions in the profiles document. The Notarial Certification Agency will publish the profiles document for subordinate entities in the repository, as described in Section 2.

5.4. Delivery and acceptance of the certificate

5.4.1. Publication of the certificate

The Notarial Certification Agency will publish the certificate in the repository referred to in section 2 of this policy, with the appropriate access controls.

Additionally, the Notarial Certification Agency will also publish the certificate on their website within a reasonable time after issuance.

5.4.2. Notification to third parties

The Notarial Certification Agency may establish cases and methods for the notification of the issuance to third parties.

If necessary, the Notarial Certification Agency shall notify the issuance to the relevant regulator, together with the associated documentation.

5.5. Key pair and certificate usage

The subordinate CA shall use the key only for signing end entity certificates and CRL, in accordance with the supervised practices of certification.

5.6. Renewal of certificates

5.6.1. Causes of key and certificate renewal

Certificates may be renewed when the end of the period of life has been reached, provided the cryptographic security of the key can be guaranteed during the period of validity of the new certificate.

5.6.2. Legitimation of renewal requests

Renewal of the certificate of a subordinate Certification Authority shall only be requested by a person responsible for it.

5.6.3. Processing of the renewal request

It shall only be accepted requests that meet the requirements described in paragraph 5.1.

In order to validate the authenticity of the request for renewal, it shall be required the person responsible for the subordinate CA to be present at the time of processing the request.

5.6.4. Publication of the certificate

The Notarial Certification Agency will publish the certificate in the repository referred to in section of this policy, with the appropriate access controls.

Additionally, the Notarial Certification Agency will publish the certificate on their website within a reasonable time after its renovation.

5.7. Renewing keys and certificates

Not applicable.

5.8. Modification of certificates

Not applicable.

5.9. Revocation and suspension of certificates

The suspension of a certificate of a subordinate Certification Authority is not permitted.

5.9.1. Causes for the revocation of certificates

The Notarial Certification Agency shall revoke a certificate of a subordinate Certification Authority due, at least, to the following reasons:

1) The ending of service by the Notarial Certification Agency in accordance with the provisions of section 6.8 of this policy.

2) Circumstances affecting the security of the key or certificate:

> a) Compromise of the private key or the infrastructure or systems of the Certification Entity that issued the certificate, provided that affects the reliability of certificates issued from that incident.
>
> b) Compromise of the private key or the infrastructure or systems of the subordinate Certification Authority.

5.9.2. Legitimation of revocation requests

Revocation of the certificate of a subordinate Certification Authority shall only be requested by a person responsible for it.

5.9.3. Obligation to obtain the certificate revocation information

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

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

The Notarial Certification Agency shall provide information to third parties who trust certificates on how and where to find the corresponding Certificate Revocation List.

5.9.4. Frequency of issue for certificate revocation lists (ARLs)

The Notarial Certification Agency shall issue a new ARL at least every 365 days. Additionally, a new ARL must be issued at a time not exceeding 24 hours after the revocation of a certificate.

It must be included in the ARL the scheduled time of issuing a new ARL, although it may be issued an ARL before the deadline stated in the previous ARL.

5.9.5. Availability of certificate status information services

Alternatively, third parties who trust the certificates may check their status in the repository of the Notarial Certification Agency, which must be available 24 hours 7 days a week.

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

5.9.6. Special requirements in case of compromise of private key

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.

The way this requirement will be fulfilled will be detailed in the Declaration of Certification Practices.

5.10. Services for certificate status checking

5.10.1. Operational characteristics of the services

The services for certificate status checking will be provided through a web query interface and the repository.

5.10.2. Availability of services

The services for certificate status checking will be available 24 hours a day, 7 days a week, year round, except for scheduled downtime.

5.10.3. Optional Features

Not defined.

6. Management, operations and physical security controls

6.1. Physical security controls

The Notarial Certification Agency must have 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 shall establish 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 will establish requirements for the following contingencies, which shall be briefly documented in the Declaration of Certification Practices:

- 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.

