Certification Practices Statement

esFIRMA

Overview

Document control

Safety Rating:	Public
Target entity:	ESFIRMA
Version:	1.13

Formal status

Prepared by:	Reviewed by:	Approved by:
Security Office Date: 13/07/2022	Security Officer Date: 13/07/2022	Safety Committee Date: 18/07/2022

Version control

See	Description of the change	Date
1.0	Creating the document	29/04/2016
1.1	Corrections	02/06/2016
1.2	ETSI Review	19/05/2017
1.3	Review certificate types	
1.4	Review Certificate Types, Acronyms and Definitions	02/06/2017
1.5	Regulatory reference adjustments, name change, certificate change 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 the 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 revision on the renewal sections.	13/11/2018
1.9	3.1.1.1 Clarification on the optional second surname. 3.1.1.2 OrganizationIdentifier conditional on CA/Browser Forum Guidelines 3.1.1.4 Adjusting typographical errors to OID descriptions 3.1.1.7 CN of the optional headquarters EV certificate	14/06/2019
1.10	Miscellaneous 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 Organization Contact Details 1.5.2 moved to 1.5.3 Organization approving the document "DEFINITIONS ACRONYMS" moved to 1.6 Acronyms and definitions 4.4.2 moved to 4.4.1 Conduct constituting 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 Processing the Certificate Renewal Application Added 4.6.4 Notification of new certificate issuance to subscriber Added 4.6.5 Conduct constituting acceptance of a certificate of renewal Added 4.6.6 Publication of the certificate of renewal 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 new certificate key requests 4.7.3 moved to 4.7.4 Notification of issuance of renewed certificate 4.7.4 moved to 4.7.5 Conduct constituting 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 Health Check 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 Subscription Termination 6.1.9 moved to 6.1.7 Purposes of using keys 6.2.9 Moved to 6.2.9 Private Key Deactivation Method 6.2.10 moved to 6.2.10 Private Key Destruction Method 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 Lifecycle Security Assessment 6.9 moved to 6.8 Time Sources Added 7.1.7 Using the Policy Restrictions Extension Added 7.1.8 Syntax and Semantic Policy Qualifiers Added 7.1.9 Processing Semantics for Certificate Policies Critical Extension 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 pursuant to judicial or administrative process Added 9.4.7 Other Disclosure Circumstances Added 9.6.2 RA representations and warranties 9.6.2 moved to 9.6.3 Warranties offered to subscribers and third parties relying on certificates Added 9.6.4 Obligation and liability of third parties 9.6.2 moved to 9.6.5 Obligation and liability of other participants 9.6.3 moved to 9.7 Disclaimer 9.6.4 moved to 9.8 Limitation of liability in case of transaction losses 9.6.5 moved to 9.9 Indemnities Added 9.10. Deadline and Completion Added 9.10.1 Term 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 Dispute Resolution Procedure 9.6.7 moved to 9.14 Applicable law Added 9.15 Compliance with Applicable Law Added 9.16 Other provisions Added 9.16.1 Entire Agreement Added 9.16.2 Assignment 9.6. moved to 9.16.3 Separability Added 9.16.4 Compliance (Attorneys' Fees and Duty Waiver) 9.6.6 moved to 9.16.5 Force majeure Added 9.17 Other provisions New certificates are included: certificate of public employee (Authentication), certificate of public employee with pseudonym (Authentication), certificate of natural person linked to entity (Authentication), certificate of natural person linked to entity (SIGNATURE), certificate of natural person with pseudonym linked to entity (Authentication), certificate of natural person with pseudonym linked to entity (SIGNATURE)	
1.11	New qualified electronic seal certificates included The e-office certificate profile is deleted. Adaptation due to regulatory change (Law 6/2020, of November 11, regulating certain aspects of electronic trust services). Added in section 5.8 Termination of service of the DPC is the detail of how the status information of the certificates is provided beyond the life time of these.	03/05/2021

	References to the Ministry of Industry, Energy and Tourism are updated by the Ministry of Economic Affairs and Digital Transformation.	
1.12	Point 5.2.1 is amended by changing the name from "Registry Administrator" to "Registry Operator". References to CA/B Forum are removed.	10/05/2021
1.13	Modification point 5.8 Termination of Service, according to the Cessation Plan Section 4.9.1 is amended to include the end of QSCD certification Amendment point 6.5.1, including the end of DCCF certification. Deletion of reference to the security document of esFIRMA from section 6.6.2 (Management operations) Replacement of "security policy" by "information security management system" in section 6.6.2 (Classification and management of information and assets) Paragraph 6.9 is added in accordance with ETSI TS 119 431-1: OVR-5.1-02 Point 9.6.4 is amended, including the Certification Chain as a checkpoint. 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 certificates in the certification chain is added to section 4.9.6.	18/07/2022

Index

1. Introduction

1.1 Presentation

This document declares esFIRMA's electronic signature certification practices.

The certificates that are issued are as follows:

- **Of Public Employee (SIGNATURE)**
  - Medium Level Public Employee
  - High Level Public Employee
- **Of Public Employee (AUTHENTICATION)**
  - High Level Public Employee
- **Public Employee with pseudonym (SIGNATURE)**
  - Medium Level Public Employee
  - High Level Public Employee
- **Public Employee with pseudonym (AUTHENTICATION)**
  - High Level Public Employee
- **From natural person linked to entity (SIGNATURE)**
  - From natural person linked to Medium level entity
  - From natural person linked to High level entity
- **From natural person linked to entity (AUTHENTICATION)**
  - From natural person linked to High level entity
- **From natural person linked to entity with pseudonym (SIGNATURE)**
  - From natural person linked to Medium level entity
  - From natural person linked to High level entity
- **From natural person linked to entity with pseudonym (AUTHENTICATION)**
  - From natural person linked to High level entity
- **Organ Seal**
  - Of Organ Seal Medium Level
- **Electronic Seal for TSA/TSU**
  - Electronic seal for TSU in HSM
- **Electronic Seal**
  - Electronic seal in software

- Electronic seal with centralized management

1.2 Document name and identification

This document is esFIRMA's "Statement of Certification Practices".

