Certification Practice Statement
Certificates of the General Council of Notaries

Version: 3.4

Validity: 08/04/2021

ancert
Agencia Notarial de Certificación

General information

Document control

Project:	**Certification Practice Statement class CGN Certificates**
Destination entity:	**Notarial Certification Agency, SLU**
Reference code:	
Version:	**3.4**
Edition date:	**24/12/2020**
File:	**DPC_CGN_V2_20210408_EN.docx**
Format:	**Microsoft Word**

Versioning

Version	Changes	Description of Change	Date of change	Publication Date
2.1	Creation	Creation of the document	27/03/2010	
2.2		Revision of the document	05/05/2010	
2.3	Section 1.3.1	Incorporation of the fingerprints of CA certificates	06/02/2010	
2.4	Logo ANCERT	New logo Ancert	11/30/2010	
2.5		Review of legal issues and format	12/21/2010	01/01/2011
2.6	Sections 1, 2, 3 and 4 Section 4.9.6	Incorporation of the class title certificates. CRL 60 days of historical information	03/01/2011	03/01/2011
2.7	Sections 4.1, 6.3.1, 6.4.1, 6.5.1, 6.9.1, 6.9.3, 6.9.6, 6.9.9, 7.7.4, 11.2, 11.6	Adequacy of controls AICPA / CICA WebTrust Program for CA v 2	01/06/2012	01/10/2012
2.8	Section 8.2	Adequacy of the protection controls for the private key to the AICPA / CICA WebTrust Program for CA requirements v 2	29 / 09/2014	11/03/2014
2.9	Section 3.1.2	Adequacy to the requirements of the CA / Browser Forum	11/24/2015	11/30/2015
3.0	Document	Adequacy of references to Regulation (EU) 910/2014. New certificates for renewed EC. Revision of section 7.8 "End of service". Definition of the maximum time to attend revocation requests. Description of signature algorithms and parameters.	05/04/2017	05/15/2017
3.1	Document	Adaptation to Regulation (EU) 2016/679 (GDPR). New FEREN certificate for remote signature. Clarification in section 5.1.2 about the identification of test certificates.	05/15/2018	05/25/2018

3.2	Document	Extension of the maximum validity period up to 5 years. Procedure for requesting remote signature certificates using valid qualified certificate of the same class and stored in smart card. FEREN certificate for remote signature with rSCD / rQSCD. Employee Certificate for remote signature with rSCD / rQSCD. Employee certificate without SSCD (software keys) LOPDP 3/2018	04/01/2019	03/05/2019
3.3	Document	Adaptation of the structure to RFC 3647. Addition of the procedure for the electronic renewal of certificates (section 4.6). Review of remote certificates issuance process (section 4.3.13). Definition of the CPSs update period and update of the CPS review procedure. (sections 1.1.5 and 9.12) Certificate status history information is now provided by OCSP (section 4.9.10) instead of CRL (where only 60 days are kept). Status information in case of compromise or end of service (Sections 5.7.3.2 and 5.8.)	02/12/2020	06/04/2020
3.4	Document	Adaptation to Spanish Law 6/2020.	24/12/2020	08/04/2021

Index

1. Introduction

This document contains the Declaration of Certification Practices for certificates of class “General Council of Notaries" issued by the Notarial Certification Agency.

1.1. Overview

1.1.1. Class of certificates of the General Council of Notaries

The “Class of certificates of the General Council of Notaries” (hereinafter “CGN Certificates”) groups the certificates issued by the Notarial Certification Agency to Notaries working in Spanish territory (certificates FEREN), Notaries who hold positions within the organization of the General Council of Notaries (CGN) or Notarial Colleges (title certificates) and employees of Notaries and Notarial Colleges of Spanish territory (certificates of employees).

1.1.2. Certificates that are issued

The following certificates are issued within the class “CGN Certificates":

1.1.2.1. FEREN Certificates

FEREN Certificates are qualified certificates, under the terms of article 28 of Regulation (EU) 910/2014. They are electronic certificates issued by the Notarial Certification Agency fulfilling the requirements regarding the verification of the identity and other circumstances of the applicants, and ensuring the reliability of the certification services they provide.

There are three types of FEREN Certificates:

- FEREN with Secure Signature Creation Device (smart card).
- FEREN Certificates for qualified remote signature.
- FEREN Certificates for advanced remote signature.

FEREN Certificates issued on card allow three functionalities, each one with a different certificate:

- The creation of the qualified electronic signature, which is the advanced electronic signature based on a qualified certificate and generated by a qualified signature creation device. , having respect to the data reported electronically the same value as the handwritten signature in relation to those recorded on paper.
- Personal authentication in electronic information systems, in physical presence or remotely. The authentication certificate can also be used to create advanced electronic signatures of electronic documents in accordance with the conditions agreed by the parties to relate to each other, or when the applicable administrative regulations expressly admit it.
- Encryption and decryption of electronic documents, with key recovery.

Cryptographic card is used as the sole support for the three certificates, with the guarantee of secure signature creation device, according to article 29 of Regulation (EU) 910/2014.

FEREN certificates for advance remote signature allow two functionalities, using a single certificate for both:

- The creation of advanced electronic signature based on a qualified certificate and generated by a centralized key management system that allows the subscriber exclusive control of the use of his keys.
- Certificate-based authentication in electronic information systems, remotely or with physical presence.

The keys for FEREN advanced remote signature certificates are generated in a FIPS 140-2 Level 3 certified cryptographic device controlled by a centralized signing software certified Common Criteria EAL 4+ ALC_FLR.2 + AVA_VAN.5, that together act as a device remote signature creation managed by ANCERT on behalf of the signer.

FEREN Certificates for qualified remote signature allow a single functionality:

- The generation of qualified electronic signature (advanced electronic signature based on a qualified certificate and generated by a qualified signature creation device), which is legally equivalent to the handwritten signature on paper.

The keys for FEREN Qualified Remote Signature Certificates are generated on a qualified remote signature creation device managed by ANCERT on behalf of the signer.

Certificates may contain additional personal information (for example, membership to Notarial Colleges, etc.), provided that this information is not special information with respect to Article 9 of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 relating to the protection of natural persons with regard to the processing of personal data and the free movement of these data which in turn, supersedes Directive 95/46 / EC.

FEREN Certificates comply with the requirements of the CA / Browser Forum established in the document "Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates".

1.1.2.2. Title Certificates

Title Certificates are qualified certificates, under the terms of article 28 of Regulation (EU) 910/2014. They are electronic certificates issued by the Notarial Certification Agency fulfilling the requirements regarding the verification of the identity and other circumstances of the applicants and ensuring the reliability of the certification services they provide.

Title Certificates can be used for three functionalities, each one with a different certificate:

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

A cryptographic card is used as the sole support for the three certificates, with the guarantee of a qualified signature creation device under the terms of article 29 of Regulation (EU) 910/2014.

Certificates may contain additional personal information (for example, the position held within the organizational structure of the General Council of Notaries, etc.), provided that this information is not special information with respect to Article 9 of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 relating to the protection of natural persons with regard to the processing of personal data and the free movement of these data which in turn, supersedes Directive 95/46 / EC.

Title certificates comply with the requirements of the CA / Browser Forum established in the document "Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates".

1.1.2.3. Certificates of Employees

Certificates of Employees are qualified certificates, under the terms of article 28 of Regulation (EU) 910/2014. They are electronic certificates issued by the Notarial Certification Agency fulfilling the requirements regarding the verification of the identity and other circumstances of the requestors and ensuring the reliability of the certification services they provide.

There are four types of Certificates Employees:

- **Certificates of Employees with secure signature** creation device (smart card).
- **Certificates of employees without secure signature** creation device.
- **Certificates of employees for remote qualified signature**.
- **Certificates of employees for remote advanced signature**.

Certificates of Employees issued in smart card can be used for three functionalities, each one with a different certificate:

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

For certificates of Employees issued in smart card, a cryptographic card is used as the sole support for the three certificates, with the guarantee of a qualified signature creation device under the terms of article 29 of Regulation (EU) 910/2014.

Certificates of Employees for advanced remote signature allow two functionalities, using a single certificate for both:

- The creation of advanced electronic signature based on a qualified certificate and generated by a centralized key management system that allows the subscriber exclusive control of the use of his keys.

- Certificate-based authentication in electronic information systems, remotely or with physical presence.

The keys of certificates of Employees for advanced remote signature are generated in a FIPS 140-2 Level 3 certified cryptographic device controlled by a centralized signing software certified Common Criteria EAL 4+ ALC_FLR.2 + AVA_VAN.5, that together act as a device remote signature creation managed by ANCERT on behalf of the signer.

Certificates of Employees for qualified remote signature allow a single functionality:

- The generation of qualified electronic signature (advanced electronic signature based on a qualified certificate and generated by a qualified signature creation device), which is legally equivalent to the handwritten signature on paper.

The keys of certificates of Employees for Qualified Remote Signature Certificates are generated on a qualified remote signature creation device managed by ANCERT on behalf of the signer.

Certificates of Employees without a secure signature creation device allow three functionalities, using a single certificate:

- The creation of advanced electronic signature based on a qualified certificate.
- Personal authentication in electronic information systems, in the physical presence or remotely.
- Encryption and decryption of electronic documents.

Certificates may contain additional personal information (for example, the position held by an employee in a Notary or Notary College, etc…), provided that this information is not special information with respect to Article 9 of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 relating to the protection of natural persons with regard to the processing of personal data and the free movement of these data which in turn, supersedes Directive 95/46 / EC.

Certificates of Employee comply with the requirements of the CA / Browser Forum established in the document "Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates".

1.2. Document name and identification

This document contains ANCERT's Declaration of Certification Practices for the class "CGN", and has been assigned the following OID: ANCERT.0.1.0.5

The OID of ANCERT is 1.3.6.1.4.1.18920.

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

Certificate	Identifier
FEREN Certificates (for signature)	ANCERT 4.1.1.2.1

FEREN Certificates (for authentication)	ANCERT 4.1.1.2 .2
FEREN certificates (for encryption)	ANCERT 4.1.1.2.3
FEREN certificates for qualified remote signature	ANCERT 4.1.1.3.1
FEREN certificates for advanced remote signature	ANCERT 4.1.1.3.2
Title certificates (for signature)	ANCERT 4.1.2.2. 1
Title Certificates (for authentication)	ANCERT 4.1.2.2.2
Title Certificates (for encryption)	ANCERT 4.1.2.2.3
Certificates of Employee (for signature)	ANCERT 4.2.1.2.1
Certificates of Employee (for authentication)	ANCERT 4.2. 1.2.2
Certificates of Employee (for encryption)	ANCERT 4.2.1.2.3
Certificates of Employee without secure signature creation device	ANCERT 4.2.1.2.4
Certificates of Employee for qualified remote signature	ANCERT 4.2.1.3.1
Certificates of Employee for advanced remote signature	ANCERT 4.2.1.3.2

The Notarial Certification Agency publishes on its website a descriptive document with the technical details of all these profiles.

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

1.3. PKI participants

This Declaration of Certification Practices regulates the provision of certification services to natural persons by the Notarial Certification Agency.

The participants in the certification services are:

1.3.1. Certification authorities

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

For this class "CGN Certificates", the Notarial Certification Agency sets the following Certification Entities:

1.3.1.1. ANCERT Certificados CGN V2

ANCERT Certificados CGN V2 is the Root Certification entity, based on a self-signed root certificate whose fingerprint with SHA-256 algorithm is:

```
CN=ANCERT Certificados CGN V2
Validity period: 05/25/2010 to 05/25/2030
Summary: F4336BC2AC75950BECCF1C1F2F9DA6DDDAFD1F41161CA71F59C76889BD474033
```

ANCERT certificados CGN V2 issues certificates for the following subordinate certification authorities:

- ANCERT Certificados FERN V2
- ANCERT Certificados para Empleados V2

1.3.1.2. ANCERT Certificados FERN V2

This subordinate Certification Authority issues electronic certificates called FEREN Certificates.

The fingerprint of this subordinate Certification Authority with SHA-256 algorithm is:

```
CN=ANCERT Certificados FERN V2
Validity period: 27/05/2010 to 27/05/2020
Summary: 55F323C5C821B66C3BC49AE71B1AA021FF9055194FCEAC3049E9B94B7F8576E4

CN=ANCERT Certificados FERN V2
Validity period: 21/06/2016 al 25/10/2030
Summary: A885EC8218B1C96730B0264ECFBBDEE06C97B701FAF80DCCB26920F5E727AD73
```

1.3.1.3. ANCERT Certificados para empleados V2

This subordinate Certification Authority issues electronic certificates called Certificates of Employees.