6.1.1. Location and construction of facilities

The location of the facilities should allow 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 quality and strength of materials of construction of the facility shall ensure adequate levels of protection against intrusion by brute force.

6.1.2. Physical Access

The Notarial Certification Agency shall establish 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 shall be required the prior identification, including closed-circuit TV filming and archiving.

This identification shall be performed by recognition of a biometric parameter of the individual, except for escorted visits.

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

6.1.3. Power and air conditioning

The computer equipment of the certification services provider shall be adequately protected against fluctuations or power outages that could damage or disrupt the service.

Facilities will 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 must be located in an environment that ensures a climate (temperature and humidity) appropriate to their optimum working conditions.

6.1.4. Exposure to water

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

6.1.5. Fire prevention and protection

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

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

6.1.6. Media storage

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

Fireproof locations or cabinets shall be used for this purpose.

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

6.1.7. Waste treatment

The removal of media, both in paper and magnetic, should be 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 shall be performed.

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

6.1.8. Backup off-site

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

6.2. Management procedures

The Notarial Certification Agency must ensure that its systems are operating safely, for which it must establish and implement procedures for the functions that affect the provision of their services.

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

6.2.1. Reliable functions

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

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

Reliable functions should include:

- Personnel responsible for security.
- System administrators.
- System operators.
- System auditors.

6.2.2. Number of people per task

Reliable functions identified in the previous section and the security policy, and its associated responsibilities, will be documented in job descriptions and described succinctly in the corresponding Declaration of Certification Practices.

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

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

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

6.2.3. Identification and authentication for each function

The Notarial Certification Agency shall identify and authenticate the staff before granting access to the corresponding reliable function.

6.2.4. Roles requiring separation of duties

The following tasks must be performed at least by two people:

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

6.3. Personnel controls

6.3.1. History, qualifications, experience and authorization requirements

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

This requirement shall apply to management staff, especially for persons involved in security procedures.

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

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

It shall not be 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 should be 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.

6.3.2. Procedures for history research

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

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

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

It must be 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 research will be repeated every three years.

6.3.3. Training requirements

The Notarial Certification Agency will train staff in reliable positions and management until they reach the necessary qualifications in accordance with the provisions of section 6.3.1 of this policy.

The training shall include 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.

6.3.4. Requirements and frequency of training update

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

6.3.5. Sequence and frequency of job rotation

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

6.3.6. Sanctions for unauthorized actions

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

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

6.3.7. Requirements for hiring professionals

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.

6.3.8. Providing documentation to staff

The Notarial Certification Agency will provide the documentation strictly required by the staff at any time, in order to be competent enough as set out in section 6.3.1 of this policy.

6.4. Security Audit Procedures

6.4.1. Types of recorded events

The Notarial Certification Agency must keep 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.

6.4.2. Review period for audit logs

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

The processing of audit logs shall consist 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 should also be documented.

6.4.3. Retention period for audit logs

Audit logs must be retained on site for at least two months after processing and, thereafter, shall be archived in accordance with section 6.5.2 of this policy.

6.4.4. Protection of audit logs

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

6.4.5. Backup procedures

It should be generate, at least, incremental backup copies of audit logs daily, and full backups weekly.

6.4.6. Log aggregation systems

The log aggregation system must be, 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.

6.4.7. Notification of audit event

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.

6.4.8. Vulnerability Scan

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

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

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

6.5. Archiving of information

The Notarial Certification Agency must ensure that all information relating to certificates is stored for an appropriate period, as provided in section 6.5.2 of this policy.

6.5.1. Types of recorded events

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

It must be stored a record of the following:

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

6.5.2. Record retention period

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

6.5.3. Archive Protection

The Notarial Certification Agency must:

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

6.5.4. Backup procedures

The Notarial Certification Agency must perform daily incremental backups and weekly full backups of all its electronic documents, according to section 6.5.1 of this policy. It shall also be performed weekly full backups for data recovery cases, in accordance with section 6.7 of this policy.

According to section 6.5.1, it should also be kept paper documents in a location outside the Notarial Certification Agency for cases of data recovery.

6.5.5. Timestamping requirements

The Notarial Certification Agency must issue certificates and CRLs using reliable date and time.