1.2.1 Certificate Identifiers

OID Number	Certificate Policies
	Of Public Employee (SIGNATURE)
1.3.6.1.4.1.47281.1.1.1	*Public Employee – High Level on Card*
1.3.6.1.4.1.47281.1.1.4	*Public Employee – Medium Level in HSM*
	Of Public Employee (AUTHENTICATION)
1.3.6.1.4.1.47281.1.1.5	*Public Employee – High Level on Card*
	Public Employee with Pseudonym (SIGNATURE)
1.3.6.1.4.1.47281.1.3.1	*Ep with Pseudonym – High Level on Card*
1.3.6.1.4.1.47281.1.3.4	*Pseudonymous EP – Medium Level in HSM*
	Public Employee with Pseudonym (AUTHENTICATION)
1.3.6.1.4.1.47281.1.3.5	*Ep with Pseudonym – High Level on Card*
	From Natural Person linked to entity (SIGNATURE)
1.3.6.1.4.1.47281.1.6.1	*From PF linked to entity – Firma-e Cualificada, in Card*
1.3.6.1.4.1.47281.1.6.4	*From PF linked to entity – Firma-e Centralizado*
	From Natural Person linked to entity (AUTHENTICATION)
1.3.6.1.4.1.47281.1.6.5	*From PF linked to entity – on Card*
	Of Natural Person with pseudonym linked to entity (SIGNATURE)
1.3.6.1.4.1.47281.1.7.1	*From PF with pseudonym linked to entity – Firma-e Cualificada, in Card*
1.3.6.1.4.1.47281.1.7.4	*From PF with pseudonym linked to entity – Firma-e Centralizado*

	Of Natural Person with pseudonym, linked to entity (AUTHENTICATION)
1.3.6.1.4.1.47281.1.7.5	*From PF with pseudonym, linked to entity – on Card*
	Organ Seal
1.3.6.1.4.1.47281.1.2.2	*Organ Seal –* *Medium Level in Software*
1.3.6.1.4.1.47281.1.2.4	*Organ Seal –* *Medium Level at HSM*
	Electronic Seal for TSA/TSU
1.3.6.1.4.1.47281.1.5.2	*E-Stamp for TSA/TSU at HSM*
	Electronic Seal
1.3.6.1.4.1.47281.1.8.2	*From Electronic Seal to Software*
1.3.6.1.4.1.47281.1.8.4	*Centralized electronic seal*

In the event of a contradiction between this Statement of Certification Practices and other esFIRMA practice and procedure documents, the provisions of this Statement of Practice 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 person, natural or legal, who issues and manages certificates for final entities, using a Certification Entity, or providing other services related to the electronic signature.

ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (ANTERIOR AULOCE SA), hereinafter ESPUBLICO, with address at Calle Bari 39 (Edif. Binary Building), C.P. 50.197, Zaragoza, CIF A-50.878.842, registered in the Mercantile Registry of Zaragoza in volume 2.649, Folio

215, sheet Z-28722, and operating under the trade name esFIRMA, commercial name which will be used throughout this document to designate it, it is a certification service provider that acts in accordance with the provisions of the regime of obligations and responsibilities of Regulation (EU) 910/2014, of 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 technical standards of the ETSI 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 their services.

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

esFIRMA AC root 2

This is the root CA in the hierarchy that issues certificates to other CAAs, and whose public key certificate has been self-signed.

Identification data:

CN:	ESFIRMA AC ROOT 2
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

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

Identification data:

CN:	ESFIRMA AC AAPP 2

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

It is the platform for managing the life cycle of the certificate exclusively, for its application, approval, issuance and revocation.

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

1.3.2 Registration Authorities

A registration authority carries out verification and identification of certificate applicants.

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

Also registering authorities of the certificates subject to this Statement of Certification Practices, due to their status as corporate certificates, are the units designated for this function by the subscribers of the certificates, such as the Secretariat of the corporation, the personnel department or the Legal Representative of the Administration, since they have the authentic records about the link of the signatories with the subscriber.

The functions of registration of subscribers are carried out by delegation and in accordance with the instructions of the certification service provider, in 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 vis-à-vis third parties.

1.3.3 End entities

The final entities are the persons and organizations receiving the services of issuance, management and use of digital certificates, for the uses of identification and electronic signature.

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

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

1.3.4 User Parties

User parties are individuals and organizations that receive digital signatures and digital certificates.

As a preliminary step to trusting the certificates, the user parties must verify them, as set out in this statement of certification practices and in the corresponding instructions available on the website of the Certification Body.

1.3.5 Other participants

Certification Service Subscribers

The subscribers of the certification service are the 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 his 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 the latter case, this person is identified on the certificate, as provided for in the following section.

The subscriber of the certification service is therefore the customer of the certification service provider, in accordance with commercial legislation, and has the rights and

obligations that are defined by the certification service provider, which are additional and are understood without prejudice to the rights and obligations of the signatories, as authorised and regulated in the European technical standards applicable to the issuance of qualified electronic certificates, in particular in ETSI EN 319 411-2, sections 5.4.2 and 6.3.4.e)

Signatories

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

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

Given the existence of certificates for uses other than electronic signatures, 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 in relation to the rights and obligations of the signatory.

1.4 Use of certificates

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

Certificate of Public Employee high level in Card

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.1.1	In the hierarchy of the EC 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 certificates of natural person public employee high level are qualified certificates 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 provisions of the technical regulations identified with the reference ETSI EN 319 411-2.

These certificates are issued to public employees to identify them as persons at the service of the Administration, body, entity of public law or other entity, linking them with 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 personnel at the service of Public Administrations.

The certificates of natural person public employee high level, work with 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, the certificates of natural person public employee high level are issued in accordance with the high assurance levels of the certificate profiles established in point 10 of the document "Profiles of Electronic Certificates" of the Secretary of State for Digitalization and Artificial Intelligence of the Ministry of Economic Affairs and Digital Transformation.

These certificates guarantee the identity of the subscriber and the signatory, and 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 the provisions of Article 25.2 of Regulation (EU) 910/2014 of the European Parliament and of the Council, of 23 July 2014, it shall have a legal effect equivalent to that of a handwritten signature.

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

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

esFIRMA does not offer key backup or recovery services. Therefore, esFIRMA will not respond 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 activated, and therefore allows you to perform, the following functions:
    a. Content commitment (to perform the function of electronic signature)

b) In the "Qualified Certificate Statements" field, the following statement appears:
    a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
    b. QcSSCD (0.4.0.1862.1.4), which reports 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 medium level in HSM

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.1.4	In the hierarchy of the EC esFIRMA

0.4.0.194112.1.0	In accordance with QCP-n policy
2.16.724.1.3.5.7.2	Medium-level Spanish public employee

The certificates of natural person public employee medium level are qualified certificates 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 provisions of the technical regulations identified with the reference ETSI EN 319 411-2.

These certificates are issued to public employees to identify them as persons at the service of the Administration, body, entity of public law or other entity, linking them with 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 personnel at the service of Public Administrations.

Certificates of natural person public employee medium level are managed centrally.

The certificates of natural person public employee medium level are issued in accordance with the average assurance levels of the certificate profiles established in point 10 of the document "Profiles of Electronic Certificates" of the Secretary of State for Digitalization 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 a 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 following applications:

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

esFIRMA does not offer key backup or recovery services. Therefore, esFIRMA will not respond 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 activated, and therefore allows us to perform, the following functions:
    a. Content commitment (to perform the function of electronic signature)

b) In the "Qualified Certificate Statements" field, the following statement appears:
    a. qCCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
c) The "User Notice" field describes the use of this certificate.