The fingerprint of this subordinate Certification Authority with SHA-256 algorithm is:

```
CN=ANCERT Certificados para empleados V2
Validity period: 27/05/2010 al 27/05/2020
Summary: 35803438853CADD413FF2692B8D8A3CD5A4F7D264DECAC008A751B616A9ED043
```

```
CN=ANCERT Certificados para empleados V2

Validity period: 21/06/2016 al 25/10/2030

Summary: E718F67C8B1F8E1FC0176A361C98E6299FD3F439CFA46EDDB46A57B4AC08B443
```

1.3.2. Registration Authorities

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.

1.3.2.1. FEREN Certificates

For the class of certificates "ANCERT FEREN ", the Dean and the members of the Notarial College Council act as the Registration Authority for Notaries belonging to the corresponding Notarial College. In turn, the Chairman of the Board of Deans acts as the Registration Authority for all Deans.

1.3.2.2. Title Certificates

For the class Title Certificates, the President of the General Council of Notaries acts as the Registration Authority for members of the Council and Deans. In turn, Deans act as Registration Authorities for members of the boards and positions of Districts of their respective Notarial Colleges.

1.3.2.3. Certificates of Employees

For the class of certificates issued by the subordinate Certification Authority “ANCERT Employee V2 Certificates", the Notary acts as the Registration Authority for employees of his notary. Secretaries of Notarial Colleges act as Registration Authorities for employees of their Colleges.

1.3.3. End Entities

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

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

1.3.3.1. Applicants for certificates

For class CGN Certificates", the applicants are:

- **FEREN Certificates:** a natural person (a Notary) that acts on his own behalf as the holder of a Notarial place in the Spanish territory.
- **Title Certificates:** a natural person (a Notary) who holds a position within the General Council of Notaries or any Notarial College, acting on behalf of such organizations.
- **Certificate of Employee:** a natural person (an employee of a notary or Notarial College) acting on his own behalf.

1.3.3.2. Certificate Subscribers

Subscribers are the individuals and organizations holders of the certificate.

For certificates of class "CGN Certificates", subscribers are:

- FEREN Certificates: the General Council of Notaries, which is the legal person identified in the certificate.
- Title Certificates: the General Council of Notaries or the Notarial College, which is the legal person identified in the certificate.
- Certificates of Employee: The Notary Office or Notarial College (where the employee works), which is the legal person identified in the certificate.

1.3.3.3. Key Holders

Key holders are the natural persons who exclusively own and / or control the cryptographic keys and are not subscribers of the certificate. 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 name and surname.

1.3.3.4. Third Parties who Trust 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 established in this Certification Practice Statement and in the corresponding legal documents.

1.4. Certificate usage

This section lists the applications for which each certificate issued for the “CGN Certificates” class can be used, and sets limitations on certain applications and prohibits certain uses of the certificates.

1.4.1. Permitted uses for certificates

Certificates of class CGN can be used for the uses described in Section 1.1.2 of this Declaration of Certification Practices.

Regarding the use of certificates, the following must be understood:

- **Authenticity of origin**: Ensures that the document or electronic communication comes from the secure signature creation device of the person or entity who claims to be from. This feature is accomplished by using electronic signature. The recipient of a digitally signed message can verify the signature using the certificate.
- **Acceptance of content by the sender**[1]: Prevents the sender of a certain message from denying, if it is convenient for him, the issuance. This is accomplished by using electronic signatures. The recipient of a digitally signed message can verify the signature using the certificate in order to prove the identity of the sender of the message and the acceptance of the content, preventing the sender from rejection.
- **Integrity**: allows the verification that an electronic document for which an electronic signature has been generated has not been modified by any external agent. To ensure integrity, cryptography uses the mathematical capabilities of summary functions (*hash functions*), in combination with electronic signature. The procedure is based on digitally sign a unique summary of the electronic document with the subscriber's private key so that any alteration of the document causes an alteration of its summary.
- **Confidentiality**: ensures that the data transmitted cannot be read by unauthorized third parties since data are encrypted.

1.4.1.1. Limits of use

All certificates must be used for their proper function and purpose as set out in section 1.1.2 of this document, and may not be used in other functions and for other purposes.

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

1.4.1.2. Prohibited uses

Certificates of class CGN are issued exclusively for the provisions of the Notarial Law, so that any non-professional use is thereof prohibited

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

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

[1] Also called "non repudiation".

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 Administration

1.5.1. Organization that manages the document

Agencia Notarial de Certificación, SL Unipersonal

Paseo General Martínez Campos, number 46 - 6º, Edificio Elcano

28010 Madrid (Spain)

NIF nº B-83395988

1.5.2. Contact details of the organization

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

- Via e-mail to the email address ancert@ancert.com .
- By phone at 912187676.
- Directly at the headquarters of the Notarial Certification Agency: Agencia Notarial de Certificación, S.L. Unipersonal Avenida de Martínez Campos, número 46.- 6º, Edificio Elcano 28010 Madrid (Spain).

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

1.5.3. Responsible for the adequacy of the Certification Practice Statement

The responsible of ANCERT's certification service determines the conformity of this Certification Practice Statement.

1.5.4. Approval procedure for the Certification Practice Statement

There is a formal creation, review and approval procedure that guarantees the proper maintenance of this document. The Security Committee of the Notarial Certification Agency is the body responsible for approval.

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

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

1.5.5. Revision frequency

The Certification Practice Statement and related documentation are reviewed and, if applicable, updated, on an annual basis.

1.6. Definitions and acronyms

1.6.1. Definitions

Certification Authority (or Certification Entity): trusted entity, responsible for issuing and revoking certificates.

Registration Authority (or Registration Entity): entity that unequivocally identifies the applicant for a certificate. The Registration Authority provides the Certification Authority with the verified data of the applicant in order to issue the corresponding certificate.

Certificate: electronic document digitally signed by a Trust Service Provider that links some signature verification data to a signer and proves his identity.

Root certificate: certificate whose subscriber is a Certification Authority and contains the Signature Verification Data of this Authority signed with the Signature Creation Data of this Authority as well.

Qualified certificate: certificate for digital signature that has been issued by a qualified trust service provider and that meets the requirements established in Annex I of the eIDAS.

Signature creation data (private key): A private key is a unique and secret number that belongs to a single person so that the person can be identified. This key is asymmetric to the corresponding public key. One key can verify and decrypt what the other has signed or encrypted.

Signature verification data (public key): a public key is a unique number that belongs to a single person but, unlike the private key, can be known by everyone. Through mathematical procedures, it is related to the private key and is used for encryption and verification of digital signatures.

Certification Practice Statement: document created by a Certification Authority that regulates the provision of certification services offered by this Authority, acting as a Trust Service Provider.

Signature creation device: hardware or software that is used to create an electronic signature.

Qualified signature creation signature device: signature creation device that meets the requirements of Annex II of the eIDAS.

Electronic signature: data in electronic format attached to other electronic data that the signer uses to sign.

Advanced signature: electronic signature that meets the requirements of article 26 of eIDAS.

Qualified Signature: An advanced electronic signature that is created using a qualified electronic signature creation device and that is based on a qualified electronic signature certificate.

HSM (Hardware Security Module): security device that generates and protects cryptographic keys.

Certificate Revocation List (CRL): signed list containing the list of revoked certificates of a Certification Authority.

OCSP (Online Certificate Status Protocol): protocol that allows the check of the status of electronic certificates.

OID (Object Identifier): identifier used to name an object. An OID consists of a node in a hierarchically assigned namespace, formally defined using the ASN.1 standard.

Trust Service Provider (TSP): a natural or legal person that provides one or more trust services, either as a qualified provider or as an unqualified provider of trust services.

1.6.2. Acronyms

ARL: Authority Revocation List

CA: Certification Authority

CN: Common Name

CRL: Certificate Revocation List

DN: Distinguished Name

DPC/CPS: Certification Practice Statement

QSCD: Qualified Signature Creation Device

GN: proper name of the certificate holder

HSM: Hardware Security Module

LFE: Law 6/2020, of November 11, regulating certain aspects of electronic trust services.

OCSP: Online Certificate Status Protocol

OID: Object Identifier

PSC: Certification Service Provider

TSP: Trust Service Provider

RA: Registration Authority

eIDAS: Regulation 910/2014 of the European Parliament and of the Council of July 23, 2014 on electronic identification and trust services for electronic transactions in the internal market (superseding Directive 1999/93 / EC)

2. Publication and Repository Responsibilities

2.1. Repository

The Notarial Certification Agency has a repository of certificates. Certificates are stored in the repository at least one year after their expiration.

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 5.7.4 of this Certification Practices Statement.

2.2. Publication of information of the certification service provider

The Notarial Certification Agency publishes the following information in its repository:

- Issued certificates, including their CA 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.
- Revisions of the Certification Practices Statement.
- Disclosure texts (Policy Disclosure Statements - PDS),
- The documents of general conditions for the subscribers and third parties trusting the certificates.

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 of this document.

The revocation status information will be published in accordance with the provisions of sections 4.9.7 and 4.9.9 of this document.

2.4. Access control

The Notarial Certification Agency does not limit reading 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 Notarial Certification Agency will use trustworthy systems for the management of the repository, so that:

- Only authorized persons can make notes and changes.
- The authenticity of the information can be verified.

- The certificates will only be available for consultation if the subscriber has given his consent.
- Any technical change affecting security requirements may be detected.

3. Identification and authentication

3.1. Naming

3.1.1. Types of names

All certificates contain a distinguished name of the person and/or organization identified in the certificate, defined in accordance with the provisions of Recommendation ITU-T X.501 and included in the field *SubjectName*.

Certificates contain alternative names for persons and organizations identified in the certificates, mainly in the field *SubjectAlternativeName*.

Personal circumstances and attributes of individuals and organizations identified in the certificate are included in predefined attributes according to the technical standards and specifications widely used in the sector or sectors where the certificates are used as well as, where appropriate, in specific attributes defined by the Notarial Certification Agency.

3.1.2. Meaning of the names

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

Names included in the certificates are treated in accordance with 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.

If the information included in the name (*CommonName, GeneralName* and/or *Surname*) is fictitious or their invalid nature is expressly indicated (e.g. using literals as "PROOFS" or "FICTICE"), the certificate is considered without legal validity, and will be only valid for technical interoperability tests.

3.1.3. Use of anonymous and pseudonymous

This class of certificates does not issue anonymous certificates or certificates with pseudonymous.

3.1.4. Interpretation of name formats

The Notarial Certification Agency uses the following naming schemes. The name components' maximum length should be the upper bounds defined in the ITU-T X.509 recommendation.

3.1.4.1. FEREN certificate (smart card)

SUBJECTNAME	
FIELD	**CONTENT**

Country (C)	"ES"
State or Province (ST)	Province
Locality (L)	Locality
Organization (O)	"Consejo General del Notariado"
Organizational Unit (OU)	Entity member of the notarial organization.
Organizational Unit (OU)	Notary Code.
Title	"Notario (" + "Firma" o "Autentica" o "Cifrado" + ")"
Surname (SU)	Last name of the Notary.
Given Name (GN)	Name of the Notary.
Serial Number	Key holder's NIF (NIF of the natural person identified, in order to be accepted by Public Administration)
Common Name (CN)	Name and surname of the Notary.
SUBJECT ALTERNATIVE NAME	
rfc822Name	Email.

3.1.4.2. FEREN certificate for advanced remote signature

SUBJECT NAME	
FIELD	**CONTENT**
Country (C)	"ES"
State or Province (ST)	Province
Locality (L)	Locality
Organization (O)	"Consejo General del Notariado"
Organizational Unit (OU)	Entity member of the notarial organization.
Organizational Unit (OU)	Notary Code.
Title	"Notario"
Surname (SU)	Last name of the Notary.
Given Name (GN)	Name of the Notary.
Serial Number	"IDCES-" + NIF of the Notary
Common Name (CN)	Name and surname + "(rSCD)"
SUBJECT ALTERNATIVE NAME	
rfc822Name	Email.

3.1.4.3. FEREN certificate for qualified remote signature

SUBJECT NAME	
FIELD	**CONTENT**
Country (C)	"ES"
State or Province (ST)	Province

Locality (L)	Locality
Organization (O)	"Consejo General del Notariado"
Organizational Unit (OU)	Entity member of the notarial organization.
Organizational Unit (OU)	Notary Code.
Title	"Notario"
Surname (SU)	Last name of the Notary.
Given Name (GN)	Name of the Notary.
Serial Number	"IDCES-" + NIF of the Notary
Common Name (CN)	Name and surname + "(qSCD)"
SUBJECT ALTERNATIVE NAME	
rfc822Name	Email.

