Certification Practice Statement

Notarial Certificates

Version: 3.5

Validity: 08/04/2021

ancert

Agencia Notarial de Certificación

General information

Documentary control

Project:	**Certification Practice Statement class Notarial Certificates**
Destination entity:	**Notarial Certification Agency, SLU**
Reference code:	
Version:	**3.5**
Date of the edition:	**24/12/2020**
File:	**DPC_NOT_V2_20210408_EN.docx**
Format:	**Microsoft Word**

Versioning

Version	Change	Description of the change	Date of change	Date of publication
2.1	Creation	Creation of the document.	27/03/2010	
2.2		Revision of the document.	05/05/2010	
2.3	Secure Server Notarial Certificate	Elimination of the reference to the EV clauses for secure server certificates.	05/10/2010	
2.4	Section 1.3.1	Addition of the fingerprints of CA certificates.	06/02/2010	
2.5	Logo ANCERT	New logo ANCERT.	11/30/2010	
2.6		Review of legal issues and format.	12/21/2010	01/01/2011
2.7	Document	Adaptation to the new requirements for the acceptance of code signing certificates in Root CA programs. CRL with 60 days of historical information.	01/30/2011	03/01/2011
2.8	Document	Adequacy of AICPA / CICA controls WebTrust Program for CA v 2	01/06 / 2012	10/01/2012
2.9	Document	Adequacy of protection controls for the private key to the AICPA / CICA WebTrust Program for CA requirements v2.	09/29/2014	03/11/2014
3.0	Document	Adequacy to the requirements of the CA / Browser Forum.	11/24/2015	11/30/2015

3.1	Document	Adequacy of references to Regulation (EU) 910/2014. New certificates for renewed EC. Revision of section 5.8 "End of service". Definition of the maximum time to attend revocation requests. Description of signature algorithms and parameters.	05/04/2017	05/15/2017
3.2	Document	Adaptation to Regulation (EU) 2016/679 (GDPR). Clarification in section 5.1.2 about the identification of test certificates. Update to CA / Browser Forum version 1.5.1 requirements.	05/15/2018	05/25/2018
3.3	Document	Notarial Certificate of Electronic Seal. LOPDP 3/2018.	04/01/2019	03/05/2019
3.4	Document	Adaptation of the structure to RFC 3647. Definition of the CPSs update period and update of the CPS review procedure. Certificate status history information is now provided by OCSP instead of CRL (where only 60 days are kept). Status information in case of compromise or end of service.	02.12.2020	06.04.2020
3.5	Document	Adaptation to Spanish Law 6/2020. CAA records check in SSL certificates issuance moved to section 3.4.2.	24/12/2020	08/04/2021

Index

General information 2
Documentary control 2
Versioning 2
Index 4
1 Introduction 15
1.1 Overview 15
1.1.1 Class of Notarial Certificates 15
1.1.2 Certificates that are issued 15
1.1.2.1 Notarial certificate for natural person 15
1.1.2.2 Notarial Corporate Certificates 16
1.1.2.3 Notarial System Certificates 17
1.2 Document name and identification 18
1.3 PKI participants 20
1.3.1 Certification authorities 20
1.3.1.1 ANCERT Certificados Notariales V2 20
1.3.1.2 ANCERT Certificados Notariales Personales V2 20
1.3.1.3 ANCERT Certificados Notariales Corporativos V2 21
1.3.1.4 ANCERT Certificados Notariales de Sistemas V2 21
1.3.2 Registration Authorities 22
1.3.3 End Entities 22
1.3.3.1 Applicants for certificates 22
1.3.3.2 Certificate Subscribers 23
1.3.3.3 Key Holders 23
1.3.3.4 Represented 24
1.3.3.5 Third Parties who Trust the Certificates 24
1.4 Certificate usage 24
1.4.1 Permitted Uses for Certificates 24
1.4.1.1 Limits of use 25
1.4.1.2 Prohibited uses 25
1.5 Policy Administration 26

1.5.1 Organization that manages the document 26

1.5.2 Contact details of the organization 26

1.5.3 Responsible for the adequacy of the Certification Practice Statement 26

1.5.4 Approval procedure for the Certification Practice Statement 26

1.5.5 Revision frequency 27

1.6 Definitions and acronyms 27

1.6.1 Definitions 27

1.6.2 Acronyms 28

2 Publication and Repository Responsibilities 29

2.1 Repository 29

2.2 Publication of information from the certification service provider 29

2.3 Frequency of publication 29

2.4 Access control 29

3 Identification and authentication 31

3.1 Naming 31

3.1.1 Types of names 31

3.1.2 Meaning of the names 31

3.1.3 Use of anonymous and pseudonymous 31

3.1.4 Interpretation of name formats 31

3.1.4.1 Notarial Certificate for Natural Persons 32

3.1.4.2 Notarial Certificate for the Representation of Natural Persons 32

3.1.4.3 Notarial Certificate for Legal Persons 33

3.1.4.4 Notarial Certificate for the Representation of Legal Persons 33

3.1.4.5 Notarial Certificate for the Representation of Legal Persons AGE 34

3.1.4.6 Notarial Certificate for Secure Server (with / without secure device) 35

3.1.4.7 Notarial Certificate for Timestamping (with / without secure device) 35

3.1.4.8 Notarial Certificate for Code Signing (with / without secure device) 36

3.1.4.9 Notarial Certificate for Secure Application (with / without secure device) 36

3.1.4.10 Notarial Certificate for Electronic Invoicing (without secure device) 37

3.1.4.11 Notarial Certificate for Electronic Seal (with / without secure device) 37

3.1.4.12 Indication of limits of use 38

3.1.4.12.1 Indication of the class of representation 38

3.1.4.12.2 Indication of the limit on the amount of financial transactions 38
3.1.4.12.3 Indication of the limit of use by other reasons 38
3.1.4.13 Indication of additional attributes of the natural person 39
3.1.4.14 Additional information relating to the representation 39
3.1.5 Uniqueness of names 40
3.1.6 Naming conflict resolution and management of registered trademarks 40
3.2 Initial identity validation 40
3.2.1 Proof of possession of the private key 40
3.2.2 Authentication of the identity of the organization 41
3.2.2.1 Required identification elements 41
3.2.2.2 Validation of the identification elements 41
3.2.3 Authentication of the identity of the natural person 41
3.2.3.1 Required identification elements 41
3.2.3.2 Validation of the identification elements 42
3.2.3.3 Need for personal presence 42
3.2.3.4 Binding of the natural person to an entity 42
3.2.4 Authentication of the identity of information systems 43
3.2.4.1 Required identification elements 43
3.2.4.2 Validation of the identification elements 43
3.2.5 Unchecked subscriber information 43
3.3 Identification and authentication for Re-key Requests 43
3.3.1 Validation for the regular renewal of certificates 43
3.3.2 Validation for the renewal of certificates after revocation 43
3.4 Identification and authentication for change of status requests 43
3.4.1 Identification and authentication for suspension requests 43
3.4.2 Identification and authentication of revocation requests 43
4 Certificate Life-Cycle Operational Requirements 45
4.1 Certificate Application 45
4.1.1 Legitimation to of issuance requests 45
4.1.2. Registration procedure: responsibilities. 46
4.2. Certificate Application Processing 46
4.2.1. Identification and authentication 46