It is not necessary that this information is digitally signed.

6.5.6. Location of the archive

The Notarial Certification Agency must have a management system for the archive located outside its own facilities as specified in section 6.5.4 of this policy.

6.5.7. Procedures for obtaining and verifying archived information

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

6.6. Key Renewal

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

6.7. Key compromise and disaster recovery

6.7.1. Corruption of resources, applications or data

Where there is an event of corruption of resources, applications or data, the Notarial Certification Agency must initiate 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.

6.7.2. Revocation of the public key of the entity

In case that the Notarial Certification Agency must revoke the public key of a Certification Authority belonging to its hierarchy, it shall be 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 section 4.9.6 of this policy.
- 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 section 6.6 of this policy.

6.7.3. Compromise of the private key of the entity

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

In case of compromise, the Notarial Certification Agency must do 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.

6.7.4. Disaster on the facilities

The Notarial Certification Agency shall develop, maintain, test and, if necessary, implement an emergency plan in case a natural or manmade disaster should occur on its facilities. This plan must describe how to restore the information systems services.

The Notarial Certification Agency must restore critical services within 24 hours following a disaster. These services are:

- Revocation of certificates.
- Publication of certificates status information.

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

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

The disaster recovery equipment must implement the physical security measures specified in the security plan, and should be equivalent to those of the main equipment.

6.8. Termination of service

The Notarial Certification Agency must ensure that potential disruptions to subscribers and third parties due to the cessation of services are minimal and, in particular, ensure continued maintenance of records required to provide evidence of certification for civil or criminal investigation.

Before termination of service, the Notarial Certification Agency must execute at least the following procedures:

- Inform all subscribers and third parties who trust the certificates.
- Remove all authorizations for acting on behalf of the Notarial Certification Agency in the process of issuing certificates.
- Execute the tasks necessary to transfer the maintenance obligations of the registration information and event log files for the respective periods indicated to the subscriber and the third parties.
- Destroy the private keys of the Certification Entity or disable their use.

The Notarial Certification Agency must state, in their practices, the procedures for the termination of service. These should include:

- Notification to affected entities.
- Transfer of obligations to others.
- How to treat the revocation status of issued certificates that have not yet expired.

7. Technical security controls

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

7.1. Generation and Installation of the key pair

7.1.1. Generation of the key pair

The Notarial Certification Agency, when acting as root Certification Authority, will generate and sign its own key pair and proceed 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 Certification Entities (root or subordinate) must be generated using cryptographic hardware that meets ISO 15408: EAL 4 (or higher), and in accordance with the provisions of CEN CWA 14167 parts 1 to 4, as appropriate, or FIPS 140-2 Level 3 (or higher) or equivalent security criteria.

The key pairs of subscribers, and operators and administrators of the registration authorities should always be generated using cryptographic devices that meet ISO 15408: EAL 4 (or higher), and in accordance with the provisions of CEN CWA 14167 parts 1 to 4, FIPS 140-2 Level 3 (or higher) or equivalent security criteria, except in the case of advanced electronic signature certificates or system certificates.

Such secure devices may be cryptographic cards, cryptographic USB tokens, or other devices, in particular secure equipment (HSM) which meets the security requirements established by current regulations for secure devices.

7.1.2. Delivery of the private key to the subscriber

The subscriber's (or key holder) private key must be delivered properly protected by a cryptographic device that meets the provisions of ISO 15408: EAL 4 + (or higher), in accordance with the provisions of CEN CWA 14169 or equivalent security criteria except in the case of advanced electronic signature certificates or system certificates.

7.1.3. Delivery of the public key to certificate issuer

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

7.1.4. Distribution of the public key

The keys of the Certification Entities must be 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 shall be 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 should be 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.

7.1.5. 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.

7.1.6. Public key parameters generation

Not defined.

7.1.7. Quality checking for public key parameters

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

7.1.8. Key generation in software or hardware

The keys of the Certification Entities will be generated in cryptographic hardware that meets the ISO 15408: EAL 4 (or higher), in accordance with the provisions of CEN CWA 14167, Part 3, or FIPS 140-2 Level 3 (or higher) or equivalent security criteria.