High level Public Employee Certificate on card for authentication

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.1.5	In the hierarchy of the EC esFIRMA
0.4.0.2042.1.2	In accordance with 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 standard certificate policy (NCP+) and comply with the provisions of the technical regulations identified with the reference ETSI EN 319 411-1.

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

These certificates of natural person public employee high level, work with 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.

The certificates of natural person public employee high level are issued in accordance with the high assurance levels of the certificate profiles established in point 10 of the document "Profiles of Electronic Certificates" of the Secretary of State for Digitalization 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 key backup or recovery services. Therefore, esFIRMA will not respond 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 activated, 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.

Certificate of Organ Seal medium level in software

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.2.2	In the hierarchy of the EC esFIRMA
0.4.0.194112.1.1	In accordance with QCP-l policy
2.16.724.1.3.5.6.2	Medium-level Spanish public employee

Medium-level electronic seal certificates are qualified certificates 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 by 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 42 of Law 40/2015, of October 1, on the Legal Regime of the Public Sector.

Medium-level organ electronic seal certificates are issued in accordance with the average assurance levels of the certificate profiles established in point 9 of the document "Electronic Certificate Profiles" of the Secretary of State for Digitalization and Artificial Intelligence of the Ministry of Economic Affairs and Digital Transformation.

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

esFIRMA does not offer key backup or recovery services. Therefore, esFIRMA will not respond 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 activated, and therefore allows us to perform, the following functions:
    a. Content commitment (to perform the function of electronic signature)

b) In the "Qualified Certificate Statements" field, the following statement appears:
    a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
c) The "User Notice" field describes the use of this certificate.

Organ Seal Certificate medium level in HSM

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.2.4	In the hierarchy of the EC esFIRMA
0.4.0.194112.1.1	In accordance with QCP-l policy
2.16.724.1.3.5.6.2	Medium-level Spanish public employee

Medium-level electronic seal certificates are qualified certificates 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 by 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 42 of Law 40/2015, of October 1, on the Legal Regime of the Public Sector.

Mid-level electronic seal certificates are managed centrally.

Medium-level organ electronic seal certificates are issued in accordance with the average assurance levels of the certificate profiles established in point 9 of the document "Electronic Certificate Profiles" of the Secretary of State for Digitalization and Artificial Intelligence of the Ministry of Economic Affairs and Digital Transformation.

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

esFIRMA does not offer key backup or recovery services. Therefore, esFIRMA will not respond 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 activated, and therefore allows us to perform, the following functions:
    a. Content commitment (to perform the function of electronic signature)

b) In the "Qualified Certificate Statements" field, the following statement appears:
    a. QcCompliance (0.4.0.1862.1.1), which informs 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

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.3.1	In the hierarchy of the EC 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

Certificates of natural persons employed by a public employee with a high level pseudonym are qualified certificates 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 provisions of the technical regulations identified with the reference ETSI EN 319 411-2.

These certificates are issued to public employees to identify them (by means of a pseudonym) as persons at the service of the Administration, body, entity of public law or other entity, linking them with 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 personnel at the service of Public Administrations.

The certificates of natural person public employee with high level pseudonym, work with 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, the certificates of natural person public employee with a high level pseudonym are issued in accordance with the high assurance levels of the certificate profiles established in point 11 of the document "Profiles of Electronic Certificates" of the Secretary of State for Digitalization 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 the provisions of Article 25.2 of Regulation (EU) 910/2014 of the European Parliament and of the Council, of July 23, 2014, it shall have a legal effect equivalent to that of a handwritten signature.

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

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

esFIRMA does not offer key backup or recovery services. Therefore, esFIRMA will not respond 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 activated, and therefore allows you to perform, the following functions:
    a. Content commitment (to perform the function of electronic signature)

b) In the "Qualified Certificate Statements" field, the following statement appears:
    a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
    b. QcSSCD (0.4.0.1862.1.4), which reports 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 pseudonym medium level, in HSM

This certificate has the following OIDs:

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

Certificates of natural person employed by public employee with pseudonym medium level are qualified certificates 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 provisions of the technical regulations identified with the reference ETSI EN 319 411-2.

These certificates are issued to public employees to identify them (by means of a pseudonym) as persons at the service of the Administration, body, entity of public law or other entity, linking them with 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 personnel at the service of Public Administrations.

Certificates of natural persons employed by public employees with a pseudonym at medium level are managed centrally.

The certificates of natural person public employee with pseudonym medium level are issued in accordance with the average assurance levels of the certificate profiles established in point 11 of the document "Profiles of Electronic Certificates" of the Secretary of State for Digitalization 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 following applications:

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

esFIRMA does not offer key backup or recovery services. Therefore, esFIRMA will not respond 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 activated, and therefore allows us to perform, the following functions:
    a. Content commitment (to perform the function of electronic signature)

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

a. qCCompliance (0.4.0.1862.1.1), which informs 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 in card for authentication

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.3.5	In the hierarchy of the EC esFIRMA
0.4.0.2042.1.2	In accordance with the NCP+ policy
2.16.724.1.3.5.4.1	Spanish public employee with high-level pseudonym

These certificates are certificates issued in accordance with the standard certificate policy (NCP+) and comply with the provisions of the technical regulations identified with the reference ETSI EN 319 411-1.

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

These certificates of natural person public employee with pseudonym high level, work with 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.

The certificates of natural person public employee with high pseudonym 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 Secretary of State for Digitalization 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 key backup or recovery services. Therefore, esFIRMA will not respond 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 activated, 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.

TSA/TSU Electronic Seal Certificate

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.5.2	In the hierarchy of the EC esFIRMA
0.4.0.194112.1.1	In accordance with QCP-l policy

TSA/TSU electronic seal certificates are qualified certificates 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 TSU to issue time stamps when they receive an application under the specifications of RFC3161.

Keys are generated in support of an HSM device.

The usage information in the certificate profile indicates the following:

a) The "key usage" field has activated, 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 informs that the certificate is issued as qualified.

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

Certificate of linked natural person, in Card for signature

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.6.1	In the hierarchy of the EC 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 provisions of the technical regulations identified with the reference ETSI EN 319 411-2.

These certificates operate 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.

These certificates guarantee the identity of the subscriber and the signatory, and 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 the provisions of Article 25.2 of Regulation (EU) 910/2014 of the European Parliament and of the Council, of 23 July 2014, it shall have a legal effect equivalent to that of a handwritten signature.

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

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

esFIRMA does not offer key backup or recovery services. Therefore, esFIRMA will not respond 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 activated, and therefore allows you to perform, the following functions:
    a. Content commitment (to perform the function of electronic signature)

e) In the "Qualified Certificate Statements" field, the following statement appears:
    a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
    b. QcSSCD (0.4.0.1862.1.4), which reports 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.

Certificate of linked natural person, centralized, for signature

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.6.4	In the hierarchy of the EC esFIRMA
0.4.0.194112.1.0	In accordance with 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 provisions of the technical regulations identified with the reference ETSI EN 319 411-2.

These certificates are managed centrally.

