Certificate Practice Statement

esFIRMA

General information

Documentary control

Security classification:	Public
Author	ESFIRMA
Version:	1.16

Formal state

Prepared by:	Reviewed by:	Approved by:
Security office Date: 21/04/2023	Security Officer Date: 21/04/2023	Security committee Date: 21/04/2023

Version control

See	Description of the change	Date
1.0	Creation of the document	29/04/2016
1.1	Submissions/Corrections	02/06/2016
1.2	ETSI review	19/05/2017
1.3	Review of certificate types	
1.4	Review of certificate types, acronyms, and definitions	02/06/2017
1.5	Adjustment of normative references, change of name, change of certificates 1.3.2, 1.3.3.1, 1.3.3.2, 1.4.1.8, 3.1.1.8, 4.3.1, 6.1.5, 9.2.1, 9.4, 9.6.2, 9.6.4	06/11/2017
1.6	6.1.1 TSA Duration	20/06/2018
1.7	Correction regarding signature in the issuance of software certificates	08/08/2018
1.8	Adaptation due to regulatory change (Regulation (EU) 910/2014 and Regulation (EU) 2016/679) and review of the renewal sections.	13/11/2018
1.9	3.1.1.1 Clarification on the optional second surname. 3.1.1.2 OrganizationIdentifier conditioned to CA/Browser Forum Guidelines 3.1.1.4 Typographical errors adjustment in OID descriptions 3.1.1.7 EV certificate CN of optional headquarters	14/06/2019
1.10	Various clarifications in 1.2.1, 1.5.4, 2.3, 3.2, 3.2.4-6, 4.1.1, 4.2.1-2, 4.3.1, 4.9.3, 4.9.10-11, 4.11.1-2, 5.2.2, 5.4.3, 5.4.8, 6.1.1, 6.1.5, 6.1.9, 6.2.5, 6.3.2, 6.5.1, 7.1, 7.1.4, 8.1 Alignment with RFC 3647 1.5.3. moved to 1.5.2 Contact information of the organization 1.5.2 moved to 1.5.3 Organization that approves the document DEFINITIONS ACRONYMS" moved to 1.6 Acronyms and definitions 4.4.2 moved to 4.4.1 Conduct that constitutes acceptance of the certificate 4.4.3 moved to 4.4.2 Certificate publication 4.4.4 moved to 4.4.3 Notification of issuance to third parties Added 4.6.1 Circumstances for certificate renewal Added 4.6.2 Who can request a renewal Added 4.6.3 Certificate renewal request processing Added 4.6.4 Notification of new certificate issuance to subscriber Added 4.6.5 Conduct that constitutes the acceptance of a renewal certificate Added 4.6.6 Publication of the renewal certificate by the CA Added 4.6.7 Notification of certificate issuance by the CA to other entities Added 4.7.2 Procedure with new identification 4.7. moved to 4.7.3 Processing of new certificate key requests 4.7.3 moved to 4.7.4 Notification of issuance of the renewed certificate 4.7.4 moved to 4.7.5 Conduct that constitutes acceptance of the certificate 4.7.5 moved to 4.7.6 Certificate publication 4.7.6 moved to 4.7.7 Notification of issuance to third parties 4.11 moved to 4.10 Certificate status checking services 4.11.1 moved to 4.10.1 Operational characteristics of services 4.11.2 moved to 4.10.2 Availability of services Added 4.10.3 Optional features 4.10 moved to 4.11 Completion of subscription 6.1.9 moved to 6.1.7 Purposes of key usage 6.2.9 moved to 6.2.9 Private key deactivation method 6.2.10 moved to 6.2.10 Method for destruction of the private key Added 6.2.11 Cryptographic module classification Added 6.4.3 Other aspects of activation data	08/06/2020

	6.6.2.5 moved to 6.6.3 Evaluation of the security of the life cycle 6.9 moved to 6.8 Time Sources Added 7.1.7 Use of the policy constraints extension Added 7.1.8 Policy qualifiers syntax and semantics Added 7.1.9 Processing semantics for the critical extension of Certificate Policies Added 7.2.2 CRL and CRL extensions Added 7.3.1 Version number Added 7.3.2 OCSP Extensions Added 9.4.1 Privacy Plan Added 9.4.2 Information treated as private Added 9.4.3 Information not considered private Added 9.4.4 Responsibility to protect private information Added 9.4.5 Notice and consent to use private information Added 9.4.6 Disclosure in accordance with a judicial or administrative process Added 9.4.7 Other circumstances of information disclosure Added 9.6.2 RA representations and warranties 9.6.2 moved to 9.6.3 Guarantees offered to subscribers and third parties who rely on certificates Added 9.6.4 Obligation and responsibility of third parties 9.6.2 moved to 9.6.5 Obligation and responsibility of other participants 9.6.3 moved to 9.7 Disclaimer 9.6.4 moved to 9.8 Limitation of liability in case of losses due to transactions 9.6.5 moved to 9.9 Indemnities Added 9.10. Deadline and Completion Added 9.10.1 Deadline Added 9.10.2 Termination Added 9.10.3 Effect of Termination and Survival Added 9.11 Individual notifications and communication with participants Added 9.12 Modifications Added 9.12.1 Modification Procedure Added 9.12.2 Notification mechanism and deadlines Added 9.12.3 Circumstances in which the OID must be changed 9.6.10 moved to 9.13 Conflict Resolution Procedure 9.6.7 moved to 9.14 Applicable legislation Added 9.15 Compliance with Applicable Law Added 9.16 Other provisions Added 9.16.1 Complete agreement Added 9.16.2 Assignment 9.6. moved to 9.16.3 Separability Added 9.16.4 Compliance (attorney fees and exemption from fees) 9.6.6 moved to 9.16.5 Force majeure Added 9.17 Other provisions New certificates are included: public employee certificate (Authentication), public employee certificate with pseudonym (Authentication), physical person certificate linked to entity (Authentication), physical person certificate linked to entity (Signature), physical person certificate with pseudonym linked to entity (Authentication), physical person certificate with pseudonym linked to entity (Signature)	
1.11	New qualified certificates for electronic seals are included The electronic headquarters certificate profile is removed. Adaptation due to regulatory change (Law 6/2020, of November 11, regulating certain aspects of electronic trust services). In section 5.8 Termination of the DPC Service, the detail of how the status information of the certificates is provided beyond their lifetime is added.	03/05/2021

	References to the Ministry of Industry, Energy and Tourism are updated to the Ministry of Economic Affairs and Digital Transformation.	
1.12	Point 5.2.1 is modified by changing the name "Registry Administrator" to "Registry Operator". References to CA/B Forum are removed.	10/05/2021
1.13	Modification of point 5.8 Service Termination, according to the Cessation Plan Point 4.9.1 is modified to include the end of QSCD certification Modification of section 6.5.1, including the end of DCCF certification. Elimination of reference to the security document of esFIRMA in section 6.6.2 (Management Operations) Substitution of "security policy" for "information security management system" in section 6.6.2 (Classification and management of information and assets) Section 6.9 is added in accordance with ETSI TS 119 431-1: OVR-5.1-02 Point 9.6.4 is modified, including the Certification Chain as a verification point. The integration system with DIR3 is added as a means for verifying the identity of the entity (3.2.2) Verification of the status of the certificates in the certification chain is added in section 4.9.6.	18/07/2022
1.14	Information about the new TSA certificate	16/03/2023
1.15	Settings information about TSA and incorporation of non-qualified time stamp	31/03/2023
1.16	New length restrictions for certificate profile elements New European subprofiles for natural persons and electronic seals Simplification of sections 3.2.2 and 3.2.3 Section 4.5.3 is added to separate the information and obligations of third parties that trust the certificates. Differences and considerations between revocation status queries of a certificate using OCSP and CRL 4.10.1	21/04/2023

Index

1. Introduction

1.1 Presentation

This document declares the electronic signature certification practices of esFIRMA.

The certificates that are issued are the following:

- **From Public Employee (SIGNATURE)**
    - From Middle-level Public Employee
    - From High-level Public Employee
- **From Public Employee (AUTHENTICATION)**
    - From High-level Public Employee
- **From Public Employee with pseudonym (SIGNATURE)**
    - From Middle-level Public Employee
    - From High-level Public Employee
- **From Public Employee with pseudonym (AUTHENTICATION)**
    - From High-level Public Employee
- **From a natural person linked to an entity (SIGNATURE)**
    - From a natural person linked to a Medium level entity
    - From a natural person linked to a High-level entity
- **From a natural person linked to an entity (AUTHENTICATION)**
    - From a natural person linked to a High-level entity
- **From a natural person linked to an entity with a pseudonym (SIGNATURE)**
    - From a natural person linked to a Medium level entity
    - From a natural person linked to a High-level entity
- **From a natural person linked to an entity with a pseudonym (AUTHENTICATION)**
    - From a natural person linked to a High-level entity
- **Of Body Seal**
    - Of Medium-level Body Seal
- **Electronic seal for TSA/TSU**
    - Of electronic seal for TSU in HSM
- **Of electronic seal**
    - Of electronic seal in software
    - Of electronic seal with centralized management

1.2 Document name and identification

This document is the "Certification Practice Statement" of esFIRMA.

1.2.1 Certificate identifiers

Número OID	Certificate policies
	From Public Employee (SIGNATURE)
1.3.6.1.4.1.47281.1.1.1	*From Public Employee - High Level on card*
1.3.6.1.4.1.47281.1.1.4	*From Public Employee - Medium Level in HSM*
	From Public Employee (AUTHENTICATION)
1.3.6.1.4.1.47281.1.1.5	*From Public Employee - High Level on card*
	From Public Employee with Pseudonym (SIGNATURE)
1.3.6.1.4.1.47281.1.3.1	*From EP with Pseudonym - High Level on Card*
1.3.6.1.4.1.47281.1.3.4	*From EP with Pseudonym - Medium Level in HSM*
	From Public Employee with Pseudonym (AUTHENTICATION)
1.3.6.1.4.1.47281.1.3.5	*From EP with Pseudonym - High Level on Card*
	From a natural person linked to an entity (SIGNATURE)
1.3.6.1.4.1.47281.1.6.1	*From PF linked to entity - Qualified Electronic Signature, on Card*
1.3.6.1.4.1.47281.1.6.4	*From PF linked to entity - Centralized Firma-e*
	From a natural person linked to an entity (AUTHENTICATION)
1.3.6.1.4.1.47281.1.6.5	*From PF linked to entity - on card*
	From a natural person with a pseudonym linked to an entity (SIGNATURE)
1.3.6.1.4.1.47281.1.7.1	*From PF with pseudonym linked to entity - Qualified Electronic Signature, on Card*

1.3.6.1.4.1.47281.1.7.4	*From PF with pseudonym linked to entity - Centralized Firma-e*
	From a natural person with a pseudonym, linked to an entity (AUTHENTICATION)
1.3.6.1.4.1.47281.1.7.5	*From PF with pseudonym, linked to entity - on Card*
	Of Body Seal
1.3.6.1.4.1.47281.1.2.2	*De Sello de Órgano –* *Medium level in software*
1.3.6.1.4.1.47281.1.2.4	*De Sello de Órgano –* *Medium Level in HSM*
	Electronic seal for TSA/TSU
1.3.6.1.4.1.47281.1.5.1	*From Sello-e to TSA/TSU in HSM*
1.3.6.1.4.1.47281.1.5.2	*Of qualified e-Seal for TSA/TSU in HSM*
	Of electronic seal
1.3.6.1.4.1.47281.1.8.2	*De Sello electrónico en software*
1.3.6.1.4.1.47281.1.8.4	*Of centralized electronic seal*

In case of contradiction between this Certification Practice Statement and other esFIRMA practice and procedure documents, the provisions of this Certification Practice Statement shall prevail.

This document is structured according to IETF RFC 3647.

1.3 Participants in certification services

1.3.1. Certification service provider

The certification service provider is the natural or legal person who issues and manages certificates for end entities, using a Certification Authority, or providing other services related to electronic signatures.

ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (formerly AULOCE SA), hereinafter referred to as ESPUBLICO, with registered office at Calle Bari 39 (Edif. Binary Building), Postal Code 50.197, Zaragoza, CIF A-50.878.842, registered in the Commercial Register of Zaragoza in volume 2.649, Folio 215, sheet Z-28722, and operating under the trade name esFIRMA, which will be used throughout this document to refer to it, is a certification service provider that operates in accordance with the obligations and responsibilities set out in the regime of Regulation (EU) 910/2014, Law 6/2020 of November 11, regulating certain aspects of electronic trust services, Organic Law 3/2018 of December 5, on the Protection of Personal Data and guarantee of digital rights, and the ETSI technical standards applicable to the issuance and management of qualified certificates, mainly ETSI EN 319 411-1 and ETSI EN 319 411-2, in order to facilitate compliance with legal requirements and international recognition of its services.

For the provision of certification services, esFIRMA has established a hierarchy of certification authorities:

esFIRMA AC root 2

This is the root certification authority of the hierarchy that issues certificates to other certification authorities, and whose public key certificate has been self-signed.

Identification data:

CN:	ESFIRMA AC RAIZ 2
Digital fingerprint SHA-256:	c6:09:f9:4f:9c:ce:20:cb:2b:a0:2e:8b:5b:33:55:20:06:c1:5d:17:78:32:26:11:07:0f:a1:4f:ff:9d:c9:16
Valid from:	2017-11-02T12:52:43Z
Valid until:	2042-11-02T12:52:43Z
RSA key length:	4,096 bits

esFIRMA AC AAPP 2

This is the certification authority within the hierarchy that issues certificates to end entities, and whose public key certificate has been digitally signed by "esFIRMA AC RAIZ 2".

Identification data:

CN:	ESFIRMA AC AAPP 2
Digital fingerprint SHA-256:	2c:18:23:61:9d:80:73:11:6c:8f:14:8b:d3:85:79:de:9c:05:39:16:02:db:ce:b9:65:73:e4:a1:88:e1:32:6e
Valid from:	2017-11-02T13:12:47Z
Valid until:	2030-11-02T13:12:47Z
RSA key length:	4,096 bits

Electronic Administration Platform

This is the exclusive certificate lifecycle management platform for its request, approval, issuance, and revocation.

To complete the information on the functionalities of the Electronic Administration Platform in certification services, please consult its documentation.

1.3.2 Registration Authorities

A registration authority performs verification and identification tasks of certificate applicants.

In general, the certification service provider itself acts as the registration authority for the identity of certificate subscribers.

The designated units for this function by the subscribers of the certificates, such as the corporation's Secretariat, the personnel department, or the legal representative of the Administration, are also registration authorities for the certificates subject to this Certification Practice Statement, due to their status as corporate certificates, since they have authentic records about the signers' connection to the subscriber.

The registration functions of subscribers are carried out by delegation and in accordance with the instructions of the certification service provider, under the terms defined by Regulation (EU) 910/2014, and Law 6/2020, of November 11, regulating certain aspects of electronic trust services, and under the full responsibility of the certification service provider towards third parties.

1.3.3 End entities

The end entities are the individuals and organizations that are the recipients of digital certificate issuance, management, and usage services, for the purposes of electronic identification and signature.

The following will be the final entities of the esFIRMA certification services:

1. Subscribers of the certification service.
2. Signers.
3. User parties.

1.3.4 User parties

The user parties are the individuals and organizations that receive digital signatures and digital certificates.

As a prerequisite to trusting the certificates, user parties must verify them, as established in this certification practice statement and in the corresponding instructions available on the Certification Authority's website.

1.3.5 Other participants

Subscribers of the certification service

The subscribers of the certification service are public administrations or entities that acquire them from esFIRMA for use in their corporate or organizational scope, and are identified in the certificates.

The subscriber of the certification service acquires a license to use the certificate, for their own use - electronic seal certificates - or in order to facilitate the certification of the identity of a specific person duly authorized for various actions in the organizational scope of the subscriber - electronic signature certificates. In this latter case, this person is identified in the certificate, as provided in the following section.

The subscriber of the certification service is therefore the client of the certification service provider, in accordance with commercial legislation, and has the rights and obligations defined by the certification service provider, which are additional and understood without prejudice to the rights and obligations of the signatories, as authorized and regulated in the applicable European technical standards for the issuance of qualified electronic certificates, especially in ETSI EN 319 411-2, sections 5.4.2 and 6.3.4.e)

Signers

The signatories are natural persons who exclusively possess or have under their exclusive control, in accordance with the obligations and responsibilities regime of Regulation (EU) 910/2014, and Law 6/2020, of November 11, regulating certain aspects of electronic trust services, the digital signature keys for identification and advanced or qualified electronic signature; typically being the holders or members of administrative bodies, in electronic signature certificates of the body, persons in the service of Public Administrations, in certificates of public employee or persons belonging to an entity, in certificates of linked natural person.

The signers are duly authorized by the subscriber and properly identified in the certificate by their full name, valid tax identification number in the jurisdiction of issuance of the certificate, or with the corresponding pseudonym in certificates of this type.

Given the existence of certificates for uses other than electronic signature, such as identification, the more generic term "natural person identified in the certificate" is also used, always with full respect for compliance with electronic signature legislation regarding the rights and obligations of the signer.

1.4 Use of certificates

This section lists the applications for which each type of certificate can be used, establishes limitations on certain applications, and prohibits certain applications of the certificates.

1.4.1 Permitted uses for certificates

The permitted uses indicated in the various fields of the certificate profiles visible on the website https://www.esfirma.com must be taken into account

High-level Public Employee Certificate on Card

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.1.1	In the hierarchy of the CA, esFIRMA
0.4.0.194112.1.2	According to the QCP-n-qscd policy
2.16.724.1.3.5.7.1	High-level Spanish public employee

The high-level public employee physical person certificates are certificates qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the technical regulations identified with reference ETSI EN 319 411-2.

These certificates are issued to public employees to identify them as individuals in the service of the Administration, organization, public law entity or other entity, linking them to it, complying with the established requirements in article 43 of Law 40/2015, of October 1, on the Legal Regime of the Public Sector, for the electronic signature of public sector employees.

The high-level public employee physical person certificates work with a secure signature creation device in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council, of July 23, 2014.

Likewise, high-level public employee physical person certificates are issued in accordance with the high assurance levels of the certificate profiles established in point 10 of the "Electronic Certificate Profiles" document of the State Secretariat for Digitization and Artificial Intelligence of the Ministry of Economic Affairs and Digital Transformation.

These certificates guarantee the identity of the subscriber and the signer, and they allow the generation of the "qualified electronic signature"; that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, therefore in accordance with what is established in article 25.2 of the Regulation (EU) 910/2014 of the European Parliament and of the Council, of July 23, 2014, will have an equivalent legal effect to that of a Signature handwritten.

They can also be used in applications that do not require the electronic signature equivalent to the written signature, such as the applications listed below:

a) Secure email signature.
b) Other digital signature applications.

esFIRMA does not offer backup or key recovery services. Therefore, esFIRMA will not be responsible in any case for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

a) The "key usage" field has the following functions enabled, and therefore allows performing:
    a. Compromiso con el contenido (Content commitment to perform the electronic signature function)

b) In the "Qualified Certificate Statements" field, the following statement appears:
    a. QcCompliance (0.4.0.1862.1.1), which reports that the certificate is issued as qualified.
    b. QcSSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a secure signature creation device.

c) The "User Notice" field describes the use of this certificate.

Certificate of Public Employee level medium in HSM

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.1.4	In the hierarchy of the CA, esFIRMA
0.4.0.194112.1.0	In accordance with the QCP-n policy
2.16.724.1.3.5.7.2	Spanish mid-level public employee

The certificates for physical person, public employee, medium level are certificates qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the technical regulations identified with reference ETSI EN 319 411-2.

These certificates are issued to public employees to identify them as individuals in the service of the Administration, organization, public law entity or other entity, linking them to it, complying with the requirements established in Article 43 of Law 40/2015, of October 1, on the Legal Regime of the Public Sector, for the electronic signature of public sector employees.

The certificates of physical person, public employee, medium level are managed in a centralized way.

Certificates for public employees at the medium level are issued in accordance with the medium assurance levels of the certificate profiles established in point 10 of the document "Electronic Certificate Profiles" of the State Secretariat for Digitization and Artificial Intelligence of the Ministry of Economic Affairs and Digital Transformation.

These certificates guarantee the identity of the subscriber and the person indicated in the certificate, and allow the generation of the "advanced electronic signature based on qualified electronic certificate".

They can also be used in applications that do not require the electronic signature equivalent to the written signature, such as the applications listed below:

a) Secure email signature.
b) Other digital signature applications.

esFIRMA does not offer backup or key recovery services. Therefore, esFIRMA will not be responsible in any case for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

a) The "key usage" field has enabled, and therefore allows us to perform, the following functions:
    a. Compromiso con el contenido (Content commitment, to perform the electronic signature function)

b) In the "Qualified Certificate Statements" field, the following statement appears:
    a. qCCompliance (0.4.0.1862.1.1), which reports that the certificate is issued as qualified.

c) The "User Notice" field describes the use of this certificate.

High-level Public Employee Certificate on a card for authentication

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.1.5	In the hierarchy of the CA, esFIRMA
0.4.0.2042.1.2	According to the NCP+ policy
2.16.724.1.3.5.7.1	High-level Spanish public employee

These certificates are certificates issued in accordance with the standardized certificate policy (NCP+) and comply with the provided by the technical regulation identified with the reference ETSI EN 319 411-1.