The keys for qualified electronic signature of end users will be generated in cryptographic devices that meet the ISO 15408: EAL 4 (or higher), in accordance with the provisions of CEN CWA 14169, or equivalent security criteria.

7.1.9. Key Usage

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

7.2. Protection of the private key

7.2.1. Cryptographic Module Standards

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

7.2.2. 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 will be known only by one person responsible for that device. No person will know more than one password.

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

7.2.3. 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.

7.2.4. Backing up the private key

Private keys of the Certification Entities must be 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 must be expressly authorized for such purposes, and should be restricted to the minimum necessary.

The security controls applied to backups of Certification Entities shall be 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 should be provided so that they can never leave the device.

7.2.5. Archive of the private key

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

End user’s private keys for the generation of signature shall not be archived.

7.2.6. 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 shall be encrypted and exported, in order to import them later in the production modules.

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

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

7.2.7. Private key activation method

The private key of each Certification Authority will be activated by running the startup procedure for secure cryptographic modules (by the persons listed in section 7.2.2).

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

7.2.8. 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.

7.2.9. Private key destruction method

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

7.3. Other aspects of key pair management

7.3.1. Public key archive

Certification Entities shall archive their public keys in a permanent way, in accordance with the provisions of section 7.2.5 of this policy.

7.3.2. Periods of use of public and private keys

Periods of use of the keys will be determined by the duration of the certificate. They shall not be used after the expiration of the certificate.

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

7.4. Activation data

7.4.1. 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 must be securely generated by the certification service provider.

7.4.2. Protection of activation data

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

7.4.3. Other aspects of the activation data

Not defined.

7.5. Computer security controls

7.5.1. Specific technical requirements for computer security

It should be ensured that access to the systems is limited to the authorized persons. In particular:

- It should be ensured effective management of the access level of users (operators, administrators and anyone with direct access to the system) to maintain system security, including user account management, auditing and modifications or denial of access privileges.
- It should be ensured that 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 should be identified before using critical applications related to the lifecycle of the certificate.
- The staff should be able to justify their activities, for example by using an event log file.
- It should be 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 should allow 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) must have access control for changes or deletion of data.

7.5.2. Assessing the level of computer security

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

7.6. Lifecycle technical controls

7.6.1. System development controls

It should be 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.

It shall also be defined procedures for updates, change control for new releases and emergency patches of these components.

7.6.2. Security management controls

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

The configuration of the systems shall be regularly audited, in accordance with the provisions of section 9.1.1 of this policy.

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

7.6.3. 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.

7.7. Network Security Controls

It should be ensure that access to different networks of the Notarial Certification Agency is restricted to authorized persons. In particular:

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

7.8. Engineering controls for cryptographic modules

It should be ensured that keys of the Certification Entities are generated in cryptographic equipment, operated by trusted staff and in a secure environment under dual control.

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

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

8. Certificate and certificate revocation list profiles

8.1. Certificate profile

Certificates will 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 shall be 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 shall publish their certificate profiles in the repository, as indicated in section 2.

8.2. Certificate revocation list profile

The Notarial Certification Agency shall publish their certificate revocation list profiles in the repository, as indicated in section 2.

9. Compliance audit

The Notarial Certification Agency should periodically conduct 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.

9.1.1. Frequency of compliance audit

It should be conducted a compliance audit 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.

9.1.2. 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 may be required the services from an independent auditor, which must demonstrate experience in security of information and auditing public key infrastructure services.

9.1.3. Relationship between the auditor and the auditee

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

9.1.4. 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 shall be detailed in the audit plan of the Notarial Certification Agency.

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

Upon the reception of the audit compliance report, the Notarial Certification Agency should discuss with the entity that performed the audit and, where appropriate, with the General Council of Notaries, the deficiencies found and define and implement 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 should be taken one of the following actions:

- Revocation of the key of the Certification Entities as described in section 6.7.2 of this policy.
- Ending the certification services, as described in Section 6.8 of this policy.