3.1.4.4. Title Certificate

SUBJECT NAME	
FIELD	**CONTENT**
Country (C)	"ES"
Organization (O)	"Consejo General del Notariado"
Organizational Unit (OU)	Entity member of the notarial organization.
Organizational Unit (OU)	Entity member of the notarial organization.
Organizational Unit (OU)	IDCN (Title Identifier)
Title	Title + "(" + "firma" o "autentica" o "cifra" + ")"
Surname (SU)	Surname.
Given Name (GN)	Name.
Serial Number	Key holder's NIF (NIF of the natural person identified, in order to be accepted by Public Administration)
Common Name (CN)	Name and surname.
SUBJECT ALTERNATIVE NAME	
rfc822Name	Corporative email address

3.1.4.5. Certificate of Employee (smart card)

SUBJECT NAME	
FIELD	**CONTENT**
Country (C)	"ES"
State or Province (ST)	Province.
Locality (L)	Locality.
Organization (O)	Notary or notarial college.
Organizational Unit (OU)	Notary or notarial college code.

Organizational Unit (OU)	Department, when appropriate.
Title	Role or title of the employee + " (" + "firma" o "autentica" o "cifra" + ")"
Surname (SU)	Surname of the employee.
Given Name (GN)	Name of the employee.
Serial Number	Key holder's NIF (NIF of the natural person identified, in order to be accepted by Public Administration)
Common Name (CN)	Name and surname of the employee.
SUBJECT ALTERNATIVE NAME	
rfc822Name	Email

3.1.4.6. Certificate of Employee without Secure Signature Creation Device

SUBJECT NAME	
FIELD	**CONTENT**
Country (C)	"ES"
State or Province (ST)	Province.
Locality (L)	Locality.
Organization (O)	Notary or notarial college.
Organizational Unit (OU)	Notary or notarial college code.
Organizational Unit (OU)	Department, when appropriate.
Title	Role or function position of the employee
Surname (SU)	Surname of the employee.
Given Name (GN)	Role or title of the employee
Serial Number	"IDCES-" + Employee NIF
Common Name (CN)	First and last name First and last name + "(notary code)"
SUBJECT ALTERNATIVE NAME	
rfc822Name	Email

3.1.4.7. Certificate of Employee for advanced remote signature

SUBJECT NAME	
FIELD	**CONTENT**
Country (C)	"ES"
State or Province (ST)	Province.
Locality (L)	Locality.
Organization (O)	Notary or notary association.
Organizational Unit (OU)	Notary or notarial college code.

Organizational Unit (OU)	Department, when appropriate.
Title	Role or function position of the employee
Surname (SU)	Surname of the employee.
Given Name (GN)	Name of the employee.
Serial Number	"IDCES-" + Employee NIF
Common Name (CN)	First and last name + "(rSCD)" First and last name + "(notary code)" + "(rSCD)"
SUBJECT ALTERNATIVE NAME	
rfc822Name	Email

3.1.4.8. Certificates of Qualified Remote Signature Employee

SUBJECT NAME	
FIELD	**CONTENT**
Country (C)	"ES"
State or Province (ST)	Province.
Locality (L)	Locality.
Organization (O)	Notary or notary association.
Organizational Unit (OU)	Notary or notarial college code.
Organizational Unit (OU)	Department, when appropriate.
Title	Role or function position of the employee
Surname (SU)	Surname of the employee.
Given Name (GN)	Name of the employee.
Serial Number	"IDCES-" + Employee NIF
Common Name (CN)	First and last name + "(rQSCD)" First and last name + "(notary code)" + "(rQSCD)"
SUBJECT ALTERNATIVE NAME	
rfc822Name	Email

3.1.4.9. Extensions and attributes

The Notarial Certification Agency publishes in the Repository the information on the syntax and semantics necessary for the processing of extensions and private attributes by third parties.

3.1.5. Uniqueness of names

The names of the subscribers of certificates are unique for each Certification Entity managed by the Notarial Certification Agency. A person can only have more than one certificate with the same name (at once) during the certificate renewal period, in order to ensure the continuity of their operations.

A name that has already been used for a given subscriber will never be assigned to a different subscriber.

3.1.6. Naming conflict resolution and management of registered trademarks

Name conflicts 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.

Applicants of certificates must not include names in their requests that may constitute infringement, by the future 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.

Likewise, 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 regarding a name conflict, according to the Spanish law, the Notarial Certification Agency may engage in the appropriate legal actions in order to block or withdraw the issued certificate.

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

3.2. Initial identity validation

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 entity, by delegation of the subscriber, during the process of personalization or delivery of the qualified signature creation device 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. Authentication of the identity of the organization

No stipulation for the certificates of the class CGN Certificates.

3.2.3. Authentication of the identity of the natural person

The process of identification and authentication of a natural person is performed exclusively by physical presence in front of:

- the Dean of the Notarial College, which acts as the registration authority, when the natural person is a Spanish Notary, for FEREN Certificates,
- the President of the Board of Deans, who acts as the registration authority when the natural person is a Spanish Dean, for FEREN Certificates,
- the President of the Board of Deans, who acts as the registration authority when the natural person is a Dean or a Spanish Notary who holds a position in the Council, for title certificates
- the Dean of the Notarial College, who acts as the registration authority when the natural person is a Spanish Notary who holds a title within a District or the Board of a Notarial College, for title certificates.
- the notary, who acts as the registration authority when the natural person is an employee of his notary, for certificates of employee.
- the Notarial college who acts as the registration authority when the natural person is an employee of the Notarial College, for certificates of employee.

3.2.3.1. Required identification elements

The types of documents that are needed to confirm the identity of an individual are only the national identity card, residence card, passport or any other legally accepted means, provided that it contains at least the following information:

- Name and surname
- Date of birth
- Legally recognized identity number

3.2.3.2. Validation of the identification elements

Validation of the elements required identification is performed exclusively by:

- **FEREN Certificates**: the Dean of the Notarial College and the notaries members of the Board for notaries belonging to this college, acting as Registration Authorities on behalf of the Notarial Certification Agency.
- **Title certificates**: the President of the Board of Deans for the Deans and other notaries holding a position on the Council, and the Dean for notaries who hold a position of District or in the Board of the Notarial College.
- **Certificates of Employee:** the Notary for his employees and the Notarial College for the employees of the college. In both cases, they act as Registration Entities on behalf of the Notarial Certification Agency.

3.2.3.3. Need for personal presence.

For certificates of class "CGN" is required the presence of the natural person identified in the certificate except when:

- the Registration Entity has previously identified the natural person, and the period of time elapsed since this identification is less than five years.
- When a valid certificate (which had been issued with physical presence, five years before at most) is used for the requesting.

3.2.3.4. Binding the natural person to the subscriber

For certificates of the class "CGN Certificates", the natural person has a link with the subscriber.

For FEREN Certificates, the Registration Entity must ensure that this relationship still exists, making the necessary checks with the help of the Notarial College.

For Title Certificates, the Registration Authority should ensure that this relationship still exists and that the position is still held.

For Certificates of Employees, the Registration Authority should ensure that this relationship still exists, making the necessary checks with the personnel responsible for staff contracts.

3.2.4. Unchecked subscriber information

Unverified subscriber information is not included in the certificate

3.3 Identification and authentication for Re-key Requests

3.2.5. 3.3.1. Validation for the regular renewal of certificates

Certificates of the class "CGN Certificates" can be renewed only during their period of validity.

Before renewing a certificate, the Notarial Certification Agency (through the relevant registration authorities) verifies that the information that was 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.

If any information of the subscriber or the key holder has changed, the new information is properly recorded, in accordance with the provisions of section 3.2.

3.3.2. Validation for certificate renewal after revocation

Not applicable, since the Notarial Certification Agency does not renew in any case certificates that have been revoked.

3.4. Identification and authentication for change of status requests

3.4.1. Identification and authentication for suspension requests

The legitimate applicant must call the number 912187676 of the Customer Service Center of the Notarial Certification Agency.

3.4.2. Identification and authentication for revocation requests

The Notarial Certification Agency checks the revocation requests, verifying that they come from an authorized person.

For the class “CGN Certificates" the revocation could be performed:

- At the request of the Registration Entity.
- At the request of the Notarial Certification Agency which may proceed to revoke the certificate when has had certain knowledge of the occurrence of one of the revocation causes listed in this document.

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

4. Certificate Life-Cycle Operational Requirements

4.1. Certificate Application

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

There are 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 made in person, producing a technical and electronic request (by the Registration Entity) using either a public key provided by the applicant (PKCS#10 or equivalent mechanism, using the user's public key and digital signature in order to prove the possession of the private key in accordance with section 3.2.13.2.1 of this document).
3) Remote request, which in any case produces a technical and electronic request for a certificate by the registration entity, with the generation of keys or using a public key provided by the applicant (PKCS#10 or equivalent mechanism, using the user's public key and digital signature in order to prove the possession of the private key in accordance with section 3.2.1 of this document).

4.1.1. Legitimation of issuance requests

The following individuals are entitled to request the issuance of a certificate:

- The person authorized by the Notarial College, for FEREN Certificates.
- The person authorized by the Notarial College or the General Council of Notaries, for Title Certificates.
- The person authorized by the Notary (in the case of employee of Notary) or by the Notarial College (if the case of employee of College), for Certificates of Employees.

4.1.2. Registration procedure: responsibilities

The registration procedure includes the physical presence before the Registration Entity, for the verification and confirmation of the applicant's personal identity. In the case of remote applications, it includes the use of an electronic instrument with a “Substantial” or “High” level according to Regulation (EU) 910/2014 that guarantees the applicant's personal identity.

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 natural person (which corresponds to 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 3.2.3 and 3.2.4 of this document.

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

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

4.2. Certificate Application Processing

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 by following the procedure below:

- It should be created a new record, in paper or electronic format.
- The key holder should be physically in person in the Registration Entity.
- The key holder should be identified with original documents identification (see section 3.2.3.1).

4.2.2. Approval or rejection of the request

If verification has not been successful or there is a suspicion that it is not correct, the registration entity must reject the request or stop the approval until proper verifications are made.

If data are verified correctly, the registry entity approves the certificate request, and notifies it to the applicant.

Then, the Certification Entity ANCERT FERN Certificates (for FEREN and Title certificates) or ANCERT Certificates for Employees (for certificates for employees of Notaries or Notarial Colleges) are requested to generate the certificate.

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

4.2.3. Resolution term to attend the request

No stipulation.

4.3. Certificate issuance

4.3.1. Actions during the issuance process

In order to issue a new certificate, the operator, acting as the registration entity, must access the certificate issuance application. Access to the application is protected, identifying the operator through its digital certificate. The application checks that the operator, once authenticated, is authorized to issue the certificate. This ensures that communication between the RA and the CA is carried out safely.

After approval of the certification request, the certificate is issued.

In general, the Notarial Certification Agency:

- Uses a procedure to generate certificates that securely bind the certificate with the registration information, including the certified public key.
- Protects the confidentiality and integrity of the registration data, especially if they are exchanged electronically with the applicant, during the pre-application.
- Includes in the certificate the information established in Annex I of Regulation (EU) 910/2014, in accordance with the provisions of sections 3.1 and 7.1 of this Certification Practice Statement.
- Indicates the date and time of issuance.
- The Notarial Certification Agency, when it provides the qualified signature creation device, uses a procedure for managing secure signature creation devices that ensures the secure delivery to the key holder.
- Uses trustworthy systems and products that are protected against any alteration and ensure technical and cryptographic security of the certification processes that they support.
- Ensures that the certificate is issued by systems that use protection against forgery and, when these systems generate private keys, the confidentiality of the keys during the process of generation is guaranteed.

4.3.1.1. Issuance in cryptographic card

The actions to be followed are as follows:

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

2a) Once authenticated, the responsible for the Registration Entity, inserts into the card reader the cryptographic card of the requestor Notary or Dean. Prior to this, ANCERT FEREN Certificates has provided the Registration Entity with blank cards and the corresponding PIN and PUK, in a sealed envelope.

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

2.c) Once authenticated, the responsible for the Registration Entity, inserts into the card reader the cryptographic card of the requestor employee of Notarial College or Notary. Prior to this, ANCERT Certificates for employees has provided the Registration Entity with blank cards and the corresponding PIN and PUK, in a sealed envelope.

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

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

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

4.3.1.2. Issuance of certificates for centralized signature

The keys for centralized signature are generated in a cryptographic module with Common Criteria EAL 4 + AVA_VAN.5 certification. The generation and activation of the keys is managed by the software solution "ANCERT Server Signing Application" that enables the signers to have exclusive control of their keys for electronic signature.

The software “ANCERT Server Signing Application” (hereinafter SSA) has been certified by the National Cryptologic Center according to the standard Common Criteria, with evaluation level EAL 4+ ALC_FLR.2 + AVA_VAN.5.

The actions to follow for the issuance of a certificate are the following:

In a Registration Entity:

1. The person assigned to this task by the Registration Entity introduces his cryptographic card into the card reader and uses his certificate as Registration Entity operator for accessing the registration application.

2. The person assigned to this task by the Registration Entity identifies the subscriber, requests an email account and a mobile phone number, and completes the registration form.