These certificates are issued to public employees to identify them as individuals in the service of the Administration, organization, public law entity or other entity, linking them to it, complying with the requirements established in Law 40/2015, of October 1, on the Legal Regime of the Public Sector.

These high-level public employee physical person certificates work with a secure signature creation device in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council, of July 23, 2014.

Certificates for high-level public employee physical persons are issued in accordance with the high assurance levels of the certificate profiles established in point 10 of the "Electronic Certificate Profiles" document of the State Secretariat for Digitization and Artificial Intelligence of the Ministry of Economic Affairs and Digital Transformation.

These certificates guarantee the identity of the subscriber and the person indicated in the certificate, and allow the authentication of the latter to applications and websites.

esFIRMA does not offer backup or key recovery services. Therefore, esFIRMA will not be responsible in any case for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

d) The "key usage" field has enabled, and therefore allows us to perform, the following functions:
   a. Digital signature (to perform the authentication function)

e) The "User Notice" field describes the use of this certificate.

Medium level Body seal Certificate in software

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.2.2	In the hierarchy of the CA, esFIRMA
0.4.0.194112.1.1	According to the QCP-l policy

2.16.724.1.3.5.6.2	Spanish mid-level public employee

The certificates of medium level electronic seal of the entity are certificates Qualified in accordance with Article 38 and Annex III of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical regulations identified with reference ETSI EN 319 411-2.

These certificates are issued for the identification and authentication of the exercise of competence in automated administrative action in accordance with article Article 42 of Law 40/2015, of October 1, on the Legal Regime of the Public Sector.

Electronic seal certificates for medium-level organs are issued in accordance with the medium assurance levels of the certificate profiles established in point 9 of the "Electronic Certificate Profiles" document of the State Secretariat for Digitization and Artificial Intelligence of the Ministry of Economic Affairs and Digital Transformation.

These certificates guarantee the identity of the subscriber and the public organization included in the certificate.

esFIRMA does not offer backup or key recovery services. Therefore, esFIRMA will not be responsible in any case for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

a) The "key usage" field has enabled, and therefore allows us to perform, the following functions:
   a. Compromiso con el contenido (Content commitment, to perform the electronic signature function)

b) In the "Qualified Certificate Statements" field, the following statement appears:
   a. QcCompliance (0.4.0.1862.1.1), which reports that the certificate is issued as qualified.

c) The "User Notice" field describes the use of this certificate.

Medium level Body seal Certificate in HSM

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.2.4	In the hierarchy of the CA, esFIRMA
0.4.0.194112.1.1	According to the QCP-l policy
2.16.724.1.3.5.6.2	Spanish mid-level public employee

The certificates of medium level electronic seal of the entity are certificates Qualified in accordance with Article 38 and Annex III of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical regulations identified with reference ETSI EN 319 411-2.

These certificates are issued for the identification and authentication of the exercise of competence in automated administrative action in accordance with article Article 42 of Law 40/2015, of October 1, on the Legal Regime of the Public Sector.

Medium-level electronic seal certificates are managed centrally.

Electronic seal certificates for medium-level organs are issued in accordance with the medium assurance levels of the certificate profiles established in point 9 of the "Electronic Certificate Profiles" document of the State Secretariat for Digitization and Artificial Intelligence of the Ministry of Economic Affairs and Digital Transformation.

These certificates guarantee the identity of the subscriber and the public organization included in the certificate.

esFIRMA does not offer backup or key recovery services. Therefore, esFIRMA will not be responsible in any case for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

a) The "key usage" field has enabled, and therefore allows us to perform, the following functions:

a. Compromiso con el contenido (Content commitment, to perform the electronic signature function)

b) In the "Qualified Certificate Statements" field, the following statement appears:

a. QcCompliance (0.4.0.1862.1.1), which reports that the certificate is issued as qualified.

c) The "User Notice" field describes the use of this certificate.

Certificate of Public Employee with High Level Pseudonym on Card

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.3.1	In the hierarchy of the CA, esFIRMA
0.4.0.194112.1.2	According to the QCP-n-qscd policy
2.16.724.1.3.5.4.1	Spanish public employee with high level pseudonym

The high-level pseudonymous certificates of public employee natural persons are certificates qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the technical regulations identified with reference ETSI EN 319 411-2.

These certificates are issued to public employees to identify them (through a pseudonym) as individuals in the service of the Administration, organization, public law entity or other entity, linking them to it, complying with the established requirements in article 43 of Law 40/2015, of October 1, on the Legal Regime of the Public Sector, for the electronic signature of public sector employees.

The high-level pseudonymous certificates of public employee natural persons work with a secure signature creation device, in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014.

Likewise, certificates for public employees with high-level pseudonyms are issued in accordance with the high assurance levels of the certificate profiles established in point

11 of the document "Electronic Certificate Profiles" of the State Secretariat for Digitization and Artificial Intelligence of the Ministry of Economic Affairs and Digital Transformation.

These certificates allow the generation of the "qualified electronic signature"; that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, therefore in accordance with what is established in article 25.2 of the Regulation (EU) 910/2014 of the European Parliament and of the Council, of July 23, 2014, will have an equivalent legal effect to that of a Signature handwritten.

They can also be used in applications that do not require the electronic signature equivalent to the written signature, such as the applications listed below:

a) Secure email signature.
b) Other digital signature applications.

esFIRMA does not offer backup or key recovery services. Therefore, esFIRMA will not be responsible in any case for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

a) The "key usage" field has the following functions enabled, and therefore allows performing:
    a. Compromiso con el contenido (Content commitment to perform the electronic signature function)

b) In the "Qualified Certificate Statements" field, the following statement appears:
    a. QcCompliance (0.4.0.1862.1.1), which reports that the certificate is issued as qualified.
    b. QcSSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a secure signature creation device.

c) The "User Notice" field describes the use of this certificate.

Certificate of Public Employee with medium level pseudonym, in HSM

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.3.4	In the hierarchy of the CA, esFIRMA
0.4.0.194112.1.0	In accordance with the QCP-n policy
2.16.724.1.3.5.4.2	Spanish public employee with medium level pseudonym

The certificates of physical person public employee with medium level pseudonym are certificates qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the technical regulations identified with reference ETSI EN 319 411-2.

These certificates are issued to public employees to identify them (through a pseudonym) as individuals in the service of the Administration, organization, public law entity or other entity, linking them to it, complying with the requirements established in Article 43 of Law 40/2015, of October 1, on the Legal Regime of the Public Sector, for the electronic signature of public sector employees.

Certificates of physical person, public employee with medium level pseudonym They are managed in a centralized way.

Certificates for public employees with a pseudonym at a medium level of assurance are issued in accordance with the medium assurance levels of the certificate profiles established in point 11 of the document "Electronic Certificate Profiles" of the State Secretariat for Digitization and Artificial Intelligence of the Ministry of Economic Affairs and Digital Transformation.

These certificates allow the generation of the "advanced electronic signature based on qualified electronic certificate".

They can also be used in applications that do not require the electronic signature equivalent to the written signature, such as the applications listed below:

c) Secure email signature.

d) Other digital signature applications.

esFIRMA does not offer backup or key recovery services. Therefore, esFIRMA will not be responsible in any case for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

a) The "key usage" field has enabled, and therefore allows us to perform, the following functions:
   a. Compromiso con el contenido (Content commitment, to perform the electronic signature function)

b) In the "Qualified Certificate Statements" field, the following statement appears:
   a. qCCompliance (0.4.0.1862.1.1), which reports that the certificate is issued as qualified.

c) The "User Notice" field describes the use of this certificate.

Certificate of Public Employee with pseudonym, high level on card for authentication

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.3.5	In the hierarchy of the CA, esFIRMA
0.4.0.2042.1.2	According to the NCP+ policy
2.16.724.1.3.5.4.1	Spanish public employee with a high-level pseudonym

These certificates are certificates issued in accordance with the standardized certificate policy (NCP+) and comply with the provided by the technical regulation identified with the reference ETSI EN 319 411-1.

These certificates are issued to public employees to identify them (through a pseudonym) as individuals in the service of the Administration, organization, public law entity or other entity, linking them to it, complying with the requirements established in Law 40/2015, of October 1, on the Legal Regime of the Public Sector.

These high-level pseudonymous physical person certificates for public employees work with a secure signature creation device in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council, of July 23, 2014.

Certificates for public employees with high-level pseudonyms are issued in accordance with the high assurance levels of the certificate profiles established in point 11 of the document "Electronic Certificate Profiles" of the State Secretariat for Digitization and Artificial Intelligence of the Ministry of Economic Affairs and Digital Transformation.

These certificates guarantee the identity of the subscriber and the person indicated in the certificate, and allow the authentication of the latter to applications and websites.

esFIRMA does not offer backup or key recovery services. Therefore, esFIRMA will not be responsible in any case for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

f) The "key usage" field has enabled, and therefore allows us to perform, the following functions:
   a. Digital signature (to perform the authentication function)

g) The "User Notice" field describes the use of this certificate.

Qualified electronic seal certificate of TSA/TSU

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.5.2	In the hierarchy of the CA, esFIRMA

0.4.0.194112.1.1	According to the QCP-l policy

The electronic seal certificates of TSA/TSU are certificates Qualified in accordance with Article 38 and Annex III of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical regulations identified with the reference ETSI EN 319 421 and ETSI EN 319 422.

This certificate allows Time Stamping Units or TSUs to issue time stamps when they receive a request under the specifications of RFC3161.

The keys are generated on a HSM device support.

The usage information in the certificate profile indicates the following:

a) The "key usage" field has enabled, and therefore allows us to perform, the following functions:
   a. Content Commitment
b) The "extend key usage" field has the function activated:
   a. TimeStamping
c) In the "Qualified Certificate Statements" field, the following statement appears:
   a. QcCompliance (0.4.0.1862.1.1), which reports that the certificate is issued as qualified.
d) The "User Notice" field describes the use of this certificate. Optional
e) It includes the "privateKeyUsage" extension, which limits the use of the private key, following the recommendations of the ETSI EN 319 421 and ETSI EN 319 422 standards.

Other considerations:

- Controls are established to ensure the cessation of use of the private key before the expiration of its validity.
- In case of certificate change, the associated keys will be destroyed as described in the life cycle.
- Private keys are destroyed once their defined usage time has expired, their replacement, revocation, or other causes.

- The destruction is carried out in such a way that the private key cannot be recovered, following the procedure established by the manufacturer of the cryptographic module that stores them.
- For long-term validation of time stamps, the latest CRL issued by esFIRMA can be used following the provided guidelines. At the time of verification, it can be considered valid if, at the time of the time stamp date, the private key was not compromised, the digital fingerprint algorithm did not present collisions, and the algorithms used were beyond the scope of cryptographic attacks at the time.

TSA/TSU Electronic Seal Certificate

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.5.1	In the hierarchy of the CA, esFIRMA
0.4.0.194112.1.1	According to the QCP-l policy

This certificate allows Time Stamping Units or TSUs to issue time stamps when they receive a request under the specifications of RFC3161.

The keys are generated on a HSM device support.

The usage information in the certificate profile indicates the following:

f) The "key usage" field has enabled, and therefore allows us to perform, the following functions:

   a. Content Commitment

g) The "extend key usage" field has the function activated:

   a. TimeStamping

h) The "User Notice" field describes the use of this certificate. Optional

i) It includes the "privateKeyUsage" extension, which limits the use of the private key, following the recommendations of the ETSI EN 319 421 and ETSI EN 319 422 standards.

Other considerations:

- Controls are established to ensure the cessation of use of the private key before the expiration of its validity.
- In case of certificate change, the associated keys will be destroyed as described in the life cycle.
- Private keys are destroyed once their defined usage time has expired, their replacement, revocation, or other causes.
- The destruction is carried out in such a way that the private key cannot be recovered, following the procedure established by the manufacturer of the cryptographic module that stores them.
- For long-term validation of time stamps, the latest CRL issued by esFIRMA can be used following the provided guidelines. At the time of verification, it can be considered valid if, at the time of the time stamp date, the private key was not compromised, the digital fingerprint algorithm did not present collisions, and the algorithms used were beyond the scope of cryptographic attacks at the time.

Certificate of natural person linked, on a card for signature

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.6.1	In the hierarchy of the CA, esFIRMA
0.4.0.194112.1.2	According to the QCP-n-qscd policy

These certificates are qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the technical regulations identified with reference ETSI EN 319 411-2.

These certificates work with a secure signature creation device in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council, of July 23, 2014.

These certificates guarantee the identity of the subscriber and the signer, and they allow the generation of the "qualified electronic signature"; that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, therefore in accordance with what is established in article 25.2 of the Regulation (EU) 910/2014 of the European Parliament and of the Council, of July 23, 2014, will have an equivalent legal effect to that of a Signature handwritten.

They can also be used in applications that do not require the electronic signature equivalent to the written signature, such as the applications listed below:

c) Secure email signature.
d) Other digital signature applications.

esFIRMA does not offer backup or key recovery services. Therefore, esFIRMA will not be responsible in any case for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

d) The "key usage" field has the following functions enabled, and therefore allows performing:
   a. Compromiso con el contenido (Content commitment to perform the electronic signature function)

e) In the "Qualified Certificate Statements" field, the following statement appears:
   a. QcCompliance (0.4.0.1862.1.1), which reports that the certificate is issued as qualified.
   b. QcSSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a secure signature creation device.

f) The "User Notice" field describes the use of this certificate. Optional

Centralized certificate for the signature of a natural person

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.6.4	In the hierarchy of the CA, esFIRMA
0.4.0.194112.1.0	In accordance with the QCP-n policy

These certificates are qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the technical regulations identified with reference ETSI EN 319 411-2.

These certificates are managed in a centralized way.

These certificates guarantee the identity of the subscriber and the person indicated in the certificate, and allow the generation of the "advanced electronic signature based on qualified electronic certificate".

They can also be used in applications that do not require the electronic signature equivalent to the written signature, such as the applications listed below:

e) Secure email signature.
f) Other digital signature applications.

esFIRMA does not offer backup or key recovery services. Therefore, esFIRMA will not be responsible in any case for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

h) The "key usage" field has enabled, and therefore allows us to perform, the following functions:
   a. Compromiso con el contenido (Content commitment, to perform the electronic signature function)

i) In the "Qualified Certificate Statements" field, the following statement appears:
   a. qCCompliance (0.4.0.1862.1.1), which reports that the certificate is issued as qualified.

j) The "User Notice" field describes the use of this certificate. Optional

Certificate of natural person linked, on a card for authentication

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.6.5	In the hierarchy of the CA, esFIRMA
0.4.0.2042.1.2	According to the NCP+ policy

These certificates are certificates issued in accordance with the standardized certificate policy (NCP+) and comply with the provided by the technical regulation identified with the reference ETSI EN 319 411-1.

These certificates work with a secure signature creation device in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council, of July 23, 2014.

These certificates guarantee the identity of the subscriber and the person indicated in the certificate, and allow the authentication of the latter to applications and websites.

esFIRMA does not offer backup or key recovery services. Therefore, esFIRMA will not be responsible in any case for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

k) The "key usage" field has enabled, and therefore allows us to perform, the following functions:
   a. Digital signature (to perform the authentication function)

l) The "User Notice" field describes the use of this certificate. Optional

Certificate of natural person linked, with pseudonym, on card for signature

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.7.1	In the hierarchy of the CA, esFIRMA

0.4.0.194112.1.2	According to the QCP-n-qscd policy

These certificates are qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the technical regulations identified with reference ETSI EN 319 411-2.

These certificates work with a secure signature creation device in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council, of July 23, 2014.

These certificates guarantee the identity of the subscriber.
These certificates guarantee the identity of the signer through a pseudonym.
These certificates they allow the generation of the "qualified electronic signature"; that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, therefore in accordance with what is established in article 25.2 of the Regulation (EU) 910/2014 of the European Parliament and of the Council, of July 23, 2014, will have an equivalent legal effect to that of a Signature handwritten.

They can also be used in applications that do not require the electronic signature equivalent to the written signature, such as the applications listed below:

e) Secure email signature.
f) Other digital signature applications.

esFIRMA does not offer backup or key recovery services. Therefore, esFIRMA will not be responsible in any case for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

g) The "key usage" field has the following functions enabled, and therefore allows performing:
   a. Compromiso con el contenido (Content commitment to perform the electronic signature function)

h) In the "Qualified Certificate Statements" field, the following statement appears:
   a. QcCompliance (0.4.0.1862.1.1), which reports that the certificate is issued as qualified.
   b. QcSSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a secure signature creation device.

i) The "User Notice" field describes the use of this certificate. Optional

Certificate of natural person linked, with pseudonym, centralized, for signature

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.6.4	In the hierarchy of the CA, esFIRMA
0.4.0.194112.1.0	In accordance with the QCP-n policy

These certificates are qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the technical regulations identified with reference ETSI EN 319 411-2.

These certificates are managed in a centralized way.
These certificates guarantee the identity of the subscriber.
These certificates guarantee the identity of the signer through a pseudonym.
These certificates allow the generation of the "advanced electronic signature based on qualified electronic certificate".

They can also be used in applications that do not require the electronic signature equivalent to the written signature, such as the applications listed below:

g) Secure email signature.
h) Other digital signature applications.

esFIRMA does not offer backup or key recovery services. Therefore, esFIRMA will not be responsible in any case for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

m) The "key usage" field has enabled, and therefore allows us to perform, the following functions:
   a. Compromiso con el contenido (Content commitment, to perform the electronic signature function)

n) In the "Qualified Certificate Statements" field, the following statement appears:
   a. qCCompliance (0.4.0.1862.1.1), which reports that the certificate is issued as qualified.

o) The "User Notice" field describes the use of this certificate. Optional

Certificate of natural person linked, with pseudonym, on card for authentication

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.7.5	In the hierarchy of the CA, esFIRMA
0.4.0.2042.1.2	According to the NCP+ policy

These certificates are certificates issued in accordance with the standardized certificate policy (NCP+) and comply with the provided by the technical regulation identified with the reference ETSI EN 319 411-1.

These certificates work with a secure signature creation device in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council, of July 23, 2014.

These certificates guarantee the identity of the subscriber.
These certificates guarantee the identity of the signer through a pseudonym.
These certificates allow the authentication of the latter to applications and websites.

esFIRMA does not offer backup or key recovery services. Therefore, esFIRMA will not be responsible in any case for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

p) The "key usage" field has enabled, and therefore allows us to perform, the following functions:
   a. Digital signature (to perform the authentication function)

q) The "User Notice" field describes the use of this certificate. Optional

Certificate of Electronic Seal in software

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.8.2	In the hierarchy of the CA, esFIRMA
0.4.0.194112.1.1	According to the QCP-l policy

These certificates are qualified in accordance with Article 38 and Annex III of Regulation (EU) 910/2014 of the European Parliament and of the Council, of July 23, 2014, and comply with the technical regulations identified with reference ETSI EN 319 411-2.

esFIRMA does not offer backup or key recovery services. Therefore, esFIRMA will not be responsible in any case for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

a) The "key usage" field has enabled, and therefore allows us to perform, the following functions:
   a. Digital signature (for authentication function)
   b. Content commitment (to perform the electronic signature function)
   c. Key encryption

b) In the "Qualified Certificate Statements" field, the following statement appears:
   a. QcCompliance (0.4.0.1862.1.1), which reports that the certificate is issued as qualified.

c) The "User Notice" field describes the use of this certificate.Optional

Certificate of Electronic Seal with centralized management

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.8.4	In the hierarchy of the CA, esFIRMA
0.4.0.194112.1.1	According to the QCP-l policy

These certificates are qualified in accordance with Article 38 and Annex III of Regulation (EU) 910/2014 of the European Parliament and of the Council, of July 23, 2014, and comply with the technical regulations identified with reference ETSI EN 319 411-2.

These certificates are managed in a centralized way.

esFIRMA does not offer backup or key recovery services. Therefore, esFIRMA will not be responsible in any case for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

d) The "key usage" field has enabled, and therefore allows us to perform, the following functions:
   a. Content commitment (to perform the electronic signature function)

e) In the "Qualified Certificate Statements" field, the following statement appears:
   a. QcCompliance (0.4.0.1862.1.1), which reports that the certificate is issued as qualified.

f) The "User Notice" field describes the use of this certificate.Optional

1.4.2 Limits and prohibitions on the use of certificates

Certificates are used for their own function and established purpose, without being able to be used for other functions and purposes.

Similarly, certificates must only be used in accordance with applicable law, especially taking into account import and export restrictions in force at any given time.

Certificates cannot be used to sign requests for issuance, renewal, suspension or revocation of certificates, nor to sign any type of public key certificates, or to sign certificate revocation lists (CRL).

The certificates have not been designed, cannot be used for and are not authorized for use or resale as equipment for controlling dangerous situations or for uses that require fail-safe performance, such as the operation of nuclear facilities, air navigation or communication systems, or weapon control systems, where a failure could directly result in death, personal injury, or severe environmental damage.

The limits indicated in the various fields of the certificate profiles, visible on the esFIRMA website https://www.esfirma.com, must be taken into account

The use of digital certificates in a way that violates this DPC and the rest of the applicable documentation, especially the contract signed with the subscriber and the disclosure texts or PDS, is considered improper use for legal purposes, and exempts esFIRMA from any responsibility for this improper use, whether by the signer or any third party.

esFIRMA does not have access authorization or legal obligation to supervise the data on which the use of a certified key can be applied. Therefore, and as a consequence of this technical impossibility of accessing the content of the message, it is not possible for esFIRMA to issue any assessment of said content, assuming therefore the subscriber, the signer or the person responsible for custody, any responsibility arising from the content associated with the use of a certificate.