4.2.2. Approval or rejection of the application 47

4.2.3. Resolution term to attend the request 47

4.3. Certificate issuance 47

4.3.1. Actions during the issuance process 47

4.3.1.1. Issuance in cryptographic card 48

4.3.1.2. Issuance in hardware cryptographic module or software 48

4.3.2. Notification of the issuance to the subscriber 49

4.4. Certificate Acceptance 49

4.4.1. Conduct constitutive of the acceptance of the certificate 49

4.4.2. Publication of the certificate 50

4.4.3. Notification of the issuance to third parties 50

4.5. Key Pair and Certificate Usage 50

4.5.1. Use by the subscriber and, where appropriate, the key holder 50

4.5.1.1. Obligations of the subscriber and, where appropriate, the key holder 50

4.5.1.2. Civil liability of the subscriber of the certificate 51

4.5.2. Use by third parties who trust the certificates 52

4.5.2.1. Obligations of the third parties that trust the certificates 52

4.5.2.2. Civil liability of the third parties that trust certificates 52

4.6. Certificate Renewal 53

4.7. Certificate Re-key 53

4.7.1. Circumstances of the renewal of the certificate with a change of keys 53

4.7.2. Legitimation to request the renewal 53

4.7.3. Processing the renewal request 53

4.7.4. Notification of the issuance of the renewed certificate 53

4.7.5. Conduct that constitutes acceptance of the certificate 53

4.7.6. Publication of the certificate 53

4.7.7. Notification of the issuance to third parties 54

4.8. Certificate Modification 54

4.9. Certificate Revocation and Suspension 54

4.9.1. Causes of revocation of certificates 54

4.9.2. Legitimation to request the revocation 55

4.9.3. Revocation request procedures 56

4.9.3.1. Revocation request for certificates for Code Signing 56

4.9.4. Time period for the request of revocation 57

4.9.5. Time period to process the revocation requests 57

4.9.6. Obligation to consult certificate revocation information 57

4.9.7. Frequency of issuance of certificate revocation lists (CRLs) 57

4.9.8. Time elapsed between generation and publication of the CRLs 57

4.9.9. Availability of certificate status checking services 57

4.9.10. Online revocation check requirements 58

4.9.11. Other forms of certificate revocation information 58

4.9.12. Special requirements in case of compromise of the private key 58

4.9.13. Causes of suspension of certificates 58

4.9.14. Legitimation to request the suspension 58

4.9.15. Procedures of request of suspension 59

4.9.16. Maximum period of suspension 59

4.9.17. Lifting the suspension 59

4.9.18. Notification of revocation or suspension 59

4.10. Certificate status Services 60

4.10.1. Operational features of the services 60

4.10.2. Availability of services 60

4.10.3. Optional features 60

4.11. End of Subscription 60

4.12. Key Escrow and Recovery 60

4.12.1. Policy and practices for key escrow and recovery 60

4.12.2. Session key encapsulation and recovery policy and practices 60

5. Facility, Management and Operational Controls 62

5.1. Physical security controls 62

5.1.1. Location and construction of facilities 63

5.1.2. Physical access 64

5.1.3. Electricity and air conditioning 64

5.1.4. Exposure to water 64

5.1.5. Fire prevention and protection 64

5.1.6. Media storage 65

5.1.7. Waste treatment 65
5.1.8. Off-site backup copies 65
5.2. Procedural controls 65
5.2.1. Reliable functions 65
5.2.2. Number of people per task 66
5.2.3. Identification and authentication for each function 67
5.2.4. Roles that require separation of tasks 67
5.3. Personnel controls 67
5.3.1. History, qualifications, experience and authorization requirements 67
5.3.2. History investigation procedures 68
5.3.3. Training requirements 68
5.3.4. Requirements and frequency of training update 69
5.3.5. Sequence and frequency of job rotation 69
5.3.6. Sanctions for unauthorized actions 69
5.3.6.1. Disciplinary procedure 69
5.3.6.2. Unauthorized activities 70
5.3.7. Requirements for hiring professionals 71
5.3.8. Provision of documentation to staff 72
5.4. Audit Logging Procedures 72
5.4.1. Types of registered events 72
5.4.2. Review period for audit logs 73
5.4.3. Retention period of audit records 73
5.4.4. Protection of audit logs 73
5.4.5. Backup procedures for audit logs 74
5.4.6. Log aggregation system 74
5.4.7. Notification of the audit event 74
5.4.8. Vulnerability Analysis 74
5.5. Records Archival 74
5.5.1. Types of archived records 74
5.5.2. Record retention period 75
5.5.3. Archive protection 75
5.5.4. Backup procedures 75

5.5.5. Timestamping requirements 76

5.5.6. Archive system 76

5.5.7. Procedures for obtaining and verifying archival information 76

5.6. Key Changeover 76

5.7. Compromise and Disaster Recovery 76

5.7.1. Incident management procedures 76

5.7.2. Corruption of resources, applications or data 77

5.7.3. Procedure in case of compromise of the private key 77

5.7.3.1. Revocation of the public key of the entity 77

5.7.3.2. Compromise of the private key of the entity 77

5.7.4. Business continuity after a disaster 78

5.8. CA or RA Termination 78

6. Technical security controls 80

6.1. Key pair generation and installation 80

6.1.1. Generation of the key pair 80

6.1.2. Delivery of the private key to the subscriber 80

6.1.3. Delivery of the public key to the certificate issuer 80

6.1.4. Distribution of the public key of the certification service provider 80

6.1.5. Key sizes 81

6.1.6. Generation of public key parameters and quality verification 81

6.1.7. Key Usage 81

6.2. Private Key Protection and Cryptographic Module Engineering Controls 81

6.2.1. Cryptographic modules standards 81

6.2.2. Control of the private key by more than one person (n of m) 81

6.2.3. Private key escrow 82

6.2.4. Backup copy of the private key 82

6.2.5. Private key archiving 82

6.2.6. Transfer of the private key to or from the cryptographic module 82

6.2.7. Storage of the private key in the cryptographic module 82

6.2.8. Private key activation method 83

6.2.9. Private key deactivation method 83

6.2.10. Destruction method of the private key 83

6.2.11. Classification of cryptographic modules 83

6.3. Other aspects of key pair management 83

6.3.1. Public key archiving 83

6.3.2. Periods of use of public and private keys 84

6.4. Activation data 84

6.4.1. Generation and installation of activation data 84

6.4.2. Protection of activation data 84

6.4.3. Other aspects of activation data 84

6.5. Computer security controls 84

6.5.1. Specific technical requirements for computer security 84

6.5.2. Assessment of the level of computer security 85

6.6. Life Cycle security controls 85

6.6.1. Systems Development Controls 85

6.6.2. Security management controls 85

6.6.3. Life cycle security controls 85

6.7. Network security controls 86

6.8. Timestamping 86

7. Certificate, CRL and OCSP Profiles 86

7.1. Certificate Profile 86

7.1.1. Version Number 87

7.1.2. Certificate extensions 87

7.1.3. Identifiers algorithm object 87

7.1.4. Name formats 87

7.1.5. Name restrictions 87

7.1.6. Object Identifier of the certificate policy 87

7.1.7. Use of the extension for policy restrictions 87

7.1.8. Syntax and semantics of policy qualifiers 87

7.1.9. Semantics of the certificate policy extension 88

7.2. CRL Profile 88

7.2.1. Version number 88

7.2.2. Certificate revocation list and extensions 88

7.3. OCSP profile 88

7.3.1. Version number 88
7.3.2. OCSP extensions 88
8. Compliance audit and other assessments 89
8.1. Frequency 89
8.2. Identification and qualification of the auditor 89
8.3. Relationship between the auditor and the auditee 89
8.4. List of elements to be audited 89
8.5. Actions to be taken as a result of a lack of conformity 89
8.6. Communication of the results 90
9. Other Business and Legal Matters 91
9.1. Fees 91
9.1.1. Fee for the issuance or renewal of certificates 91
9.1.2. Fee for the access to the certificates 91
9.1.3. Fee for access to certificate status information 91
9.1.4. Fees for other services 91
9.1.5. Refund Policy 91
9.2. Financial responsibility 91
9.2.1. Insurance coverage 91
9.2.2. Other assets 91
9.2.3. Insurance coverage for subscribers and third parties who trust the certificates 92
9.3. Confidentiality of Business Information 92
9.3.1. Scope of confidential information 92
9.3.2. Non-confidential information 92
9.3.3. Responsibility to protect confidential information 93
9.3.3.1. Disclosure of suspension and revocation information 93
9.3.3.2. Legal disclosure of information 93
9.3.3.3. Disclosure of information at the request of the owner 93
9.3.3.4. Other circumstances for the disclosure of information 93
9.4. Privacy of Personal Information 93
9.5. Intellectual property rights 95
9.5.1. Ownership of certificates and revocation information 95
9.5.2. Ownership of the certificate policies and the Certification Practices Statement 96

9.5.3. Ownership of information related to names 96
9.5.4. Key Ownership 96
9.6. Representations and Warranties 96
9.6.1. Model of obligations of the service provider 96
9.6.2. Guarantees offered to subscribers and third parties who trust the certificates 97
9.7. Disclaimer of Warranties 98
9.8. Limitation of Liability 98
9.8.1. Limitation of liability of the Certification Authority 98
9.8.2. Fortuitous events and force majeure 99
9.9. Indemnity clauses 99
9.9.1. Indemnity clauses for the subscriber 99
9.9.2. Indemnity clause for third parties that trust the certificates 99
9.10. Term and Termination 100
9.10.1. Effective starting date 100
9.10.2. Ending date 100
9.10.3. Effect of termination and survival 100
9.11. Individual notices and communications with participants 100
9.12. Amendments 100
9.12.1. Procedure for modifications 100
9.12.2. Notification period and procedures 100
9.12.3. Circumstances for the change of the OID 101
9.13. Dispute Resolution Procedures 101
9.14. Governing law 101
9.15. Compliance with Applicable Law 101
9.16. Miscellaneous provisions 101
9.16.1. Entire Agreement 101
9.16.2. Subrogation 101
9.16.3. Severability 102
9.16.4. Applications 102
9.16.5. Major cause 102
9.17. Other provisions 102

1 Introduction

This document contains the Declaration of Certification Practices that regulates the class of certificates “Notarial Certificates”, issued by the Notarial Certification Agency.

1.1 Overview

1.1.1 Class of Notarial Certificates

The "Notarial Certificates" groups all the certificates issued by the Notarial Certification Agency to the public, acting a Notary as the Registration Entity, thus providing the highest level of legal assurance.

1.1.2 Certificates that are issued

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

1.1.2.1 Notarial certificate for natural person

Notarial Certificates for natural person 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 two types of Notarial Certificates:

- **Notarial Certificate for natural person**: certificate issued to natural persons acting on their own behalf.
- **Notarial Certificate for the representation of natural person:** certificate issued to natural person in representation of another natural person.