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 a 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 following applications:

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

esFIRMA does not offer key backup or recovery services. Therefore, esFIRMA will not respond 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 activated, and therefore allows us to perform, the following functions:
    a. Content commitment (to perform the function of electronic signature)

i) In the "Qualified Certificate Statements" field, the following statement appears:
    a. qCCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
j) The "User Notice" field describes the use of this certificate.

Certificate of linked natural person, on card for authentication

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.6.5	In the hierarchy of the EC esFIRMA
0.4.0.2042.1.2	In accordance with the NCP+ policy

These certificates are certificates issued in accordance with the standard certificate policy (NCP+) and comply with the provisions of the technical regulations identified with the reference ETSI EN 319 411-1.

These certificates operate 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.

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 key backup or recovery services. Therefore, esFIRMA will not respond 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 activated, 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.

Certificate of linked natural person, with pseudonym, in Card for signature

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.7.1	In the hierarchy of the EC 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 provisions of the technical regulations identified with the reference ETSI EN 319 411-2.

These certificates operate 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.

These certificates guarantee the identity of the subscriber.
These certificates guarantee the identity of the signatory by means of a pseudonym.
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 the provisions of Article 25.2 of Regulation (EU) 910/2014 of the European Parliament and of the Council, of July 23, 2014, it shall have a legal effect equivalent to that of a handwritten signature.

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

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

esFIRMA does not offer key backup or recovery services. Therefore, esFIRMA will not respond 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 activated, and therefore allows you to perform, the following functions:
    a. Content commitment (to perform the function of electronic signature)

h) In the "Qualified Certificate Statements" field, the following statement appears:
    a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
    b. QcSSCD (0.4.0.1862.1.4), which reports 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.

Certificate of a linked natural person, 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 EC esFIRMA
0.4.0.194112.1.0	In accordance with 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 provisions of the technical regulations identified with the reference ETSI EN 319 411-2.

These certificates are managed centrally.
These certificates guarantee the identity of the subscriber.
These certificates guarantee the identity of the signatory by means of 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 following applications:

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

esFIRMA does not offer key backup or recovery services. Therefore, esFIRMA will not respond 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 activated, and therefore allows us to perform, the following functions:
    a. Content commitment (to perform the function of electronic signature)

n) In the "Qualified Certificate Statements" field, the following statement appears:
    a. qCCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
o) The "User Notice" field describes the use of this certificate.

Certificate of a related natural person, 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 EC esFIRMA
0.4.0.2042.1.2	In accordance with the NCP+ policy

These certificates are certificates issued in accordance with the standard certificate policy (NCP+) and comply with the provisions of the technical regulations identified with the reference ETSI EN 319 411-1.

These certificates operate 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.

These certificates guarantee the identity of the subscriber.
These certificates guarantee the identity of the signatory by means of a pseudonym.
These certificates allow the authentication of the latter to applications and websites.

esFIRMA does not offer key backup or recovery services. Therefore, esFIRMA will not respond 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 activated, 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.

Electronic Seal Certificate in software

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.8.2	In the hierarchy of the EC esFIRMA
0.4.0.194112.1.1	In accordance with 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 23 July 2014 and comply with the provisions of the technical regulations identified with the reference ETSI EN 319 411-2.

esFIRMA does not offer key backup or recovery services. Therefore, esFIRMA will not respond 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 activated, and therefore allows us to perform, the following functions:
    a. Digital signature (for authentication function)
    b. Content commitment (to perform the function of electronic signature)
    c. Key encryption

b) In the "Qualified Certificate Statements" field, the following statement appears:
    a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
c) The "User Notice" field describes the use of this certificate.

Electronic Seal Certificate with centralized management

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.8.4	In the hierarchy of the EC esFIRMA
0.4.0.194112.1.1	In accordance with 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 23 July 2014 and comply

with the provisions of the technical regulations identified with the reference ETSI EN 319 411-2.

These certificates are managed centrally.

esFIRMA does not offer key backup or recovery services. Therefore, esFIRMA will not respond 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 activated, and therefore allows us to perform, the following functions:
    a. Content commitment (to perform the function of electronic signature)

e) In the "Qualified Certificate Statements" field, the following statement appears:
    a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
f) The "User Notice" field describes the use of this certificate.

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 in other functions and for other purposes.

Similarly, licences should be used only in accordance with applicable law, especially taking into account the import and export restrictions in place at any given time.

Certificates cannot be used to sign requests for issuance, renewal, suspension, or revocation of certificates, or to sign public key certificates of any kind, or to sign certificate revocation lists (CRLs).

Certificates have not been designed, cannot be used and are not authorized for use or resale as equipment for the control of dangerous situations or for uses that require fail-safe actions, such as the operation of nuclear facilities, navigation or air communications

systems, or arms control systems, where a failure could directly lead to death, personal injury or severe environmental damage.

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

The use of the digital certificates in a way that breaches 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 for the appropriate legal purposes, and exempts esFIRMA from any responsibility for this improper use, either of the signatory or of any third party.

esFIRMA has no access authorization or legal obligation to monitor 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, thus assuming the subscriber, the signatory or the person responsible for the custody, any responsibility arising from the content associated with the use of a certificate.

Likewise, it will be attributable to the subscriber, the signatory or the person responsible for custody, any liability that may arise from the use of the same outside the limits and conditions of use contained in this DPC, the legal documents binding with each certificate, or the contracts or agreements with the registration entities or with its subscribers, as well as any other improper use thereof derived from this section or that can be interpreted as such in accordance with current legislation.

The certificates are used exclusively and only from the Electronic Administration Platform or extensions and complements of the same that the company ESPUBLICO makes available to the subscriber.

1.5 Policy Administration

1.5.1 Organization that administers the document

Security Office of ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (esFIRMA)

CALLE BARI 39 (Binary Building)
50197 - ZARAGOZA
(+34) 976300110

Registration Identification	Mercantile Registry of Zaragoza
Tome	2649
Folio	215
Leaf	Z-28722
CIF	A-50.878.842

1.5.2 Contact details of the organisation

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

1.5.3 Organization approving the document

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

The security committee of esFIRMA, formed by the President of the same, the Head of Information and Service and the Head of Security of esFirma, has the responsibility for the approval of this Statement of Practices.

Both the functions and the members of this 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 makes revisions at least annually of this document or when required by changes in the guidelines and documents with which it must comply.

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

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

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

The action of the Security Office occurs at the request of its responsible according to the needs that arise.

esFirma can make changes that do not require notification when these do not directly affect the rights of the signatories and subscribers of the certificates or of the subscribers of the stamps.
When esFirma is going to introduce changes that modify the rights of the signatories and subscribers of the certificates and of the subscribers of stamps, it must notify it publicly in order to submit its comments to the Security Office for 15 days following the publication of the future changes.