3. The person assigned to this task by the Registration Entity signs the certificate request with his card.

4. The subscriber of the certificate signs the record of the registration process, which is automatically generated by the system.

Through a telematic process, if the subscriber has a valid qualified electronic certificate of the same class on a cryptographic card:

1. The subscriber authenticates with his certificate in the software system for requesting certificates for remote signature. The certificate used for authentication must be of the same class as the certificate that is going to be issued.

2. The subscriber fills the application form with an email account and a mobile phone number.

3. The subscriber signs the certificate request electronically.

4. The Registration Entity application automatically validates the data included in the request, its legitimacy and the electronic signature of the request.

The rest of the procedure is the same regardless of the origin of the request:

5. The subscriber receives an SMS with a single-use and temporary validity code on his mobile phone to complete the issuance of their certificate.

6. The subscriber downloads on his mobile phone the application to control the activation of the keys.

7. The subscriber enters his data in the signature activation application and the code he received in step 5.

8. The signature activation application asks the user for a PIN code to protect the access to his key of signature.

9. The signature activation application generates a pair of signature activation keys linked to the user and the device.

10. The signature activation application sends the public key for signature activation and the user's PIN to the SSA using a secure communication protocol.

11. The SSA system authenticates the request and generates the subscriber's signature key protected by the PIN, a cryptographic module key and the signature activation key.

12. The SSA system generates a PKCS # 10 request for the signature key pair generated in point 11.

13. The Certification Entity generates the certificate for electronic signature corresponding to the request in point 12.

14. The SSA system binds the certificate for electronic signature with its key pair and activates the key pair for the validity period of the certificate.

15. The SSA system generates a certificate for the subscriber's signature activation key.

16. The signature activation application receives the certificate of the signature activation key, completing the initialization process of the key activation device.

4.3.1.3. Issuance of software certificates

The actions to be followed are as follows:

1. The person assigned to this task by the Registration Entity introduces his cryptographic card into the card reader and uses his certificate as Registration Entity operator for accessing the registration application.

2. The person assigned to this task by the Registration Entity identifies the subscriber and validates his data.

3. The person assigned to this task by the Registration Entity signs the certificate request with his card.

4. The person assigned to this task by the Registration Entity signs the record of the issuance process with his card.

5. The subscriber receives a one-time request code to complete the issuance of the electronic certificate.

6. The subscriber runs on his personal computer an application provided by the Registration Entity to complete the issuance of his certificate, hereinafter the application.

7. The subscriber authenticates through the application in the services of the Registration Entity with his credentials and sends the request code.

8. The subscriber receives a one-time authentication code in his email.

9. The subscriber generates the key pair with the application and sends a PKCS # 10 file as proof of possession of the key pair together with the authentication code to the Registration Entity.

10. The Registration Entity requests from the Certification Authority the electronic certificate.

11. The Certification Authority issues the electronic certificate.

12. The Registration Entity returns the electronic certificate to the application, completing the issuance process.

13. The subscriber signs the record of the certificate issuance process.

The subscriber can install the electronic certificate on his personal computer or make a backup copy by means of the application.

4.3.2. Notification of the issuance to the subscriber

The Notarial Certification Agency notifies, in the act of issuance or later, the issuance of the certificate to the subscriber or, where appropriate, to the key holder.

4.4. Certificate Acceptance

The Notarial Certification Agency:

- Provides the subscriber or key holder with access to the certificate, delivering the qualified device.
- Provide the applicant or the key holder with a certificate delivery document with the following minimum contents:

  a) Basic information about the policy and uses of the certificate, especially including information about the Notarial Certification Agency and the applicable Certification Practices Statement, such as its obligations, faculties and responsibilities

  b) Information about the certificate and the signature creation device.

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

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

  e) Responsibility of the subscriber and, where appropriate, the key holder.

  f) Method of exclusive imputation to the subscriber and, where appropriate, to the key holder, of his private key and of his data of activation of the certificate and the qualified device, in accordance with the provisions of sections 6.2 and 6.4 of this document.

  g) The date of delivery and acceptance.

4.4.1. Conduct constitutive of the acceptance of the certificate

Acceptance of the Certificates by the Subscriber should be understood from the time of issuance and delivery by the Notarial Certification Agency, and the signature of the corresponding delivery document.

By accepting the Certificate, the Subscriber also accepts the terms of use and the conditions stated in this Certification Practice Statement.

In any case, by accepting a Certificate issued by the Notarial Certification Agency, the Subscriber declares:

- That all the information delivered during the Certificate application procedure is true.
- That the Certificate will be used exclusively for legal purposes and authorized by the Notarial Certification Agency in accordance with this Certification Practice Statement and always within the scope determined in the Certification Policy.
- That ensures its exclusive control over the Signature creation Data that correspond to the Signature verification Data included in the Certificate issued by the Notarial Certification Agency and linked to his personal identity, which, in any case, will include the actions and measures necessary to prevent its loss, disclosure, modification, or use by someone other than the Subscriber.

The Notarial Certification Agency will consider any Certificate accepted by the Subscriber and published in its corresponding repository to be valid, provided that it has not expired and that no reason for revocation is known.

4.4.2. Publication of the certificate

Once the certificate has been issued, the Notarial Certification Agency automatically publishes a copy in the Repository referred to in section 2.1 of this Certification Practice Statement, with the relevant access controls.

4.4.3. Notification of the issuance to third parties

The Notarial Certification Agency does not notify the issuance of certificates 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, key holder

The Notarial Certification Agency obliges the subscriber to:

- If the subscriber generates his own keys, to:

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

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

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

- Provide the Notarial Certification Agency and its registration entities with complete and proper information, 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 issuance to third parties.
- Comply with the obligations established for the subscriber in this Certification Practice Statement.
- Use the certificate in accordance with the provisions of section 1.4 of this Certification Practice Statement.
- Be diligent in the custody of the private key, in order to avoid unauthorized uses, in accordance with the provisions of sections 6.1, 6.2 and 6.4 of this Certification Practice Statement, not allowing the use of the private key to any other person.
- Notify the Notarial Certification Agency and any other person trusting the certificate, without unjustifiable delays:

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

  b) Loss of control over the private key or the qualified device, due to the compromise of the activation data (for example, the PIN code of the qualified signature creation device, or the activation device) or for any other reason.

  c) The inaccuracies or changes in the content of the certificate that the subscriber or the key holder know or could know.
- Cease in the use of the private key after the period indicated in section 6.3.2 of this Certification Practice Statement.
- Transfer to the key holders their 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.

The subscriber of the certificate for electronic signature that generates digital signatures using the private key corresponding to his public key included in the certificate, acknowledges, in the corresponding legal document, that these electronic signatures are electronic signatures equivalent to handwritten signatures, in accordance with the provisions of the Article 25 of Regulation (EU) 910/2014.

4.5.1.2. Civil liability of the subscriber of the certificate

The Notarial Certification Agency obliges the subscriber and, where appropriate, the key holder, to guarantee:

- In case the subscriber was the certificate applicant, that all the statements made in the request are correct.
- That all the information provided by the subscriber that is included in the certificate is correct.
- That the certificate is used exclusively for legal and authorized uses, in accordance with this Certification Practice Statement.
- That each digital signature created using the public key included in the certificate is the subscriber's digital signature and that the certificate has been accepted and is operational (nor expired neither revoked) at the time of signature creation.
- That the subscriber is an end entity and not a certification service provider, and that he will not use the private key corresponding to the public key included in the certificate to sign any other certificate (or any other certified public key format), or Certificate Revocation List, neither as a certification service provider nor in any other case.
- That he will only create digital signatures while he is sure that no unauthorized person has ever had access to his private key.
- That the subscriber is solely responsible for the damages caused by his breach of the duty to protect the private key.

4.5.2. Use by third parties who trust the certificates

4.5.2.1. Obligations of the third parties who trust the certificates

In accordance with the general conditions of use, the Notarial Certification Agency obliges 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 status 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.
- Be aware of any limitations on the use of the certificate, regardless of whether these limitations are included in the certificate itself or in the contract signed with the third party that trusts the certificate.
- Be aware of any precaution established in a contract or in another instrument, regardless of its legal nature.
- Not to monitor, manipulate or reverse engineer 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 the certification services of the Notarial Certification Agency or the General Council of Notaries, without prior written permission.

- Regarding the certificates for generating electronic signatures, recognize that the electronic signatures correctly verified with the certificates, are electronic signatures equivalent to handwritten signatures, in accordance with article 25 of Regulation (EU) 910/2014.

4.5.2.2. Civil liability of the third parties that trust the certificates

In accordance with the general conditions of use, the Notarial Certification Agency obliges the third party that trusts the certificates to recognize that:

- has enough information to make an informed decision in order to trust the certificate or not.
- is 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 that trusts the certificates.

4.6. Certificate Renewal

The certificates within their period of validity can be renewed by a specific and simplified renewal procedure, in order to maintain the continuity of the certification service.

The renewal of the certificates can be performed with or without the renewal of the keys, in this case in accordance with the provisions of section 4.7 of this document.

The Notarial Certification Agency notifies the subscriber with a minimum of 45 days before the expiration date at the email address included in the certificate. The Notarial Certification Agency may send more notifications by email to the subscriber as a reminder before the expiration date of the certificate.

4.6.1. Circumstances for the renewal of a certificate

A certificate may only be renewed electronically if all the following circumstances exist:

- The certificate has not expired.
- The certificate is nor revoked neither suspended.
- The information contained in the certificate has not changed.
- The subscriber or the holder of the keys has been authorized to renew their certificate by the Registration Entity.
- No more than 5 years have elapsed since the last physical presence of the subscriber or the holder of the key in the Registration Entity.

Additionally, for renewals without changing the keys, their size and algorithm must also comply with the current cryptographic security requirements at the time of the renewal.

In the case of renewals with physical presence, the provisions will be the same as for the issuance of a new certificate.

4.6.2. Legitimization to request the renewal

Before the issuance and delivery of a renewed certificate there must exist a renewal request, which occurs at the instance of the subscriber or the key holder, as appropriate:

- Directly from the subscriber or key holder, in simplified telematic processes.

- Indirectly through the Registration Entity, at the request of the subscriber or key holder in the procedure with physical presence.

Prior to the renewal request, the Notarial Certification Agency will inform the subscriber if some term or condition has changed since the initial issuance of the certificate to be renewed.

4.6.3. Processing of the renewal

Telematic requests for renewal will include the serial number of the original certificate, type of certificate, its period of validity and the full name of the subscriber or key holder. The subscriber or key holder will sign the request with their current signature certificate, which is also included in the request.

The processing of renewal requests includes the following steps:

- Validation of the electronic signature of the request (the signature of the subscriber or the operator of the Registration Entity, as applicable).
- Verification that all the circumstances specified in section 4.6.1 exist.
- Verification that the request does not contain errors.
- Automatic issuance and delivery of the new certificate. The validity period of the new certificate will in accordance with its policy.
- Revocation of the certificate that was renewed.

4.6.4. Notification of the issuance of the renewed certificate

The Notarial Certification Agency notifies the issuance of the renewed certificate to the subscriber or the key holder at the email address included in the certificate.

4.6.5. Conduct that constitutes acceptance of the certificate

Acceptance of the Certificate by the Subscriber is understood to be given since the moment of the issuance and delivery of the certificate by the Notarial Certification Agency.

4.6.6. Publication of the certificate

The Notarial Certification Agency publishes the renewed certificate in the Repository referred to in section 2.1, with the appropriate security controls.

4.6.7. Notification of the issuance to third parties

No stipulation

4.7. Certificate Re-key

4.7.1. Circumstances for the renewal of the certificate with a change of keys

The certificates must be renewed, together with the keys, when reaching the end of their validity period, or the end of the period of life of the qualified device in which they are stored.

4.7.2. Legitimation to request the renewal

Before the issuance and delivery of a renewed certificate there must exist a renewal request, which occurs at the instance of the subscriber or the key holder, as appropriate.

4.7.3. Processing the renewal request

The renewal request may be made and sent by the subscriber or the key holder, with their valid certificate, as proof of private key possession, provided that no more than five years have elapsed since the issuance of the certificate to be renewed. The processing of these requests will be done in accordance with what is specified in section 4.6.3.

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

In the case of renewal of certificates that have expired or have been revoked, there is no automatic renewal, and the procedures for the issuance of a new certificate must be followed.

For certificate renewals in physical presence, the procedures for the issuance of a new certificate must be followed.

4.7.4. Notification of the issuance of the renewed certificate

The Notarial Certification Agency notifies the issuance of the certificate to the subscriber and the key holder, as appropriate, at the email address included in the certificate.

4.7.5. Conduct that constitutes acceptance of the certificate

No stipulation.

4.7.6. Publication of the certificate

The Notarial Certification Agency publishes the renewed certificate in the Repository referred to in section 2.1, with the appropriate security controls.