The Notarial certificates for natural persons allow 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.

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, 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.

Notarial Certificates for natural person 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 Notarial Corporate Certificates

Notarial Corporate 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.

Notarial certificates of electronic seal are qualified electronic seals, under the terms of article 38 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 four types of Notarial Corporate Certificates:

- **Notarial Certificate for Legal Person**, issued to legal persons or entities without legal personality, with identification of a natural person who acts as custodian of the certificate, in accordance with the provisions of article 7, and the additional provision third of Law 59/2003, on Electronic Signature.
- **Notarial Certificate for the representation of Legal Person**, issued to legal persons, with identification of a natural person who acts as representative of the legal person. The AGE Notarial Certificate for the representation of Legal Person is a type of certificate whose profile follows the specifications of Annex 1 of the document "Electronic Certificate Profiles", dated April 2016, published by the Ministry of Finance and Public Administrations of the Government of Spain.
- **Notarial Certificate for Electronic Invoicing,** issued to natural or legal persons for electronic invoicing or to provide electronic invoicing services to third parties.
- **Notarial Certificate for Electronic Seal**, issued to legal persons for the creation of advanced or qualified electronic seals.

The Notarial Certificates Persons of electronic signature for Legal Person and for the representation of Legal allow three functionalities, using a single Certificate for each one of them:

- 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.

The Notarial Certificates for Electronic Invoicing allow a single use of the certificate, the signing of invoices.

The Notarial Certificates for Electronic Seal allow the creation of qualified or advanced electronic seals depending on whether a qualified creation device is used or not.

The Notarial Certificates for Legal Person can only be used, by mandate of article 7 of Law 59/2003 of Electronic Signature, in the context of Public Administration services and in the contracting of goods or services necessary for the entity's core business activity or other administrative activities such as the contracting of tangible and intangible supplies or auxiliary services.

Notarial Certificates for Legal Person issued to entities without a legal entity are issued for the sole purpose of use in communications and data transmission with the State Tax Administration Agency and with other public tax authorities, according to the 3rd additional provision of Law 59/2003 of 19 December and the Order EHA/3256/2004 of September 30, issued by the Ministry of Economy and Finance, which establishes the terms in which electronic certificates may be issued to entities without legal personality as referred to in article 35.4 of the General Tax Law.

With the entry into force of Regulation (EU) 910/2014 on July 1, 2016, from that date on, no new Notarial Certificates of Legal Person have been issued.

Qualified signature creation devices are used as support for the three certificates for electronic signature with secure device guarantee, under the terms of article 29 of Regulation (EU) 910/2014.

Qualified electronic seal creation devices are used as support for electronic seal certificates with secure device guarantee, under the terms of article 39 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.

Notarial Corporate 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 Notarial System Certificates

Notarial System Certificates provide security for information system and communications. These certificates are not considered qualified certificates, in accordance with Regulation (EU) 910/2014.

There are five types of Notarial System Certificates:

- **Notarial System Certificates for Secure Server**, which are issued to natural or legal persons, as owners of SSL servers, in order to establish secure communications between the server and SSL/TLS client .
- **Notarial System Certificates for Timestamping,** which are issued to natural or legal persons, as owners of timestamping servers.
- **Notarial System Certificates for code signing**, which are issued to individuals or legal entities, as editors of source code for public distribution.
- **Notarial System Certificates for secure application**, which are issued to natural or legal persons, as owners of software applications requiring authentication, digital signature or encryption features.
- **Notarial System Certificates for OCSP Trusted Responder**, which are issued to natural or legal persons, as owners of OCSP servers.

All functionalities of each Notarial System Certificate are contained in a single certificate in various types of security modules, including cryptographic equipment.

Notarial System Certificates are issued in adherence and compliance with the requirements defined by the CA/Browser Forum 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 "Notarial Certificates” and has been assigned the following OID: ANCERT.0.1.0.2

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
Notarial Certificate for natural person (signature)	ANCERT.1.1.1.2.1
Notarial Certificate for natural person (authentication)	ANCERT.1.1 .1.2.2
Notarial Certificate for natural person (encryption)	ANCERT.1.1.1.2.3
Notarial Certificate for the representation of natural person (signature)	ANCERT.1.1.2.2.1
Notarial Certificate for the representation of natural person (authentication)	ANCERT.1.1.2.2.2
Notarial Certificate for the representation of natural person (encryption)	ANCERT.1.1.2.2.3

Notarial System Certificate for Secure Server (with SSCD)	ANCERT.1.2.1.2.1
Notarial System Certificate for Secure Server (without SSCD)	ANCERT.1.2.1.2.2
Notarial System Certificate for Timestamp (with SSCD)	ANCERT.1.2.3.2.1
Notarial System Certificate for Timestamp (without SSCD)	ANCERT.1.2.3.2.2
Notarial System Certificate for code signing (with SSCD)	ANCERT.1.2.5.2.1
Notarial System Certificate for code signing (without SSCD)	ANCERT.1.2.5.2.2
Notarial System Certificate for secure application (with SSCD)	ANCERT.1.2.6.1 .1
Notarial System Certificate for secure application (without SSCD)	ANCERT.1.2.6.1.2
Notarial System Certificate for OCSP Trusted Responder (without SSCD)	ANCERT.1.2.7.1.2
Notarial Certificate for Legal Person (signature)	ANCERT.1.3.1.2.1
Notarial Certificate for Legal Person (authentication)	ANCERT.1.3.1.2.2
Notarial Certificate for Legal Person (encryption)	ANCERT.1.3.1.2.3
Notarial Certificate for the representation of Legal Person (signature)	ANCERT.1.3.2.2.1
Notarial Certificate for the representation of Legal Person (authentication)	ANCERT .1.3.2.2.2
Notarial Certificate for the representation of Legal Person (encryption)	ANCERT. 1.3.2.2.3
Notarial Certificate for the representation of Legal Person AGE (signature)	ANCERT. 1.3.2.3.1
Notarial Certificate for the representation of Legal Person AGE (authentication)	ANCERT. 1.3. 2.3.2
Notarial Certificate for Electronic Invoicing (without SSCD)	ANCERT 1.3.3.1.2
Notarial Certificate for Electronic Seal (with SSCD)	ANCERT 1.3.4.1.1

Notarial Certificate for Electronic Seal (without SSCD)	ANCERT.1.3.4.1.2

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 the general public by the Notarial Certification Agency with Notarial intervention.

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 “Notarial Certificates”, the Notarial Certification Agency sets the following Certification Entities.

1.3.1.1 ANCERT Certificados Notariales V2

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

```
CN =ANCERT Certificados Notariales V2
Validity period: 05/25/2010 to 05/25/2030
Summary: 4BE8B5A1C76C6AEAD0611918FCCF9DBD398B67FB12294758BDF994D0F9682F60
```

ANCERT Certificados Notariales V2 issues certificates for the following subordinate Certification Entities:

- ANCERT Certificados Notariales Personales V2.
- ANCERT Certificados Notariales Corporativos V2.
- ANCERT Certificados Notariales de Sistemas V2.

1.3.1.2 ANCERT Certificados Notariales Personales V2

This subordinate Certification Entity issues electronic certificates for natural persons and for the representation of natural persons.

The digital footprint of this subordinate Certification Entity with SHA-256 algorithm is:

```
CN =ANCERT Certificados Notariales Personales V2
Validity period: 27/05/2020 to 27/05/2010
```

```
Summary: A6A176268AE84BAC15DE7289AB6F5C7BDAB75B2EB864C33908074034C9B5DABA


CN =ANCERT Certificates Personal Notariales V2

Validity period: 25/10/2030 21/06/2016 to the

Summary: C4472508C3BC689FC59E8BF77A6DDEDFBB29A43316BD0946D544E54DFC001535
```

1.3.1.3 ANCERT Certificados Notariales Corporativos V2

This subordinate Certification Entity issues electronic certificates for legal persons, for the representation of legal persons, for electronic seals and for electronic invoicing.

The fingerprint of this subordinate Certification Entity based on SHA-256 algorithm is:

```
CN =ANCERT Certificados Notariales Corporativos V2

Validity period: 27/05/2020 27/05/2010 to the

Summary: 88C2BF64188E40B821A5990F29D822F219706EA6790500F376CE8E4DF2EA3E07


CN =ANCERT Certificados Notariales Corporativos V2

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

Summary:  0CA8B7A01506CAFAA1879E7491C662F8264EB3A2F1F0E0657DA3D6A912FF1487
```

1.3.1.4 ANCERT Certificados Notariales de Sistemas V2

This subordinate Certification Entity issues the following certificates:

- Notarial System Certificate for Secure Server
- Notarial System Certificate for Timestamping
- Notarial System Certificate for Code Signing
- Notarial System Certificate for Secure Application
- Notarial System Certificate for OCSP Trusted Responder

The fingerprint of this subordinate Certification Entity based on the SHA-256 algorithm is:

```
CN =ANCERT Certificados Notariales de Sistemas V2

Validity period: 05/27/2010 to 05/27/2020

Summary: B89EE1F6E629A5ADF95E317F7ECC485A424BEF06BCD4055E6251BC61BD8A5CF4


CN = ANCERT Certificados Notariales de Sistemas V2

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

Summary: 186B5083F6CBE72E94172B57424B0DB7F0F58B2BAE8D7A9C946A4BBB5B4FD7F0
```

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.