To publicly notify the changes produced will be published in the "documentation" section on the website https://www.esfirma.com

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 (*or also CA*)	*Certificate Authority* Certification Authority
AR (or also AR)	*Registration Authority* Registration Authority
CPD	Data Processing Center
CPS (or also DPC)	*Certification Practice Statement*. Certification Practices Statement
CRL (or also LRC)	*Certificate Revocation List.* List of revoked certificates
DN	*Distinguished Name.* Distinguished name within the digital certificate
ID	National Identity Document
ETSI IN	*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.* Certificate Status Access Protocol
OID	*Object Identifier*. Object Identifier
PDS	*PKI Disclosure Statements* PKI Disclosure Text.
PIN	*Personal Identification Number*. Personal identification number
PKI	*Public Key Infrastructure*. Public Key Infrastructure

QSCD (or also DCCF)	*Qualified Electronic Signature/Seal Creation Device.* Qualified signature/stamp creation device
QCP	*Qualified Certificate* Policy Qualified Certificate Policy
QCP-n	*Qualified Certificate Policy-natural person* Qualified certificate 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. Encryption algorithm type
SHA	*Secure Hash Algorithm.* Secure Hash Algorithm
SSL	*Secure Sockets Layer.* A protocol designed by Netscape and made a network standard, it allows the transmission of encrypted information between an Internet browser and a server.
TCP/IP	*Transmission Control. Protocol/Internet Protocol*. System of protocols, defined within the framework of the IEFT.
TSA	*Time Stamping* Authority Electronic Time Stamping Authority
TSU	*Time Stamping Unit* Time Stamping Unit.
UTC	*Coordinated Universal Time* Coordinated Universal Time
VPN	*Virtual Private Network.* Virtual Private Network

1.6.2 Definitions

Certification Authority	*It is the entity responsible for the issuance and management of digital certificates.*
Registration Authority	*Entity responsible for the management of applications, identification and registration of applicants for a certificate. You can be part of the Certification Authority or be an outsider.*
Certificate	*File that associates the public key with some identifying data of the Subject/Signatory and is signed by the CA.*
Public key	*A publicly known mathematical value used for verification of a digital signature or data encryption.*
Private key	*Mathematical value known only to the Subject/Signer and used for the creation of a digital signature or data decryption.* *The private key of the CA will be used for certificate signing and signing CRL's.* *The private key of the TSA service will be used to sign the time stamps.*
CPS	*Set of practices adopted by a Certification Authority for the issuance of certificates in accordance with a specific certification policy.*
CRL	*A file that contains a list of certificates that have been revoked in a given period of time and that is signed by the CA.*
Activation Data	*Private data, such as PIN's or passwords used for the activation of the private key*
DCCF	*Qualified signature creation device. Software or hardware element, conveniently certified, used by the Subject / Signatory for the generation of electronic signatures, so that cryptographic operations are carried out within the device and its control is guaranteed only by the Subject / Signatory.*
Digital signature	*The result of the transformation of a message, or any type of data, by the application of the private key in conjunction with known algorithms, thus guaranteeing:* *a) that the data have not been modified (integrity)* *b) that the person signing the data is who they claim to be (identification)*

	c) that the person who signs the data cannot deny having done so (not repudiation at source)
OID	*Unique numeric identifier registered under ISO standardization and referred to a given object or object class.*
Key pair	*Set formed by the public and private key, both related to each other mathematically.*
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 with a special power of attorney to carry out certain procedures in the name and representation of the entity.*
Subscriber	*In the context of this document the legal entity that owns the certificate (at the corporate level)*
Subject/Signatory	*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 Party	*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 Deposit of certificates

esFIRMA has a Certificate Repository, in which the information related to the certification services is published:

https://www.esfirma.com

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

2.2 Publication of certification information

esFIRMA publishes the following information, in its Deposit:

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

2.3 Frequency of publication

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

Changes to the Statement of Certification Practices are governed by section 1.5 of this document.

Certificate revocation status information is published in accordance with sections 4.9.7 and 4.9.8 of this Statement of Certification Practices.

2.4 Access control

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

esFIRMA uses reliable systems for the Deposit, so that:

- Only authorized persons may make annotations and modifications.
- The authenticity of the information can be verified.
- Any technical changes affecting security requirements can be detected.

3. Identification and authentication

3.1 Initial registration

3.1.1 Types of names

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

The names contained in the certificates are as follows.

3.1.1.1 Certificate of signature of public employee, high level, on card

Country (C)	"IS"
Organization (O)	Name ("official" name) of the Administration, body, entity under public law or other entity subscribing to the certificate, to which the employee is linked
organizationalUnitName (OU)	ELECTRONIC CERTIFICATE OF PUBLIC EMPLOYEE
organizationIdentifier	Organization identifier according to ETSI technical standard EN 319 412-1
Surname	First and second (optional) surname, according to identity document (ID / Passport)
Given Name	First name, according to identity document (DNI/Passport)
Serial Number	EMPLOYEE DNI/NIE
Common Name (CN)	Name Surname1 Surname2 – EMPLOYEE NIF
OID certificate type : 2.16.724.1.3.5.7.1.1	QUALIFIED CERTIFICATE OF SIGNATURE OF HIGH LEVEL PUBLIC EMPLOYEE
Name of the OID subscribing entity: 2.16.724.1.3.5.7.1.2	Name of the subscriber entity
NIF OID subscriber entity : 2.16.724.1.3.5.7.1.3	NIF subscription entity
DNI/NIE of the OID manager: 2.16.724.1.3.5.7.1.4	DNI or NIE of the person in charge

OID given name : 2.16.724.1.3.5.7.1.6	First name of the person responsible for the certificate
First surname OID: 2.16.724.1.3.5.7.1.7	First surname of the person responsible for the certificate
Second surname OID: 2.16.724.1.3.5.7.1.8	Second surname of the person responsible for the certificate. Optional.
Email OID: 2.16.724.1.3.5.7.1.9	Email of the person responsible for the certificate. Optional.

3.1.1.2 Certificate of signature of public employee, medium level, in HSM

Country (C)	"IS"
Organization (O)	Name ("official" name) of the Administration, body or entity of public law subscribing to the certificate, to which the employee is linked
organizationalUnitName (OU)	ELECTRONIC CERTIFICATE OF PUBLIC EMPLOYEE
organizationIdentifier	Organization identifier according to ETSI technical standard EN 319 412-1
Surname	First and second (optional) surname, according to identity document (ID / Passport)
Given Name	First name, according to identity document (DNI/Passport)
Serial Number	EMPLOYEE DNI/NIE
Common Name (CN)	Name Surname1 Surname2 – EMPLOYEE NIF
OID certificate type : 2.16.724.1.3.5.7.2.1	ELECTRONIC CERTIFICATE OF PUBLIC EMPLOYEE OF MEDIUM LEVEL
Name of the OID subscribing entity : 2.16.724.1.3.5.7.2.2	Name of the subscriber entity
NIF oid subscriber entity : 2.16.724.1.3.5.7.2.3	NIF subscriber entity
DNI/NIE of the OID manager: 2.16.724.1.3.5.7.2.4	DNI or NIE of the person in charge
OID Personal Authentication Number : 2.16.724.1.3.5.7.2.5	NRP or PIN of the person responsible for the subscriber of the certificate
OID given name : 2.16.724.1.3.5.7.2.6	First name of the person responsible for the certificate

First surname OID: 2.16.724.1.3.5.7.2.7	First surname of the person responsible for the certificate
Second surname OID: 2.16.724.1.3.5.7.2.8	Second surname of the person responsible for the certificate. Optional.
Email OID: 2.16.724.1.3.5.7.2.9	Email of the person responsible for the certificate. Optional.