Likewise, the subscriber, the signer or the person responsible for custody shall be liable for any responsibility that may arise from the use of the same outside the limits and conditions of use set forth in this DPC, the binding legal documents for each certificate, or the contracts or agreements with the registration entities or their subscribers, as well as for any other improper use thereof arising from this section or that may be interpreted as such in accordance with current legislation.

Certificates are used exclusively and solely from the Electronic Administration Platform or extensions and add-ons of the same that the company ESPUBLICO makes available to the subscriber.

1.5 Policy administration

1.5.1 Organization that manages the document

Office of Security of ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (esFIRMA)
CALLE BARI 39 (Binary Building Edif.)
50197 - ZARAGOZA
(+34) 976300110

Identification Registry	Registro Mercantil de Zaragoza
Tomo	2649
Folio	215
Sheet	Z-28722
CIF	A-50.878.842

1.5.2 Organization contact information

ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (esFIRMA)
CALLE BARI 39 (Binary Building Edif.)
50197 - ZARAGOZA
(+34) 976300110

1.5.3 Organization that approves the document

Security Committee from ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (esFIRMA)

The security committee of esFIRMA, formed by its President, the Information and Service Manager, and the Security Manager of esFirma, is responsible for the approval of this Practices Statement.

Both the functions and the members of said Committee are defined in the Security Policy of esFirma.

1.5.4 Document management procedures

The document and organization system of esFIRMA guarantees, through the existence and application of the corresponding procedures, the correct maintenance of this document and the service specifications related to it.

esFIRMA carries out reviews of this document at least annually or when required by changes in the guidelines and documents it must comply with.

As defined in the Security Policy of esFIRMA, the Security Office will be the entity responsible for maintaining this document.

The Security Office is responsible for drafting, maintaining and managing the DPC, dissemination texts (PDS), delivery and acceptance sheets, and the rest of the legal documentation (agreements, contracts, etc.) of esFirma.

Whenever there are significant changes in the management of the certificates defined in this DPC, a new revision of this document is created, which is recorded in the initial "version control" table within the "general information" section.

The actions of the Security Office occur at the request of its manager based on the needs that arise.

esFirma can make changes that do not require notification when they do not directly affect the rights of the signers and subscribers of the certificates or the subscribers of the seals.
When esFirma is going to introduce changes that modify the rights of signers and subscribers of certificates and subscribers of seals, it must notify publicly so that they can present their comments to the Security Office during the 15 days following the publication of the future changes.

To publicly notify the changes that have occurred, they will be published in the "documentation" section on the website https://www.esfirma.com

The revisions of this DPC will be published on the esFirma website after being approved by the Esfirma Security Committee.

1.6 Acronyms and definitions

1.6.1. Acronyms	
AC (could refer to different things depending on the context, such as Access Control, Alternating Current, or Auto-configuration. Without more context, it is not possible to provide an accurate translation.)*or also CA*)	*Certificate Authority* Certification Authority
AR (or also RA)	*Registration Authority* Registration Authority
CPD	Data Processing Center
CPS (or also DPC)	*Certification Practice Statement*. Certificate Practice Statement
CRL (or also LRC)	*Certificate Revocation List.* List of revoked certificates
DN	*Distinguished Name.* Distinguished name within the digital certificate
DNI	Documento Nacional de Identidad
ETSI EN	*European Telecommunications Standards Institute - European Standard.*
EV (for SSL)	*Extended Validation* Extended validation, in SSL certificates.
FIPS	*Federal Information Processing Standard Publication*
HSM	*Hardware Security Module* Hardware Security Module

IETF	*Internet Engineering Task Force*
NIF	Tax Identification Number
NTP	*Network Time Protocol* Network Time Protocol.
OCSP	*Online Certificate Status Protocol.* Protocol for accessing the status of certificates
OID	*Object Identifier*. Object identifier
PDS	*PKI Disclosure Statements* PKI Disclosure Text.
PIN	*Personal Identification Number (PIN)*. Personal identification number
PKI	*Public Key Infrastructure*. Public Key Infrastructure (PKI)
QSCD (or also DCCF)	*Qualified Electronic Signature/Seal Creation Device.* Qualified signature/seal creation device
QCP	*Qualified Certificate Policy* Qualified certificate policy
QCP-n	*Qualified Certificate Policy-natural person* Qualified certificates policy for natural persons.
QCP-l	*Qualified Certificate Policy-legal person* Qualified certificate policy for legal entities.
QCP-n-qscd	*Qualified Certificate Policy-natural person-qscd* Qualified certificate policy for natural persons on qualified signature/seal device
QCP-l-qscd	*Qualified Certificate Policy-legal person-qscd* Qualified certificate policy for legal entities with qualified signature/seal device
RFC	*Request for Comments* RFC Document
RSA	Rivest-Shamir-Adleman. Type of encryption algorithm
SHA	*Secure Hash Algorithm.* Secure Hash Algorithm
SSL	*Secure Sockets Layer.* Protocol designed by Netscape

	and converted into a network standard, allows the transmission of encrypted information between an Internet browser and a server.
TCP/IP	*Transmission Control Protocol/Internet Protocol (TCP/IP)*. System of protocols, defined within the framework of the IETF.
TSA	*Time Stamping Authority* Electronic Time-Stamping Authority
TSU	*Time Stamping Unit* Time Stamping Authority.
UTC	*Coordinated Universal Time* Coordinated Universal Time (UTC)
VPN	*Virtual Private Network.* Virtual Private Network (VPN)

1.6.2 Definitions

Certification Authority	*It is the entity responsible for the issuance and management of digital certificates.*
Registration Authority	*Entity responsible for managing requests, identifying and registering certificate applicants. It may be part of the Certification Authority or external to it.*
Certificate	*File that associates the public key with some identifying data of the Subject/Signer and is signed by the CA.*
Public key	*Publicly known mathematical value used for the verification of a digital signature or data encryption.*
Private key	*Mathematical value known only by the Subject/Signer and used for the creation of a digital signature or the decryption of data.* *The private key of the CA will be used for certificate signing and CRL signing.* *The private key of the TSA service will be used for the signature of the time stamps.*
CPS	*Set of practices adopted by a Certification Authority for issuing certificates in compliance with a specific certification policy.*
CRL	*File containing a list of certificates that have been revoked within a certain period of time and that is signed by the CA.*
Activation Data	*Private data, such as PINs or passwords used to activate the private key*
DCCF	*Qualified Signature Creation Device. Software or hardware element, duly certified, used by the Subject/Signer for the generation of electronic signatures, so that the cryptographic operations are carried out within the device and its control is guaranteed only by the Subject/Signer.*
Digital signature	*The result of the transformation of a message, or any type of data, by applying the private key in conjunction with known algorithms, guaranteeing in this way:* *a) that the data has not been modified (integrity)* *b) that the person who signs the data is who they claim to be (identification)* *c) that the person who signs the data cannot deny having done*

	so (non-repudiation at origin)
OID	*Unique numerical identifier registered under ISO standardization and referring to a specific object or class of object.*
Key pair	*Set consisting of the public and private key, both mathematically related to each other.*
PKI	*Set of hardware, software, human resources, procedures, etc., that make up a system based on the creation and management of public key certificates.*
Applicant	*In the context of this document, the applicant will be a natural person authorized with a special power of attorney to carry out certain procedures on behalf and representation of the entity.*
Subscriber	*In the context of this document, the legal entity that owns the certificate (at a corporate level)*
Subject/Signer	*In the context of this document, the natural person whose public key is certified by the CA and has, or has exclusive access to, a valid private key to generate digital signatures.*
User Part	*In the context of this document, a person who voluntarily trusts the digital certificate and uses it as a means of accrediting the authenticity and integrity of the signed document*

2. Publication of information and deposit of certificates

2.1 Certificate deposit

esFIRMA has a certificate repository, where information related to certification services is published:

https://www.esfirma.com

This service is available 24 hours a day, 7 days a week and, in case of system failure outside the control of esFIRMA, it will make its best efforts to make the service available again within the period established in section 5.7.4 of this Certification Practice Statement.

2.2 Publication of certification information

esFIRMA publishes the following information in its Deposit:

- The lists of revoked certificates and other certificate revocation status information.
- The applicable certificate policies.
- The Certification Practice Statement.
- The disclosure texts (PKI Disclosure Statements - PDS), at least in Spanish and English language.

2.3 Publication frequency

The information of the certification service provider, including policies and the Certification Practice Statement, is published as soon as it becomes available.

Changes to the Certification Practice Statement are governed by the provisions set forth in section 1.5 of this document.

The certificate revocation status information is published in accordance with the provisions of sections 4.9.7 and 4.9.8 of this Certification Practice Statement.

2.4 Access control

esFIRMA does not limit read access to the information established in section 2.2, but establishes controls to prevent unauthorized persons from adding, modifying or deleting records from the Repository, to protect the integrity and authenticity of the information, especially the revocation status information.

esFIRMA employs reliable systems for the Deposit, so that:

- Only authorized personnel may make annotations and modifications.
- The authenticity of the information can be verified.
- Any technical change that affects security requirements can be detected.

3. Identification and authentication

3.1 Initial registration

3.1.1 Types of names

All certificates contain a distinguished name X.501 in the field *Subject*, including a component *Common Name* (CN), related to the identity of the subscriber and the natural person identified in the certificate, as well as various additional identity information in the field *SubjectAlternativeName*.

The names contained in the certificates are the following.

3.1.1.1 High-level employee public signature certificate on card

Country (C)	“ES”
Organization (O)	Name (official name) of the Administration, organization, public law entity or other subscribing entity of the certificate, to which the employee is linked
organizationalUnitName (OU)	ELECTRONIC CERTIFICATE OF PUBLIC EMPLOYEE
organizationIdentifier	Organization Identifier according to the technical standard ETSI EN 319 412-1
Surname	First and second (optional) surname, according to identification document (DNI/Passport)
Given Name	First name, according to identification document (ID/Passport)
Serial Number	Employee's DNI/NIE
Common Name (CN)	Name Surname1 Surname2 - Employee's ID number
Type of certificate OID: 2.16.724.1.3.5.7.1.1	QUALIFIED CERTIFICATE OF HIGH-LEVEL PUBLIC EMPLOYEE SIGNATURE
Name of the subscribing entity OID: 2.16.724.1.3.5.7.1.2	Name of the subscribing entity
NIF of subscribing entity OID: 2.16.724.1.3.5.7.1.3	NIF entity subscription
DNI/NIE of the responsible person OID: 2.16.724.1.3.5.7.1.4	ID card or foreigner identification number of the responsible person

Given name OID: 2.16.724.1.3.5.7.1.6	Given name of the certificate holder
First surname OID: 2.16.724.1.3.5.7.1.7	First surname of the certificate holder
Second surname OID: 2.16.724.1.3.5.7.1.8	Second surname of the certificate holder. Optional.
Email OID: 2.16.724.1.3.5.7.1.9	Email address of the certificate holder. Optional.

3.1.1.2 Public employee signature certificate, medium level, in HSM

Country (C)	"ES"
Organization (O)	Name (official name) of the Administration, organization or public law entity that subscribes the certificate, to which the employee is linked
organizationalUnitName (OU)	ELECTRONIC CERTIFICATE OF PUBLIC EMPLOYEE
organizationIdentifier	Organization Identifier according to the technical standard ETSI EN 319 412-1
Surname	First and second (optional) surname, according to identification document (DNI/Passport)
Given Name	First name, according to identification document (ID/Passport)
Serial Number	Employee's DNI/NIE
Common Name (CN)	Name Surname1 Surname2 - Employee's ID number
Type of certificate OID: 2.16.724.1.3.5.7.2.1	ELECTRONIC CERTIFICATE OF MEDIUM LEVEL PUBLIC EMPLOYEE
Name of the subscribing entity OID: 2.16.724.1.3.5.7.2.2	Name of the subscribing entity
NIF of subscribing entity OID: 2.16.724.1.3.5.7.2.3	Subscriber entity's tax identification number
DNI/NIE of the responsible person OID: 2.16.724.1.3.5.7.2.4	ID card or foreigner identification number of the responsible person
Personal authentication number OID: 2.16.724.1.3.5.7.2.5	NRP or NIP of the certificate subscriber's responsible person
Given name OID: 2.16.724.1.3.5.7.2.6	Given name of the certificate holder

First surname OID: 2.16.724.1.3.5.7.2.7	First surname of the certificate holder
Second surname OID: 2.16.724.1.3.5.7.2.8	Second surname of the certificate holder. Optional.
Email OID: 2.16.724.1.3.5.7.2.9	Email address of the certificate holder. Optional.

3.1.1.3 High-level employee public authentication certificate on a card

Country (C)	"ES"
Organization (O)	Name (official name) of the Administration, organization, public law entity or other subscribing entity of the certificate, to which the employee is linked
organizationalUnitName (OU)	ELECTRONIC CERTIFICATE OF PUBLIC EMPLOYEE
organizationIdentifier	Organization Identifier according to the technical standard ETSI EN 319 412-1
Surname	First and second (optional) surname, according to identification document (DNI/Passport)
Given Name	First name, according to identification document (ID/Passport)
Serial Number	Employee's DNI/NIE
Common Name (CN)	Name Surname1 Surname2 - Employee's ID number
Type of certificate OID: 2.16.724.1.3.5.7.1.1	HIGH AUTHENTICATION LEVEL ELECTRONIC CERTIFICATE FOR PUBLIC EMPLOYEE
Name of the subscribing entity OID: 2.16.724.1.3.5.7.1.2	Name of the subscribing entity
NIF of subscribing entity OID: 2.16.724.1.3.5.7.1.3	NIF entity subscription
DNI/NIE of the responsible person OID: 2.16.724.1.3.5.7.1.4	ID card or foreigner identification number of the responsible person
Given name OID: 2.16.724.1.3.5.7.1.6	Given name of the certificate holder
First surname OID: 2.16.724.1.3.5.7.1.7	First surname of the certificate holder
Second surname OID: 2.16.724.1.3.5.7.1.8	Second surname of the certificate holder. Optional.

Email OID: 2.16.724.1.3.5.7.1.9	Email address of the certificate holder. Optional.

3.1.1.4 Organizational Seal Certificate, medium level, in software

Country (C)	"ES"
Organization (O)	Name (official name of the organization) of the subscriber
organizationalUnitName (OU)	ELECTRONIC SEAL
organizationIdentifier	Organization Identifier according to the technical standard ETSI EN 319 412-1
Serial Number	DNI/NIE of the subscribing organization
Common Name (CN)	Name of system or application for automatic processing.
Type of certificate OID: 2.16.724.1.3.5.6.2.1	MEDIUM LEVEL ELECTRONIC SEAL
Name of the subscribing entity OID: 2.16.724.1.3.5.6.2.2	Name of the subscribing entity
NIF of subscribing entity OID: 2.16.724.1.3.5.6.2.3	NIF of subscribing entity
System name OID: 2.16.724.1.3.5.6.2.5	System name
Email OID: 2.16.724.1.3.5.6.2.9	Email address of the seal's responsible person

3.1.1.5 Organizational Seal Certificate, medium level, in HSM

Country (C)	"ES"
Organization (O)	Name (official name of the organization) of the subscriber
organizationalUnitName (OU)	ELECTRONIC SEAL
organizationIdentifier	Organization Identifier according to the technical standard ETSI EN 319 412-1
Serial Number	DNI/NIE of the subscribing organization
Common Name (CN)	Name of system or application for automatic processing.
Type of certificate OID: 2.16.724.1.3.5.6.2.1	MEDIUM LEVEL ELECTRONIC SEAL
Name of the subscribing entity OID: 2.16.724.1.3.5.6.2.2	Name of the subscribing entity

NIF of subscribing entity OID: 2.16.724.1.3.5.6.2.3	NIF of subscribing entity
System name OID: 2.16.724.1.3.5.6.2.5	System name

3.1.1.6 Certificate for high-level pseudonymous digital signature of public employee on a card

Country (C)	"ES"
Organization (O)	Name (official name) of the Administration, organization or public law entity that subscribes the certificate, to which the employee is linked
organizationalUnitName (OU)	ELECTRONIC CERTIFICATE OF PUBLIC EMPLOYEE WITH PSEUDONYM
organizationIdentifier	Organization Identifier according to the technical standard ETSI EN 319 412-1
Pseudonym	Mandatory pseudonym according to ETSI EN 319 412-2 for this type of certificates
Common Name (CN)	Seudónimo y el Organismo
Type of certificate OID: 2.16.724.1.3.5.4.1.1	HIGH-LEVEL PSEUDONYMOUS ELECTRONIC CERTIFICATE OF PUBLIC EMPLOYEE
Name of the subscribing entity OID: 2.16.724.1.3.5.4.1.2	Name of the subscribing entity
NIF of subscribing entity OID: 2.16.724.1.3.5.4.1.3	NIF of subscribing entity
Pseudonym OID: 2.16.724.1.3.5.4.1.12	Pseudonym used by the signer and authorized by the subscriber

3.1.1.7 Public employee signature certificate with pseudonym, medium level, in HSM

Country (C)	"ES"
Organization (O)	Name (official name) of the Administration, organization or public law entity that subscribes the certificate, to which the employee is linked
organizationalUnitName (OU)	ELECTRONIC CERTIFICATE OF PUBLIC EMPLOYEE WITH PSEUDONYM
organizationIdentifier	Organization Identifier according to the technical standard ETSI EN 319 412-1

Pseudonym	Mandatory pseudonym according to ETSI EN 319 412-2 for this type of certificates
Common Name (CN)	Seudónimo y el Organismo
Type of certificate OID: 2.16.724.1.3.5.4.2.1	MEDIUM LEVEL PSEUDONYMOUS ELECTRONIC CERTIFICATE FOR PUBLIC EMPLOYEE
Name of the subscribing entity OID: 2.16.724.1.3.5.4.2.2	Name of the subscribing entity
NIF of subscribing entity OID: 2.16.724.1.3.5.4.2.3	NIF of subscribing entity
Pseudonym OID: 2.16.724.1.3.5.4.2.12	Pseudonym used by the signer and authorized by the subscriber

3.1.1.8 Certificate of authentication of public employee, with pseudonym, high level, on card

Country (C)	"ES"
Organization (O)	Name (official name) of the Administration, organization, public law entity or other subscribing entity of the certificate, to which the employee is linked
organizationalUnitName (OU)	ELECTRONIC CERTIFICATE OF PUBLIC EMPLOYEE
organizationIdentifier	Organization Identifier according to the technical standard ETSI EN 319 412-1
Pseudonym	Mandatory Pseudonym according to ETSI EN 319 412-2
Common Name (CN)	Position or role or "PSEUDONYM" - IDENTIFICATION NUMBER - OFFICIAL NAME OF THE ORGANIZATION
Type of certificate OID: 2.16.724.1.3.5.4.1.1	CERTIFICATE OF AUTHENTICATION OF PUBLIC EMPLOYEE WITH PSEUDONYM
Name of the subscribing entity OID: 2.16.724.1.3.5.4.1.2	Name of the subscribing entity
NIF of subscribing entity OID: 2.16.724.1.3.5.4.1.3	NIF of subscribing entity

3.1.1.9 Electronic Seal Certificate of TSA/TSU

Country (C)	"ES"
Organization (O)	Name (official name of the organization) of the subscriber

organizationIdentifier	Organization Identifier according to the technical standard ETSI EN 319 412-1
Common Name (CN)	Name of the STU

3.1.1.10 Certificate of signature of a natural person linked, on a card

Subprofile Spain:

Country (C)	"ES"
Organization (O)	Name (official name) of the certificate subscriber entity, to which the employee is linked
organizationIdentifier	Organization Identifier according to the technical standard ETSI EN 319 412-1
Surname	First and second (optional) surname, according to identification document (DNI/Passport)
Given Name	First name, according to identification document (ID/Passport)
Serial Number	DNI/NIE of the natural person
Common Name (CN)	Surname1 Surname2 Name - ID number of natural person (SIGNATURE)
Type of certificate OID: 1.3.6.1.4.1.47281.0.7.1	CERTIFICATE OF INDIVIDUAL LINKED TO ENTITY
Name of the subscribing entity OID: 1.3.6.1.4.1.47281.0.7.2	Name of the subscribing entity
NIF of subscribing entity OID: 1.3.6.1.4.1.47281.0.7.3	NIF entity subscription
DNI/NIE of the responsible person OID: 1.3.6.1.4.1.47281.0.7.4	ID card or foreigner identification number of the responsible person
Given name OID: 1.3.6.1.4.1.47281.0.7.6	Given name of the certificate holder
First surname OID: 1.3.6.1.4.1.47281.0.7.7	First surname of the certificate holder
Second surname OID: 1.3.6.1.4.1.47281.0.7.8	Second surname of the certificate holder. Optional.
Email OID: 1.3.6.1.4.1.47281.0.7.9	Email address of the certificate holder. Optional.