For the class of Notarial Certificates, a Spanish Notary always acts as the Registration Authority.

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, 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 the class Notarial Certificates, the applicants are:

- **Notarial Certificates for natural persons:** a natural person who acts in his own name.
- **Notarial Certificates for the representation of natural persons**: a natural person who acts as a legal or voluntary representative of another natural person.
- **Notarial Certificates for legal persons**: a natural person, who acts as a legal or voluntary representative of a legal person or entity without legal personality, or the board of the legal person.
- **Notarial Certificates for the representation of legal persons**: a natural person, who acts as a legal or voluntary representative of a legal person. This natural person will be able to request a certificate for himself or, within the scope of his representation, to request a certificate for other natural persons to whom have previously been delegated (by public document) all or some of the faculties of the applicant.
- **Notarial Certificates for electronic invoicing:** a natural person, who acts in his own name or as the legal or voluntary representative of a legal person or entity without legal personality.
- **Notarial Certificates for electronic seals:** a natural person, who acts as a legal or voluntary representative of a legal person or entity without legal personality, or the board of the legal person.

- **Notarial Certificates for secure servers**: a natural person, who acts in his own name or as a legal or voluntary representative of a legal person.
- **Notarial Certificates for timestamping**: a natural person, who acts in his own name or as a legal or voluntary representative of a legal person.
- **Notarial Certificates for code signing**: a natural person, who acts in his own name or as a legal or voluntary representative of a legal person.
- **Notarial Certificates for secure applications:** a natural person, who acts in his own name or as a legal or voluntary representative of a legal person.
- **Notarial Certificates for OCSP trusted responders**: a natural person, who acts in his own name or as a legal or voluntary representative of a legal person.

1.3.3.2 Certificate Subscribers

Subscribers are the individuals and organizations acting as holders of the certificate.

For the class Notarial Certificates, the subscribers are:

- **Notarial Certificates for natural persons:** the natural person identified in the certificate.
- **Notarial Certificates for the representation of natural persons**: the natural person identified in the certificate as the representative.
- **Notarial Certificates for legal persons:** the legal person identified in the certificate.
- **Notarial Certificates for the representation of legal persons**: the legal person identified in the certificate.
- **Notarial Certificates for electronic invoicing:** the natural or legal person identified in the certificate.
- **Notarial Certificates for electronic seals:** the legal person identified in the certificate.
- **Notarial Certificates for secure servers**: the natural or legal person identified in the certificate.
- **Notarial Certificates for timestamping**: the natural or legal person identified in the certificate.
- **Notarial Certificates for code signing**: the natural or legal person identified in the certificate.
- **Notarial Certificates for secure applications:** the natural or legal person identified in the certificate.
- **Notarial Certificates for OCSP trusted responders**: the natural or 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.

Only Notarial Certificates for legal persons use the notion of key holder, which are:

- **Notarial Certificates for legal persons:** the natural person who acts as custodian.
- **Notarial Certificates for the representation of legal persons**: the natural person who acts as representative.
- **Notarial Certificates for electronic invoicing**: the natural person who acts as custodian.
- **Notarial Certificates for electronic seals:** the natural person who acts as custodian.

1.3.3.4 Represented

Natural or legal persons in whose name the applicants request Notarial Certificates for the representation of natural persons or for the representation of legal persons, are considered as represented.

The identification of the natural or legal person represented is included within the certificate, in accordance with section 3 of this Certification Practice Statement.

1.3.3.5 Third Parties who Trust the Certificates

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

As a previous step to trust the 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 class Notarial Certificates 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 Notarial Certificates can be used for the uses described in section 1.1.2 of this Certification Practice Statement.

In relation to 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.
- **Server Authenticity**: Ensures that electronic communication comes from the server who claims to be from. The user can verify the authenticity of the server 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 Certification Practice Statement and must 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 existing in each moment.

Certificates may contain additional limits of use in the form of attributes within the field *Subject Directory Attributes*, as indicated in section 3.1.4 of this Certification Practice Statement, as well as in the general conditions of use of certificates. Third parties should consider these limitations before relying on certificates.

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

1.4.1.2 Prohibited uses

Notarial 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 when expressly permitted.

Notarial Certificates for code signing can not be used to sign any code that might be considered malicious (including in this term "spyware" and "malware") that can be downloaded by a user on his computer without his consent.

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 Certification Practice Statement can be modified at any time by the Notarial Certification Agency. Those subscribers with a valid certificate who do not accept the changes may ask for the revocation of their certificates.

The revocation so requested shall not give the right to claim any compensation, not even the partial refund of the price of the certificate, unless the rectification or modification of the

Certification Practice Statement implies a limitation of the rights of use or a restriction on the scope of application on the certificate, in which case the refund may be requested.

1.5.5 Revision frequency

The Certification Practice Statement and the informative texts 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 Practice Statement.

2.2 Publication of information from 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 certificate revocation status information will be published in accordance with the provisions of sections 4.9.7 and 4.9.9 of this Certification Practice Statement.

2.4 Access control

The Notarial Certification Agency does not limit reading access to the information described 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, mainly in the field *Subject Directory Attributes.*

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. The use of pseudonyms is only allowed in Notarial Certificates for Electronic Invoicing.

3.1.4 Interpretation of name formats

The Notarial Certification Agency uses the following name schemes, for each of the following certificates. The name components’ maximum length should be the upper bounds defined in the ITU-T X.509 recommendation.

3.1.4.1 Notarial Certificate for Natural Persons

SUBJECT NAME	
FIELD	**CONTENT**
Country (C)	Country (nationality of the identified natural person, indicating the code of two letters specified in ISO 3166)
Organizational Unit (OU)	"Autorizado ante Notario" + Notary Identification
Organizational Unit (OU)	"Certificado Notarial Personal (" + "Signature" or "Authentic" or "Encryption" + ")"
Surname (SU)	Surname of the identified natural person.
Given Name (GN)	Name of the identified natural person.
Serial Number (SN)	NIF (of the identified natural person, for the purpose of the admission by the Spanish Administrations)
Common Name (CN)	Name and surname of the identified natural person.
SUBJECT ALTERNATIVE NAME	
rfc822Name	Email of the identified natural person.
SUBJECT DIRECTORY ATTRIBUTES	
dateOfBirth	Date of birth.
CountryOfCitizenship	Nationality of the subscriber.
ANCERT.10.1.4	Additional circumstances of the natural person

3.1.4.2 Notarial Certificate for the Representation of Natural Persons

SUBJECT NAME	
FIELD	**CONTENT**
Country (C)	Country (nationality of the identified natural person, indicating the two letter code specified in ISO 3166)
Organizational Unit (OU)	"Autorizado ante Notario" + Notary Identification
OrganizationalUnit (OU)	"Certificado Notarial de Representación Personal (" + "Signature" or "Authentic" or "Encryption" + ")"
Title	Representative Role or function
Surname (SU)	Surname of the identified natural person.
Given Name (GN)	Name of the identified natural person.
Serial Number (SN)	NIF (of the identified natural person, for the purpose of the admission by the Spanish Administrations)
Common Name (CN)	Name and surname of the identified natural person.
SUBJECT ALTERNATIVE NAME	
rfc822Name	Email of the identified natural person.
SUBJECT DIRECTORY ATTRIBUTES	

DateOfBirth	Date of birth.
CountryOfCitizenship	Nationality of the subscriber.
ANCERT.10.1.1	Level of representation.
ANCERT.10.1.3	Document of representation.
ANCERT.10.1.4	Additional attributes of the natural person.
ANCERT.10.1.5	Limit of use.
ANCERT.10.1.6	Registry data of the representation.
ANCERT.10.1.7	Represented person (natural person)

3.1.4.3 Notarial Certificate for Legal Persons

SUBJECT NAME	
FIELD	**CONTENT**
Country (C)	Country (nationality of the identified natural person, indicating the two letter code specified in ISO 3166)
Organization (O)	Name of the subscriber entity.
Organizational Unit (OU)	"Autorizado ante Notario" + Notary Identification
Organizational Unit (OU)	"Certificado Notarial Corporativo (" + "Signature" or "Authentic" or "Encryption" + ")"
Title	Role or function of the custodian.
Surname (SU)	Surname of the custodian.
Given Name (GN)	Name of the custodian.
OID "1.3.6.1.4.1.18838.1.1"	NIF of the custodian (NIF of the identified natural person, for the purpose of the admission by the Spanish Administrations)
Serial Number	NIF of the subscriber entity.
Common Name (CN)	Name of the subscriber entity.
SUBJECT ALTERNATIVE NAME	
Rfc822Name	Email.
SUBJECT DIRECTORY ATTRIBUTES	
dateOfBirth	Date of birth.
CountryOfCitizenship	Nationality of the subscriber.
ANCERT.10.1.1	Level of representation.
ANCERT.10.1.3	Document of representation.
ANCERT.10.1.5	Limit of use.
ANCERT.10.1.6	Registry data of the representation.