3.1.1.3 Certificate of authentication of public employee, high level, on card

Country (C)	"IS"
Organization (O)	Name ("official" name) of the Administration, body, entity under public law or other entity subscribing to the certificate, to which the employee is linked
organizationalUnitName (OU)	ELECTRONIC CERTIFICATE OF PUBLIC EMPLOYEE
organizationIdentifier	Organization identifier according to ETSI technical standard EN 319 412-1
Surname	First and second (optional) surname, according to identity document (ID / Passport)
Given Name	First name, according to identity document (DNI/Passport)
Serial Number	EMPLOYEE DNI/NIE
Common Name (CN)	Name Surname1 Surname2 – EMPLOYEE NIF
OID certificate type : 2.16.724.1.3.5.7.1.1	ELECTRONIC CERTIFICATE OF PUBLIC EMPLOYEE OF HIGH LEVEL OF AUTHENTICATION
Name of the OID subscribing entity: 2.16.724.1.3.5.7.1.2	Name of the subscriber entity
NIF OID subscriber entity : 2.16.724.1.3.5.7.1.3	NIF subscription entity
DNI/NIE of the OID manager: 2.16.724.1.3.5.7.1.4	DNI or NIE of the person in charge
OID given name : 2.16.724.1.3.5.7.1.6	First name of the person responsible for the certificate
First surname OID: 2.16.724.1.3.5.7.1.7	First surname of the person responsible for the certificate
Second surname OID: 2.16.724.1.3.5.7.1.8	Second surname of the person responsible for the certificate. Optional.

Email OID: 2.16.724.1.3.5.7.1.9	Email of the person responsible for the certificate. Optional.

3.1.1.4 Organ seal certificate, medium level, in software

Country (C)	"IS"
Organization (O)	Name ("official" name of the organization) of the subscriber
organizationalUnitName (OU)	ELECTRONIC SEAL
organizationIdentifier	Organization identifier according to ETSI technical standard EN 319 412-1
Serial Number	DNI/NIE of the subscribing organization
Common Name (CN)	System name or automatic process application.
OID certificate type : 2.16.724.1.3.5.6.2.1	MEDIUM LEVEL ELECTRONIC SEAL
Name of the OID subscribing entity : 2.16.724.1.3.5.6.2.2	Name of the subscriber entity
NIF oid subscriber entity : 2.16.724.1.3.5.6.2.3	NIF subscriber entity
OID system name : 2.16.724.1.3.5.6.2.5	System name
OID Email : 2.16.724.1.3.5.6.2.9	Email of the stamp manager

3.1.1.5 Organ seal certificate, medium level, in HSM

Country (C)	"IS"
Organization (O)	Name ("official" name of the organization) of the subscriber
organizationalUnitName (OU)	ELECTRONIC SEAL
organizationIdentifier	Organization identifier according to ETSI technical standard EN 319 412-1
Serial Number	DNI/NIE of the subscribing organization
Common Name (CN)	System name or automatic process application.
OID certificate type : 2.16.724.1.3.5.6.2.1	MEDIUM LEVEL ELECTRONIC SEAL

Name of the OID subscribing entity : 2.16.724.1.3.5.6.2.2	Name of the subscriber entity
NIF oid subscriber entity : 2.16.724.1.3.5.6.2.3	NIF subscriber entity
OID system name : 2.16.724.1.3.5.6.2.5	System name

3.1.1.6 Certificate of signature of public employee with pseudonym, high level, on card

Country (C)	"IS"
Organization (O)	Name ("official" name) of the Administration, body or entity of public law subscribing to the certificate, to which the employee is linked
organizationalUnitName (OU)	ELECTRONIC CERTIFICATE OF PUBLIC EMPLOYEE WITH PSEUDONYM
organizationIdentifier	Organization identifier according to ETSI technical standard EN 319 412-1
Pseudonym	Mandatory pseudonym according to ETSI EN 319 412-2 for this type of certificates
Common Name (CN)	Pseudonym and the Agency
OID certificate type : 2.16.724.1.3.5.4.1.1	ELECTRONIC CERTIFICATE OF PUBLIC EMPLOYEE WITH HIGH LEVEL PSEUDONYM
Name of the OID subscribing entity : 2.16.724.1.3.5.4.1.2	Name of the subscriber entity
NIF oid subscriber entity : 2.16.724.1.3.5.4.1.3	NIF subscriber 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 Certificate of signature of public employee with pseudonym, medium level, in HSM

Country (C)	"IS"
Organization (O)	Name ("official" name) of the Administration, body or entity of public law subscribing to the certificate, to which the employee is linked

organizationalUnitName (OU)	ELECTRONIC CERTIFICATE OF PUBLIC EMPLOYEE WITH PSEUDONYM
organizationIdentifier	Organization identifier according to ETSI technical standard EN 319 412-1
Pseudonym	Mandatory pseudonym according to ETSI EN 319 412-2 for this type of certificates
Common Name (CN)	Pseudonym and the Agency
OID certificate type : 2.16.724.1.3.5.4.2.1	ELECTRONIC CERTIFICATE OF PUBLIC EMPLOYEE WITH PSEUDONYM OF MEDIUM LEVEL
Name of the OID subscribing entity : 2.16.724.1.3.5.4.2.2	Name of the subscriber entity
NIF oid subscriber entity : 2.16.724.1.3.5.4.2.3	NIF subscriber entity
OID Pseudonym: 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)	"IS"
Organization (O)	Name ("official" name) of the Administration, body, entity under public law or other entity subscribing to the certificate, to which the employee is linked
organizationalUnitName (OU)	ELECTRONIC CERTIFICATE OF PUBLIC EMPLOYEE
organizationIdentifier	Organization identifier according to ETSI technical standard EN 319 412-1
pseudonym	Mandatory Pseudonym according to ETSI EN 319 412-2
Common Name (CN)	Position or position or "PSEUDONYM" – IDENTIFICATION NUMBER - OFFICIAL NAME OF THE ORGANISM
OID certificate type : 2.16.724.1.3.5.4.1.1	CERTIFICATE OF AUTHENTICATION OF PUBLIC EMPLOYEE WITH PSEUDONYM
Name of the OID subscribing entity : 2.16.724.1.3.5.4.1.2	Name of the subscriber entity
NIF oid subscriber entity : 2.16.724.1.3.5.4.1.3	NIF subscriber entity