Subprofile Europe:

Country (C)	Country

Organization (O)	Name (official name) of the certificate subscriber entity, to which the employee is linked
organizationIdentifier	Organization Identifier according to the technical standard ETSI EN 319 412-1
Surname	First and second (optional) last name, according to identity document
Given Name	First name, in accordance with identity document
Serial Number	Identity document number of the natural person
Common Name (CN)	Surname1 Surname2 Name - document number (SIGNATURE)
Type of certificate OID: 1.3.6.1.4.1.47281.0.19.1	PV
Name of the subscribing entity OID: 1.3.6.1.4.1.47281.0.19.2	It corresponds with the subject's organization
Subscriber entity identifier OID: 1.3.6.1.4.1.47281.0.19.3	It corresponds with the organizationIdentifier of the subject
Responsible person identifier OID: 1.3.6.1.4.1.47281.0.19.4	ID card or foreigner identification number of the responsible person
Given name OID: 1.3.6.1.4.1.47281.0.19.6	Given name of the certificate holder
First surname OID: 1.3.6.1.4.1.47281.0.19.7	First surname of the certificate holder
Second surname OID: 1.3.6.1.4.1.47281.0.19.8	Second surname of the certificate holder. Optional.
Subscribing entity unit OID: 1.3.6.1.4.1.47281.0.19.10	Corresponds with OrganizationUnit of the subject. Optional

3.1.1.11 Certificate of signature of a natural person linked, in HSM

Subprofile Spain:

Country (C)	“ES”
Organization (O)	Name (official name) of the subscribing entity, to which the employee is linked
organizationIdentifier	Organization Identifier according to the technical standard ETSI EN 319 412-1
Surname	First and second (optional) surname, according to identification document (DNI/Passport)

Given Name	First name, according to identification document (ID/Passport)
Serial Number	Employee's DNI/NIE
Common Name (CN)	Apellido1 Apellido2 Nombre - NIF natural person
Type of certificate OID: 1.3.6.1.4.1.47281.0.7.1	CERTIFICATE OF INDIVIDUAL LINKED TO ENTITY
Name of the subscribing entity OID: 1.3.6.1.4.1.47281.0.7.2	Name of the subscribing entity
NIF of subscribing entity OID: 1.3.6.1.4.1.47281.0.7.3	NIF entity subscription
DNI/NIE of the responsible person OID: 1.3.6.1.4.1.47281.0.7.4	ID card or foreigner identification number of the responsible person
Given name OID: 1.3.6.1.4.1.47281.0.7.6	Given name of the certificate holder
First surname OID: 1.3.6.1.4.1.47281.0.7.7	First surname of the certificate holder
Second surname OID: 1.3.6.1.4.1.47281.0.7.8	Second surname of the certificate holder. Optional.
Email OID: 1.3.6.1.4.1.47281.0.7.9	Email address of the certificate holder. Optional.

Subprofile Europe:

Country (C)	Country
Organization (O)	Name (official name) of the certificate subscriber entity, to which the employee is linked
organizationIdentifier	Organization Identifier according to the technical standard ETSI EN 319 412-1
Surname	First and second (optional) last name, according to identity document
Given Name	First name, in accordance with identity document
Serial Number	Identity document number of the natural person
Common Name (CN)	Surname1 Surname2 Name - document number
Given name OID: 1.3.6.1.4.1.47281.0.19.6	First name of the certificate holder, corresponds to Given Name
First surname OID: 1.3.6.1.4.1.47281.0.19.7	First surname of the certificate holder
Second surname OID: 1.3.6.1.4.1.47281.0.19.8	Second surname of the certificate holder. Optional.

3.1.1.12 Authentication certificate of a natural person linked, on card

Subprofile Spain:

Country (C)	"ES"
Organization (O)	Name (official name) of the certificate subscriber entity, to which the employee is linked
organizationIdentifier	Organization Identifier according to the technical standard ETSI EN 319 412-1
Surname	First and second (optional) surname, according to identification document (DNI/Passport)
Given Name	First name, according to identification document (ID/Passport)
Serial Number	Employee's DNI/NIE
Common Name (CN)	Surname1 Surname2 Name - NIF natural person (AUTHENTICATION)
Type of certificate OID: 1.3.6.1.4.1.47281.0.7.1	CERTIFICATE OF INDIVIDUAL LINKED TO ENTITY
Name of the subscribing entity OID: 1.3.6.1.4.1.47281.0.7.2	Name of the subscribing entity
NIF of subscribing entity OID: 1.3.6.1.4.1.47281.0.7.3	NIF entity subscription
DNI/NIE of the responsible person OID: 1.3.6.1.4.1.47281.0.7.4	Corresponds with the subject's SerialNumber
Given name OID: 1.3.6.1.4.1.47281.0.7.6	Given name of the certificate holder
First surname OID: 1.3.6.1.4.1.47281.0.7.7	First surname of the certificate holder
Second surname OID: 1.3.6.1.4.1.47281.0.7.8	Second surname of the certificate holder. Optional.
Email OID: 1.3.6.1.4.1.47281.0.7.9	Email address of the certificate holder. Optional.

Subprofile Europe:

Country (C)	Country
Organization (O)	Name (official name) of the certificate subscriber entity, to which the employee is linked

organizationIdentifier	Organization Identifier according to the technical standard ETSI EN 319 412-1
Surname	First and second (optional) last name, according to identity document
Given Name	First name, in accordance with identity document
Serial Number	Identity document number of the natural person
Common Name (CN)	Surname1 Surname2 Name - document number (AUTHENTICATION)
Given name OID: 1.3.6.1.4.1.47281.0.19.6	First name of the certificate holder, corresponds to Given Name
First surname OID: 1.3.6.1.4.1.47281.0.19.7	First surname of the certificate holder
Second surname OID: 1.3.6.1.4.1.47281.0.19.8	Second surname of the certificate holder. Optional.

3.1.1.13 Certificate of signature of a natural person linked, on a card, with a pseudonym

Subprofile Spain:

Country (C)	“ES”
Organization (O)	Name (official name) of the certificate subscriber entity, to which the employee is linked
organizationIdentifier	Organization Identifier according to the technical standard ETSI EN 319 412-1
Pseudonym	Mandatory Pseudonym according to ETSI EN 319 412-2
Common Name (CN)	Position or "PSEUDONYM" - IDENTIFICATION NUMBER - ENTITY NAME

Subprofile Europe:

Country (C)	Country
Organization (O)	Name (official name) of the certificate subscriber entity, to which the employee is linked
organizationIdentifier	Organization Identifier according to the technical standard ETSI EN 319 412-1
Pseudonym	Mandatory Pseudonym according to ETSI EN 319 412-2
Common Name (CN)	PSEUDONYM - ENTITY NAME

3.1.1.14 Certificate of signature of a natural person linked, in HSM

Subprofile Spain:

Country (C)	"ES"
Organization (O)	Name (official name) of the subscribing entity, to which the employee is linked
organizationIdentifier	Organization Identifier according to the technical standard ETSI EN 319 412-1
Pseudonym	Mandatory Pseudonym according to ETSI EN 319 412-2
Common Name (CN)	Position or "PSEUDONYM" - IDENTIFICATION NUMBER - ENTITY NAME

Subprofile Europe:

Country (C)	Country
Organization (O)	Name (official name) of the certificate subscriber entity, to which the employee is linked
organizationIdentifier	Organization Identifier according to the technical standard ETSI EN 319 412-1
Pseudonym	Mandatory Pseudonym according to ETSI EN 319 412-2
Common Name (CN)	PSEUDONYM - ENTITY NAME

3.1.1.15 Certificate of linked natural person authentication, on card, with pseudonym

Subprofile Spain:

Country (C)	"ES"
Organization (O)	Name (official name) of the certificate subscriber entity, to which the employee is linked
organizationIdentifier	Organization Identifier according to the technical standard ETSI EN 319 412-1
Common Name (CN)	Position or "PSEUDONYM" - IDENTIFICATION NUMBER - ENTITY NAME

Subprofile Europe:

Country (C)	Country
Organization (O)	Name (official name) of the certificate subscriber entity, to which the employee is linked

organizationIdentifier	Organization Identifier according to the technical standard ETSI EN 319 412-1
Pseudonym	Mandatory Pseudonym according to ETSI EN 319 412-2
Common Name (CN)	PSEUDONYM - ENTITY NAME

3.1.1.16 Electronic seal certificate, in software

Subprofile Spain:

Country (C)	“ES”
Organization (O)	Name (official name of the organization) of the subscriber
organizationalUnitName (OU)	ELECTRONIC SEAL
organizationIdentifier	Organization Identifier according to the technical standard ETSI EN 319 412-1
Serial Number	DNI/NIE of the subscribing organization
Common Name (CN)	Name of system or application for automatic processing.

Subprofile Europe:

Country (C)	Country
Organization (O)	Name (official name of the organization) of the subscriber
organizationIdentifier	Organization Identifier according to the technical standard ETSI EN 319 412-1
Serial Number	Identification of the subscribing organization (legalPersonSemanticsIdentifier)

3.1.1.17 Centralized management electronic seal certificate

Subprofile Spain:

Country (C)	“ES”
Organization (O)	Name (official name of the organization) of the subscriber
organizationalUnitName (OU)	ELECTRONIC SEAL
organizationIdentifier	Organization Identifier according to the technical standard ETSI EN 319 412-1
Serial Number	DNI/NIE of the subscribing organization
Common Name (CN)	Name of system or application for automatic processing.

Subprofile Europe:

Country (C)	Country
Organization (O)	Name (official name of the organization) of the subscriber
organizationIdentifier	Organization Identifier according to the technical standard ETSI EN 319 412-1
Serial Number	Identification of the subscribing organization (legalPersonSemanticsIdentifier)

3.1.2. Meaning of the names

The names contained in the fields *SubjectName* and *SubjectAlternativeName* the certificates are understandable in natural language, in accordance with what is established in the previous section.

3.1.3 Use of anonymous and pseudonymous

Under no circumstances can pseudonyms be used to identify an entity/company/organization, and anonymous certificates are never issued, except in cases where, for reasons of public security, electronic signature systems may only refer to the professional identification number of the public employee.

3.1.4 Interpretation of name formats

Name formats will be interpreted in accordance with the law of the country of establishment of the subscriber, in their own terms.

The "country" field will always be Spain as the certificates are issued exclusively to Spanish Public Administrations.

The certificate shows the relationship between a natural person and the Administration, organization, public law entity or other entity with which it is linked, regardless of the nationality of the natural person. This derives from the corporate nature of the certificate, of which the corporation is the subscriber, and the natural person linked is the person authorized to use it.

In certificates issued to Spanish subscribers, the "serial number" field must include the signer's NIF for the purpose of admitting the certificate for carrying out procedures with the Spanish Administrations.

3.1.5 Uniqueness of names

The names of certificate subscribers will be unique for each certificate policy of esFIRMA.

It will not be possible to assign a subscriber name that has already been used to a different subscriber, a situation that should not arise in principle, thanks to the presence of the Tax Identification Number, or equivalent, in the naming scheme.

A subscriber may request more than one certificate provided that the combination of the following values existing in the request is different from a valid certificate:

- Tax Identification Number (TIN) or other legally valid identifier of the natural person.
- Tax Identification Number (TIN) or other legally valid identifier of the subscriber.
- Certificate Type (Certificate Description Field).

3.1.6 Resolution of disputes regarding names

Certificate applicants shall not include names in the requests that may infringe, by the future subscriber, on third-party rights.

esFIRMA will not be obliged to determine in advance that a certificate applicant has industrial property rights over the name that appears in a certificate application, but will proceed to certify it in principle.

Likewise, it shall not act as an arbitrator or mediator, nor in any other way shall it resolve any dispute concerning the ownership of personal or organizational names, domain names, trademarks or trade names.

However, in the event of receiving a notification regarding a name conflict, in accordance with the legislation of the subscriber's country, they may take the appropriate actions aimed at blocking or withdrawing the issued certificate.

In any case, the certification service provider reserves the right to reject a certificate request due to a name conflict.

Any controversy or conflict arising from this document will be definitively resolved through the legal arbitration of an arbitrator, within the framework of the Spanish Court of Arbitration, in accordance with its Regulations and Statutes, which is entrusted with the administration of the arbitration and the appointment of the arbitrator or arbitration tribunal. The parties acknowledge their commitment to comply with the award issued in the contractual document that formalizes the service.

3.2 Initial validation of identity

The identity of certificate subscribers is established at the time of signing the contract between esFIRMA and the subscriber or prior to the activation of the esFIRMA service, at which point the existence of the subscriber and the documentation provided to justify their identity, position and/or condition in which they sign, and their address are verified, in accordance with the provisions of the administrative law regulations applicable.

The identity of the natural persons identified in the certificates is validated through the corporate records of the Administration, organization, public law entity or other subscriber entity of the certificates. The subscriber will produce a certification of the necessary data, and will send it to esFIRMA, through the means that it enables, for the registration of the identity of the signatories. When the subscriber does not have a Secretariat, this certification will be issued by the designated Certification Service Manager.

The person responsible for the processing of personal data of each Administration, organization, public entity or other entity, is each one of them, with esFIRMA being in charge of the processing of said data.

To avoid any conflict of interest, Public Administrations or other subscribing entities are independent entities from the Trusted Service Provider "esFIRMA" and the company ESPUBLICO[1].

3.2.1 Proof of possession of private key

The possession of the private key is demonstrated by virtue of the reliable procedure for delivery and acceptance of the certificate by the signer from the Electronic Administration Platform, by signing the acceptance sheet, and its use in said platform.

1. 3.2.2 Entity identification

In public administrations, the documentation proving the existence of the public administration, organization or public law entity is not required, since said identity is part of the corporate scope of the General State Administration or other State Public Administrations.

EsFIRMA verifies the existence of each Public Administration, organization, or public law entity, when necessary, before the inventory of public sector entities of the Ministry of Finance and Public Function, before an Official Gazette of its scope, or through integration with the Common Directory System (DIR3).https://www.hacienda.gob.es/es-ES/CDI/Paginas/Inventario/Inventario.aspx

In case the entity is not part of the corporate scope of the General Administration of the State or other State AAPP, ESFIRMA will verify the existence of the entity through the documents or consultation of relevant public records as indicated in the administrative law regulations that are applicable.

Natural persons with the capacity to act on behalf of an Administration, organization, public law entity, or other entity subscribing to the certificates may act as representatives of the same in relation to the provisions of this DPC, provided that there is a prior situation of legal or voluntary representation between the natural person and the Administration,

[1] Ap 6.2.2.q) de ETSI EN 319 411-1

organization, public law entity, or other entity subscribing to the certificates, which requires recognition by esFIRMA, which will be carried out through one of the following procedures:

1. In the event that the person holding the position of Secretary has the power of public faith, the following documents will be collected and verified:
    a. Certificate of the Secretary in which the legal representative is named, with the following information:
        i. Full name of the legal representative
        ii. Document: Representative's NIF (tax identification number)
        iii. Tax ID of the entity being represented
        iv. Name of the entity being represented
        v. Postal address of the entity being represented

2. In the event that the person holding the position of Secretary does not have the power of public faith, the following documents will be collected and verified:
    a. A certificate from the Secretary of the appointment of the legal representative that includes the following information:
        i. Representative's information:
            1. Full name of the legal representative
            2. Document: Representative's NIF (tax identification number)
        ii. Data of the entity being represented:
            1. CIF
            2. Name
            3. Mailing address
        iii. Information about the validity of the representation
    b. Official documentation that allows to accredit the data related to the representation or the capacity to act held by the legal representative.
    c. All necessary documents to prove the aforementioned points in a reliable manner, in accordance with the provisions of the applicable administrative law, and their registration in the corresponding public registry if required.

After verifying the collected documentation, the Legal Representative will proceed to sign the certification services contract between esFIRMA (ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA) and the entity through which the conditions under which ESFIRMA will provide certification services to the entity are regulated, which is established as a Registration Authority, appointing the authorized Operators to exercise the corresponding functions of the RA.

Once the electronic documents are signed, the RA functions will be activated for the users of the entity who are listed in the contract as authorized operators to perform this function.

3.2.3 Authentication of the identity of a natural person

This section describes the methods for verifying the identity of a natural person identified in a certificate.

The procedure to request and generate certificates is carried out through an electronic procedure in the Electronic Administration Platform available to the subscriber and signers.

The electronic procedure for issuing a certificate to a natural person will follow the following steps and the following documents will be generated:

1. Request from the individual through the Electronic Administration Platform (with its corresponding entry registration and opening of the file).
2. A certificate in which the Verification Operator certifies the connection between the applicant and the entity.
3. Issuance order signed by the Authorization Operator of the entity, which is registered for outgoing and notified to ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (attaching a copy of the certificate and the user's request).

The electronic procedure for issuing an electronic seal certificate will follow the following steps and the following documents will be generated:

1. Issuance order from the Legal Representative through the Electronic Administration Platform (with its corresponding entry registration and file opening). To submit this request, the Legal Representative must identify themselves on the platform using electronic identification means, for which the physical presence of the person has been guaranteed according to Article 8 of the eIDAS Regulation in relation to the "substantial" or "high" security levels.

3.2.3.1 In the certificates

The identification information of the natural persons identified in the certificates is validated by comparing the information from the request of the Administration, organization, public law entity or other subscriber entity of the certificates, with the records of the Administration, organization, public law entity or other entity to which it is linked, generated as indicated in point 3.2 of this DPC, ensuring the correctness of the information to be certified.

3.2.3.2 Need for personal presence

To request certificates, direct physical presence is not required due to the already accredited relationship between the individual and the Administration, agency, public law entity, or other entity to which they are linked. This accreditation is reflected in the validation of the request by the Verification Operator authorized by the subscriber, who attests to the in-person and unique identification of the signer.

To accept the certificate, the direct physical presence of the signer is not necessary since it can be done through an advanced electronic signature. During this process, the identity of the individual identified in the certificate is confirmed.

3.2.3.3 Linking of the natural person

The documentary justification of the link between a natural person identified in a certificate and the Administration, organization, public law entity or other entity is given by its registration in the Personnel Registers of the Administration, organization, public law entity or other entity to which the natural person is linked.

3.2.4 Unverified subscriber information

esFIRMA does not include any unverified subscriber information in the certificates.

3.2.5 Interoperability criteria

esFIRMA does not have interoperability relationships with other external certification authorities.

esFIRMA does not issue certificates for subordinate CAs to third parties and its issuing CA is not technically limited.

3.3 Identification and authentication of renewal requests

3.3.1 Validation for routine certificate renewal

esFirma does not perform certificate renewals. esFirma will issue a new certificate, following the request procedure registered in the Electronic Administration Platform.

3.3.2 Identification and authentication of renewal after revocation

esFIRMA does not perform certificate renewals.

3.4 Identification and authentication of the revocation request

esFIRMA authenticates requests and reports related to the revocation of a certificate, verifying that they come from an authorized person.
The acceptable methods for such verification are the following:

- The submission of a revocation request by the subscriber or the natural person identified in the certificate, signed electronically.
- The use of the "identity verification phrase," or other personal authentication methods, consisting of information known only to the natural person identified in the certificate, and which allows them to automatically revoke their certificate.
- Physical appearance at an office of the subscribing entity.
- Other means of communication, such as the telephone, when there are reasonable guarantees of the identity of the revocation requester, at the discretion of esFIRMA.

esFIRMA does not perform certificate suspensions. Suspension requests are treated as revocation requests.

4. Certificate lifecycle operation requirements

4.1 Certificate request

4.1.1 Legitimation to request issuance

The Administration, organization, public law entity or other entity must sign a certification service provision contract with esFIRMA.

Likewise, prior to the issuance and delivery of a certificate, there is a certificate request on a certificate request form through the Electronic Administration Platform.

There is an authorization from the subscriber for the applicant to make the request, which is legally formalized through a certificate request form signed by said applicant on behalf of the Administration, organization, public law entity or other entity.

4.1.2 Registration procedure and responsibilities

esFIRMA receives certificate requests made by Administrations, organizations, public law entities or other entities.

The requests are made through an electronic document, completed by the Administration, organization, public entity or other entity, whose recipient is esFIRMA, which will include the data of the people to whom certificates will be issued. The request will be made by the operator authorized by the subscriber (certification authority) and who has been identified in the contract between this subscriber and esFIRMA.

The application must be accompanied by supporting documentation for the identity and other circumstances of the natural person identified in the certificate, in accordance with the provisions of section 3.2.3. A physical address or other data that allow contacting the natural person identified in the certificate must also be provided.

4.2 Processing of the certification request

4.2.1 Execution of identification and authentication functions

Once a certificate request is received, esFIRMA ensures that the certificate requests are complete, accurate, and properly authorized before processing them.

If so, esFIRMA verifies the provided information, checking that the requirements described in section 3.2 have been correctly fulfilled.

The supporting documentation for the approval of the request must be kept and properly registered and with security and integrity guarantees for a period of 15 years from the expiration of the certificate or the completion of the service provided, even in the event of early loss of validity due to revocation, as the certificates are qualified.

esFIRMA maintains documented procedures that identify and require additional verification activity for high-risk certificate requests, phishing or other fraudulent uses, consulting different domain reputation lists and esFIRMA's own risk mitigation criteria.

4.2.2 Approval or rejection of the request

esFIRMA approves the certificate request and proceeds to its issuance and delivery, after the request that occurs in the Electronic Administration Platform.

In case of suspicion that the information is not correct or may affect the reputation of the Certification Authority or subscribers, esFIRMA will deny the request, or stop its approval until it has carried out the complementary checks it deems appropriate.

In case the additional checks do not confirm the accuracy of the information to be verified, esFIRMA will definitively deny the request.

esFIRMA notifies the applicant of the approval or denial of the request.

esFIRMA may automate the procedures for verifying the correctness of the information that will be contained in the certificates, and for approving the requests.