4.7.7. Notification of the issuance to third parties

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

4.8. Certificate Modification

The modification of certificates, except the modification of the certified public key, which is considered renewal, is treated as an issuance of a new certificate, in accordance with sections 4.1 to 4.4 of this Certification Practice Statement.

4.9. Certificate Revocation and Suspension

4.9.1. Causes of revocation of certificates

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

1) Circumstances that affect the information contained in the certificate:

a) Modification of data included in the certificate.

b) Some data included in the certificate request is known to be incorrect.

c) Some data included in the certificate is known to be incorrect.

2) Circumstances that affect the security of the key or the certificate:

a) Compromise of the private key or the infrastructure or systems of the Certification Entity that issued the certificate, provided that it affects the reliability of the certificates issued since that incident.

b) Infringement, by the Notarial Certification Agency, of the requirements set forth in the certificate management procedures established in this Certification Practice Statement.

c) Compromise or suspicion of compromise of the security of the key or the certificate of the subscriber or key holder.

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

e) The irregular use of the certificate by the subscriber or the key holder, or the lack of diligence in the custody of the private key.

3) Circumstances that affect 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 the activation data of the subscriber or key holder.

4) Circumstances that affect the subscriber or the holder of keys:

a) Termination of the legal relationship between the Notarial Certification Agency and the subscriber.

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

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

d) Violation, by the subscriber or the key holder, of their obligations, responsibility and guarantees, established in the delivery document or in this Certification Practice Statement.

e) The supervening incapacity or the death of the subscriber or the key holder.

f) In the case of certificates for communities, the extinction of the legal person acting as the subscriber of the certificate, as well as the ending of the authorization of the subscriber to the key holder, or the end of the relationship between subscriber and key holder.

g) The existence of a revocation request from the subscriber, in accordance with the provisions of section 3.4.2 of this Certification Practice Statement.

5) Other circumstances:

a) The suspension of the digital certificate for a period longer than that established in section 4.9.16 of this Certification Practice Statement.

b) The termination of the service by the Notarial Certification Agency, in accordance with the provisions of section 5.8 of this Certification Practice Statement.

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

In this case, the actions performed during the suspension period are considered invalid, as long as the certificate is finally revoked. They are valid if the suspension is lifted and the certificate returns to the valid status.

4.9.2. Legitimation to request the revocation

They are authorized to request the revocation of a certificate:

- In any case, the subscriber in whose name the certificate was issued. The Notarial College or the Notary, as subscriber of the certificate, must act through a natural person with sufficient legal powers to revoke the certificate.

4.9.3. Revocation request procedures

The entity intending to revoke a certificate should request it to the Notarial Certification Agency or, where appropriate, to any authorized registration entity, and should provide the following information:

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

In those cases where immediate revocation of the certificate is required, a call shall be made requesting the suspension, or an email shall be sent to the Notarial Certification Agency at the electronic address *revocacion@ancert.com*.

Before proceeding with the revocation, the request is authenticated in accordance with the requirements established in section 3.4.2 of this Certification Practice Statement,

If the recipient of the request is a registration entity, it must:

- Identify and authenticate the applicant.
- Verify that the applicant is authorized to request the revocation of the certificate.
- Generate the request by accessing the online application for revoking certificates.

The revocation request is processed upon receipt.

The subscriber and, where appropriate, the key holder, are informed about the change of the status of the revoked certificate.

The Notarial Certification Agency cannot reactivate the certificate, once revoked.

4.9.4. Time period for the request of revocation

Revocation requests will be sent reasonably diligently as soon as the cause of revocation is known.

Outside the hours of attention of the Registration Authorities, the subscriber can request the precautionary suspension of the certificate contacting the Customer Service according to the procedure established in section 4.9.15.

4.9.5. Time period to process the revocation requests

The time elapsed between the reception of a revocation request and the execution of the change of status of the corresponding certificate will not exceed 24 hours in any case, including the time of dissemination of the information of the revocation information.

4.9.6. Obligation to consult certificate revocation information

Third parties that trust certificates must check the status of those certificates that they want to trust.

One method by which the status of certificates can be verified is by consulting the latest Certificate Revocation List issued by the Certification Entity that issued the certificate.

The Notarial Certification Agency provides information to third parties that trust certificates about how and where to find the corresponding Certificate Revocation List; among other methods, by including the web address of publication of the list in the certificates.

4.9.7. Frequency of issuance of certificate revocation lists (CRLs)

The Notarial Certification Agency issues a new CRL at least every 24 hours. Additionally, a new CRL will be issued after the suspension or revocation of a certificate.

The scheduled time to issue a new CRL is indicated in the CRL, although a CRL can be issued before the term indicated in the previous CRL.

Revoked certificates are removed from the CRL 60 days after their expiration date.

4.9.8. Time elapsed between generation and publication of the CRLs

Once the CRLs are generated, they are published at the distribution points indicated in the certificate extension with a propagation time of less than fifteen minutes.

4.9.9. Availability of certificate status checking services

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

This service is available 24 hours a day, 7 days a week. In the event of failure of the certificate status checking systems for causes beyond the control of the Notarial Certification Agency, it will make its best efforts to ensure that this service remains inactive for the minimum possible time.

4.9.10. Online revocation check requirements

The OCSP request to check the status of a certificate must include the serial number of the certificate and the identifying information of the issuer certificate authority.

The OCSP service offers status information on certificates beyond their validity period.

The response generated by the OCSP service contains the status information of the certificate at the time of the query. If the request cannot be processed, the server will generate an error response. The third party validating the certificate must ensure that the certificate used to sign the OCSP response, is a certificate with the extended key usage for OCSP signing and that it has been issued by the same certification authority as the certificate included in the request.

4.9.11. Other forms of certificate revocation information

Alternatively, third parties who trust certificates can check their status at the Notarial Certification Agency's Certificate Repository, which is available 24 hours a day, 7 days a week, at the web address https://www.ancert.com .

4.9.12. Special requirements in case of compromise of the private key

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

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

4.9.13. Causes of suspension of certificates

The Notarial Certification Agency can 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.

4.9.14. Legitimation to request the suspension

The subscriber, the natural person or an authorized third party may request the suspension of a certificate.

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

4.9.15. Procedures of request of suspension

In order to request a suspension electronically, the subscriber or the key holder should make a phone call to the number 912187676 of the Customer Service Center of the Notarial Certification Agency. For the appropriate evidentiary purposes, the conversation between the operator and the applicant for the suspension may be subject to recording and storing on a qualified device.

It is not allowed to request the suspension of a certificate by email.

4.9.16. Maximum period of suspension

The maximum suspension period is sixty (60) calendar days from the date in which the Notarial Certification Agency has effective knowledge of any of the causes of suspension, and this is stated in the Certificate Repository and in the Certificate Revocation List.

4.9.17. Lifting the suspension

Subscribers may request the lifting of the suspension during the sixty (60) days following the suspension, by calling the number 912187676 of the Customer Service Center of the Notarial Certification Agency. For the appropriate evidentiary purposes, the conversation between the operator and the applicant will be subject to recording.

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

In all cases, once the suspension of the Certificate has been lifted, it will be published immediately in the Certificate Repository of the Notarial Certification Agency, producing from that moment effects with respect to third parties, and it will also be updated conveniently the Certificate Revocation List (CRL) within the maximum period of twenty-four (24) hours.

In the event that the suspension has come from the Notarial Certification Agency, it may only proceed to lift the suspension of the certificate when by reliable means it has had reliable knowledge of the extinction of the cause that motivated the suspension. In this case, immediately afterwards it shall be removed the Certificate from the Revocation List.

4.9.18. Notification of revocation or suspension

The subscriber whose certificate has been suspended or revoked must be informed of that fact, as well as, where appropriate, of the lifting of the suspension, so the Notarial Certification Agency will notify it by email or by postal letter or even by phone when this notification has not been possible by any of the two previous formsº.

Notwithstanding the provisions of the preceding paragraph, the notification shall be deemed duly completed when it has been made by email to the address that appears on the certificate and, therefore, previously accepted by the user of the certificate.

However, if the system produces an error message or rejects the communication, it will be understood that the Notarial Certification Agency has sufficiently fulfilled with its obligation when the notification has been sealed. In order to further justify compliance with due diligence, the

Notarial Certification Agency will keep for fifteen years the electronic proof of the communication of the revocation or suspension.

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

4.10. Certificate status Services

4.10.1. Operational features of the services

The certificate status checking services are provided by a web query interface, by the Certificate Repository, and by the OCSP service.

4.10.2. Availability of services

Certificate status checking services are available 24 hours a day, 7 days a week, year round, except for scheduled stops.

4.10.3. Optional features

No stipulation.

4.11. End of 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 Certification Practice Statement.

4.12. Key Scrow and Recovery

4.12.1. Policy and practices for key scrow and recovery

The Notarial Certification Agency does not store or retrieve keys from subscribers or key holders, except for the encryption keys, which are stored in the Agency Notarial of Certification, with appropriate security controls that prevent unauthorized access by third parties.

Encryption keys can only be retrieved at the request of the natural person identified in the certificate, and in the case of a court order, executing the corresponding procedure implemented by the Notarial Certification Agency.

4.12.2. Session key encapsulation and recovery policy and practices

No stipulation.

5. Facility, Management, and Operational Controls

5.1. Physical Security Controls

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

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

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

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

- Physical access controls.
- Protection against natural disasters.
- Fire protection measures.
- Failure of support systems (power electronics, telecommunications, etc.)
- Collapse of the structure.
- Floods
- Theft protection.
- Trespassing and unauthorized entry.
- Disaster recovery.
- Unauthorized departure of equipment, information, media and applications used for the services of the certification service provider.

5.1.1. Location and construction of the facilities

The location of the facilities allows the presence of security forces in a reasonably time since an incident was notified.

The quality and strength of materials of construction of the facility ensure adequate levels of protection against intrusion by brute force.

5.1.2. Physical access

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

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

This identification is performed by recognition of biometric parameters of the individual, except for escorted visits.

The generation of cryptographic keys of the Certification Entities, as well as their storage, is managed in specific dependencies for these purposes, and require dual access and permanence.

5.1.3. Electricity and air conditioning

The Notarial Certification Agency's computer equipment is suitably protected against fluctuations or power cuts, which could damage them or disrupt the service.

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

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

5.1.4. Exposure to water

The Notarial Certification Agency has adequate flood detection systems to protect equipment and assets against such eventuality.

5.1.5. Fire prevention and protection

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

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

5.1.6. Media storage

The media used for the storage of information guarantees both its integrity and its confidentiality, in accordance with the established classification of the information.

Fireproof locations or cabinets are used for this purpose.

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

5.1.7. Waste treatment

The removal of media, both in paper and magnetic, is done by ensuring the impossibility of recovering the information.
In the case of magnetic media, a full formatting, permanent erasure or physical destruction of the support is performed.

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

5.1.8. Off-site backup copies

Periodically, the Notarial Certification Agency stores backup copies of the information systems, in physically separate premises, other than where the equipment is located.

5.2. Procedural controls

The Notarial Certification Agency ensures that its systems are operated safely, establishing and implementing procedures for the management of functions that affect the provision of its services.

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

5.2.1. Reliable functions

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

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

Reliable functions include:

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

5.2.2. Number of people per task

The trusted roles identified in the previous section and in the security policy, and their associated responsibilities, have been documented in job descriptions.

These descriptions have been made taken into account that there is a separation of sensitive functions, as well as a minimum grant of privilege, when possible.

To determine the sensitivity of the function, the following elements have been considered:

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

5.2.3. Identification and authentication for each function

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

5.2.4. Roles that require separation of tasks

The following tasks are performed by at least two people:

- Physical access management.
- Management of provider's computer applications.
- Configuration management and change control.
- Archive management.
- Cryptographic equipment asset management.
- Generation of certificates for Certification Authorities.

5.3. Personnel Controls

5.3.1. History, qualifications, experience and authorization requirements

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

This requirement applies 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 is free of personal interests that may conflict with the development of the function that has been entrusted.

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

- Academic history, including the alleged degree.
- Previous work, up to five years, including professional references and verification of the claimed work.
- Late payment.
- As far as current legislation allows, criminal records.

5.3.2. History investigation procedures

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

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

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

It is obtained the consent from the candidate for conducting this previous research, protecting all his personal information in accordance with the Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights.

The research is repeated every three years.

5.3.3. Training requirements

The Notarial Certification Agency trains staff in reliable positions and management until they reach the necessary qualifications in accordance with the provisions of section 5.3.1 of this Certification Practice Statement.

The training includes the following contents:

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

5.3.4. Requirements and frequency of training update

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

5.3.5. Sequence and frequency of job rotation

The Notarial Certification Agency can establish methods of job rotation for the provision of the service, in order to cover the 24x7 needs of the service.