3.1.4.4 Notarial Certificate for the Representation of Legal Persons

SUBJECT NAME

FIELD	CONTENT
Country (C)	Country (nationality of the identified natural person, indicating the two-letter code specified in ISO 3166)
Organization (O)	Name of the suscriber entity.
Organizational Unit (OU)	"Autorizado ante Notario" + Notary Identification
Organizational Unit (OU)	"Certificado Notarial Corporativo de Representación (" + "Signature" or "Authentic" or "Encryption" + ")"
Title	Role or function of the custodian.
Surname (SU)	Surname of the representative natural person.
Given Name (GN)	Name of the representative natural person.
Serial Number (SN)	NIF of the representative (of the identified natural person, for the purpose of the admission by the Spanish Administrations)
Common Name (CN)	Name and surname of the representative.
SUBJECT ALTERNATIVE NAME	
Rfc822Name	Email.
SUBJECT DIRECTORY ATTRIBUTES	
ANCERT.10.1.1	Class of representation.
ANCERT.10.1.3	Document of representation.
ANCERT.10.1.4	Additional circumstances of the natural person.
ANCERT.10.1.5	Limit of use.
ANCERT.10.1.6	Registry data of the representation.
ANCERT.10.1.7	Represented person (legal person)

3.1.4.5 Notarial Certificate for the Representation of Legal Persons AGE

SUBJECT NAME	
FIELD	**CONTENT**
Description (2.5.4.13)	Public document that accredits the power of attorney of the representative or the registry data. In the Company Registry: Reg: XXX / Sheet: XXX / Volume: XXX / Section: XXX / Book: XXX / Folio: XXX / Date: dd-mm-yyyy / Registration: XXX Power of Attorney: Notary: Name Surname1 Surname2 / Num Protocol: XXX / Date: dd-mm-yyyy If the representation provides from Official Bulletins: Bulletin: XXX / / Date: dd-mm-yyyy / Resolution number: XXX
Country (C)	Country (nationality of the identified natural person, indicating the two-letter code specified in ISO 3166)

Organization (O)	Business Name, as it appears in Registry data.
Organization Identifier (2.5.4.97)	NIF of the represented entity (using the semantics proposed by ETSI standard EN319 412-1)
Organizational Unit (OU)	"Autorizado ante Notario" + Notary Identification
Organizational Unit (OU)	"Certificado Notarial Corporativo de Representación (" + "Signature" or "Authentic" or "Encryption" + ")"
Surname (SU)	Surname of the representative natural person (as stated in the DNI / NIE).
Given Name (GN)	Name of the representative natural person (as stated in the DNI / NIE).
Serial Number (SN)	DNI / NIE of the representative (using the semantics proposed by ETSI EN319 412-1 standard)
Common Name (CN)	DNI / NIE Name Surname1 (R: NIF) AUTENTIC / FIRMA
SUBJECT ALTERNATIVE NAME	
Rfc822Name	Email.

3.1.4.6 Notarial Certificate for Secure Server (with / without secure device)

SUBJECT NAME[2]	
FIELD	**CONTENT**
Country (C)	Country (nationality of the identified natural person, indicating the two letter code specified in the ISO 3166 standard)
Organization (O)	Name of the subscriber entity.
Organizational Unit (OU)	"Autorizado ante Notario" + Notary Identification
Organizational Unit (OU)	"Certificado Notarial de Servidor Seguro"
Surname (SU)	Surname of the subscriber natural person.
Given Name (GN)	Name of the subscriber natural person.
Serial Number (SN)	CIF or NIF of the subscriber natural person or entity.
Common Name (CN)	Name of the server and domain. (optional)
SUBJECT ALTERNATIVE NAME	
Rfc822Name	Email.
DnsName	Name of the server and domains.

3.1.4.7 Notarial Certificate for Timestamping (with / without secure device)

SUBJECT NAME[3]	
FIELD	**CONTENT**

[2] The name components' maximum length shall be the one defined in RFC 5280.

[3] The name components' maximum length shall be the one defined in RFC 5280.

Country (C)	Country (nationality of the identified natural person, indicating the two letter code specified in ISO 3166)
Organization (O)	Name of the suscriber entity.
Organizational Unit (OU)	"Autorizado ante Notario" + Notary Identification
Organizational Unit (OU)	"Certificado Notarial de Sello de Tiempo"
StampSurname (SU)	Surname of the subscriber natural person.
Given Name (GN)	Name of the subscriber natural person.
Serial Number (SN)	CIF or NIF of the subscriber natural person or entity.
Common Name (CN)	Name of the time stamping authority.
SUBJECT ALTERNATIVE NAME	
rfc822Name	Email of the identified natural person.

3.1.4.8 Notarial Certificate for Code Signing (with / without secure device)

SUBJECT NAME[4]	
FIELD	**CONTENT**
Country (C)	Country (nationality of the identified natural person, indicating the two-letter code specified in ISO 3166)
Organization (O)	Name of the suscriber entity.
Organizational Unit (OU)	"Autorizado ante Notario" + Notary Identification
Organizational Unit (OU)	"Certificado Notarial de Firma de Código"
Surname (SU)	Surname of the subscriber natural person.
Given Name (GN)	Name of the subscriber natural person.
Serial Number (SN)	CIF or NIF of the subscriber natural person or entity.
Common Name (CN)	Name of the code editor.
SUBJECT ALTERNATIVE NAME	
rfc822Name	Email of the identified natural person.

3.1.4.9 Notarial Certificate for Secure Application (with / without secure device)

SUBJECT NAME	
FIELD	**CONTENT**
Country ©	Country (nationality of the identified natural person, indicating the two letter code specified in the ISO 3166 standard)
Organization (O)	Name of the suscriber entity.
Organizational Unit (OU)	"Autorizado ante Notario" + Notary Identification

[4] The name components' maximum length shall be the one defined in RFC 5280.

Organizational Unit (OU)	"Certificado Notarial Certificate de Aplicación Segura"
Surname (SU)	Surname of the subscriber natural person.
Given Name (GN)	Name of the subscriber natural person.
Serial Number (SN)	CIF or NIF of the subscriber natural person or entity.
Common Name (CN)	Identification of the secure application.
SUBJECT ALTERNATIVE NAME	
rfc822Name	Email of the identified natural person.

3.1.4.10 Notarial Certificate for Electronic Invoicing (without secure device)

SUBJECT NAME	
FIELD	**CONTENT**
Country (C)	Country (nationality of the identified natural person, indicating the two letter code specified in ISO 3166)
Organization (O)	Name of the subscriber entity or natural person.
Organizational Unit (OU)	"Autorizado ante Notario" + Notary Identification
Organizational Unit (OU)	"Certificado Notarial de facturación electrónica"
Pseudonym	Pseudonym: Custodian of the certificate for invoicing.
Serial Number (SN)	CIF or NIF of the subscriber individual or entity.
Common Name (CN)	Name of the subscriber entity.
SUBJECT ALTERNATIVE NAME	
Rfc822Name	Email.

3.1.4.11 Notarial Certificate for Electronic Seal (with / without secure device)

SUBJECT NAME	
FIELD	**CONTENT**
Country (C)	Country (nationality of the identified natural person, indicating the two letter code specified in ISO 3166)
Organization (O)	Company name, as it appears in the Registry data.
Organization Identifier (2.5.4.97)	CIF of the subscriber entity (using the semantics proposed by ETSI standard EN319 412-1)
Organizational Unit (OU)	"Autorizado ante Notario" + Notary Identification
Organizational Unit (OU)	"Certificado Notarial Corporativo de Sello Electrónico"
Common Name (CN)	Name used to refer to the subscriber entity (it may not match exactly the company name)
SUBJECT ALTERNATIVE NAME	
Rfc822Name	Email.

3.1.4.12 Indication of limits of use

3.1.4.12.1 Indication of the class of representation

This limit of use is contained in the attribute ANCERT.10.1.1, within the field *Subject Directory Attributes* of the following certificates:

- Notarial Certificate for the Representation of Natural Persons.
- Notarial Certificate for Legal Persons.
- Notarial Certificate for the Representation of Legal Persons.

This limit of use corresponds to the level of guarantee in relation to the representation, also indicating the absence of guarantee with respect to the representation for a natural person, with the following possibilities:

- "No guarantee", which is used to indicate that the Certificate is issued without having verified if the person has any power of attorney to act.
- "Limited powers", which is used to indicate that the certificate is issued having verified that the person has some power of attorney to act. In this case, ANCERT.10.1.5 attribute on limit of use must be used, which includes the power of attorney by reference.
- "General Powers", which is used to indicate that the certificate is issued having verified that the person has all the general powers of attorney, either for being a legal or organic representative, or for being a voluntary representative with general powers to act.

3.1.4.12.2 Indication of the limit on the amount of financial transactions

This limit of use limit is contained in the attribute *QcEuLimitValue* within the extension *Qualified Certificate Statements* of the following certificates:

- Notarial Certificate for the Representation of Natural Persons.
- Notarial Certificate for Legal Persons.
- Notarial Certificate for the Representation of Legal Persons.
- Notarial Certificate for Electronic Invoicing.