4.2.3 Deadline for resolving the request

esFIRMA attends certificate requests in the order they are received, within a reasonable period of time, and a maximum time guarantee can be specified in the certificate issuance contract.

The requests remain active until their approval or rejection.

4.3 Certificate issuance

4.3.1 Actions of the CA during the issuance process

After the approval of the certification request, the certificate is securely issued and made available to the signer for acceptance by sending a link to the mobile device and/or email address designated by the subscriber in the certificate request, according to the procedure indicated in section 4.4.2 or through the messaging system of the Electronic Administration Platform.

During the process, esFIRMA:

- Protects the confidentiality and integrity of the registration data it has.
- Uses reliable systems and products that are protected against any alteration and that guarantee the technical and, where appropriate, cryptographic security of the certification processes they support.
- Generate the key pair, through a certificate generation procedure securely linked to the key generation procedure.
- It uses a certificate generation procedure that securely links the certificate with the registration information, including the certified public key.
- Ensures that the certificate is issued by systems that use protection against forgery and guarantee the confidentiality of the keys during the process of generating such keys.
- Includes in the certificate the information established in Annex 1 of Regulation (EU) 910/2014, in accordance with the provisions of sections 3.1.1 and 7.1.
- Indicates the date and time when a certificate was issued.

4.3.2 Notification of issuance to the subscriber

esFIRMA notifies the issuance of the certificate to the Administration, organization, public law entity or other subscriber entity of the certificate, and to the natural person identified in the certificate, through their email addresses, already included in the information of the Electronic Administration Platform.

4.4 Certificate delivery and acceptance

During this process, esFIRMA must perform the following actions:

- Definitively accrediting the identity of the natural person identified in the certificate, with the collaboration of the Administration, organization, public law entity or other entity in accordance with the provisions of sections 3.2.2, 3.2.3, and 4.3.1.
- Deliver the certificate delivery and acceptance form to the natural person identified therein, which includes the following minimum contents:
    - Basic information about the use of the certificate, including especially information about the certification service provider and the applicable Certification Practice Statement, such as its obligations, powers, and responsibilities
    - Information about the certificate.
    - Recognition, by the signer, of receiving the certificate and acceptance of the mentioned elements.
    - Regime of obligations of the signer.
    - Responsibility of the signer.
    - Method of exclusive attribution to the signer, of their private key and their certificate activation data, in accordance with the provisions of sections 6.2 and 6.4.
    - The date of the delivery and acceptance act.
- Obtain the signature, written or electronic, of the person identified in the certificate.

When necessary, the Administration, organization, public law entity or other entity collaborates in these processes, and must documentarily register the previous acts and keep the aforementioned original documents (delivery and acceptance sheets), sending an electronic copy to esFIRMA, as well as the originals when esFIRMA requires access to them.

4.4.1 Conduct that constitutes acceptance of the certificate

After the approval of the certification request, the certificate is securely issued and the signer is notified for acceptance by sending a link to the mobile device and/or email address designated by the subscriber in the certificate request or through the messaging system of the Electronic Administration Platform.

In software-issued certificates, the certificate and keys are managed in an HSM, with the signer having exclusive control over their use.

In certificates issued on a card, these are sent to the subscriber's certification authority, and the corresponding PIN is sent directly to the signer's postal address.

In addition, the acceptance of the certificate by the natural person identified in the certificate is carried out by signing the delivery and acceptance form through the Electronic Administration Platform.

4.4.2 Certificate publication

In the case of the TSA/TSU certificate, esFIRMA publishes it on its website.

4.4.3 Notification of issuance to third parties

esFIRMA does not notify any third-party entities of the issuance.

4.5 Use of the key pair and the certificate

4.5.1 Use by the subscriber or signer

esFIRMA obliges to the following:

- To provide esFIRMA with complete and adequate information, in accordance with the requirements of this Certification Practice Statement, especially regarding the acceptance procedure.
- Express your prior consent to the issuance and delivery of a certificate.
- Use the certificate in accordance with what is established in section 1.4.
- When the certificate works together with a DCCF, it recognizes its ability to produce qualified electronic signatures, which are equivalent to handwritten signatures, as well as other types of electronic signatures and mechanisms for encrypting information.
- Be especially diligent in the custody of your private key, in order to prevent unauthorized uses, in accordance with the provisions of sections 6.1, 6.2 and 6.4.
- Communicate to esFIRMA and any person who believes they can trust the certificate, without unjustified delays:
    - The loss, theft or potential compromise of your private key.
    - The loss of control over your private key, due to the compromise of activation data (for example, the PIN code) or for any other reason.
    - Inaccuracies or changes in the content of the certificate that the subscriber knows or could know.
- Stop using the private key after the period indicated in section 6.3.2.
- That all the information provided by the signer contained in the certificate is correct.
- That the certificate is used exclusively for legal and authorized purposes, in accordance with the Certification Practice Statement.
- That no unauthorized person has ever had access to the private key of the certificate, and that he/she is solely responsible for damages caused by failure to protect the private key.
- That the signer is an end entity and not a certification service provider, and that they will not use the private key corresponding to the public key listed in the certificate to sign any certificate (or any other format of certified public key), nor Certificate Revocation List, nor certification service provider title, nor in any other case.

4.5.2 Use by the subscriber

esFIRMA obligates the subscriber contractually to:

- To provide the Certification Authority with complete and adequate information, in accordance with the requirements of this Certification Practice Statement, especially regarding the acceptance procedure.
- Express your prior consent to the issuance and delivery of a certificate.
- Use the certificate in accordance with what is established in section 1.4.
- Communicate to esFIRMA and any person that the subscriber deems trustworthy, without unjustified delays:
    - The loss, theft or potential compromise of your private key.
    - The loss of control over your private key, due to the compromise of activation data (for example, the PIN code) or for any other reason.
    - Inaccuracies or changes in the content of the certificate that the subscriber knows or could know.
    - The loss, alteration, unauthorized use, theft or compromise, when it exists, of the card.
- To transfer to the natural persons identified in the certificate the compliance with their specific obligations, and to establish mechanisms to ensure their effective compliance.
- Do not monitor, manipulate or perform reverse engineering acts on the technical implementation of esFIRMA certification services, without prior written permission.
- Do not compromise the security of the certification services of the certification service provider of esFIRMA, without prior written permission.
- That all statements made in the application are correct.
- That all the information provided by the subscriber contained in the certificate is correct.
- That the certificate is used exclusively for legal and authorized purposes, in accordance with the Certification Practice Statement.
- That no unauthorized person has ever had access to the private key of the certificate, and that he/she is solely responsible for damages caused by failure to protect the private key.
- That the subscriber is an end entity and not a certification service provider, and that they will not use the private key corresponding to the public key listed

in the certificate to sign any certificate (or any other format of certified public key), nor Certificate Revocation List, nor certification service provider title or in any other case.

4.5.3 Use by the third party that trusts certificates

esFIRMA informs the third party who relies on certificates that they must assume the following obligations:

- Seek independent advice on whether the certificate is appropriate for the intended use.
- Verify the validity, suspension or revocation of the issued certificates, for which it will use information about the status of the certificates.
- Verify all certificates in the certificate hierarchy before trusting the digital signature or any of the certificates in the hierarchy.
- Recognize that to be considered a qualified certificate, it must be included in the National Trust List (Trusted List).
- Recognize that verified electronic signatures, produced on a qualified signature creation device (QSCD), have the legal status of qualified electronic signatures; that is, equivalent to handwritten signatures, as well as that the certificate allows the creation of other types of electronic signatures and encryption mechanisms.
- Take into account any limitation on the use of the certificate, regardless of whether it is in the certificate itself or in the contract of a third party that relies on the certificate.
- Take into account any precaution established in a contract or other instrument, regardless of its legal nature.
- Do not monitor, manipulate or perform reverse engineering acts on the technical implementation of esFIRMA certification services, without prior written permission.
- Do not compromise the security of the esFIRMA certification services without prior written permission.

esFIRMA informs the third party who relies on certificates that they must assume the following responsibilities:

- That has enough information to make an informed decision whether to trust the certificate or not.
- Which is solely responsible for trusting or not trusting the information contained in the certificate.
- Who will be solely responsible if they fail to comply with their obligations as a third party that trusts the certificate.

4.6. Certificate renewal

esFIRMA does not perform certificate renewal. esFirma will issue a new certificate, following the request procedure registered in the Electronic Administration Platform.

4.6.1 Circumstances for certificate renewal

Not applicable.

4.6.2 Who can request a renewal

Not applicable.

4.6.3 Processing of certificate renewal request

Not applicable.

4.6.4 Notification of new certificate issuance to the subscriber

Not applicable.

4.6.5 Conduct that constitutes the acceptance of a renewal certificate

Not applicable.

4.6.6 Publication of the renewal certificate by the CA

Not applicable.

4.6.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.7 Renewal of keys and certificates

4.7.1 Who can request the certificate for a new public key

Not applicable.

4.7.2 Procedure with new identification

Not applicable.

4.7.3 Processing of new certificate key requests

esFIRMA will warn the subscriber of the need to proceed with a new personal appearance of the signer and signature of the acceptance sheet, in those cases where it is necessary due to the expiration of the legal identification period of 5 years.

Said personification and identification will be carried out in accordance with what is indicated in section 3.2.

The signature of the acceptance sheet will be carried out in accordance with what is indicated in section 4.4.2.

4.7.4 Notification of the issuance of the renewed certificate

Not applicable because there are no renewals.

4.7.5 Conduct that constitutes acceptance of the certificate

Not applicable.

4.7.6 Certificate publication

Not applicable.

4.7.7 Notification of issuance to third parties

esFIRMA does not notify third parties of the issuance.

4.8 Modification of certificates

The modification of certificates will be treated as a new issuance of certificate, applying what is described in sections 4.1, 4.2, 4.3 and 4.4.

4.9 Revocation and suspension of certificates

4.9.1 Causes for revocation of certificates

esFIRMA will extinguish the validity of electronic certificates through revocation when any of the following causes occur:

1) Circumstances affecting the information contained in the certificate:
    a) Modification of any of the data contained in the certificate, after the corresponding issuance of the certificate that includes the modifications.
    b) Discovery that some of the data contained in the certificate request is incorrect.
    c) Discovery that some of the data contained in the certificate is incorrect.

2) Circumstances affecting the security of the key or certificate:
    a) Compromise of the private key, infrastructure or systems of the certification service provider that issued the certificate, provided that it affects the reliability of the certificates issued from that incident.
    b) Infringement, by esFIRMA, of the requirements provided 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 issued certificate.

d) Unauthorized access or use, by a third party, of the private key corresponding to the public key contained in the certificate.

e) The irregular use of the certificate by the natural person identified in the certificate, or the lack of diligence in the custody of the private key.

3) Circumstances affecting the subscriber or the natural person identified in the certificate:

a) Termination of the legal relationship for the provision of services between esFIRMA and the subscriber.

b) Modification or termination of the underlying legal relationship or cause that led to the issuance of the certificate to the natural person identified in the certificate.

c) Violation by the certificate applicant of the pre-established requirements for its application.

d) Infringement by the subscriber or by the person identified in the certificate, of their obligations, responsibilities and guarantees, established in the corresponding legal document.

e) The incapacity or death of the key holder.

f) The extinction of the legal entity that subscribed the certificate, as well as the end of the subscriber's authorization to the key holder or the termination of the relationship between the subscriber and the person identified in the certificate.

g) Subscriber's request for certificate revocation, in accordance with section 3.4.

4) Other circumstances:

a) The termination of the esFIRMA certification service, in accordance with what is established in section 5.8.

b) The use of the certificate that is harmful and continuous for esFIRMA. In this case, use is considered harmful based on the following criteria:

   - The nature and number of complaints received.
   - The identity of the entities that submit the complaints.
   - The relevant legislation in force at all times.

  - The response of the subscriber or the person identified in the certificate to the received complaints.

c) Loss of certification of any of the qualified signature creation devices that esFIRMA was using as a Qualified Trust Service Provider

4.9.2 Legitimation to request revocation

The revocation of a certificate can be requested:

- The person identified in the certificate, by means of a request addressed to esFIRMA or the subscriber.
- The certificate subscriber, by means of a request addressed to esFIRMA.

4.9.3 Revocation request procedures

The revocation request shall include the following information:

- Revocation request date.
- Identity of the subscriber or signer.
- Detailed reason for the revocation request.

The request must be authenticated, by means of esFIRMA, in accordance with the requirements established in section 3.4 of this policy, before proceeding with the revocation.

esFIRMA may include any other requirement for the confirmation of revocation requests[2].

The revocation service is located in the Electronic Administration Platform, where the signer and the subscriber manage their certificates.

In case the recipient of a revocation request by an identified natural person in the certificate is the subscribing entity, once the request is authenticated, it must send a request to esFIRMA in this regard.

[2] Ap 6.2.4.a) iii) de ETSI EN 319 411-1

The revocation request will be processed upon receipt, and the subscriber and the natural person identified in the certificate will be informed about the change of status of the revoked certificate.

esFIRMA does not reactivate the certificate once it has been revoked.

There is a 24/7 service available at the phone number +34 976 579 516, to request the revocation of certificates. The communication is recorded and registered, to be used as support and guarantee of acceptance of the requested revocation.

4.9.4 Temporal deadline for revocation request

Revocation requests will be sent immediately once the cause of revocation is known, and will not exceed 24 hours[3].

4.9.5 Temporal processing period of the request

Revocation will occur immediately upon receipt, during esFIRMA's regular operating hours, and will not exceed 60 minutes[4].

4.9.6 Obligation to consult certificate revocation information by third parties

Third parties must verify the status of those certificates in which they wish to trust.

One method to verify the status of certificates is by consulting the latest Certificate Revocation List issued by the esFIRMA Certification Authority.

The Certificate Revocation Lists are published in the Certification Authority Repository, as well as in the following web addresses, indicated within the certificates:

- *CA ROOT:*

[3] Ap 6.2.4.a) vi) de ETSI EN 319 411-1

[4] Ap 6.2.4.a) vii) de ETSI EN 319 411-1

  - https://crls2.esfirma.com/acraiz/acraiz2.crl
  - https://crls1.esfirma.com/acraiz/acraiz2.crl

- *INTERMEDIATE CA:*
  - https://crls1.esfirma.com/acaapp/acaapp2.crl
  - https://crls2.esfirma.com/acaapp/acaapp2.crl

In addition, third parties must verify the status of the certificates included in the certification chain.

4.9.7 Frequency of issuance of certificate revocation lists (CRLs)

esFIRMA issues a CRL at least every 24 hours and whenever a revocation occurs.

The CRL indicates the scheduled time for issuing a new CRL, although a CRL can be issued before the deadline indicated in the previous CRL, to reflect revocations.

The CRL obligatorily maintains the revoked or suspended certificate until it expires.

4.9.8 Maximum term for CRLs publication

The CRLs are published in the Repository within a reasonable immediate period after their generation, which in no case exceeds a few minutes.

4.9.9 Availability of online certificate status checking services

esFIRMA informs about the revocation status of certificates, through the OCSP protocol, which allows to know the validity status of certificates online from the following addresses:

- http://ocsp.esfirma.com/acaapp2/
- http://ocsp1.esfirma.com/acaapp2/
- http://ocsp2.esfirma.com/acaapp2/

In case of failure of the certificate status verification systems due to causes beyond the control of esFIRMA, it must make its best efforts to ensure that this service remains inactive for the shortest possible time, which may not exceed one day.

esFIRMA provides information to third parties who rely on certificates about the operation of the certificate status information service.

Certificate status checking services are free to use[5].

esFIRMA keeps available the revocation status information after the validity period of the certificate[6].

4.9.10 Obligation to consult certificate status checking services

It is mandatory to check the status of certificates before trusting them, as a priority, through access to the OCSP service.

esFIRMA supports the GET method for OCSP.

esFIRMA updates the OCSP at least every four days and immediately under normal conditions.

OCSP responses have a maximum expiration time of 48 hours.

To know the status of subordinate CA certificates, the information provided through OCSP is updated at least every six months and within 24 hours of revocation of a subordinate CA certificate.

If the OCSP responder receives a status request for a certificate that has not been issued, it will return *revoked, certificateHold January 1, 1970*, registering such requests as part of the security response procedures of esFIRMA.

[5] Ap 6.3.10 de ETSI EN 319 411-2

[6] Ap 6.3.10.b) de ETSI EN 319 411-2

4.9.11 Other forms of certificate revocation information

Alternatively, third parties who rely on certificates may verify the revocation status of the certificates by consulting the most recent CRLs issued by esFIRMA. These are published on the esFIRMA website, as well as at the web addresses indicated in the certificates.

esFIRMA does not delegate its OCSP responses through OCSP stapling.

4.9.12 Special requirements in case of compromise of the private key

The compromise of the private key of esFIRMA is notified to all participants in the certification services, as far as possible, by publishing this fact on the esFIRMA website, as well as, if deemed necessary, in other means of communication, including paper.

4.9.13 Causes for suspension of certificates

esFIRMA does not perform certificate suspension.

4.9.14 Request for suspension

esFIRMA does not perform certificate suspension

4.9.15 Procedures for requesting suspension

esFIRMA does not perform certificate suspension.

4.9.16 Maximum suspension period

esFIRMA does not perform certificate suspension.

4.10 Certificate status checking services

4.10.1 Operational characteristics of services

The certificate status checking services are provided through a web query interface, on the website https://www.esfirma.com

They can also be verified by accessing the OCSP service at the web addresses indicated in section 4.9.9

Revocation entries in a CRL or OCSP response are never removed.

Differences and considerations between revocation status queries of a certificate using OCSP and CRL:

- Both OCSP and CRL show the most recent information about the revocation status of a non-expired certificate. However, the CRL requires a publication process of a few minutes that can result in temporary discrepancies between both methods. Eventually, the revocation status of a non-expired certificate is the same when queried via OCSP and CRL.
- CRLs do not include revoked certificates that have already expired, while OCSP does include such information. By adding expired certificates to a CRL, the time required to verify the validity of certificates is increased, as the list is larger and takes longer to download and process. In addition, there is an indefinite growth in CRLs until the end of the issuer's validity.
- EsFIRMA issues a Last CRL, which refers to the last CRL issued before the CRL issuer's certificate ceases to be valid due to expiration, revocation, or other cases. This CRL, along with an LTA signature file, is used to verify whether a certificate was valid or not at a given time. If the Last CRL cannot be validated, it must be assumed that the certificate is invalid. Once the Last CRL has been verified, the certificate's status in the CRL must be checked.
- OCSP requires real-time connection with the certification authority to obtain the revocation status, while CRLs can be downloaded and stored locally for offline use.
- OCSP can be less private than CRLs, as OCSP requests can reveal to the certification authority the sites a client is visiting.

4.10.2 Availability of services

The certificate status checking service and the time stamping service are available 24 hours a day, 7 days a week, all year round, except for scheduled downtime.

The certificate status checking services are free to use.

4.10.3 Optional features

Not applicable.

4.11 Completion of subscription

After the validity period of the certificate has elapsed, the subscription to the service will end.

4.12 Key deposit and recovery

4.12.1 Key storage and recovery policy and practices

esFIRMA does not provide key storage and recovery services.

4.12.2 Policy and practices for encapsulation and recovery of session keys

Without stipulation.

5. Physical, management, and operational security controls

5.1 Physical security controls

esFIRMA has established physical and environmental security controls to protect the resources of the facilities where the systems, the systems themselves, and the equipment used for the registration and approval of requests, technical generation of certificates, and management of cryptographic hardware operations are located.

Specifically, the physical and environmental security policy applicable to certificate generation services, cryptographic devices, and revocation management has established requirements for the following contingencies:

- Physical access controls.
- Protection against natural disasters.
- Fire protection measures.
- Failure of support systems (electrical power, telecommunications, etc.)
- Collapse of the structure.
- Floods.
- Anti-theft protection.
- Unauthorized output of equipment, information, media and applications related to components used for the services of the certification service provider.

These measures are applicable to the facilities where the certificates are produced under the full responsibility of esFIRMA, which provides it from its high-security facilities, both main and, where appropriate, contingency operation, which are duly audited periodically.

The facilities have preventive and corrective maintenance systems with 24/7 assistance 365 days a year, with assistance within 24 hours of notification.

5.1.1 Location and construction of facilities

Physical protection is achieved by creating clearly defined security perimeters around the services. The quality and strength of the construction materials of the facilities guarantee adequate levels of protection against brute force intrusions and are located in a low-risk area for disasters, allowing for quick access.

The room where cryptographic operations are carried out in the Data Processing Center:

- It has redundancy in its infrastructures.
- It has several alternative sources of electricity and cooling in case of emergency.
- Maintenance operations do not require the Center to be offline at any time.
- 99.995% monthly reliability

esFIRMA has facilities that physically protect the provision of certificate request approval services and revocation management, from the commitment caused by unauthorized access to systems or data, as well as the disclosure of them

5.1.2 Physical access

The data center where the CA of esFIRMA is located has a TIER IV qualification.

Physical access to the esFIRMA facilities where certification processes are carried out is limited and protected by a combination of physical and procedural measures. Thus:

- It is limited to expressly authorized personnel, with identification at the time of access and registration of it, including closed circuit television filming and its archive.

- Access to the rooms is done with identification card readers.

- Prior authorization from esFIRMA administrators who have the key to open the cage is required to access the RAC where cryptographic processes are located in the hosting service.

5.1.3 Electricity and air conditioning

The esFIRMA facilities have current stabilizer equipment and a duplicated electrical power supply system for equipment with a power generator.