3.1.1.9 TSA/TSU Electronic Seal Certificate

Country (C)	"IS"
Organization (O)	Name ("official" name of the organization) of the subscriber
organizationalUnitName (OU)	ESFIRMA CERTIFICATION AUTHORITY
Serial Number	DNI/NIE of the subscribing organization
organizationIdentifier	Organization identifier according to ETSI technical standard EN 319 412-1
Common Name (CN)	Name of the TSU

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

Country (C)	"IS"
Organization (O)	Name ("official" name) of the entity subscribing to the certificate, to which the employee is linked
organizationIdentifier	Organization identifier according to ETSI technical standard EN 319 412-1
Surname	First and second (optional) surname, according to identity document (ID / Passport)
Given Name	First name, according to identity document (DNI/Passport)
Serial Number	DNI/NIE of the natural person
Common Name (CN)	Surname1 Surname2 Name – NIF natural person (SIGNATURE)

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

Country (C)	"IS"
Organization (O)	Name ("official" name) of the subscriber entity, to which the employee is linked
organizationIdentifier	Organization identifier according to ETSI technical standard EN 319 412-1
Surname	First and second (optional) surname, according to identity document (ID / Passport)
Given Name	First name, according to identity document (DNI/Passport)
Serial Number	EMPLOYEE DNI/NIE
Common Name (CN)	Surname1 Surname2 Name – NIF natural person

3.1.1.12 Certificate of authentication of a related natural person, on card

Country (C)	"IS"
Organization (O)	Name ("official" name) of the entity subscribing to the certificate, to which the employee is linked
organizationIdentifier	Organization identifier according to ETSI technical standard EN 319 412-1
Surname	First and second (optional) surname, according to identity document (ID / Passport)
Given Name	First name, according to identity document (DNI/Passport)
Serial Number	EMPLOYEE DNI/NIE
Common Name (CN)	Surname1 Surname2 Name – NIF natural person (AUTHENTICATION)

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

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

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

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

3.1.1.15 Certificate of authentication of a related natural person, on a card, with a pseudonym

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

3.1.1.16 Electronic seal certificate, in software

Country (C)	"IS"
Organization (O)	Name ("official" name of the organization) of the subscriber
organizationalUnitName (OU)	ELECTRONIC SEAL
organizationIdentifier	Organization identifier according to ETSI technical standard EN 319 412-1
Serial Number	DNI/NIE of the subscribing organization
Common Name (CN)	System name or automatic process application.

3.1.1.17 Electronic seal certificate with centralised management

Country (C)	"IS"
Organization (O)	Name ("official" name of the organization) of the subscriber
organizationalUnitName (OU)	ELECTRONIC SEAL
organizationIdentifier	Organization identifier according to ETSI technical standard EN 319 412-1
Serial Number	DNI/NIE of the subscribing organization
Common Name (CN)	System name or automatic process application.

3.1.2. Meaning of names

The names contained in the *SubjectName* and *SubjectAlternativeName* fields of the certificates are understandable in natural language, as set out in the previous section.

3.1.3 Use of anonymous and pseudonyms

In no case can pseudonyms be used to identify an entity/company/organization, and in no case are anonymous certificates issued, except that, for reasons of public security, electronic signature systems may refer only to the professional identification number of the public employee.

3.1.4 Interpretation of name formats

Name formats shall be interpreted in accordance with the law of the subscriber's country of establishment, on their own terms.

The field "country" will always be Spain because it is the certificates issued exclusively to the Spanish Public Administrations.

The certificate shows the relationship between a natural person and the Administration, body, 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 a subscriber, and the natural person linked to the person authorized to use it.

In certificates issued to Spanish subscribers, the "serial number" field must include the NIF of the signatory, for the purpose of admitting the certificate for the completion of procedures with the Spanish Administrations.

3.1.5 Uniqueness of names

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

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

A subscriber can request more than one certificate as long as the combination of the following values in the request was different from a valid certificate:

- Tax Identification Number (NIF) or other legally valid identifier of the natural person.
- Tax Identification Number (NIF) or other legally valid identifier of the subscriber.
- Certificate Type (Certificate description field).

3.1.6 Resolution of disputes concerning names

Certificate applicants shall not include names in applications that may infringe the rights of third parties by the prospective subscriber.

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 in principle will proceed to certify it.

You will not act as an arbitrator or mediator, or otherwise resolve any dispute concerning the ownership of names of persons or organizations, domain names, trademarks or trade names.

However, if you receive a conflict of name notification, in accordance with the law of the subscriber's country, you may take appropriate action to block or withdraw the issued certificate.

In any case, the certification service provider reserves the right to reject a certificate application due to a conflict of names.

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

3.2 Initial identity validation

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

The identity of the natural persons identified in the certificates is validated through the corporate records of the Administration, body, public law entity or other entity subscribing to the certificates. The subscriber will produce a certification of the necessary data, and will send it to esFIRMA, by 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 Responsible for the designated certification service.

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

To avoid any conflict of interest, the Public Administrations or other subscribing entities are independent entities of the Trust 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 of delivery and acceptance of the certificate by the signatory from the Electronic Administration Platform, when signing the acceptance sheet, and its use on said platform.

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

3.2.2 Identification of the entity

Certificates of public employee, pseudonymous public employee, organ seal

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

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

Natural persons with the capacity to act on behalf of an Administration, body, 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 previous situation of legal or voluntary representation between the natural person and the Administration, body, entity of public law or other entity subscribing to the certificates, which requires their recognition by esFIRMA, which will be carried out through the following procedure:

1. A certificate of secretariat of the agreement of the plenary in which the legal representative is appointed, with the following data:
    a. as a representative:
        i. Name and surname
        ii. Document: NIF of the representative
    b. The identification data of the subscriber it represents:
        i. Name of the Administration, body, entity under public law or other entity.
        ii. Information on the extent and validity of the applicant's powers of representation.
        iii. Document: NIF of Administration, organism, entity of public law or other entity.
        iv. Document: Documents that serve to prove the aforementioned points in a reliable manner in accordance with what is indicated in

the regulations of administrative law that are applicable, and their registration in the corresponding public registry if so required.

c. The data relating to the representation or the capacity to act that it holds:
    i. The validity of the representation or the capacity to act (start and end date).
    ii. The scope and limits, if any, of representation or capacity to act:
        1. TOTAL. Representation or total capacity.
        2. PARTIAL. Representation or partial capacity.

2. A contract for the provision of certification services signed by esFIRMA (ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA) and the legal representative of the Administration, which includes:
3. A Protocol to be signed by each authorized operator (including its obligations).

Once the documents have been signed electronically, the AR functions will be activated to the users of the City Council that appear in the contract as authorized operators to perform this function.