The limit of amount limit is encoded according to the definition in the specification ETSI TS 101 862, including the following fields:

- Currency, according to norm ISO 4217.
- Amount.
- Exponent.

The limit value is calculated using the following formula:: Value = Amount × 10^{Exponent}

3.1.4.12.3 Indication of the limit of use by other reasons

This limit of use is contained in the attribute ANCERT.10.1.5 within the field *Subject Directory Attributes* of the following certificates:

- Notarial Certificate for the Representation of Natural Persons.
- Notarial Certificate for Legal Persons.
- Notarial Certificate for the Representation of Legal Persons.
- Notarial Certificate for Electronic Invoicing.
- Notarial Certificates for Secure Application.
- Notarial Certificate for Timestamping.

This attribute is always used when the attribute ANCERT.10.1.1 has the value "Poderes limitados".

Applies to any limits of use of the certificate (it is understood that different from the limit of amount), expressed as a URL that contains the list of powers of attorney /faculties of the representative.

3.1.4.13 Indication of additional attributes of the natural person

Notarial Certificates can incorporate additional attributes of the requesting natural person, such as: membership of a professional college, honorary positions, etc ...) within the attribute ANCERT.10.1.4 of *Subject Directory Attributes*.

3.1.4.14 Additional information relating to the representation

Certificates including any representation contain the following specific information, which are contained in attributes within the field *Subject Directory Attributes*:

The representation document is contained in the attribute ANCERT.10.1.3.

This attribute includes the name and surname of the authorizing Notary of the representation document, as well as the number and year of the corresponding protocol in case of power of attorney, or to the Entity or granting Body, if this representation is not derived from a power of attorney.

The attribute ANCERT.10.1.6 contains the registry data of the representation.

This attribute contains information relating to the registration of the deed or legal information about the appointment of the representative, registered in the legal or administrative registry corresponding to the natural or legal person, when it was mandatory.

The attribute ANCERT.10.1.7 contains the identification of the represented person.

This attribute includes a distinguished name attribute formed by a combination of the following components:

- When the represented is a natural person:
    - Country.
    - Surname.
    - Given Name.
    - Serial Number.

- When the represented is a legal person:
    - Country.
    - Organization.
    - Serial Number.

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

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 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 establishes reasonable controls to ensure that applicants for a certificate have rights over the trademarks included in a certificate request by consulting the database of the Spanish Patent and Trademark Office.

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

In any case, the Notarial Certification Agency reserves the right to reject a certificate request due to name conflict.

3.2 Initial identity validation

This section declares the identification and authentication procedures that must be used during the registration of subscribers, including entities and individuals, which must 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

In general, supporting documentation must be provided by the applicant regarding the following points:

- Full legal name of the organization.
- Legal status of the organization.
- Tax identification number.
- Registry identification data.

3.2.2.1 Required identification elements

The document necessary to prove to the Notary the identity of the legal person is the deed of constitution or, in the case of organizations whose constitution does not require a deed, any public document proving the identity of the organization .

3.2.2.2 Validation of the identification elements

The role of Registration Entity is assumed by a Spanish Notary, in charge of checking the supporting documentation provided by the applicant.

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 a Spanish notary, who acts as the registration entity.

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 other lawful means, provided that it contains at least the following information:

- Name and surname.
- Birthdate.
- Tax Identity Number (NIF or, where appropriate, NIE)

In the case of Notarial Certificates of Personal Representation, it is also necessary to accredit the applicant as a representative of another natural person, deed, public document or, if applicable judicial or administrative resolution from where the representation derives.

When the certificate includes other attributes of the natural person (membership of a professional college, honorary positions, ...,), the Notary should check and collect the appropriate documents proving these circumstances.

The requestor can submit original documentation within ten days prior to the requesting of the certificate. It is the responsibility of the subscriber to communicate to the Notarial Certification Agency, any possible change in personal attributes.

3.2.3.2 Validation of the identification elements

The validation of the required identification elements is performed exclusively by a Spanish Notary, checking the validity, originality, authenticity and sufficiency of the documentation provided.

3.2.3.3 Need for personal presence

For certificates that identify a natural person, it is required the presence of the person identified in the certificate.

For Notarial Certificates for Legal Persons, it won't be required the physical presence of the person acting as custodian if (and included in the deed as such) if afforded a requesting document with the signature legitimated by a notary.

3.2.3.4 Binding of the natural person to an entity

For Notarial certificates, this binding between a natural person and an entity exists only for Notarial Certificates for Legal Persons and for Notarial Certificates for the Representation of Legal Persons.

For Notarial Certificates for Legal Persons, this natural person is called custodian. For Notarial Certificates for the Representation of Legal Persons, this natural person is the representative.

The document to prove the condition of representative of an entity is a deed or a public document from which derives the representation derives.

When a natural person acts as a representative of an entity, the Notary shall evaluate the adequacy of the faculties verifying the data provided either by consulting the registry either by checking the proper public documents when those are not of compulsory registration.

In the case of consulting the Companies Registry, even assuming no registration of the faculties, the Notary may authorize the issuance covered by commercial laws (the case in which the accreditation of the faculties is documented in a deed authorized by the Notary acting as registration entity). This request should be addressed to the Companies Registry to obtain information about the involved organizations.

For Notarial Corporate Certificates, the notary must check the alleged faculties, in accordance with the provisions of the Law on Electronic Signature.

3.2.4 Authentication of the identity of information systems

3.2.4.1 Validation of the identification elements

It should be checked the following ownership information: contact, organization, full name and contact details.

3.2.5 Unchecked subscriber information

Unverified subscriber information is not included in the certificate.

3.3 Identification and authentication for Re-key Requests

3.3.1 Validation for the regular renewal of certificates

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

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

The electronic signature based on a certificate can be used to request its renewal, always before its expiration.

If any information of the subscriber or the key holder has changed, these changes will be properly recorded in accordance with the provisions of section 3.2 of this Certification Practice Statement.

3.3.2 Validation for the renewal of certificates 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.

For the appropriate evidentiary purposes, the conversation between the operator and the applicant may be recorded.

3.4.2 Identification and authentication of revocation requests

The Notarial Certification Agency checks the revocation requests, verifying that they come from an authorized person, using the following methods:

- In front of a notary with the same requirements as for the issuance request, regarding the identification and ownership of the certificate to revoke.
- By means of the valid electronic signature of the revocation request made with the certificate to be revoked.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

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

There may be the following types of requests:

1) Pre-request, consisting of an electronic or in-person request for a certificate (it does not contain a public key, nor is it digitally signed).

2) Request, generated in person and producing a technical and electronic request by the registration entity, with the generation of keys or using a public key provided by the applicant (PKCS # 10 or compatible mechanism including the public key and the digital signature, in order to prove the possession of the private key, in accordance with section 3.2.1 of this Certification Practice Statement).

4.1.1 Legitimation to of issuance requests

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

1) The natural person who will be the subscriber.

2) The representative of a natural or legal person, including the board of an entity with the previous agreement of all its members.

3) The custodian of notarial certificate for legal person.

In order for third parties to trust the terms of a certificate issued to a natural person in representation of another natural person, is required the concurrence of two elements, one subjective and another objective, which are respectively the following:

1) The notary checks the alleged faculties of the natural person who requests the certificate.

2) The certificate includes, in generic or specific terms, the faculties according to the provisions of this document, in accordance with the provisions of section 3.1.4.12 of this Certification Practice Statement.

Additionally, when the requestor is a representative of a legal person requesting certificates for other natural persons, it is required the presence in front of a notary who acts as registration entity, identifying individuals who will be identified in certificates and have the status of key holders.

The certificates will be requested for these persons, depending on the scope of the representation that they have previously been granted in public documents, and within the faculties of delegation held by the person acting as the applicant.

The faculties of representation included in the certificates have to agree with those described in the corresponding public documents.

The notary checks that the requestor acted as the representative of the legal person when the faculties were legally granted. The reception of the certificate has to be done necessarily by the key owner, and must be included in the corresponding policy.

4.1.2. Registration procedure: responsibilities.

The registration process should include the physical presence in front of a Spanish notary, for the verification and confirmation of the applicant's personal identity, as well as the provision of the corresponding documentation, the completion of forms, and the signing of contracts.

During this phase, the Notary ensures that the certificate requests are complete, accurate and duly authorized, and informs the subscriber or the key holder, as appropriate, of the terms and conditions applicable to the certificate.

The aforementioned information is communicated in a durable medium, on paper or electronically and in easily understandable language.

The request is accompanied by supporting documentation of the identity and other circumstances of the applicant, the future subscriber and the key holder, as appropriate, in accordance with the provisions of sections 3.2.2 and 3.2.3 of this Certificate Practice Statement.

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.

4.2. Certificate Application Processing

4.2.1. Identification and authentication

Once a certificate request has been received, the Notary verifies the information provided, in accordance with section 3.2 of this Certification Practice Statement.