The rooms that house computer equipment have temperature control systems with air conditioning equipment.

5.1.4 Exposure to water

The facilities are located in a low flood risk area.

The rooms where computer equipment is housed have a humidity detection system.

5.1.5 Fire prevention and protection

The facilities and assets of esFIRMA have automatic fire detection and extinguishing systems.

5.1.6 Storage of media

Only authorized personnel have access to storage media.

The highest level classified information is stored in a safe box outside the Data Processing Center facilities.

5.1.7 Waste treatment

The elimination of media, both paper and magnetic, is carried out through mechanisms that guarantee the impossibility of recovering the information.

In the case of magnetic media, formatting, permanent deletion, or physical destruction of the media is carried out, using specialized software that performs a minimum of 3 deletion passes and with variable deletion patterns.

In the case of paper documentation, by means of shredders or in bins arranged for this purpose to be subsequently destroyed, under control.

5.1.8 Off-site backup copy

esFIRMA uses a secure external storage for the custody of documents, magnetic and electronic devices that are independent of the operations center.

At least two persons expressly authorized for access, deposit or withdrawal of devices are required.

5.2 Procedure controls

esFIRMA guarantees that its systems are operated securely, for which it has established and implemented procedures for the functions that affect the provision of its services.

The staff of esFIRMA carries out administrative and management procedures in accordance with the security policy.

5.2.1 Reliable functions

esFIRMA has identified, in accordance with its security policy, the following functions or roles as reliable:

- **Internal Auditor:** Responsible for compliance with operational procedures. This is a person external to the Information Systems department. The tasks of the internal auditor are incompatible in time with the tasks of Certification and incompatible with Systems. These functions will be subordinated to the operations management, reporting both to it and to the technical management.
- **System Administrator**: Responsible for the proper operation of the hardware and software support of the certification platform
- **CA Administrator**: Responsible for the actions to be carried out with the cryptographic material, or with the performance of any function that involves the activation of the private keys of the certification authorities described in this document, or any of its elements.

- **CA Operator:** Responsible jointly with the CA Administrator for the custody of cryptographic key activation material, also responsible for backup copy operations and maintenance of the CA.
- **Registration Authority:** Person responsible for approving the certification requests made by the subscriber.
- **Security Officer**: Responsible for coordinating, controlling and enforcing the security measures defined by the security policies of esFIRMA. They must be in charge of aspects related to information security: logical, physical, networks, organizational, etc.
- **Information and Service Manager**: Defines the requirements for information and services in terms of security. This role has the ultimate responsibility for the use made of the information and services and therefore for their level of protection.
- **Validation Specialist**: Responsible for validating certificate requests.
- **Revocation Officer:** Responsible for the operation of changing the status of certificates.

The people who hold the previous positions are subject to specific investigation and control procedures.

5.2.2 Number of people per task

esFIRMA guarantees at least two people to perform the tasks detailed in the corresponding Certification Policies. Especially in the handling of the custody device of the root Certification Authority keys.

5.2.3 Identification and authentication for each function

The individuals assigned to each role are identified by the internal auditor who will ensure that each person performs the operations for which they are assigned.

Each person only controls the assets necessary for their role, thus ensuring that no person accesses unassigned resources.

Access to resources is carried out depending on the asset through cryptographic cards and activation codes.

5.2.4 Roles that require separation of duties

The following tasks are performed, at least, by two people:

- Issuance and revocation of certificates, and access to the repository.
- Generation, issuance, and destruction of certificates from the Certification Authority.
- Deployment of the Certification Authority.

5.2.5 PKI management system

The PKI system is composed of the following modules:

- Component/module for the management of the Subordinate Certification Authority.
- Registration Authority management component/module.
- Request management component/module.
- Key management component/module (HSM).
- Database component/module.
- CRL management component/module.
- Component/module for managing the OCSP service.
- Component/module for the management of the Time Stamping Authority (TSA)

5.3 Personnel controls

5.3.1 Requirements for history, qualifications, experience, and authorization

All personnel who perform tasks qualified as reliable, have been working in the production center for at least one year and have fixed employment contracts.

All personnel are qualified and have been properly trained to perform the operations assigned to them.

Personnel in positions of trust do not have personal interests that conflict with the performance of the function entrusted to them.

esFIRMA ensures that the registration personnel are trustworthy to perform registration tasks.

The Registration Operator has completed a training course to perform validation tasks for requests.

In general, esFIRMA will remove an employee from their trusted functions when knowledge of the commission of any criminal act that could affect the performance of their functions is obtained.
esFIRMA will not assign an unsuitable person to a trusted or management position, especially if they have been convicted of a crime or offense that affects their suitability for the position.

5.3.2 History investigation procedures

esFIRMA performs checks on the background of potential employees before their hiring or access to the job position.

esFIRMA obtains the unequivocal consent of the data subject for such prior investigation, and processes and protects all their personal data in accordance with REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and with Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights.

The investigation will be repeated with sufficient periodicity.

All checks are carried out to the extent permitted by applicable legislation. The reasons that may lead to rejecting a candidate for a reliable position are the following:

- Falsehoods in the job application made by the candidate.
- Very negative or unreliable professional references regarding the candidate.

The job application informs about the need to undergo a previous investigation, warning that the refusal to undergo the investigation will imply the rejection of the application.

5.3.3 Training requirements

esFIRMA trains personnel in reliable and management positions in accordance with the Certification Policies. To do this, the corresponding actions are defined in the ESFIRMA Training Plan.

The training includes, at least, the following contents:

- Principles and security mechanisms of the certification hierarchy, as well as the user environment of the person to be trained.
- Tasks that the person must perform.
- Policies and security procedures of esFIRMA. Use and operation of machinery and installed applications.
- Management and processing of security incidents and commitments.
- Business continuity and emergency procedures.
- Procedure for management and security in relation to the processing of personal data.

5.3.4 Training requirements and frequency of updates

esFIRMA updates the training of personnel according to their needs, and with sufficient frequency to perform their functions competently and satisfactorily, especially when substantial modifications are made to certification tasks

5.3.5 Sequence and frequency of job rotation

Not applicable.

5.3.6 Sanctions for unauthorized actions

esFIRMA has a sanctioning system to determine the responsibilities derived from unauthorized actions, appropriate to the applicable labor legislation and, in particular, coordinated with the sanctioning system of the collective agreement that applies to the personnel.

Disciplinary actions include suspension and dismissal of the person responsible for the harmful action, proportionate to the severity of the unauthorized action.

5.3.7 Requirements for hiring professionals

Employees hired to perform trustworthy tasks previously sign confidentiality clauses and operational requirements used by esFIRMA. Any action that compromises the security of accepted processes could, once evaluated, lead to the termination of the employment contract.

In the event that all or part of the certification services are operated by a third party, the controls and provisions made in this section, or in other parts of the DPC, will be applied and complied with by the third party that performs the operation functions of the certification services. However, the certification entity will be responsible in any case for the effective execution. These aspects are specified in the legal instrument used to agree on the provision of certification services by a third party other than esFIRMA.

5.3.8 Supply of documentation to personnel

The certification service provider will provide the documentation that its personnel strictly requires at all times, in order to perform their work competently and satisfactorily.

5.4 Security audit procedures

5.4.1 Types of registered events

esFIRMA produces and stores a record, at least, of the following events related to the security of the entity:

- System power on and off.
- Attempts to create, delete, set passwords, or change privileges.
- Login attempts and session end.
- Attempts of unauthorized access to the CA system through the network.
- Attempts of unauthorized access to the file system.
- Physical access to the logs.
- Changes in system configuration and maintenance.

- Records of the applications of the CA.
- Turning on and off the AC application.
- Changes in the details of the CA and/or its keys.
- Changes in the creation of certificate policies.
- Generation of own keys.
- Creation and revocation of certificates.
- Records of the destruction of the media containing the keys, activation data.
- Events related to the life cycle of the cryptographic module, such as reception, use, and uninstallation of it.
- The activities of firewalls and routers[7]
- The key generation ceremony and the key management databases.
- Physical access records.
- System maintenance and configuration changes.
- Changes in personnel.
- Reports of commitments and discrepancies.
- Records of the destruction of material containing key information, activation data, or personal information of the subscriber, in the case of individual certificates, or the natural person identified in the certificate, in the case of organization certificates.
- Possession of activation data, for operations with the private key of the Certification Entity.
- Complete reports of physical intrusion attempts on the infrastructures that support the issuance and management of certificates.

The registry entries include the following elements:

- Date and time of entry.
- Serial number or sequence of the entry, in automatic records.
- Identity of the entity that enters the registration.
- Type of input.

All events related to the preparation of qualified signature creation devices used by signers or custodians are recorded[8].

[7] Ap 6.4.5.a) de ETSI EN 319 411-1

[8] Ap 6.4.5.a) de ETSI EN 319 411-2

5.4.2 Frequency of audit record processing

esFIRMA reviews its logs when a system alert is triggered due to the existence of an incident.

The processing of audit logs involves reviewing the logs, including verifying that they have not been manipulated, a brief inspection of all log entries, and a more in-depth investigation of any alerts or irregularities in the logs. The actions taken as a result of the audit review are documented.

esFIRMA maintains a system that allows to ensure:

- Sufficient space for log storage
- That log files are not overwritten.
- That the stored information includes at least: type of event, date and time, user who executes the event and result of the operation.
- The log files will be stored in structured files that can be incorporated into a database for later exploration.

5.4.3 Audit record retention period

esFIRMA stores log information for a period of between 1 and 15 years, depending on the type of information recorded.

esFIRMA makes these audit records available to its Qualified Auditor, upon request.

5.4.4 Protection of audit logs

The logs of the systems:

- They are protected from manipulation, deletion or removal[9] by signing the files that contain them.
- They are stored in fireproof devices.

[9] Ap 7.10.f) de ETSI EN 319 401

- Its availability is protected by storing it in facilities external to the center where the CA is located.

Access to log files is reserved only for authorized personnel. Likewise, devices are handled at all times by authorized personnel.
There is an internal procedure that details the management processes of devices containing audit log data.

5.4.5 Backup copy procedures

esFIRMA has an appropriate backup procedure so that, in case of loss or destruction of relevant files, the corresponding backup copies of the logs are available within a short period of time.

esFIRMA has implemented a secure backup procedure for audit logs, making a weekly copy of all logs on an external medium. Additionally, a copy is kept in an external custody center.

5.4.6 Location of the audit record accumulation system

The information from the event audit is collected internally and automatically by the operating system, network communications, and certificate management software, as well as manually generated data, which will be stored by authorized personnel. All of this makes up the audit record accumulation system.

5.4.7 Notification of audit event to the event causer

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

5.4.8 Vulnerability analysis

The vulnerability analysis is covered by the esFIRMA audit processes.

Vulnerability analyses must be executed, reviewed, and revised through an examination of these monitored events. These analyses must be performed daily, monthly, and annually.

The audit data of the systems are stored in order to be used in the investigation of any incident and to locate vulnerabilities.

The security program of esFIRMA includes an annual risk assessment.

5.5. Information files

esFIRMA guarantees that all information related to certificates is kept for an appropriate period of time, as established in section 5.5.2 of this policy.

5.5.1 Types of archived records

The following documents involved in the certificate lifecycle are stored by esFIRMA (or by the registration entities):

- All system audit data (PKI, TSA and OCSP).
- All data related to certificates, including contracts with signers and data related to their identification and location
- Requests for issuance and revocation of certificates, including all reports related to the revocation process[10].
- All specific choices that the signer or subscriber makes during the subscription agreement[11].
- Type of document submitted in the certificate application.
- Identity of the Registration Authority that accepts the certificate request.
- Unique identification number provided by the previous document.
- All certificates issued or published.

[10] Ap 6.4.5.h) de ETSI EN 319 411-1

[11] Ap 6.4.5.c) iv) de ETSI EN 319 411-1

- CRLs issued or records of the status of the generated certificates.
- The history of generated keys.
- The communications between the elements of the PKI.
- Certification Policies and Practices
- All audit data identified in section 5.4
- Certification request information.
- Documentation provided to justify certification requests.
- Certificate lifecycle information.

esFIRMA is responsible for the correct filing of all this material.

5.5.2 Record retention period

esFIRMA archives the records specified above for at least 15 years.

5.5.3 File protection

esFIRMA protects the file so that only duly authorized persons can access it. The file is protected against viewing, modification, deletion or any other manipulation by storing it in a reliable system.

esFIRMA ensures the correct protection of files by assigning qualified personnel for their handling and storing them in fireproof safes and external facilities.

5.5.4 Backup copy procedures

esFIRMA has an external storage center to guarantee the availability of copies of the electronic file archive. Physical documents are stored in secure locations with restricted access only to authorized personnel.

esFIRMA at least performs daily incremental backup copies of all its electronic documents and performs weekly full backup copies for data recovery purposes.

In addition, esFIRMA (or the organizations that perform the registration function) keeps a copy of the paper documents in a secure location different from the facilities of the certification entity itself.

5.5.5 Date and time stamping requirements

The records are dated with a reliable source via NTP.

esFIRMA has a procedure that describes the configuration of the times of the equipment used in the issuance of certificates.
The time used to record events in the audit log must be synchronized with UTC at least once a day[12].

It is not necessary for this information to be digitally signed.

5.5.6 Location of the file system

esFIRMA has a centralized system for collecting information on the activity of the equipment involved in the certificate management service.

5.5.7 Procedures for obtaining and verifying archive information

esFIRMA has a procedure that describes the process to verify that the archived information is correct and accessible.

5.6 Key renewal

Before the use of the private key of the AC/SUBCA/TSA expires, a key change will be made. The old AC/SUBCA and its private key will only be used for the signature of CRLs while there are active certificates issued by said AC/SUBCA. A new AC/SUBCA/TSA will be generated with a new private key and a new DN. The private key of the TSA will be destroyed.

The subscriber's key change is carried out by performing a new issuance process.

[12] Ap 7.10.d) de la ETSI EN 319 401

5.7 Key compromise and disaster recovery

5.7.1 Incident management and commitment management procedures

Backup copies of the following information are stored in external storage facilities to esFIRMA, which are made available in case of compromise or disaster: technical data of certificate request, audit data, and database records of all issued certificates.

The backup copies of the private keys of esFIRMA are generated and maintained in accordance with what is established in section 6.2.4

5.7.2 Corruption of resources, applications or data

When an event of corruption of resources, applications or data occurs, the incident will be reported to security, and the appropriate management procedures will be initiated, which include escalation, investigation and incident response. If necessary, the key compromise or disaster recovery procedures of esFIRMA will be initiated.

5.7.3 Compromise of the private key of the entity

In case of suspicion or knowledge of the compromise of esFIRMA, key compromise procedures will be activated, led by a response team that will evaluate the situation, develop an action plan, which will be executed under the approval of the management of the Certification Authority.

In case of compromise of the private key of esFIRMA, it may happen that the states of the certificates and revocation processes using this key may not be valid[13]. In any case, all active certificates will be revoked, subsequently generating a last CRL in which all revoked certificates, whether expired or not, will be included. The instructions for validating a certificate or timestamp will be published on the esFIRMA website.

esFIRMA has developed a contingency plan to recover critical systems, if necessary, in an alternative data center.

[13] Ap 6.4.8.g) ii) de ETSI EN 319 411-1

The case of compromise of the root key must be taken as a separate case in the contingency and business continuity process. This incident affects, in case of key replacement, the recognitions by different private and public applications and services. Recovery of key effectiveness in business terms will depend mainly on the duration of these processes. The contingency and business continuity document will address purely operational terms for the new keys to be available, but not their recognition by third parties.

Any failure to achieve the goals set by this Contingency Plan will be treated as reasonably unavoidable unless such failure is due to a breach of the CA's obligations to implement such processes.

5.7.4 Business continuity after a disaster

esFIRMA will restore critical services (suspension and revocation, and publication of certificate status information) in accordance with the existing Business Continuity Plan.
esFIRMA has an alternative center available in case it is necessary for the implementation of the certification systems described in the business continuity plan.

Both the revocation management service and the consultation service are considered critical services and are included in the esFIRMA Business Continuity Plan.

5.8 Termination of service

esFIRMA ensures that possible interruptions to subscribers and third parties are minimal as a result of the cessation of certification service provider services and, in particular, ensures continuous maintenance of the records required to provide certification evidence in the event of civil or criminal investigation.

Before ending its services, esFIRMA develops a Termination Plan, with the following provisions:

- It will provide the necessary funds to continue the completion of revocation activities.
- It will communicate to the Ministry of Economic Affairs and Digital Transformation, with a minimum notice of 2 months, the cessation of its

activity and the destination of the certificates specifying whether the management is transferred and to whom, or whether its validity will be extinguished.

- It will also communicate to the Ministry of Economic Affairs and Digital Transformation the opening of any bankruptcy proceedings against esFIRMA as well as any other relevant circumstance that may prevent the continuation of the activity.
- It will inform all Signers/Subscribers, Third Parties that trust and other AC's with which it has agreements or other types of relationships of the cessation with a minimum notice of 6 months.
- It will transfer the management of certificates with validity to third-party providers provided there is consent from their holders or, failing that, proceed to the termination of their validity (contained in points b) and c) of the communication in point 1.1).
- It will transfer the obligations of ESFIRMA to the new provider in charge of managing the certificates, maintaining the registration information, maintaining the status of the revocation process, and maintaining the event log files during their respective time periods, as indicated to subscribers, users, and parties that rely on the certificates.
- Information will be provided about the characteristics of the new provider to whom ESFIRMA transfers certificate management.
- It will revoke any authorization to subcontracted entities to act on behalf of the CA in the certificate issuance process.
- It will destroy or disable the private keys of the CA for use.
- The certificates of the Time Stamping Units (TSU) will be revoked.
- All active certificates and the verification and revocation system will be maintained until the expiration of all certificates issued for 15 years. For this purpose, a last CRL will be issued that will include all revoked certificates, whether or not they have expired, establishing the necessary means to guarantee their long-term preservation.

6. Technical security controls

6.1 Generation and installation of the key pair

6.1.1 Key pair generation

The key pair of the intermediate certification entity "ESFIRMA AC AAPP 2" is created by the root certification entity "ESFIRMA AC RAIZ 2" according to the esFIRMA ceremony procedures, within the high security perimeter intended for this task.

The activities carried out during the key generation ceremony have been recorded, dated and signed by all individuals participating in it, in the presence of a CISA Auditor. Such records are kept for audit and monitoring purposes for an appropriate period determined by esFIRMA.

To generate the key for root and intermediate certification entities, devices with Common Criteria EAL 4+ or FIPS 140-2 Level 3 certifications are used.

ROOT	4,096 bits	25 years
INTERMEDIATE	4,096 bits	13 years
- End-entity certificates	2,048 bits	2 years
- TSA certificate	4,096 bits	5 years (2 years private key)

More information in the following locations of the PDS:

CERTIFICATE	PDS
From Public Employee (SIGNATURE)	Spanish: https://esfirma.com/doc-pki/PDS-V2.0/PDS-AAPP-ES.pdf English:

CERTIFICATE	PDS
	https://esfirma.com/doc-pki/PDS-V2.0/PDS-AAPP-EN.pdf
From Public Employee - High Level 1.3.6.1.4.1.47281.1.1.1	
From Public Employee - Middle Level 1.3.6.1.4.1.47281.1.1.4	
From Public Employee (AUTHENTICATION)	
From Public Employee - High Level 1.3.6.1.4.1.47281.1.1.5	
From Public Employee with Pseudonym (SIGNATURE)	
From EP with Pseudonym - High Level 1.3.6.1.4.1.47281.1.3.1	
From EP with Pseudonym - Medium Level 1.3.6.1.4.1.47281.1.3.4	
From Public Employee with Pseudonym (AUTHENTICATION)	
From Public Employee with Pseudonym - 1.3.6.1.4.1.47281.1.3.5	
Of Body Seal	
From Body Seal - Medium Level 1.3.6.1.4.1.47281.1.2.2	
From Body Seal - Centralized Medium Level *1.3.6.1.4.1.47281.1.2.4*	
From a natural person linked to an entity (SIGNATURE)	Spanish: https://esfirma.com/doc-pki/PDS-V2.0/PDS-PFV-ES.pdf English: https://esfirma.com/doc-pki/PDS-V2.0/PDS-PFV-EN.pdf
From PF linked to entity - Qualified TSP 1.3.6.1.4.1.47281.1.6.1	
From PF linked to entity - Centralized F 1.3.6.1.4.1.47281.1.6.4	

CERTIFICATE	PDS
From a natural person linked to an entity (AUTHENTICATION)	
From PF linked to entity 1.3.6.1.4.1.47281.1.6.5	
From a natural person with a pseudonym linked to an entity (SIGNATURE)	
From PF with pseudonym linked to entity - Qualified Signature 1.3.6.1.4.1.47281.1.7.1	
From PF with pseudonym linked to entity - Centralized Signature 1.3.6.1.4.1.47281.1.7.4	
From a natural person with a pseudonym, linked to an entity (AUTHENTICATION)	
From PF with pseudonym, linked to entity 1.3.6.1.4.1.47281.1.7.5	
Of electronic seal	
De Sello electrónico en software 1.3.6.1.4.1.47281.1.8.2	
Of centralized electronic seal 1.3.6.1.4.1.47281.1.8.4	
Electronic seal for TSA/TSU	Spanish: https://esfirma.com/doc-pki/PDS-V1.5/TSADS-ES.pdf English: https://esfirma.com/doc-pki/PDS-V1.5/TSADS-EN.pdf
From Sello-e to TSA/TSU in HSM 1.3.6.1.4.1.47281.1.5.2	

In card certificates, the subscriber authorizes the signer to generate their private and public keys within a qualified electronic signature creation device, and requests, on behalf of the signer, the issuance of the certificate to esFIRMA.