5.3.6. Sanctions for unauthorized actions

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

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

5.3.6.1. Disciplinary procedure

The staff of the Notarial Certification Agency is obliged to comply with the following:

- Use the material means of the Notarial Certification Agency without engaging in activities that would be considered unlawful or which infringe the rights of the entity or third parties, or that might violate the moral or ethical rules and etiquette of such networks.
- Do not send confidential information to outside by hardware or by any means of communication, including simple visualization or access, except when expressly authorized by the Notarial Certification Agency.

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

In order to ensure compliance with the internal regulations of the Notarial Certification Agency, it reserves the right to review, without prior notice, the computer systems (email files, files on the hard drive of personal computers, voice mails, print queues, etc.). Inspections are performed with the prior approval of the Security Department, in accordance with the procedure established in the applicable regulations.

The Notarial Certification Agency can remove from its computer system any material that it considers offensive or potentially illegal.

5.3.6.2. Unauthorized activities

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

- Share or provide user IDs and/or password provided by the Notarial Certification Agency with other third party, including the staff. In case of violation of this prohibition, the employee shall be solely responsible for the acts of the third person using these user IDs.
- Trying to distort or falsify system LOG records.
- Trying to decipher keys, encryption algorithms and other security elements involved in telematic processes of the Notarial Certification Agency.
- Destroy, alter, disable or otherwise damage data, programs or electronic documents the Notarial Certification Agency or third parties.
- Willfully hinder other employees' access to the network through mass consumption of computing resources and telematic the Notarial Certification Agency, as well as actions that damage, interrupt or generate errors in the system.

- Send emails in bulk or commercial or advertising purposes without the consent of the recipient (spam).
- Read, delete, copy or modify e-mail messages or files of other employees.
- Use the system to attempt to access restricted areas of computer systems the Notarial Certification Agency or third parties.
- Try to increase the privilege level of an employee in the system.
- Voluntarily introduce programs, viruses, macros, applets, ActiveX controls or any other logic device or sequence of characters that are causing or are likely to cause any alteration in the computer system the Notarial Certification Agency or third parties. The employee will be required to use antivirus software and updates to prevent entry into the system from any element intended to destroy or corrupt computer data.
- Enter, download from Internet, reproduce, and use or distribute software unless expressly authorized by the Notarial Certification Agency.
- Install illegal copies of any program, including standardized copies.
- Remove any programs installed illegally.
- Using telematic resources of the Notarial Certification Agency including the Internet, for activities unrelated to the work of the employee.
- Transfer to the corporate network of the Notarial Certification Agency obscene, immoral or offensive, and in general, superfluous contents.
- Use information and/or log in as natural or legal persons identified or identifiable in the network without the necessary legitimacy for use.
- Create files containing personal data without authorization the Notarial Certification Agency.
- Crossing information concerning personal data from different files or services with the aim of establishing personality profiles, buying habits or any kind of preferences, without the express permission of the Notarial Certification Agency.
- Any other activity specifically prohibited in the security policy the Notarial Certification Agency and current legislation on protection of personal data.
- Treat personal data, in writing or orally, without the proper authorization by the Notarial Certification Agency.
- The use of bypass systems, designed to avoid protective measures, and other files that could compromise protection systems or resources.

5.3.7. Requirements for hiring professionals

The Notarial Certification Agency can hire professionals for any function, even for a reliable position, in which case they undergo the same controls as other employees.

If the professional does not have to undergo such controls, he is constantly accompanied by a reliable employee, when he is on the premises of the Notarial Certification Agency.

5.3.8. Provision of documentation to staff

The Notarial Certification Agency provides the documentation to the staff, in order for them to be sufficiently competent in accordance with the provisions of section 5.3.1 of this Certification Practice Statement.

5.4. Audit Logging Procedures

5.4.1. Types of registered events

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

- Turning on/off of the systems.
- Starting and ending of the software for the certification authority or the registration authority.
- Attempts to create, delete, change passwords or user permissions within the system.
- Generation and changes in the keys of the Certification Entity.
- Changes in the policies for issuing certificates.
- System login/logout attempts.
- Unauthorized access attempts to the network of the Certification Entity.
- Unauthorized attempts to the file system.
- Failed attempts to read a certificate, and events of 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.

5.4.2. Review period for audit logs

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

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

Actions taken during the audit review are also documented.

5.4.3. Retention Period of Audit Records

Audit logs must be retained on site for at least two months after processing and, thereafter, shall be archived in accordance with section 5.5.2 of this Certification Practice Statement.

5.4.4. Protection of audit logs

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

5.4.5. Backup procedures for audit logs

At least incremental backup copies are generated daily and full copies weekly.

5.4.6. Log aggregation system

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

5.4.7. Notification of the 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.

5.4.8. Vulnerability analysis

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

Internal and external vulnerability analysis of the systems are performed at least quarterly. Additionally, a penetration test is also performed annually (by an external company).

5.5. Records Archival

The Notarial Certification Agency guarantees that all the information related to the certificates is kept for an appropriate period of time, as established in section 5.5.2 of this Certification Practice Statement.

5.5.1. Types of archived records

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

A record is kept of the following:

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

5.5.2. Record retention period

The Notarial Certification Agency keeps the records specified in the previous section permanently, with a minimum of fifteen (15) years counted from the time of issuance of the certificate.

5.5.3. Archive protection

The Notarial Certification Agency:

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

5.5.4. Backup procedures

The Notarial Certification Agency makes daily incremental backup copies of all its electronic documents, according to section 5.5.1 of this Certification Practice Statement. In addition, it makes also full backups weekly for data recovery cases, in accordance with section 5.7 of this Certification Practice Statement.

According to section 5.5.1, it shall be kept paper documents in a location outside the Notarial Certification Agency for cases of data recovery, as established in section 5.7 of this Certification Practice Statement.

5.5.5. Timestamping requirements

The Notarial Certification Agency issues certificates and CRLs with reliable date and time information. All information systems are synchronized with an accurate source of date and time.

5.5.6. Archive system

The Notarial Certification Agency has an archive data maintenance system outside its own facilities, as specified in section 5.5.4 of this Certification Practice Statement.

5.5.7. Procedures for obtaining and verifying archival information

Only people authorized by the Notarial Certification Agency have access to archival data, either in the same facilities of the Notarial Certification Agency or at its external location.

5.6. Key Changeover

The Notarial Certification Agency has established a plan for the renewal of the keys corresponding to certificates of infrastructure, so that the continuity of services is guaranteed.

5.7. Compromise and Disaster Recovery

5.7.1. Incident management procedures

The Notarial Certification Agency has established the procedures that apply to incident management and, especially, to those incidents that affect the security of its keys.

5.7.2. Corruption of resources, applications or data

When an event of corruption of resources, applications or data occurs, the Notarial Certification Agency will initiate the necessary steps, in accordance with the security plan, the business continuity and disaster recovery plan, or equivalent documents, to bring the system back to normal operation.

5.7.3. Procedure in case of compromise of the private key

5.7.3.1. Revocation of the public key of the entity

If the Notarial Certification Agency must revoke the public key of a Certification Entity belonging to its hierarchy, it will perform the following actions:

- Report this fact, when it may happen, to the General Council of Notaries and the entity in charge of the supervision of the Trust Service Providers.
- Report the fact by publishing a CRL, as established in section 4.9.7 of this Certification Practice Statement.
- Make every effort to report the revocation to all subscribers to whom the Notarial Certification Agency has issued certificates, as well as to third parties who trust its certificates.
- Perform a key renewal, as long as the revocation was not due to the termination of the service by the Notarial Certification Agency, as established in section 5.6 of this Certification Practice Statement.

5.7.3.2. Compromise of the private key of the entity

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

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

- Revoke the certificate of the Certification Entity affected.
- Inform all subscribers and third parties of the compromise.
- Indicate that the certificates and the revocation status information that have been delivered using the key of this Certification Entity are no longer valid.

For the restoration of the service, the Notarial Certification Agency will generate a new key pair and certificate for the Certification Entity. From that moment, the new CRLs and the OCSP Responder certificate will be signed with the new Entity key to continue the service of provision of certificate revocation status.

5.7.4. Business continuity after a disaster

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

The Notarial Certification Agency is able to restore critical services within 24 hours of the disaster. These services are as follows:

- Revocation of certificates.
- Publication of certificate revocation information.

The location of the disaster recovery systems must have the physical security protections detailed in the security plan.

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

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

5.8. CA or RA Termination

Before the end of its activity the Notarial Certification Agency will perform the following actions:

- It will provide the necessary funds (through civil liability insurance) to continue the completion of the revocation activities until the definitive cessation of its activity.
- It will inform all subscribers and entities with which it has agreements, as well as all third parties, other trusted service providers and relevant authorities, including the competent supervisory body, of the cessation at least two months in advance.
- It will revoke the authorization to process new requests to all registration entities that act on behalf of the Certification Entity in the process of issuing certificates.
- It will transfer its obligations regarding the maintenance of registration information, those of the status information of the certificates and the records of audit events to the General Council of Notaries during the period indicated to the signers and users.
- At the time of cessation, it will generate a CRL with all the certificates revoked throughout the history of the Certification Authority and with the value of expiration date (nextUpdate) "99991231235959Z". This CRL will be published at the address specified as the distribution point for revocation lists in the certificates.
- The private keys of the Certification Authority, including their backup copies, will be destroyed or disabled for use.

6. Technical Security Controls

The Notarial Certification Agency employs reliable systems and products, which are protected against any alteration and guarantee the technical and cryptographic security of the certification processes.

6.1. Key pair generation and installation

6.1.1. Generation of the key pair

The Notarial Certification Agency, when it acts as the root Certification Entity, generates and signs its own key pair and proceeds to generate the keys for each subordinate Certification Entity, all this in accordance with the key ceremony, within the high security perimeter specifically dedicated to this task.

All cryptographic keys must be generated following the algorithm recommendations and minimum key length defined in ETSI TS 119 312.

The key pairs of end entities with guarantee of secure device are generated by the Notarial Certification Agency or end entities, in secure devices such as cryptographic cards. The creation of the public and private keys (2048 bits RSA) is executed internally by the card itself, so that both the robustness of the keys and the impossibility of a compromise in the generation process are guaranteed.

The key pairs managed in a centralized form by the Notarial Certification Agency are generated in cryptographic modules in combination with the "ANCERT Server Signing Application" solution. The creation of public and private keys (2048 bits RSA) is carried out internally by the cryptographic module, so that both the robustness of the keys and the impossibility of compromising them in the generation process are guaranteed. The key pair is protected with a key derived from the user's PIN code in combination with a key from the cryptographic module, so that its use is not possible either outside the cryptographic module or without the authorization of the signer.

The keys of the final entities without a secure device guarantee are generated by the final entities on their own computers.

6.1.2. Delivery of the private key to the subscriber

The subscriber's (or key holder) private key with guarantee of secure device is delivered properly protected by the cryptographic device mentioned in the previous section.

When the Keys are generated by Notarial Certification Agency in PKCS#12 format the appropriate security measures shall be established in order to guarantee a safely delivery to the subscriber / key holder.

This section is not applicable when the key is generated by the end entity.

6.1.3. Delivery of the public key to the certificate issuer

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

6.1.4. Distribution of the public key of the certification service provider

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

The public key of each Certification Entity is published in the Depository, in the form of a self-signed certificate or signed by another Certification Entity, together with a statement that the key authenticates the Certification Entity.

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

Users can access the Repository to obtain the public keys of the Certification Entities.

Additionally, for S / MIME applications, the message may contain a chain of certificates, which in this way are distributed to users.

6.1.5. Key sizes

The length of the RSA keys of the Certification Bodies is at least 4096 bits, while that of the other types of certificates is at least 2048 bits.

6.1.6. Generation of public key parameters and quality verification

The Notarial Certification Agency can establish methods for checking the quality of public key parameters.

Key Size: 4096 (Certification Bodies) / 2048 (End Entities)

algorithm key generation: rsagen1

algorithm *padding:*EMSA-pkcs1-v1_5

digest algorithm: SHA-256

6.1.7. Key Usage

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

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic modules standards

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

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

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

The password is only known by one person responsible for that device. No person knows more than one password.

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

6.2.3. Private key escrow

Only private keys of end-entity certificates whose sole use is encryption are escrowed. The recovery of an encryption private key requires of the multiperson control detailed in section 6.2.2.

In the case of certificates for centralized signature, the Notarial Agency custodies the signer's key and enables the corresponding technical mechanisms to guarantee exclusive control by the signer.

6.2.4. Backup copy of the private key

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

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

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

The copies of the private keys for centralized signature are protected by the signer's activation data and are only accessible by the signer.

6.2.5. Private key archiving

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

Private keys for electronic signature of end users are not archived.

6.2.6. Transfer of the private key to or from the cryptographic module

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

The private keys of the Certification Entities are stored in encrypted files with fragmented keys and in cryptographic devices (from where they cannot be extracted).