This verification is done generally in the presence of the requestor, with the following exceptions:

- Applications made by applicants for Notarial Certificates for the Representation of Legal Persons, may require the presence of the representatives.
- Applications of Notarial Certificates for Legal Persons involving a signature legitimated by a notary will not require the presence of the custodian.

For Notarial Systems Certificates containing domain names, it is necessary to establish an online connection to any internet domain registry to obtain the document accrediting the possession of the domain name.

In addition to this verification, the DNS entry of type Certification Authority Authorization (CAA) will be verified and processed for each domain included in the certificate, in accordance with the provisions of RFC 6844 and section 3.2.2.8 of the document “Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates” of the CA / Browser Forum.

4.2.2. Approval or rejection of the application

In general, when the provided documentation is insufficient, the notary will not authorize the issuance of the certificate.

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

4.2.3. Resolution term to attend the request

No stipulation.

4.3. Certificate issuance

Generally, the issuance of Notarial Certificates uses a secure signature creation device, except for Notarial Systems Certificates which may also be issued as software certificates.

The issuance of Notarial Certificates for electronic seals with the guarantee of a secure device uses a secure signature creation device for electronic seals.

A qualified device is a cryptographic card, a USB device or any other type of device, especially cryptographic machinery (HSM), that meets the requirements established by Annex II of Regulation (EU) 910/2014 and that appears in the list of qualified signature creation devices referred to in article 31 of this regulation.

4.3.1. Actions during the issuance process

In order to issue a new certificate, the Notary, acting as the registration entity, must access to the certificate issuance application. Access to the application is protected, identifying the operator by his 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 done in a secure way.

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

In all cases, 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 registration data, especially if they are exchanged electronically with the requestor 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.

- In cases where the Notarial Certification Agency provides the secure signature creation device, follow a procedure for the management of secure devices to ensure that the device is delivered in a secure way to the applicant or the key holder, as appropriate.
- 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 guarantee.

4.3.1.1. Issuance in cryptographic card

The actions to be followed are as follows:

1. The notary inserts his cryptographic card (containing the certificate which identifies him as a registration authority) into the card reader and accesses the registration application.

2. Once authenticated, the Notary inserts the cryptographic card of the key holder into the card reader, which has previously been delivered by the Notary along with the corresponding PIN and PUK codes in a sealed envelope.

3. The Notary completes the registration form with the information provided by the applicant, and requests the issuance of the certificate.

4. The registration application requests the PIN corresponding to the cryptographic card of the applicant, to activate the key generation procedure.

5. 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 notary, being automatically stored in the subscriber's cryptographic card.

4.3.1.2. Issuance in hardware cryptographic module or software

The actions to be followed for issuance in this medium are the following:

1. The applicant must present the file in PKCS#10 format containing the certificate request to the Notary.

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

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

4. If the data is correct, the Notary completes the certificate request form and sends the request to the Notarial Certification Agency.

5. Within a maximum period of 48 hours, the applicant can obtain their Notarial Certificate by downloading it from the address www.ancert.com.

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.

For system certificates or certificates of other types issued with keys generated in secure devices owned by the applicant, it is notified that the certificate is available within a maximum period of 48 hours, and that the applicant can obtain his Notarial Certificate by downloading it from the address www.ancert.com .

4.4. Certificate Acceptance

The Notarial Certification Agency:

- Provides the subscriber or key holder with access to the certificate, delivering, where appropriate, the qualified device.
- The Notary, as the registration entity, authorizes a policy in the presence of the applicant or, where appropriate, the key holder, with the acceptance of the general issuing conditions and including the following minimum content:

  a) Basic information about the policy and uses of the certificate, including information on the Notarial Certification Agency and the applicable Certification Practices Statement, their duties, faculties and responsibilities.

  b) Information about the certificate and the qualified device, as appropriate.

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

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

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

  f) The procedure for the secure delivery to the subscriber and the holder of the private key, activation data and, where appropriate, of the qualified device, in accordance with the provisions of sections 6.2 and 6.4 of this Certification Practice Statement.

  g) The date of delivery and acceptance.

4.4.1. Conduct constitutive of the acceptance of the certificate

The acceptance of the certificate by the Subscriber should be understood from the time of issuance and delivery by the Notarial Certification Agency, and the signature before Notary of the corresponding policy.

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:

a) That all information provided during the Certificate application procedure is true.

b) That the Certificate will be used exclusively for legal purposes and authorized by the Notarial Certification Agency, according to this Certification Practice Statement and always within the scope determined in each Certification Policy.

c) That ensures his 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 and merely as an example , will include the actions and measures necessary to prevent its loss, disclosure, modification, or use by a third party other than the subscriber.

The Notarial Certification Agency considers any certificate accepted by the subscriber and published in its corresponding certificate 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 corresponding certificate repository, in accordance with the provisions of section 2.1 of this Certification Practice Statement and complying 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, the key holder

By the general conditions of issuance, the Notarial Certification Agency requires 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, 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, through the general conditions of issuance, 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 and, where appropriate, to correctly generate this key and use properly the qualified signature device.

4.5.2. Use by third parties who trust the certificates

4.5.2.1. Obligations of the third parties that 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 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 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

Certificate renewal is not allowed without changing keys.

4.7. Certificate Re-key

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

The certificates must be renewed together with the keys when the end of their validity period is reached, 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 is a request for renewal of the certificate, which occurs at the request 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.

If the information to include in the renewed certificate has not changed, including 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

Without 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[5].

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) Modification of the Certification Practice Statement that is not accepted by the certificate subscriber.

c) 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.

The general issuance conditions establish the obligation to request the revocation of the certificate in case of having knowledge of any of the circumstances indicated above.

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, either a natural person or an entity. In the case of an entity, it must act through a natural person with sufficient legal powers to revoke the certificate.

[5] In particular, for certificates for code signing it is the subscriber's responsibility that the certificate is not used to sign any type of code that may be considered hostile (including spyware and malware). Upon receiving a complaint, if a misuse of the certificate has been verified, this will constitute an immediate cause for the revocation.

- In the case of certificates for legal representation, also the represented, either a natural person or an entity. If the represented is an entity, it must act through a natural person with sufficient legal powers to revoke the powers alleged by the custodian at the time of obtaining the certificate, or the representation relationship that appears in the certificate.
- Any Notary acting as a registration entity.

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 Notary acting as the registration entity, he must:

- Identify the applicant in accordance with the requirements established in section 3.4.2 3 of this Certification Practice Statement.
- Verify that the applicant is authorized to request the revocation of the certificate.
- Authorize a certificate revocation policy.
- Generate the request by accessing the online revocation application.

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.

4.9.3.1. Revocation request for certificates for Code Signing

When a third party detects that a Code Signing certificate issued by the Notarial Certification Agency is being used to sign hostile code, they can report it to the address revocacion@ancert.com. It must be provided in the corresponding mail, details of the certificate and contact information so that the Notarial Certification Agency can communicate with the complainant to study the case. As soon as the Notarial Certification Agency can resolve whether a prohibited use of the certificate is being made or not, it will proceed to execute the revocation request or to deny it.

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 the 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 the 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 or legal person represented by the subscriber or an authorized third party may request the suspension of a certificate.

The Notarial Certification Agency may also request the suspension 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

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 may be subject to recording.

The applicant for lifting the suspension must respond with the password that would have been stated for this purpose in the certificate application process. In case the answer coincides with said password, the operator will proceed to lift the certificate suspension.

In all cases, once the suspension of the Certificate has been lifted, it will be published on the spot in the Certificate Depository of the Notarial Certification Agency, producing from that moment effects with respect to third parties, and included in the List of Revoked Certificates (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 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 through a web query interface, the Certificate Repository, and 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 Escrow and Recovery

4.12.1. Policy and practices for key escrow and recovery

The Notarial Certification Agency does not store or retrieve keys from subscribers or key holders except for 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

We distinguish in this section the following domains:

- Certificate creation domain.

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

- User registration and card management domain.

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

5.1. Physical security controls

Certificate creation domain

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

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

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

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

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

User registration and card management domain

The Notarial Certification Agency, through the notary offices, has established physical and environmental security controls to protect the resources of the facilities where the systems and the equipment are located and used for the registration and approval of certificate requests, as well as the management of cryptographic cards.

Specifically, the physical and environmental security policy applicable to the services of registration and approval of certificate requests, as well as the management of cryptographic cards, has established requirements for the following contingencies:

- Physical access controls.
- 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.

These measures are applicable to the notary office's facilities where the approval of certificate applications and the management of cryptographic cards are operated, under the full responsibility of the Notarial Certification Agency.

The Notarial Certification Agency has established in the facilities of the notary's office, physical and environmental security controls to protect the services of approval, issuance and card management.

5.1.1. Location and construction of facilities

In all domains

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

Certificate Creation Domain

The Notarial Certification Agency has facilities that physically protect the provision of certificate generation services, from the compromise caused by unauthorized access to systems or data, as well as their disclosure.

The location of the facilities allows the presence of security forces within a reasonably period of time since an incident was notified to them.

The Notarial Certification Agency maintains disaster recovery facilities for the certificate generation services, with security perimeters comparable to those of the main facilities.