In certificates generated in HSM or software, the subscriber authorizes the signer or seal creator to generate their private and public keys, and requests, on behalf of the signer or seal creator, the issuance of the certificate to esFIRMA.

esFIRMA never generates keys in software to be sent through insecure channels to the signer.

The keys are generated using the RSA public key algorithm, with a minimum length of 2048 bits, the elliptic curve public key algorithm 1.2.840.10045.3.1.7 (NIST-P256/secp256r1) of 256 bits.

6.1.2 Sending the private key to the signer

In certificates on secure signature creation devices, the private key is properly protected inside said secure device.

In software certificates, the signer's private key is created in the computer system used by the signer when requesting the certificate, so the private key is properly protected within the signer's computer system.

6.1.3 Sending the public key to the certificate issuer

The method for submitting the public key to the certification service provider is PKCS#10, another equivalent cryptographic proof, or any other method approved by esFIRMA.

When the keys are generated in a DCCF, esFIRMA ensures that the public key sent to the certification service provider comes from a key pair generated by said DCCF[14].

6.1.4 Distribution of the public key of the certification service provider

The keys of esFIRMA are communicated to third parties who trust certificates, ensuring the integrity of the key and authenticating its origin, by publishing it in the Repository.

Users can access the Repository to obtain public keys, and additionally, in S/MIME applications, the data message may contain a chain of certificates, which are thus distributed to users.

The certificate of the root and subordinate CAs will be available to users on the esFIRMA website.

[14] Ap 6.5.1.b) de ETSI EN 319 411-2

6.1.5 Key sizes

The length of the keys of the Root Certification Authority is RSA 4096 bits.

The length of the keys of the subordinate Certification Authority is RSA 4096 bits.

The length of the TSA keys is RSA 4096 bits.

The keys of the end-entity certificates are RSA 2048 or 4096 bits or elliptic curve public key 1.2.840.10045.3.1.7 (NIST-P256/secp256r1) of 256 bits.

6.1.6 Generation of public key parameters and quality checking

The public key of the Root CA, the subordinate CAs, and the subscriber certificates are encoded according to RFC 5280.

Quality of public key parameters

- Module Length = 4096
- Key generation algorithm: rsagen1
- Cryptographic hash functions: SHA256.

All keys are generated on equipment assets, in accordance with what is indicated in section 6.1.1.

6.1.7 Key usage purposes

The uses of keys for CA certificates are exclusively for the signing of certificates and CRLs.

The uses of keys for end-entity certificates are exclusively for digital signature and non-repudiation.

6.2 Protection of the private key and controls of the cryptographic modules

6.2.1 Cryptographic Module Standards

Regarding the modules that manage esFIRMA keys and electronic signature certificate subscribers, the required level is ensured according to the standards indicated in the previous sections.

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

A multi-person control is required to activate the private key of the CA. In the case of this DPC, there is a specific policy **3 out of 5** people for the activation of the keys.

The cryptographic devices are physically protected as determined in this document.

6.2.3 Private key deposit

esFIRMA does not store copies of signers' private keys.

6.2.4 Private key backup copy

esFIRMA makes a backup copy of the private keys of the CAs that make their recovery possible in case of disaster, loss or deterioration of them. Both the generation of the copy and its recovery require the participation of at least two people.

These recovery files are stored in fireproof cabinets and in the external custody center.

The signer's keys in hardware cannot be copied since they cannot leave the cryptographic device.

6.2.5 Private key file

The private keys of the CAs are archived for a period of **10 years** After the issuance of the last certificate. They will be stored in secure fireproof files and in the external custody center. At least the collaboration of two people will be necessary to recover the private key of the CAs on the initial cryptographic device.

6.2.6 Introduction of the private key into the cryptographic module

The private keys are generated directly in the cryptographic production modules of esFIRMA.

6.2.7 Storage of private keys in cryptographic modules

The private keys of the Certification Authority are stored encrypted in the cryptographic production modules of esFIRMA.

6.2.8 Private key activation method

The private key of esFIRMA is activated by executing the corresponding secure start-up procedure of the cryptographic module, by the persons indicated in section 6.2.2.

The keys of the CA are activated through an m of n process.

The activation of the private keys of the Intermediate CA is managed with the same m of n process as the CA keys.

6.2.9 Private Key Deactivation Method

To deactivate the private key of esFIRMA, follow the steps described in the manual of the corresponding cryptographic equipment administrator.

On their part, the signer must enter the PIN for the new activation.

6.2.10 Private key destruction method

Prior to the destruction of the keys, the certificate of the public keys associated with them will be revoked.

Devices that store any part of the private keys of esFIRMA will be physically destroyed or reset at a low level. The steps described in the cryptographic equipment administrator's manual will be followed for the elimination.

Finally, the backup copies will be securely destroyed.

The signer's keys in software can be destroyed by deleting them, following the instructions of the application that hosts them.

The signer's hardware keys may be destroyed using a special software application at the RA or esFIRMA facilities.

6.2.11 Cryptographic module classification

The cryptographic modules are subject to the engineering controls provided for in the standards indicated throughout this section.

The key generation algorithms used are commonly accepted for the use of the key they are intended for.

All cryptographic operations of esFIRMA are performed in modules with FIPS 140-2 level 3 certifications.

6.3 Other key pair management aspects

6.3.1 Public key file

esFIRMA routinely archives its public keys, in accordance with section 5.5 of this document.

6.3.2 Periods of use of the 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.

6.4 Activation data

6.4.1 Generation and installation of activation data

The activation data of the devices that protect the private keys of esFIRMA are generated in accordance with what is established in section 6.2.2 and the key ceremony procedures.

The creation and distribution of such devices is registered.

Likewise, esFIRMA securely generates activation data.

6.4.2 Activation data protection

The activation data of the devices that protect the private keys of the root and subordinate certification authorities are protected by the holders of the cryptographic module administrator cards, as stated in the key ceremony document.

The certificate signer is responsible for protecting their private key with the strongest possible password. The signer must remember this password.

6.4.3 Other aspects of activation data

Not applicable.

6.5. Computer security controls

esFIRMA employs reliable systems to offer its certification services. esFIRMA has carried out computer controls and audits in order to establish a management of its computer assets appropriate to the level of security required in the management of electronic certification systems.

The equipment used is initially configured with the appropriate security profiles by the esFIRMA systems personnel, in the following aspects:

- Operating system security configuration.
- Application security configuration.
- Correct sizing of the system.
- User and permission settings.
- Log events configuration.
- Backup and recovery plan.
- Antivirus configuration.
- Network traffic requirements.

6.5.1 Specific technical requirements for computer security

Each esFIRMA server includes the following functionalities:

- Access control to SubCA services and privilege management.
- Imposition of separation of duties for privilege management.
- Identification and authentication of roles associated with identities.
- Subscriber's history archive and SubCA and audit data.
- Security event auditing.
- Security self-diagnosis related to SubCA services.
- Mechanisms for key and SubCA system recovery.

The exposed functionalities are carried out through a combination of operating system, PKI software, physical protection, and procedures.

In the event that esFIRMA distributes qualified signature creation devices, it will verify at all times that such devices continue to be certified as DCCF[15].

The verification of the certification of the DCCF is carried out throughout the validity period of the certificate[16]If the DCCF were to lose its certification as such, esFIRMA will proceed to revoke the certificates issued in said DCCF, informing their holders.

esFIRMA requires multi-factor authentication for all accounts capable of directly causing the issuance of certificates.

6.5.2 Evaluation of the level of computer security

The certification authority and registration applications used by esFIRMA are reliable.

6.6 Technical controls of the life cycle

[15] Ap 6.5.1.a) de ETSI 319 411-2

[16] Ap 6.5.1.c) de ETSI EN 319 411-2

6.6.1 System development controls

The applications are developed and implemented by esFIRMA according to development and change control standards.

The applications have methods for verifying integrity and authenticity, as well as for correcting the version to be used.

6.6.2 Security management controls

esFIRMA carries out the precise activities for the training and awareness of employees in security matters. The materials used for training and descriptive documents of the processes are updated after approval by a security management group. In carrying out this function, it has an annual training plan.

esFIRMA requires, through contract, security measures equivalent to any external provider involved in certification tasks.

Classification and management of information and assets

esFIRMA maintains an inventory of assets and documentation and a procedure for managing this material to ensure its use.

The information security management system of esFIRMA details the information management procedures where it is classified according to its level of confidentiality.

The documents are classified into four levels: PUBLIC, RESTRICTED, INTERNAL USE, and CONFIDENTIAL.

Management operations

esFIRMA has an adequate incident management and response procedure, through the implementation of an alert system and the generation of periodic reports.

esFIRMA has documented the entire procedure related to the functions and responsibilities of the personnel involved in the control and manipulation of elements contained in the certification process.

Treatment of media and security

All media are treated securely in accordance with the requirements of information classification. Media containing sensitive data are securely destroyed if they are not going to be required again.

System planning

The Systems department of esFIRMA maintains a record of the capabilities of the equipment. Together with the resource control application of each system, a possible resizing can be foreseen.

Incident reports and response

esFIRMA has a procedure for tracking incidents and their resolution.

Operational procedures and responsibilities

esFIRMA defines activities assigned to people with a trusted role, different from those in charge of carrying out daily operations that do not have a confidentiality nature.

Access system management

esFIRMA makes every reasonable effort to confirm that the access system is limited to authorized personnel.

In particular:

AC General

- Controls based on firewalls, antivirus, and IDS in high availability are available.
- Sensitive data is protected through cryptographic techniques or access controls with strong identification.
- esFIRMA has a documented procedure for managing user registration and deregistration, as well as a detailed access policy outlined in its security policy.

- esFIRMA has procedures to ensure that operations are carried out in accordance with the role policy.
- Each person is associated with a role to perform certification operations.
- The esFIRMA staff is responsible for their actions through the confidentiality commitment signed with the company.

Certificate generation

The authentication for the issuance process is carried out through an m out of n system of operators for the activation of the private key of esFIRMA.

Revocation management

Revocation will be carried out through strong authentication to the applications of an authorized administrator. The log systems will generate the evidence that guarantees the non-repudiation of the action carried out by the esFIRMA administrator.

Revocation status

The application of the revocation status has an access control based on authentication with certificates or with double identification factor to prevent the attempt to modify the revocation status information.

6.6.3 Evaluation of the security of the life cycle

esFIRMA ensures that the cryptographic hardware used for certificate signing is not tampered with during transportation by inspecting the delivered material.

The cryptographic hardware is moved on supports prepared to prevent any manipulation.

esFIRMA registers all relevant information of the device to add it to the asset catalog.

The use of cryptographic hardware for certificate signing requires the use of at least two trusted employees.

esFIRMA performs periodic test trials to ensure the proper functioning of the device.

The cryptographic hardware device is only handled by trusted personnel.

The private signature key of esFIRMA stored in the cryptographic hardware will be deleted once the device has been removed.

The configuration of the esFIRMA system, as well as its modifications and updates, are documented and controlled.

esFIRMA has a maintenance contract for the device. Changes or updates are authorized by the security manager and are reflected in the corresponding work records. These configurations will be carried out by at least two trustworthy persons.

6.7 Network security controls

esFIRMA protects physical access to network management devices, and has an architecture that orders the traffic generated based on its security characteristics, creating clearly defined network sections. This division is carried out through the use of firewalls.

The confidential information that is transferred over unsecured networks is encrypted using SSL protocols or the VPN system with two-factor authentication.

6.8 Time Sources

esFIRMA has a time synchronization procedure coordinated via NTP. The time value in the TSU is traceable to a time value distributed by a
UTC(k) laboratory, the ROA (Royal Observatory of the Navy) and maintains the accuracy of
clock with at least four STRATUM-1 time sources.

6.9 Signature algorithms and parameters of the centralized signature system

The centralized signature service generates keys for signers with the RSA algorithm with a key length of 2048 bits with probable primes using the algorithm FIPS 186-4 B.3.6 and

DRBG (Deterministic Random Bit Generator) in Real Random Mode (hardware noise) according to NIST SP 800-90A and continuous test according to FIPS 140-2. Outside the HSM module, keys are stored encrypted with the AES-GCM algorithm and a key length of 256 bits. The encryption key is derived from the user PIN and the HSM master key. The HSM master key uses the ECDSA NIST-P256/secp256r1 algorithm (OID 1.2.840.10045.3.1.7) and requires 3 out of 5 cards for activation and was generated in a high-security initialization ceremony. The user PIN is derived from a server salt with the PBKDF2-SHA1 algorithm. The transport of the SAD (Signature Activation Data) from the SIC (Signature Interaction Component) to the SAM (Signature Activation Module) is protected by AES-GCM with a 256-bit key derived from a key exchange using the ECDH algorithm according to NIST SP 800-56A. The server key is published in the esFirma web repository, in the "Remote signature security information" section. The system allows generating electronic signatures with the RSA PKCS#1 v1.5 algorithm, DSA with elliptic curve key and SHA-256 and SHA-512 summary algorithm.

7. Certificate profiles, CRL and OCSP

7.1 Certificate profile

All qualified certificates issued under this policy comply with the X.509 version 3 standard, RFC 5280, RFC 3739 and the following ETSI standards:

- ETSI EN 319 412-2 for certificates issued to natural persons
- ETSI EN 319 412-3 for certificates issued to legal persons
- ETSI EN 319 412-5 for the definition of QCStatements of qualified certificates according to RD (EU) 910/2014.

esFIRMA generates non-sequential certificate serial numbers greater than zero (0) that contain at least 128 bits of output from a CSPRNG.

7.1.1 Version number

esFIRMA issues X.509 Version 3 certificates

7.1.2 Certificate extensions

The certificate extensions are detailed in the profile documents that are accessible from the esFIRMA website https://www.esfirma.com

7.1.3 Object Identifiers (OID) of algorithms

The object identifier of the signature algorithm is:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption
- 1.2.840.10045.4.3.2 sha256WithECDSA

The object identifier of the public key algorithm is:

- 1.2.840.113549.1.1.1 rsaEncryption
- 1.2.840.10045.3.1.7 NIST-P256/secp256r1
-

7.1.4 Name Format

Certificates must contain the necessary information for their use, as determined by the corresponding policy.

The encoding of the certificate follows the RFC 5280 recommendation "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL)
View profiles at https://www.esfirma.com

7.1.5 Restriction of names

The names contained in the certificates are restricted to X.500 "Distinguished Names", which are unique and unambiguous.

7.1.6 Object Identifier (OID) of certificate types

All certificates include a certificate policy identifier under which they have been issued, in accordance with the structure indicated in point 1.2.1

7.1.7 Use of the policy constraints extension

Not applicable

7.1.8 Policy qualifiers syntax and semantics

Not applicable

7.1.9 Processing semantics for the critical extension of Certificate Policies

The "Certificate Policy" extension identifies the policy that defines the practices that esFIRMA explicitly associates with the certificate. The extension may contain a policy qualifier. See 7.1.6

7.1.10 Length restrictions of the elements

For all profiles, the following maximum length restrictions in characters are established for the following elements:

Element	**Maximum Length esFIRMA**	**Length Base**	**Standard**
2.5.4.42 *(givenName,GN)*	**127**	32000***	RFC5280
2.5.4.10 (organizationName)	**256**	64	RFC5280
2.5.4.11 (organizationalUnitName)	**256**	32	RFC5280
2.5.4.4 (surnames)	**256**	40	RFC5280
2.5.4.3 (commonName, CN)	**400**	64	RFC5280
2.5.4.5 (serialNumber,SN)	32*	32	RFC5280
2.5.4.97 (organizationIdentifier)	**32**	MAX**	X520
2.5.4.65 (pseudonym)	**64***	128	RFC5280
2.5.4.12 (title)	64*	64	RFC5280
*The ETSI EN 319 412-2 4.2.4 and ETSI EN 319 412-3 4.2.1 standards allow exceeding the limits set in RFC 5280 (provided it is indicated in the DPC) for the subject fields indicated according to the type of certificate (givenName, surname, pseudonym, commonName, organizationName, and organizationalUnitName), but not the rest of the fields. The length of these fields is in accordance with RFC 5280. ** MAX indicates that the upper limit is not specified (RFC5280 Appendix B. ASN1 Notes) *** 32000 ub-name used instead of ub-givenname (16)			

The maximum lengths for the rest of the elements are specified in RFC-5280

7.2 Certificate Revocation List Profile

According to the IETF RFC 3280 standard

7.2.1 Version number

The CRLs issued by esFIRMA are version 2.

7.2.2 CRL and CRL extensions

crlExtensions:

2.5.29.35 (Authority key identifier)

2.5.29.20 (CRL Number)

crlEntryExtensions

2.5.29.21 (ReasonCode)

7.3 OCSP Profile

According to the IETF RFC 6960 standard

7.3.1 Version number

The OCSP issued by esFIRMA are version 3.

7.3.2 OCSP Extensions

responseExtensions

Id: 1.3.6.1.5.5.7.48.1.2 (OCSP Nonce Extension)

Critical: true

8. Compliance audit

esFIRMA has announced the start of its activity as a certification service provider by the Ministry of Economic Affairs and Digital Transformation and is subject to the necessary control reviews by this organization.

8.1 Frequency of compliance audit

esFIRMA carries out an annual compliance audit, in addition to internal audits that it carries out at its own discretion or at any time, due to suspicion of non-compliance with any security measure.

esFIRMA supervises the compliance of this document and strictly controls the quality of its service by performing self-audits at least quarterly against a randomly selected sample of the largest certificate or at least three percent of the certificates issued by it during the period beginning immediately after the previous self-audit.

8.2 Identification and qualification of the auditor

Audits are carried out by an independent external auditing firm that demonstrates technical competence and experience in computer security, information system security, and compliance audits of public key certification services, and related elements.

8.3 Auditor's relationship with the audited entity

Audit companies are well-known with specialized departments in carrying out computer audits, so there is no conflict of interest that could distort their performance in relation to esFIRMA.

8.4 List of auditable items

The audit verifies regarding esFIRMA:

a) That the entity has a management system that guarantees the quality of the service provided.

b) That the entity complies with the requirements of the DPC and other documentation related to the issuance of different digital certificates.

c) That the DPC and other legal documentation related to it, complies with what was agreed by esFIRMA and with what is established in the current regulations.

d) That the entity manages its information systems appropriately

In particular, the audited elements will be the following:

a) Processes of the CA, ARs and related elements.

b) Information systems.

c) Protection of the data processing center.

d) Documents.

8.5 Actions to be taken as a result of nonconformity

Once the compliance audit report is received by the management, the deficiencies found are analyzed with the auditing firm that carried out the audit, and a corrective plan is developed and executed to solve said deficiencies.

If esFIRMA is unable to develop and/or execute said plan or if the deficiencies found pose an immediate threat to the security or integrity of the system, it must immediately notify the senior management of esFIRMA who may take the following actions:

- Temporarily cease operations.
- Revoke the CA key and regenerate the infrastructure.
- Terminate the service of the CA.
- Other complementary actions that may be necessary.

8.6 Treatment of audit reports

Audit result reports are delivered to the esFIRMA senior management within a maximum period of 15 days after the audit execution.

9. Commercial and legal requirements

9.1 Fees

9.1.1 Certificate issuance or renewal fee

esFIRMA may establish a fee for the issuance of certificates, which, if applicable, will be duly informed to subscribers.

9.1.2 Certificate access fee

esFIRMA has not established any fee for accessing certificates.

9.1.3 Certificate status information access fee

esFIRMA has not established any fee for accessing certificate status information.

9.1.4 Fees for other services

Without stipulation.

9.1.5 Refund policy

Without stipulation.

9.2 Financial responsibility

esFIRMA has sufficient financial resources to maintain its operations and fulfill its obligations, as well as to face the risk of liability for damages, as established in ETSI EN 319 401-1 7.12 c), in relation to the management of the termination of services and cessation plan.

9.2.1 Insurance coverage

esFIRMA has a guarantee of coverage of its sufficient civil liability, through a professional civil liability insurance that complies with the obligations and responsibilities regime of Regulation (EU) 910/2014, and with article 9.3.b) of Law 6/2020, of November 11, regulating certain aspects of trusted electronic services, with a minimum insured amount of 3,000,000 euros.

9.2.2 Other assets

Without stipulation.

9.2.3 Insurance coverage for subscribers and third parties who rely on certificates

esFIRMA has a sufficient civil liability coverage guarantee, through a professional civil liability insurance that complies with the obligations and responsibilities regime of Regulation (EU) 910/2014, and with article 9.3.b) of Law 6/2020, of November 11, regulating certain aspects of electronic trust services with a minimum insured amount of 3,000,000 euros.

9.3 Confidentiality of information

9.3.1 Confidential information

The following information is kept confidential by esFIRMA:

- Certificate requests, approved or denied, as well as any other personal information obtained for the issuance and maintenance of certificates, except for the information indicated in the following section.
- Private keys generated and/or stored by the certification service provider.
- Transaction records, including complete records and audit logs of transactions.
- Internal and external audit records, created and/or maintained by the Certification Authority and its auditors.
- Business continuity and emergency plans.
- Security policies and plans.
- Documentation of operations and remaining operation plans, such as archiving, monitoring, and other similar activities.