9.1.6. Treatment of audit reports

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

10. Business and legal requirements

10.1. Fees

10.1.1. Fee for the issuance or renewal of certificates

The Notarial Certification Agency may establish a fee for the issuance or renewal of certificates, which must be approved by the General Council of Notaries.

10.1.2. Fee for certificate access

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

10.1.3. Certificate status information fee

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

10.1.4. Fees for other services

Not defined.

10.1.5. Refund policy

The Notarial Certification Agency must have a refund policy which shall be documented in its Declaration of Certification Practices.

10.2. Financial Capacity

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

The Notarial Certification Agency does not perform as trustee or representative of users or third parties who trust the certificates.

10.2.1. Insurance Coverage

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

The guaranteed amount shall be 3,000,000 Euros or higher.

10.2.2. Other assets

Not defined.

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

Not defined.

10.3. Confidentiality

10.3.1. Confidential information

The following information, at least, will be 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."

10.3.2. Non-confidential information

The following information will be 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.

10.3.3. Disclosure of suspension and revocation information

See the previous section.

10.3.4. 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 section 10.5of this policy.

10.3.5. Disclosure by request of the holder

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

10.3.6. Other circumstances for information disclosure

Not defined.

10.4. Protection of personal data

In order to provide certification services, the Notarial Certification Agency needs to collect and store certain information, including personal information. Such information will be collected directly from those affected, with their explicit consent or without when permitted by law.

It shall be only collected data necessary for issuing and maintaining the certificate.

The Notarial Certification Agency shall develop a privacy policy in accordance with Organic Law 15/99 of December 13th on the Protection of Personal Data, and describe 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.

The Notarial Certification Agency will not disclose or lease personal information, except as provided in sections 10.3.2 to 10.3.6 of this policy, and Section 6.8 in case of termination of the Certification Entity.

According to the LOPD, confidential information shall be protected from loss, destruction, damage, forgery and unauthorized or unlawful processing.

10.5. Intellectual Property Rights

10.5.1. 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, as defined in section 1.4, and in accordance with the corresponding conditions of use.

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

10.5.2. 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.

10.5.3. 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 section 3.1 of this policy.

10.5.4. 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.

10.6. Obligations and Liability

10.6.1. Model of obligations of the provider certification

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

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

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

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

This requirement may be 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 sections 4.5.1,4.5.2,10.2,10.6.7,10.6.8,10.6.9 and 10.6.10 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 section 1.4.2 of 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.

10.6.2. 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, shall establish and reject warranties and applicable limitations of liability.

The Notarial Certification Agency shall, at least, ensure the subscriber:

- That there is 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 shall guarantee 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 section 4.4 of this certification policy.
- That the approval of the certificate request and the issuance have 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 shall be 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.

10.6.3. Rejection of other warranties

The Notarial Certification Agency may reject any other warranty not legally enforceable, except as provided in section 10.6.2.

10.6.4. Limitation of liability

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 may limit its liability by including usage limits, and limits on the value of transactions for which the certificate can be used.

10.6.5. Indemnity clauses

10.6.5.1. Indemnity clause for the subscriber

The Notarial Certification Agency may include in the general conditions of issuance of certificates, a clause by which the subscriber agrees 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.

10.6.5.2. Indemnity clause for third parties who trust the certificates

The Notarial Certification Agency may include 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 the third parties who trust the certificates.
- Overconfidence on certificates.
- Negligence to determine the status of a certificate (if it has been suspended or revoked).

10.6.6. Fortuitous event or force majeure

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

10.6.7. Applicable Law

The Notarial Certification Agency shall specify, 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.

10.6.8. Severability clause, survival, entire agreement and notification

The Notarial Certification Agency shall specify, 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 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 10.6.1 (Obligations and responsibility), 0 (Audit of compliance) and 10.3 (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.

10.6.9. Jurisdiction clause

The Notarial Certification Agency shall specify, 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.

10.6.10. Conflict Resolution

The Notarial Certification Agency shall specify, 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 shall be resolved by applying the same criteria of competence that in case of signed handwritten documents.