User registration and card management domain

The Notarial Certification Agency, in the domain of the notary office, has facilities that physically protect the provision of services for the approval of certificate requests, card management and processing of revocation, and compromises caused by unauthorized access to systems or data, as well as their disclosure.

5.1.2. Physical access

Certificate creation domain

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

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

This identification is performed using double factor authentication techniques, including an employee proximity card and PIN codes, except in the case of escorted visits.

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

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

User registration and card management domain.

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

5.1.3. Electricity and air conditioning

In all domains

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

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

5.1.4. Exposure to water

In all domains

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

5.1.5. Fire prevention and protection

Certificate creation domain

All 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 the keys of Certification Entities, have a specific and additional fire protection system.

User registration and card management domain

All facilities and assets of the Notarial Certification Agency, in the facilities of the notary office, have automatic fire detection and extinction, in accordance with local fire prevention regulations.

5.1.6. Media storage

In all domains

The storage of information media guarantees both its integrity and its confidentiality, in accordance with the classification of the information that has been established.

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

In all domains

The elimination of media, both paper and magnetic, is done through mechanisms that guarantee 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.

In the case of paper documentation, it undergoes a physical destruction treatment.

5.1.8. Off-site backup copies

In all domains

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

In all domains

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

Certificate creation domain

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 Notarial Certification Agency.

Reliable functions include:

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

Individuals holding the above positions are subject to specific control procedures.

User registration and card management domain

The Notarial Certification Agency, for the facilities in the notary office, identifies in its security policy reliable functions or roles.

Persons required to hold such responsibilities are formally designated by the notary.

Reliable functions include:

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

Individuals holding the above positions are subject to specific control procedures.

5.2.2. Number of people per task

Certificate creation domain

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 considering that there is a separation of sensitive functions, and 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.

The most sensitive tasks, such as accessing and managing the Certification Authority's cryptographic hardware and the associated keys, require multiple trustworthy people. Specifically, the internal control procedures have been designed to ensure that at least two reliable people are required to access the device physically or logically.

Access to the Certification Entity's cryptographic hardware by multiple trustworthy people is strictly controlled throughout the entire life cycle, from the receipt and inspection to its final destruction (physical or logical).

User registration and card management domain

The reliable functions identified in the security policy of the certification service provider, and their associated responsibilities, are documented in job descriptions.

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

5.2.3. Identification and authentication for each function

In all domains

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

Certificate creation domain

The following tasks are performed by at least two people:

- Physical Access management.
- Software management.
- Configuration management and change control.
- Archive management.
- Management of cryptographic equipment.
- Generation, issuance and destruction of certificates for Certification Authorities.
- Issuance and revocation of certificates, and access to the repository

User registration and card management domain

The certificate request is made by the customer and the approval is the responsibility of the Notary.

The notary will be in charge of the secure printing and management of the card.

5.3. Personnel controls

5.3.1. History, qualifications, experience and authorization requirements

In all domains

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

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.

Personnel holding reliable positions are free from personal interests that may conflict with the development of the function that have 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

Certificate creation domain

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

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

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

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

The following verifications are made:

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

The research is repeated every three years.

User registration and card management domain

The Notarial Certification Agency will verify the existence of the Notary position.

5.3.3. Training requirements

In all domains

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

In all domains

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

Certificate creation domain

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

User registration and card management domain

Not applicable

5.3.6. Sanctions for unauthorized actions

Domain of creation of certificates

The Notarial Certification Agency has a sanctioning 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 personnel.

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

User registration and card management domain

Not applicable

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.
- Try to distort or falsify system LOG records.
- Try 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.
- Install, 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.
- Use 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

Certificate creation domain

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

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

User registration and card management domain

Not applicable

5.3.8. Provision of documentation to staff

Certificate creation domain

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.

User registration and card management domain

Not applicable

5.4. Audit Logging Procedures

5.4.1. Types of registered events

Certificate creation domain

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

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

User registration and card management domain

The Notarial Certification Agency, through the notary office, keeps records for the following information:

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

5.4.2. Review period for audit logs

In all domains

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

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

Actions taken during the audit review are also documented.

5.4.3. Retention period of audit records

In all domains

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

In all domains

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

5.4.5. Backup procedures for audit logs

In all domains

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

5.4.6. Log aggregation system

In all domains

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

5.4.7. Notification of the audit event

In all domains

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

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

5.4.8. Vulnerability Analysis

Certificate Creation Domain

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

In all domains

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

Certificate Creation Domain

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

A record is kept for the following information:

- Certificate life cycle information
- Identity of the Notary that processes the certificate request.
- The Audit data identified in section 5.4.

User registration and card management domain

The Notarial Certification Agency (through the notary office) will keep records for the following information:

- Type of document presented in the certificate request.
- Unique identification number provided by the previous document.
- The location of copies of certificate requests, and the document signed by the subscriber or by the key holder, as appropriate, which is integrated into the Notary's protocol.

5.5.2. Record retention period

In all domains

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

In the special case of the certificates for code signing, all records related to their life cycle are kept for a minimum of twenty (20) years counted from the time of the issuance of the certificate.

The Notarial Certification Agency keeps audit records for all the components of the systems directly or indirectly related to the issuance of electronic certificates for a minimum of seven (7) years from the time of the issuance of the certificate.

5.5.3. Archive protection

In all domains

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 the registration data corresponding to the subscriber (or the key holder).

5.5.4. Backup procedures

In all domains

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.

Certificate creation domain

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

User registration and card management domain

Same measures as for the procedures of the notary office.

5.5.5. Timestamping requirements

Certificate creation domain

The Notarial Certification Agency issues certificates and CRLs with reliable date and time information. This information is not digitally signed. All the information systems include the registration of the time where they were executed. This time comes from an accurate date and time source. All systems are synchronized with this source of date and time.

User registration and card management domain

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

It is not necessary that this information is digitally signed.

5.5.6. Archive system

In all domains

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

In all domains

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

Certificate creation domain

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

User registration and card management domain

Not applicable

5.7. Compromise and Disaster Recovery

5.7.1. Incident management procedures

Certificate creation domain

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.

User registration and card management domain

Same measures as for the incident management system of the Notary's protocol.

5.7.2. Corruption of resources, applications or data

Certificate creation domain

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.

User registration and card management domain.

The incident should be communicated to the Security Manager of the notary office and the procedures for the management of the incident should be initiated, including escalation, investigation and response to the incident.

5.7.3. Procedure in case of compromise of the private key

5.7.3.1. Revocation of the public key of the entity

Certificate creation domain

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.

User registration and card management domain

Not applicable for this domain.

5.7.3.2. Compromise of the private key of the entity

Certificate creation domain

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

In case of compromise, the Notarial Certification Agency will perform 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.

User registration and card management domain.

Not applicable for this domain.

5.7.4. Business continuity after a disaster

Certificate creation domain

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

User registration and card management domain

Not applicable for this domain.

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, which can be cryptographic USB cards or tokens, or hardware security modules (HSM):

- Cryptographic card or USB token. The creation of the public and private keys (2048 bits RSA) is done internally by the card or token itself, so that both the robustness of the keys and the impossibility of compromise in the generation process are guaranteed.
- Hardware security modules (HSM). The creation of the public and private keys (2048 bits RSA) is done internally by the hardware security module itself, so that both the robustness of the keys and the impossibility of compromise in the generation process are guaranteed.

For end entity certificates without a secure device guarantee, the keys are generated by software in the operating system or computer applications of the end users.

6.1.2. Delivery of the private key to the subscriber

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

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 Entities 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 Entities) / 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 the 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 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 multi person control detailed in section 6.2.2.

Other subscriber's private keys are not escrowed.

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.

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

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

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

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.

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.

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.

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

In cases where the Notarial Certification Agency provides the subscriber with a qualified device for creating a signature (card or USB token), then the activation data of the device is generated in a secure way. 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 subscriber of the card should know. Three consecutive incorrect attempts to enter the PIN cause the card to be blocked. To unlock the card, the subscriber must enter the PUK code and, likewise, three consecutive incorrect attempts to enter the PUK cause the card to be irreversibly blocked.

In case of use of a qualified HSM device, the subscriber must properly configure the signature activation data system, guaranteeing, when appropriate, that the signer has exclusive control over the use of the electronic signature key.

6.4.2. Protection of activation data

The Notarial Certification Agency can generate and provide the subscriber 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 its own signature creation device (eg, 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 applications 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. Systems Development Controls

A 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.

Change control procedures are used for new versions, updates 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 according to their protection needs, consistent with the current risk analysis.

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

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

6.6.3. Life cycle security controls

No additional stipulations.

6.7. Network security controls

It must be guaranteed that 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.

Key generation algorithms are accepted for the intended uses of the keys.

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 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 this 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 Notaries.

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

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 general 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 the 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 Practice Statement.
- 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. Limitation of Liability

9.8.1. Limitation 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 Certificate Practice Statement.

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. Indemnity clauses

9.9.1. Indemnity clauses for the subscriber

The Notarial Certification Agency includes in the general conditions for issuing certificates, a clause by which 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 the 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 Certification Entity must be 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.