- Any other information identified as "Confidential".

9.3.2 Non-confidential information

The following information is considered non-confidential:

- The certificates issued or in the process of being issued.
- The linking of the subscriber to a certificate issued by the Certification Authority.
- The name and surnames of the natural person identified in the certificate, as well as any other circumstance or personal data of the holder, in the event that it is significant for the purpose of the certificate.
- The email address of the natural person identified in the certificate, or the email address assigned by the subscriber, in the event that it is significant depending on the purpose of the certificate.
- The economic uses and limits indicated in the certificate.
- The validity period of the certificate, as well as the certificate issuance date and expiration date.
- The serial number of the certificate.
- The different states or situations of the certificate and the date of the beginning of each of them, specifically: pending generation and/or delivery, valid, revoked, suspended or expired and the reason that caused the change of state.
- The certificate revocation lists (CRLs), as well as the remaining revocation status information.
- Any other information not indicated in the previous section.

9.3.3 Disclosure of suspension and revocation information

See the previous section.

9.3.4 Legal disclosure of information

esFIRMA only discloses confidential information in legally established cases.

Specifically, the records that support the reliability of the data contained in the certificate, as well as the records related to the reliability of the data and those related to the operation[17], will be disclosed if required to provide evidence of certification in a judicial proceeding, even without the consent of the certificate subscriber.

esFIRMA will indicate these circumstances in the privacy policy provided in section 9.4.

9.3.5 Disclosure of information at the request of the data subject

esFIRMA includes, in the privacy policy provided in section 9.4, provisions to allow the disclosure of subscriber information and, where appropriate, the natural person identified in the certificate, directly to them or to third parties.

9.3.6 Other circumstances of information disclosure

Without stipulation.

9.4 Privacy of personal information

esFIRMA undertakes to comply with the regulations on the protection of personal data, with the corresponding security measures, as set out in REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, and in Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights.

esFIRMA obtains the personal data contained in the files by capturing the data from the SUBSCRIBER, who must have legally obtained them from the corresponding person, under the conditions provided for in the regulations on electronic signature and on the protection of personal data.

esFIRMA has the condition of data processor and, as such, processes the data solely for the purposes set out in this Certification Practice Statement in accordance with the

[17] Apartado 7.10.c) de la ETSI EN 319 401

instructions of the data controller, which is the SUBSCRIBER and which are included in Annex*Annex 1: For the processing of personal data by ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A. as DATA PROCESSOR*, which governs the service provision contract "Gestiona" between the SUBSCRIBER and ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A.

9.4.1 Privacy Plan

esFIRMA has developed a privacy policy in accordance with REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, and with Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights, and has documented it in this Certification Practice Statement, as well as in Annex "Annex 1: *For the processing of personal data by ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A. as DATA PROCESSOR* which governs the service provision contract "Gestiona" between the SUBSCRIBER and ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A., the aspects, procedures and security and organizational measures in compliance with the regime of obligations and responsibilities contained in the previous regulations.

9.4.2 Information treated as private

Personal information about an individual that is not publicly available in the
The contents of a certificate or CRL are considered private.

9.4.3 Information not considered private

The personal information about an individual available in the contents of a certificate or CRL is considered non-private as it is necessary for the provision of the contracted service, without prejudice to the rights corresponding to the owner of the personal data under the LOPD/RGPD legislation.

9.4.4 Responsibility to protect private information

Confidential information in accordance with regulations on personal data protection is protected against loss, destruction, damage, falsification, and unlawful or unauthorized processing, in accordance with the provisions set out in this document, which are aligned with the obligations provided for in REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, and in Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights.

9.4.5 Notice and consent to use private information

Before entering into a contractual relationship, interested parties will be offered the

Prior information about the processing of your personal data and the exercise of your rights will be provided, and if applicable, the necessary consent for the differentiated processing of the main treatment for the provision of contracted services will be obtained.

9.4.6 Disclosure in accordance with a judicial or administrative process

esFIRMA does not disclose or transfer personal data, except in the cases provided for in sections 9.3.2 to 9.3.6, and in section 5.8, in the event of termination of the certification service.

9.4.7 Other circumstances of information disclosure

Personal data is not transferred to third parties except for legal obligation.

9.5 Intellectual Property Rights

9.5.1 Ownership of certificates and revocation information

Only esFIRMA enjoys intellectual property rights over the certificates it issues, without prejudice to the rights of subscribers, key holders and third parties, to whom it grants a non-exclusive license to reproduce and distribute certificates, free of charge, provided that the reproduction is complete and does not alter any element of the certificate, and is necessary in relation to digital signatures and/or encryption systems within the scope of use of the certificate, and in accordance with the documentation that binds them.

Additionally, the certificates issued by esFIRMA contain a legal notice regarding their ownership.

The same rules apply to the use of certificate revocation information.

9.5.2 Ownership of the Certification Practice Statement

Only esFIRMA enjoys intellectual property rights over this Certification Practice Statement.

9.5.3 Ownership of information related to names

The subscriber and, where applicable, the natural person identified in the certificate, retains all rights, if any, to the trademark, product or trade name contained in the certificate.

The subscriber is the owner of the distinguished name of the certificate, formed by the information specified in section 3.1.1

9.5.4 Key ownership

The key pairs are owned by the signers of the certificates.

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

9.6 Obligations and civil liability

9.6.1 Obligations of the Certification Authority "esFIRMA

esFIRMA guarantees, under its full responsibility, that it complies with all the requirements established in the DPC, being the sole responsible for the compliance with the described procedures, even if a part or all of the operations are subcontracted externally.

esFIRMA provides certification services in accordance with this Certification Practice Statement.

Prior to the issuance and delivery of the certificate to the subscriber, esFIRMA informs the subscriber of the terms and conditions regarding the use of the certificate, its price, and its usage limitations, through a subscriber contract that incorporates by reference the disclosure texts (PDS) of each of the acquired certificates.

The disclosure text document, also known as PDS, complies with the content of Annex A of ETSI EN 319 411-1 v1.1.1 (2016-02), which can be transmitted electronically using a durable means of communication over time and in understandable language.
esFIRMA communicates changes permanently[18] that arise in their obligations by publishing new versions of their legal documentation on their website https://www.esfirma.com

esFIRMA links subscribers, key holders, and third parties who rely on certificates through said disclosure text or PDS, in written and understandable language, with the following minimum contents:

- Prescriptions to comply with the provisions set out in sections 4.5.3, 9.2, 9.6.7, 9.6.8, 9.6.9 and 9.6.10.
- Indication of the applicable policy, with an indication that certificates are not issued to the public.
- Statement that the information contained in the certificate is correct, except for notification to the contrary by the subscriber.
- Consent for the storage of the information used for the subscriber's registration and for the transfer of such information to third parties, in case of termination of operations of the Certification Authority without revocation of valid certificates.
- Limits of use of the certificate, including those established in section 1.4.2
- Information on 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 applies when the subscriber acts as a third party that trusts the certificate.

[18] Ap 6.2.3.b) de ETSI EN 319 411-1

- The way in which the financial liability of the Certification Authority is guaranteed.
- Applicable limitations of liability, including the uses for which the Certification Authority accepts or excludes its liability.
- Period of information archive for certificate requests.
- Period of audit log retention.
- Applicable dispute resolution procedures.
- Applicable law and competent jurisdiction.
- If the Certification Authority has been declared compliant with the certification policy and, where appropriate, with which system.

9.6.2. Obligation and responsibility of the RA

The RAs are the entities delegated by the CA to perform the tasks of registration and approval of certificate requests, therefore the RA is also bound in the terms defined in the Certification Practices for the issuance of certificates, mainly:

• Comply with the provisions of this CPS and the corresponding PDS.

• Protect your private keys that will serve you to carry out your functions.

• Verify the identity of the Subjects/Signers and Applicants of the certificates when necessary, definitively accrediting the identity of the Signer in the case of individual certificates, or the key holder in the case of organization certificates, in accordance with the provisions set forth in the corresponding sections of this document.

• Verify the accuracy and authenticity of the information provided by the Applicant.

• Provide the Signer, in case of individual certificates, or the future holder of
keys, in case of organization certificates, access to the certificate.

• Deliver, if applicable, the corresponding cryptographic device.

• Archive, for the period established by current legislation, the documents provided by the applicant or Signatory.

• Comply with the provisions of the contracts signed with esFIRMA and with the Subject/Signer.

• Inform esFIRMA of the revocation causes, as long as they become aware.

• Provide basic information about the policy and use of the certificate, including
especially information about esFIRMA and the Statement of Practices of
Applicable certification, as well as its obligations, powers and responsibilities.

• Provide information about the certificate and the cryptographic device.

- Collect information and evidence from the certificate holder and, where appropriate, the cryptographic device, and acceptance of such elements.
- Inform the exclusive attribution method to the holder of the private key and their certificate activation data, and, where appropriate, the cryptographic device, in accordance with the corresponding sections of this document.

These obligations apply even in cases of entities delegated by these, such as the face-to-face verification points (PVP).

Information about the use and responsibilities of the subscriber is provided through the Acceptance of the terms of use prior to confirmation of the certificate request and via email.

The RAs sign a service provision contract with esFIRMA through which esFIRMA delegates the registration functions to the RAs, consisting mainly of:

1.- Obligations prior to the issuance of a certificate.

a) Properly inform applicants of their obligations and responsibilities regarding the signature.

b) The proper identification of applicants, who must be qualified individuals or authorized to request a digital certificate.

c) The correct verification of the validity and expiration of that data from the applicants and
of the Entity, in case there is a relationship of linkage or representation.

d) Access the Registration Authority application to manage requests and issued certificates.

2.- Obligations once the certificate has been issued.

a) To subscribe to Digital Certification Service Provision contracts with applicants. In most issuance processes, this contract is formalized through the acceptance of conditions on the web pages that are part of the process
of certificate issuance, and the issuance cannot be carried out without having first accepted the terms of use.

b) The maintenance of certificates during their validity (expiration, suspension, revocation).

c) Archive the copies of the documentation presented and the contracts duly signed by the applicants in accordance with the Certification Policies published by esFIRMA and current legislation.

Therefore, the RAs are responsible for the consequences in case of non-compliance with their registration duties, and through which they also undertake to respect the internal regulatory rules of the esFIRMA certification authority (Policies and CPS), which must be perfectly controlled by the RAs and which must serve as a reference manual for them.
In case of a claim by a Subject, an Entity, or a user, the CA must provide the
Proof of diligent performance and if it is found that the origin of the claim lies in an error in the validation or verification of the data, the CA may, under the agreements signed with the RAs, make the responsible RA bear the consequences.
Because, although legally the CA is the legal entity responsible to the Subject, an Entity, or User Party, and has a liability insurance for this purpose, according to the current agreement, the RA has the contractual obligation to "correctly identify and authenticate the Applicant and, where appropriate, the corresponding Entity", and therefore must respond to esFIRMA for its failures.
Of course, it is not the intention of esFIRMA to unload all the responsibility for possible damages whose origin would come from a breach of the tasks delegated to the RA. For this reason, like what is foreseen for the CA, the RA is subject to a control regime that will be exercised by esFIRMA, not only through file controls and file conservation procedures assumed by the RA by conducting audits to evaluate, among others, the resources used and the knowledge and control of the operational procedures to offer RA services.
The same responsibilities must be assumed by the RAs in the event of non-compliance by the
delegated entities such as the face-to-face verification points (PVP), without
without prejudice to their right to pass on the charges to them.

9.6.3 Guarantees offered to subscribers and third parties who rely on certificates

esFIRMA, in the documentation that links it with subscribers and third parties who trust in certificates, establishes and rejects guarantees, and applicable limitations of liability.

esFIRMA, at a minimum, guarantees to the subscriber:

- That there are no errors of fact in the information contained in the certificates, known or made by the Certification Authority.
- That there are no errors of fact in the information contained in the certificates, due to lack of due diligence in the management of the certificate request or in its creation.

- That the certificates comply with all the material requirements established in the Certification Practice Statement.
- That the revocation services and the use of the Repository comply with all the material requirements established in the Certification Practice Statement.

esFIRMA, at least, will guarantee to the third party who trusts the certificate:

- That the information contained or incorporated by reference in the certificate is correct, except when indicated otherwise.
- That in the approval of the certificate request and in the issuance of the certificate, all the material requirements established in the Certification Practice Statement have been met.
- The speed and security in the provision of services, especially revocation services.

Additionally, esFIRMA guarantees to the subscriber and the third party who trusts the certificate:

- That the certificate contains the information that a certificate must contain Qualified, in accordance with Annex 1 of Regulation (EU) 910/2014.
- That, in the event that the private keys of the subscriber or, where appropriate, the natural person identified in the certificate are generated, their confidentiality is maintained during the process.
- The responsibility of the Certification Authority, within the limits established. In no event shall ESFIRMA be liable for fortuitous events or force majeure.
- The private key of the certification entity used to issue certificates has not been compromised, unless esFIRMA has communicated otherwise.
- Has not originated or introduced false or erroneous statements in the information of any certificate, nor have you failed to include necessary information provided by the subscriber and validated by esFIRMA, at the time of issuance of the certificate.
- All certificates meet the formal and content requirements of this Practices Statement, including all current and applicable legal requirements.
- You are bound by the operational and security procedures described in this Statement of Practices.

9.6.4 Obligation and responsibility of third parties

It will be the obligation of the User Party to comply with what is established in the current regulations and, in addition:

- Verify the validity of the certificates and the entire certification chain, before performing any operation based on them. esFIRMA has various mechanisms to perform this verification, such as access to lists of revoked certificates or to online OCSP query services.
- To know and adhere to the guarantees, limits, and responsibilities applicable to the acceptance and use of the certificates in which you trust, and to accept to adhere to them.
- Check the validity of the qualification of a signature associated with a certificate issued by esFIRMA by verifying that the certification authority that issued the certificate is published in the trust list of the corresponding national supervisor.

9.6.5 Obligation and responsibility of other participants

Not stipulated

9.7. Warranty exemption

According to current legislation, the responsibility of esFIRMA and its RAs does not extend to those cases in which the improper use of the certificate originates from conducts attributable to the Subject, and to the User Party for:

- Not having provided adequate information, initially or subsequently such as
- consequence of modifications of the circumstances reflected in the electronic certificate, when their inaccuracy could not be detected by the certification service provider
- Having incurred negligence with respect to the conservation of signature creation data and its confidentiality.
- Not having requested revocation of the electronic certificate data in case of doubt about maintaining confidentiality
- Having used the signature after the validity period of the electronic certificate has expired
- Exceed the limits stated in the electronic certificate.

- The User Party is responsible for attributable behaviors if it acts negligently, that is, when it does not verify or take into account the restrictions contained in the certificate regarding its possible uses and transaction amount limit; or when it does not take into account the validity status of the certificate
- Of the damages caused to the Subject or third parties who rely on the inaccuracy of the data contained in the electronic certificate, if they have been accredited through a public document, registered in a public registry if required.
- Improper or fraudulent use of the certificate in case the Subject/Holder has transferred it or authorized its use in favor of a third party under a legal transaction such as mandate or power of attorney, being the exclusive responsibility of the Subject/Holder to control the keys associated with their certificate.

esFIRMA and its RAs will not be responsible in any case when faced with any of these circumstances:

- State of War, natural disasters or any other case of Force Majeure.
- For the use of certificates as long as it exceeds what is established in the current regulations and Certification Policies
- For the improper or fraudulent use of certificates or CRLs issued by the CA
- For the use of the information contained in the Certificate or in the CRL.
- Due to the harm caused during the period of verification of the revocation causes.
- Due to the content of the digitally signed or encrypted messages or documents.
- Due to the non-recovery of documents encrypted with the Subject's public key.

9.8. Limitation of liability in case of losses due to transactions

The maximum limit that esFIRMA allows in economic transactions is 0 (zero) euros.

9.9. Indemnities

See section 9.2

9.10. Deadline and Completion

9.10.1 Deadline

See section 5.8

9.10.2 Termination

See section 5.8

9.10.3 Effect of Termination and Survival

See section 5.8

9.11. Individual notifications and communication with participants

Any notification regarding this CPS will be made by email or
by certified mail addressed to any of the addresses referred to in section contact details 1.5.2.

9.12. Amendments

9.12.1 Modification procedure

The CA reserves the right to modify this document for technical reasons or to reflect any changes in procedures that have occurred due to legal or regulatory requirements (eIDAS, National Supervisory Bodies, etc.) or as a result of work cycle optimization. Each new version of this CPS replaces all previous versions, which remain, however, applicable to certificates issued while those versions were in force and until the first expiration date of those certificates. At least one annual update will be published. These updates will be reflected in the version table at the beginning of the document.
Changes that can be made to this CPS do not require notification unless they directly affect the rights of the Subjects/Signers of the certificates, in which case they may submit their comments to the policy administration organization within 15 days of publication.

9.12.2 Notification mechanism and deadlines

All proposed changes to this policy will be immediately published on the esFIRMA website. In this same document there is a section for changes and versions where you can learn about the changes made since its creation and the date of such modifications.
Changes to this document are communicated to those organizations and third-party companies that issue certificates under this CPS as well as to the corresponding auditors. Changes to this CPS will be especially notified to National Supervision organizations.

The Signers/Subscribers and affected Third Parties who trust can submit their comments to the policy administration organization within 15 days following the receipt of the notification.

9.12.3 Circumstances in which the OID must be changed

Not stipulated

9.13 Conflict resolution procedure

esFIRMA establishes, in the subscriber contract, and in the disclosure or PDS text, the applicable mediation and conflict resolution procedures.

9.14. Applicable legislation

esFIRMA establishes, in the subscriber contract and in the disclosure or PDS text, that the applicable law for the provision of services, including certification policy and practices, is Spanish law.

9.15. Compliance with Applicable Law

See point 9.14

9.16. Other provisions

9.16.1 Complete agreement

The Holders and third parties who rely on the Certificates assume in full the content of this Certification Practice Statement and Policy

9.16.2 Assignment

The parties to this DPC may not assign any of their rights or obligations under it or applicable agreements without the written consent of esFIRMA.

9.16.3 Severability

esFIRMA establishes, in the subscriber contract, and in the disclosure or PDS text, clauses of divisibility, survival, entire agreement and notification:

- By virtue of the divisibility clause, the invalidity of one clause shall not affect the remainder of the contract.
- By virtue of the survival clause, certain rules will remain in force after the end of the legal relationship regulating the service between the parties. To this end, the Certification Authority ensures that at least the requirements contained in sections 9.6.1 (Obligations and responsibilities), 8 (Conformity audit), and 9.3 (Confidentiality) continue to be in force after the termination of the service and the general conditions of issuance/use.
- By virtue of the entire agreement clause, it will be understood that the legal document regulating the service contains the complete will and all agreements between the parties.
- Under the notification clause, the procedure by which the parties notify each other of facts will be established.

9.16.4 Compliance (lawyer fees and exemption of fees)

esFIRMA may request compensation and attorney fees from a party for
damages, losses and expenses related to the conduct of said party. The fact that
Not enforcing a provision of this CPS does not waive the right of esFIRMA
to enforce the same provisions later or the right to enforce
any other provision of this CPS. To be effective, any waiver must be in writing and signed by esFIRMA

9.16.5 Force majeure

esFIRMA includes in the disclosure text or PDS, clauses that limit its liability in case of fortuitous events and in case of force majeure.

9.17 Other provisions

9.17.1 Subscriber indemnity clause

esFIRMA includes in the contract with the subscriber a clause by which the subscriber undertakes to indemnify the Certification Authority for any damage arising from any action or omission resulting in liability, damage or loss, expense of any kind, including legal and attorney's fees that may be incurred, for the publication and use of the certificate, when any of the following causes occur:

- Falsehood or erroneous statement made by the certificate user.
- Certificate user error when providing request data, if there was intent or negligence in relation to the Certification Entity or any person who relies on the certificate.
- Negligence in protecting the private key, using a reliable system, or maintaining the necessary precautions to prevent the compromise, loss, disclosure, modification, or unauthorized use of said key.
- Employment by the subscriber of a name (including common names, email address, and names of...) Domain), or other information in the certificate, that infringes intellectual or industrial property rights of third parties.

9.17.2 Third party indemnity clause that relies on the certificate

esFIRMA includes in the disclosure text or PDS, a clause by which the third party who relies on the certificate agrees to indemnify the Certification Authority from any damage arising from any action or omission resulting in liability, damage or loss, expense of any kind, including legal and attorney fees that may be incurred, for the publication and use of the certificate, when any of the following causes occur:

- Failure to comply with the obligations of the third party who relies on the certificate.
- Reckless trust in a certificate, given the circumstances.

- Failure to verify the status of a certificate to determine that it is not suspended or revoked.

The third party that relies on the certificate agrees to hold ESFIRMA harmless from any damage arising from any action or omission resulting in liability, damage or loss, expense of any kind, including legal and attorney fees that may be incurred, for the publication and use of the certificate, when any of the following causes occur:
- Non-compliance with the obligations of the third party who trusts the certificate.
- Reckless trust in a certificate, given the circumstances.
- Lack of verification of the status of a certificate, to determine that it is not
is suspended or revoked.
- Failure to verify all prescribed security measures in the
DCP or other applicable regulations.

ESFIRMA will not be responsible for the damages caused in the terms indicated in article 11 of Law 6/2020, of November 11, regulating certain aspects of electronic trust services.