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

6.2.7. Storage of the private key in the cryptographic module

The private keys of the Certification Entities are generated directly in the cryptographic modules.

In cases where private keys are stored outside the cryptographic modules, they will be protected in a way that ensures the same level of protection as if they were physically inside the cryptographic modules.

6.2.8. Private key activation method private

The key of each Certification Authority is activated by executing the corresponding secure startup procedure of the cryptographic module, by the people indicated in section 6.2.2.

The subscriber's private keys are activated by entering the PIN in the cryptographic device or signing application.

The private keys for centralized signature are activated using a key activation protocol (SAP) with a double authentication factor: a PIN code chosen by the signer and a pair of activation keys linked to the device in the mobile phone application controlled by the signer. The Notarial Certification Agency does not store the activation PIN code of the signer's centralized keys. The signer can change the activation PIN of his centralized keys at any time through the activation application of his mobile phone.

6.2.9. Private key deactivation method

The private keys of the Root Certification Authority are automatically deactivated when the last of the devices used for their activation (as described in section 6.2.2) is removed.

The private keys of the subordinate Certification Authorities are automatically deactivated when the software supporting the Certification Authority is stopped.

For certificates for qualified signature issued in smart card, when the cryptographic device is removed from the reader or disconnected from the computer, or the application using them closes the session, then the PIN code shall be entered again.

For certificates for electronic signature with centralized keys, the signer's key is entered, activated and deactivated in the cryptographic module in each signing operation.

6.2.10. Destruction method of the private key

For the destruction of the private keys of the Certification Entity and its activation data, the devices that contain them will be physically destroyed or erased at a low level, following the procedures specified by the manufacturer. After, any existing backup will be securely destroyed.

For the destruction of the private keys of the final entities in hardware, a device collection service is made available to the subscribers for its secure physical destruction, in addition with a software application for the secure deletion of the devices through the Registration Entities and the certification Entity.

Private signing keys with centralized management are safely removed, including their backups, when the associated certificate is revoked or expires.

6.2.11. Classification of cryptographic modules

The modules of the Certification Entity must be certified against a proper protection profile, in accordance with Common Criteria EAL 4+, or FIPS 140-2 Level 3.

The European standard for the devices of the subscribers is the EU Commission Implementing Act (EU) 2016/650 of April 25, 2016.

The eligible devices are all those that are on the list of qualified devices for electronic signature, notified according to the eIDAS regulation.

The keys for centralized signature keys are generated on Common Criteria certified cryptographic hardware, with EAL 4 + AVA_VAN.5 assurance level.

6.3. Other aspects of key pair management

6.3.1. Public key archiving

The Certification Entities shall archive their public keys in a permanent way, in accordance with the provisions of section 5.5 of this Certification Practice Statement.

6.3.2. Periods of use of public and private keys

The periods of use of the keys are determined by the duration of the certificate, after which they can no longer be used.

As an exception, the private key can continue to be used for decrypting documents, even after the certificate expires.

6.4. Activation data

6.4.1. Generation and installation of activation data

The Notarial Certification Agency provides the subscriber with a qualified signature creation device, so that the activation data of the device is securely generated by the Notarial Certification Agency.

To generate a signature or activate the card it is necessary to enter the secret activation code (PIN) that only the key holder of the card should know. Three consecutive incorrect attempts to enter the PIN cause the card to be blocked. To unlock the card, the cardholder must enter the PUK code and, likewise, three consecutive incorrect attempts to enter the PUK cause the card to be irreversibly blocked.

To sign with a certificate with centralized keys, the signer must have initialized the signature activation application on their mobile phone and his signature activation key must be installed on the device. The user must enter their secret activation code (PIN) which is sent through a secure key activation protocol (SAP), authenticated in the centralized signature system (SSA) with their activation key. Three consecutive failed attempts at PIN entry cause the SSA to lock the signing key. The user has a PUK code to unlock their signature key and has a maximum of 10 consecutive wrong attempts that cause the signature key to be irreversibly blocked. The PUK code cannot be used to retrieve a signing key once it has been disabled.

6.4.2. Protection of activation data

The Notarial Certification Agency can generate and provide the key holder with the activation data of the qualified signature creation device using secure procedures, such as face-to-face or remote delivery, in which case the activation data will be distributed separately from the signature creation device (for example, being delivered at different times, or by different routes).

6.4.3. Other aspects of activation data

No stipulation.

6.5. Computer security controls

6.5.1. Specific technical requirements for computer security

It is guaranteed that access to the systems is limited to duly authorized individuals. In particular:

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

6.5.2. Assessment of the level of computer security

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

6.6. Life Cycle security controls

6.6.1. System Development Controls

An analysis of security requirements has been performed during the phases of specification and design of any application used by certification and registration authorities, in order to ensure that systems are secure.

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

6.6.2. Security management controls

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

The configuration of the systems is regularly audited, in accordance with the provisions of section 8.1 of this Certification Practice Statement.

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

6.6.3. Life cycle security controls

No additional stipulations.

6.7. Network security controls

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

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

6.8. Timestamping

The Notarial Certification Agency obtains the time for its systems from the Royal Navy Observatory (ROA) following the NTP protocol through the Internet. All systems are synchronized with this source of time using the NTP protocol.

7. Certificate, CRL and OCSP Profiles

7.1. Certificate Profile

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

- Serial number, which is a unique code with respect to the distinguished name of the issuer.
- Signature algorithm.
- The distinguished name of the issuer.
- Beginning of the validity period of the certificate, in Universal Coordinated Time, encoded according to RFC 3280
- End of the validity period of the certificate, in Universal Coordinated Time, encoded according to RFC 3280
- Distinguished name of the subject.
- Public key of the subject, encoded according to RFC 3280
- Signature, generated and encoded according to RFC 3280

The certificates comply with the following standards:

- RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile May 2008.
- ITU-T Recommendation X.509: Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997, with its subsequent updates and corrections.

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

- EN 319 412: Certificate Profile
- RFC 3739: Internet X.509 Public Key Infrastructure - Qualified Certificate Profile, March 2004 (as long as it does not conflict with EN 319 412)

7.1.1. Version number

All certificates contain a field with the version number. The value of the field is the integer value "2" using the X.509 version 3 standard.

7.1.2. Certificate extensions

The Notarial Certification Agency publishes a document with the detail of all the certificate profiles in the Repository indicated in section 2.

7.1.3. Identifiers algorithm object

The Notarial Certification Agency uses the algorithm sha256WithRSAEncrypton, with OID 1.2.840.113549.1.1.11, to sign all its certificates.

7.1.4. Name formats

Name formats are specified in the document with the detail of all certificate profiles published in the Repository indicated in section 2.

7.1.5. Name restrictions

No additional stipulation.

7.1.6. Object Identifier of the certificate policy

The Notarial Certification Agency will include in the Certificate Policy extension (OID 2.5.29.32) the object identifier associated with the policy of each certificate according to section 1.2.

7.1.7. Use of the extension for policy restrictions

No additional stipulation.

7.1.8. Syntax and semantics of policy qualifiers

The Notarial Certification Agency will include in the Certificate Policy extension (OID 2.5.29.32) a qualifier with the following elements:

- CPS Pointer: contains an electronic address pointing to the Certificate Practices Statement and the rest of relevant documentation for the certificate.
- User Notice: Contains a concise textual description regarding the certificate.

7.1.9. Semantics of the certificate policy extension

The Certificate Policy (OID 2.5.29.32) extension of the certificates allows identifying the policy associated with the certificate and the electronic address where the information of this policy can be found.

7.2. CRL Profile

The certificate revocation lists are in accordance with the following standards:

- RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile April 2002.

7.2.1. Version number

The generated CRLs have version number 2.

7.2.2. Certificate revocation list and extensions

The generated CRLs contain the following extensions:

- Authority key Identifier (OID 2.5.29.35)
- CRL Number (OID 2.5.29.20)

7.3. OCSP profile

The OCSP responses from the Notarial Certification Agency are in accordance with RFC 6960 and are signed by the OCSP Responder whose certificate has been signed by the same Certification Entity that issued the certificate which is being consulted.

7.3.1. Version number

All OCSP Responder certificates contain a field with the version number. The value of the field is the integer value "2" using the X.509 version 3 standard.

7.3.2. OCSP extensions

The detail of the OCSP Responder certificate profile can be found in the document with all the certificate profiles published in the Repository indicated in the Section 2.

OCSP responses will include the ExtendedRevoke extension (OID 1.3.6.1.5.5.7.48.1.9).

8. Compliance audit and other assessments

The Notarial Certification Agency periodically conducts audits of compliance to assure compliance with the security and operational requirements needed to meet the certification services policy of the General Council of Not.

8.1. Frequency

A conformity audit is conducted annually, in addition to the internal audits that may performed at any time, due to a suspected breach of any security measure or due to a compromise of keys.

8.2. Identification and qualification of the auditor

The Notarial Certification Agency hires the services of external independent auditors to perform the annual compliance audits. These auditors must prove experience in computer security, in Information Systems security and with compliance audits of Trust Service Providers and related. The auditors must be accredited according to EN 319 403.

8.3. Relationship between the auditor and the auditee

Compliance audits are conducted by an independent entity and must not have any conflict of interest with the Notarial Certification Agency that may affects the ability to perform audit services.

8.4. List of elements to be audited

The elements to be audited are the following:

- Public key certification processes.
- Information systems.
- Protection of the processing center.
- Documentation of the service.

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

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

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

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

- Revocation of the key of the Certification Entities, as described in section 5.7.3 of this Certification Practice Statement.

- Termination of the certification services, as described in section 5.8 of this Certification Practice Statement.

8.6. Communication of the results

The audit reports will be delivered to the Security Committee, for their analysis, within a maximum period of 15 days after the completion of the audit, for their evaluation and diligent management.

9. Other Business and Legal Matters

9.1. Fees

9.1.1. Fee for the issuance or renewal of certificates

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

9.1.2. Fee for the access to the certificates

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

9.1.3. Fee for the access to certificate status information

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

9.1.4. Fees for other services

Without stipulation.

9.1.5. Refund policy

The Notarial Certification Agency has the following fee refund policy:

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

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

9.2. Financial responsibility

The Notarial Certification Agency has enough financial resources to maintain its operations and fulfill its obligations, as well as to face the risk of liability for damages.

The Notarial Certification Agency does not act as a fiduciary agent or representative in any way of users or trusted third parties.

9.2.1. Insurance coverage

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

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

9.2.2. Other assets

Without stipulation.

9.2.3. Insurance coverage for subscribers and third parties who trust certificates

Without stipulation.

9.3. Confidentiality of Business Information

9.3.1. Scope of confidential information

The following information, as a minimum, is kept confidential by the Notarial Certification Agency:

- Certificate applications, 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.
- Operational documentation, such as archiving, monitoring, and analogues.
- All other information identified as "Confidential".

9.3.2. Non-confidential information

The following information is considered non-confidential:

- Issued 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 subscriber 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 limits of amount defined in the certificate.
- Validity period of the certificate, and the dates of issuance and expiration.
- Serial number.
- The different 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 change of status.
- 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.

9.3.3. Responsibility to protect confidential information

9.3.3.1. Disclosure of suspension and revocation information

See previous section.

9.3.3.2. Legal disclosure of information

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

Specifically, the records that guarantee the reliability of the data contained in the certificate are disclosed if the Notarial Certification Agency is required to offer evidence of certification in the event of a legal proceeding, even without the consent of the certificate subscriber.

These circumstances are indicated in the privacy policy provided in section 9.4 of this Certification Practice Statement.

9.3.3.3. Disclosure of information at the request of the owner

The Notarial Certification Agency includes, in the privacy policy provided in section 9.4 of this Certification Practice Statement, prescriptions to allow the disclosure of the subscriber's information and, where appropriate, the key holder, directly to them or to third parties.

9.3.3.4. Other circumstances for the disclosure of information

No stipulation.

9.4. Privacy of Personal Information

For the provision of the service, the Notarial Certification Agency needs to collect and store certain information, including personal information.

The Notarial Certification Agency has developed a privacy policy, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the management of personal data and its free circulation, and superseding the Directive 95/46 / EC (GDPR) and Organic Law 3/2018, of December 5, on the Protection of Personal Data and digital rights.

The Notarial Certification Agency has performed the corresponding analysis of the risks that may arise by the processing of personal data and has adopted the appropriate security and control measures to guarantee the rights of people and to mitigate the risks caused by harm or direct material damage, by violation of principles or rights, or because it fails to comply with any obligation established in the data protection regulations.

In order to perform their activity, the Registration Entities will access to personal data. The Notarial Certification Agency will have the condition of Responsible for the management of this data, and will decide on the purpose, content and use of personal data. The registration entities will be considered Data Processors, and they must use these personal data solely and exclusively for the purposes described in the Certification Practice Statement.

The Registration Entities, in compliance with the provisions of article 28 of the GDPR, must:

1. Process personal data according to the instructions of the Notarial Certification Agency.

2. Guarantee and protect public liberties and the fundamental rights of natural persons, and, especially, their honor and personal and family privacy.
3. Keep professional secrecy regarding personal data, not disclosing to third parties the information obtained as a result of a contractual relationship. This obligation shall continue even after the end of the relation with the Notarial Certification Agency.
4. Comply with all the technical and organizational measures necessary to guarantee the security of the processes involving personal data, processing center, facilities, equipment, systems, programs and people involved in the processing of personal data.
5. To implement appropriate technical and organizational measures to ensure the security and integrity of personal data and avoid its alteration, loss, or unauthorized access, given the state of technology, the nature of the data stored, and the potential risks, whether they come from human or natural action. The security measures that must be applied will, in any case, be adequate to mitigate the risks derived from the risk analysis that must be performed in accordance with the GDPR.
6. Send to the Notarial Certification Agency the personal data of the applicants and / or subscribers of certificates using secure communications.
7. Process the data in accordance with the provisions of the contract with the Notarial Certification Agency, and not use this data for any other purpose, nor communicate them (not even for their preservation) to other people.
8. Only access the personal data of the Notarial Certification Agency when it was necessary to perform the contracted services.
9. Destroy or return all the personal data once, for any reason, the relationship with the Notarial Certification Agency ends except for those data that the law requires to keep for a minimum of 15 years.

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

The Notarial Certification Agency is exonerated from any responsibility that may be generated by the breach by the persons in charge of the Treatment of their described obligations. In such cases of non-compliance, they will be considered responsible for the treatment and will be responsible for the infractions that they have incurred personally.

In accordance with the provisions of article 13 of the GDPR, the applicant / subscriber is informed that the personal data that is included in the forms, contracts or documents completed during the process of requesting the issuance of a Certificate, will be registered in a file created for this purpose. The Notarial Certification Agency will only provide the certification services if the forms are filled in entirely with true information.

The legality of the processing of personal data is covered by the contractual execution of the trust services. The applicant/subscriber communicates to the Notarial Certification Agency his data that will be processed for the uses and purposes of providing the trust services in the terms established in the Law and this Declaration of Certification Practices.

In accordance with the provisions of the aforementioned article of the GDPR, the applicant / subscriber, or any user of the certificates consents to the communication to third parties that trust certificates, of his personal data included in the certificate and published in the Repository. This information is published in the website www.ancert.com exclusively for the purpose of allowing the consultation of the certificates issued by the Notarial Certification Agency and their validity, as well as to consult the certificates revoked by the Notarial Certification Agency in the Certificate Repository and the Certificate Revocation Lists.

Third parties that trust certificates may only use the information in accordance with the described purposes. However, and in general, any processing, storage or use for purposes other than the above requires the prior consent of the data owners. It is noted that the RGPD sanctions with fines that can reach up to 4% of the annual turnover with a maximum of 20 million euros for each of the infractions or breaches of the legal provisions, regardless of any criminal proceedings that can be derived from the Criminal Code as well as civil claims from the damaged.

The applicant / subscriber may exercise the rights of access, rectification, deletion, limitation, portability and opposition according to the GDPR by sending the request to the address that appears in section 1.5.2 of this Certification Practice Statement, and also has the right to file a claim with a supervisory authority.

9.5. Intellectual property rights

9.5.1. 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.

The OIDs owned by the Notarial Certification Agency have been registered in the IANA (Internet Assigned Number Authority) under branch 1.3.6.1.4.1. This OID is the number 18920 (ANCERT), and can be consulted at:

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

The total or partial use of any of the OIDs assigned to the Notarial Certification Agency is prohibited except for the uses described in the Certificates or in the Certificate Repository.

Any extraction and / or reuse of all or a substantial part of the contents or databases that the Notarial Certification Agency makes available to certificate subscribers is prohibited.

9.5.2. Ownership of the certificate policies and the Certification Practices Statement

The General Council of Notaries is the only entity that owns intellectual property rights over the certificate policies.

The Notarial Certification Agency owns this Certification Practice Statement.

9.5.3. Ownership of information related to names

The subscriber and, where appropriate, the key holder, retains any right, if any, regarding the brand, product or commercial name contained in the certificate.

The subscriber is the owner of the distinguished name of the certificate, consisting of the information specified in section 3.1 of this Certification Practice Statement.

9.5.4. Key Ownership

Key pairs are owned by the certificate subscribers.

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

9.6. Representations and Warranties

9.6.1. Model of obligations of the service provider

The Notarial Certification Agency guarantees, under its full responsibility, that it complies with all the requirements established in each certificate policy for which it issues certificates.

It is the only entity responsible for compliance with the procedures described in this Certification Practice Statement, even when part or all the operations are outsourced externally.

The Notarial Certification Agency provides its certification services in accordance with this Certification Practices Statement, which in turn, details its functions, operating procedures and security measures.

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

This requirement is fulfilled, among other means, by means of an applicable "Certificate Policy Disclosure Text", published and transmitted electronically, using a means of communication that is durable over time, and in understandable language.

Subscribers, key holders and third parties who trust certificates are obliged by the provisions of the certificate delivery documents and the general conditions of use of certificates, which are written in understandable language, and which have the following minimum content:

- Prescriptions to comply with the provisions in sections 4.5.1, 4.5.2, 9.2, 9.10, 9.13, 9.15 and 9.16 of this Certification Practice Statement.
- Indication of the applicable policy, indicating whether the certificates are issued to the public and the need to use a qualified device.
- Statement indicating 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 1.4.1.1 of this Certification Practice Statement.
- Information about how to validate a certificate, including the requirement to check the status of the certificate, and the conditions under which the certificate can be reasonably trusted, which is applicable when the subscriber acts as a third party that trusts the certificate.
- Information on how the patrimonial responsibility of the Notarial Certification Agency is guaranteed.
- Applicable limitations of liability, including the uses for which the Notarial Certification Agency accepts or excludes its liability.
- Archive period for certificate request information.
- Archive period of audit logs.
- Procedures for dispute resolution.
- Applicable law and jurisdiction.
- If the Certification Entity has been declared in accordance with the certification policy and, if applicable, in accordance with which system.

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

9.6.2. Guarantees offered to subscribers and third parties who trust certificates

The Notarial Certification Agency, in the documentation for the delivery of certificates and in the general conditions of use of certificates, establishes and rejects warranties and applicable limitations of liability.

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

- That there are no factual errors in the information contained in the certificates known by the Notarial Certification Agency and, where applicable, by the registration entity.
- That there are no factual errors in the information contained in the certificates due to lack of due diligence in the management of the certificate request or the generation.
- That certificates meet all requirements established in the Declaration of Certification Practices.
- That revocation services and the repository meet all requirements established in the Declaration of Certification Practices.

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

- That the information contained or incorporated by reference in the certificate is correct, except where otherwise indicated.

- In case of certificates published in the repository, that the certificate has been issued to the subscriber identified in it and that the certificate has been accepted in accordance with section 4.4 of this certification policy.
- That the approval of the certificate request and the issuance has met the requirements established in the Declaration Certification Practices.
- The speed and security in the provision of services, especially revocation and repository services.

In addition, when it issues an electronic signature certificate, it guarantees the subscriber and the third party that trusts the certificate:

- That the certificate includes the information that a qualified certificate must include, in accordance with Annex I of Regulation (EU) 910/2014.
- The responsibility of the Notarial Certification Agency, with the legal limits established.

9.7. Disclaimer of Warranties

The Notarial Certification Agency rejects any other guarantee that is not legally required, except those contemplated in section 9.6.2.

Specifically, the Notarial Certification Agency does not guarantee the cryptographic algorithms used nor is liable for damages caused by external attacks on against these algorithms, provided that it has applied due diligence according to the state of the art, and it has acted in accordance with the provisions in this Certification Practice Statement and the Law 6/2020 and its implementing regulations.

9.8. Limitations of Liability

9.8.1. Limitations of liability of the Certification Authority

The Notarial Certification Agency limits its responsibility to the issuance and management of certificates and, where appropriate, the issuance of key pairs of subscribers and cryptographic devices (for signature and signature verification, as well as encryption or decryption) provided by the Notarial Certification Agency.

The Notarial Certification Agency limits its liability by including limits on the use of the certificate, and limits on the value of the transactions for which the certificate can be used, in accordance with the provisions of section 1.4.1.1 of this Declaration of Practices of Certification

All legal, contractual or extra-contractual responsibilities, direct or indirect damages that may derive from such uses are the responsibility of the subscriber. In no case may the subscriber nor the damaged third parties claim compensation or indemnification from the Notarial Certification Agency for damages or liabilities arising from the use of the keys or certificates for encryption.

9.8.2. Fortuitous events and force majeure

The Notarial Certification Agency includes clauses in the general conditions of use of certificates to limit its liability in case of fortuitous events and force majeur,.

9.9. Indemnities clauses

9.9.1. Indemnity clause for the subscriber

The subscriber agrees to exonerate the Notarial Certification Agency from any damage arising from any action or omission resulting in liability, damage or loss, expense of any kind, and also from any legal consequence, due to 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, if there was fraud or negligence with respect to the Notarial Certification Agency, the registration entity or any person who trusts the certificate.
- Negligence in the protection of the private key, in the use of a reliable system or in maintaining the necessary precautions to avoid the compromise, loss, disclosure, modification or unauthorized use of that key.
- Use by the subscriber of a name (including common names, email address and domain names), or other information in the certificate, that infringes the intellectual or industrial property rights of third parties.

9.9.2. Indemnity clause for third parties that trust certificates

The Notarial Certification Agency includes, in the general conditions of use of certificates, a clause by which the third party that trusts the certificate agrees to exclude the 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 party that trust certificates.
- Overconfidence on certificates.
- Negligence to determine the status of a certificate (determine if it has been suspended or revoked).

9.10. Term and Termination

9.10.1. Effective starting date

The Certification Practice Statement has effects since the time of publication.

9.10.2. Ending date

The current Certification Practices Statement will be superseded when a new version of the document is published.

The new version will entirely replace the previous document.

9.10.3. Effect of termination and survival

For current certificates issued under a previous Certification Practice Statement, the new version will prevail over the previous one in everything that does not oppose it.

9.11. Individual notices and communications with participants

The Notarial Certification Agency establishes, in its binding legal contracts with subscribers and verifiers, notification clauses, which establish the procedure for notifications.

In general, the website will be used to make any type of notification and communication.

9.12. Amendments

9.12.1. Procedure for modifications

The Notarial Certification Agency may unilaterally modify the Certification Practices Statement and the rest of the legal documentation as long as it proceeds according to the following procedure:

- The modification will be justified from a technical, legal point of view or commercial, and must be endorsed by the General Management of the Notarial Certification Agency.
- All the technical and legal implications of the new version of specifications should be considered.
- A modification control will be established to guarantee that the resulting specifications meet the requirements that were intended to be met and that gave rise to the change.
- The implications that the change of specifications has on the user must be established, considering the need to notify them of such modifications.

Modifications to this document will be approved by the Security Committee and the General Management of the Notarial Certification Agency.

9.12.2. Notification period and procedures

A revision of the Certification Practice Statement will be performed with the periodicity defined in section 1.5.5 or when it has to be modified.

The updated versions of the Certification Practices Statement, together with the list of modifications, can be consulted in the Repository indicated in section 2.

9.12.3. Circumstances for the change of the OID

The OID must be changed if the procedure described in section 9.12.1 is modified.

9.13. Dispute Resolution Procedures

The Notarial Certification Agency establishes, in the general conditions of use of certificates, the applicable mediation and conflict resolution procedures.

Discrepancy situations arising from the use of the certificates will be resolved by applying the same competence criteria as in the case of handwritten documents.

9.14. Governing law

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

9.15. Compliance with Applicable Law

The Notarial Certification Agency establishes, in the general conditions of use of certificates, a competent jurisdiction clause, indicating that international judicial competence corresponds to Spanish judges.

Territorial and functional competence is determined by the rules of private international law and procedural law rules that are applicable.

9.16. Miscellaneous Provisions

The Notarial Certification Agency establishes, in the general conditions of use of certificates, clauses of divisibility, survival, full agreement and notification.

9.16.1. Entire Agreement

Under the entire agreement clause, it will be understood that the legal document regulating the service contains the complete will and all the agreements between the parties.

9.16.2. Subrogation

The rights and duties associated with the status of Certification Entity cannot be assigned to third parties of any kind, nor can any third entity be subrogated in the legal position of a Certification Entity.

In case of assignment or subrogation, the aforementioned Certification Entity is terminated.

9.16.3. Severability

Under the divisibility clause, the invalidity of a clause will not affect the rest of the contract.

9.16.4. Applications

Without additional stipulation.

9.16.5. Major cause

As specified in section 9.8.2.

9.17. Other provisions

Without additional stipulation.