Certificates of natural person linked to entity or electronic seal

The issuance of certificates of natural person linked to entity requires the prior verification of the identity of the subscriber through the relevant documentation that esFIRMA requires depending on the type of entity.

3.2.3 Authentication of the identity of a natural person

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

Certificates of public employee and public employee with pseudonym

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

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

1. User request through the Electronic Administration Platform (with its corresponding check-in and file opening)
2. a certificate in which the Validation Operator certifies that this person is linked to the Administration.
3. Petition signed by the operator authorized by the entity (or by the legal representative), who registers for departure and notifies ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (attaching a copy of the certificate and the employee's request).

Certificates of related natural person and certificates of electronic seal

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

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 of the person linked to the entity through the Electronic Administration Platform (with its corresponding registration of entry and opening of the file).
2. A report of the verification operator designated by the Legal Representative, which states the face-to-face and univocal identification of the signatory, as well as the link of the signatory with the entity.
3. Issuance order signed by the verification and authorization operator of the entity designated by the Legal Representative, which is registered as an exit and notified to ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (attaching a copy of the certificate and the employee's request).

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

1. Request of the Legal Representative of the legal entity or entity or other authorized person through the Electronic Administration Platform (with its corresponding registration of entry and opening of the file). To submit such an application, the person must identify themselves on the platform using means of electronic identification, for which the presence of the natural person has been

guaranteed in accordance with Article 8 of the eIDAS Regulation in relation to the "substantial" or "high" security levels.

2. In case of application submitted by authorized, the corresponding authorization document of the Legal Representative.
3. Issuance order signed by the Legal Representative or verification and authorization operator of the entity designated by him, which is registered as an exit and is notified to ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (attaching a copy of the certificate and the employee's application).

3.2.3.1 On certificates

The identification information of the natural persons identified in the certificates is validated by comparing the information of the application of the Administration, body, public law entity or other entity subscribing to the certificates, with the records of the Administration, body, 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

Certificates of public employee and public employee with pseudonym

For the application of the certificates, the direct physical presence is not required due to the already accredited relationship between the natural person and the Administration, body, entity of public law or other entity to which it is linked, and because this request is made by an operator authorized by the subscriber in the contract.

Nor is the direct physical presence of the signatory necessary to accept the certificate since it can be done by advanced electronic signature.
During this procedure, the identity of the natural person identified in the certificate is confirmed.

Certificates of natural person linked to entity

For the application of the certificates of Natural Person linked to entity, the Legal Representative of the entity or the verification operator designated by him will record the face-to-face and unequivocal identification of the signatory.

3.2.3.3 Attachment of the natural person

The documentary justification of the link of a natural person identified in a certificate with the Administration, organism, entity of public law or other entity is given by its constancy in the Personnel Registers of the Administration, organism, entity of public law 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 subordinate CA certificates to third parties and its issuing CA is not technically limited.

3.3 Identification and authentication of renewal applications

3.3.1 Validation for routine renewal of certificates

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

3.3.2 Renewal identification and authentication after revocation

esFIRMA does not perform certificate renewals.

3.4 Identification and authentication of the revocation request

EsFIRMA authentic requests and reports relating to the revocation of a certificate, verifying that they come from an authorized person.

The acceptable methods for such verification are as follows:

- The sending of a revocation request by the subscriber or the natural person identified in the certificate, electronically signed.
- The use of the "identity verification phrase", or other methods of personal authentication, which consists of information known only to the natural person identified in the certificate, and which allows him to automatically revoke his certificate.
- The natural personation in an office of the subscriber entity.
- Other means of communication, such as the telephone, when there are reasonable guarantees of the identity of the applicant for revocation, in the opinion of esFIRMA.

esFIRMA does not perform certificate suspensions. Requests for suspension are treated as requests for revocation.

4. Certificate Lifecycle Operation Requirements

4.1 Certificate application

4.1.1 Legitimation to request the issuance

The Administration, body, entity of public law or other entity must sign a contract for the provision of certification services with esFIRMA.

Also, prior to the issuance and delivery of a certificate, there is a request for certificates on a certificate application sheet through the Electronic Administration Platform.

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

4.1.2 Registration procedure and responsibilities

esFIRMA receives requests for certificates, made by Administrations, bodies, public law entities or other entities.

The applications are implemented by means of a document in electronic format, completed by the Administration, body, entity of public law or other entity, whose addressee is ESFIRMA, which will include the data of the persons to whom certificates will be issued. The request will be made by the operator authorized by the subscriber (responsible for certification) and who has been identified in the contract between this subscriber and esFIRMA.

The application must be accompanied by documentation supporting 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 information, must also be accompanied to contact the natural person identified in the certificate.

4.2 Processing of the certification application

4.2.1 Execution of identification and authentication functions

Once a certificate request is received, esFIRMA ensures that certificate applications are complete, accurate and duly authorized, before processing them.

If yes, esFIRMA verifies the information provided, verifying that the requirements described in section 3.2 have been correctly met.

The documentation justifying the approval of the application must be kept and duly registered and with guarantees of security and integrity during the period of 15 years from the extinction of the certificate or the completion of the service provided, even in case of anticipated loss of validity by 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 application

esFIRMA approves the request for the certificate 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 that it may affect the reputation of the Certification Body or the subscribers, esFIRMA will deny the request, or stop its approval until it has carried out the complementary checks it deems appropriate.

In the event that the additional checks do not result in the correction of the information to be verified, esFIRMA will definitively deny the request.

esFIRMA notifies the applicant of the approval or refusal of the application.

esFIRMA will be able to automate the procedures of verification of the correctness of the information that will be contained in the certificates, and of approval of the applications.

4.2.3 Deadline for resolving the request

esFIRMA attends to requests for certificates on a first-come, first-served basis, within a reasonable time, and a guarantee of maximum term may be specified in the certificate issuance contract.

Requests remain active until approved or rejected.

4.3 Issuance of the certificate

4.3.1 CA shares during the issuance process

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

During the process, esFIRMA:

- It protects the confidentiality and integrity of the registration data it has.
- It 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.
- Generates the key pair, using a certificate generation procedure securely linked to the key generation procedure.
- It employs a certificate generation procedure that securely links the certificate to registration information, including the certified public key.
- It ensures that the certificate is issued by systems that use counterfeit protection and that guarantee the confidentiality of the keys during the process of generating those keys.
- It includes in the certificate the information set out in Annex 1 to Regulation (EU) 910/2014, in accordance with sections 3.1.1 and 7.1.
- Indicates the date and time a certificate was issued.

4.3.2 Notification of the broadcast to the subscriber

esFIRMA notifies the issuance of the certificate to the Administration, body, public law entity or other entity subscribing to 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 Delivery and acceptance of the certificate

During this process, esFIRMA must perform the following actions:

- Definitively accredit the identity of the natural person identified in the certificate, with the collaboration of the Administration, body, 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 delivery and acceptance sheet of the certificate to the natural person identified in it, which has the following minimum contents:
    - Basic information about the use of the certificate, including in particular information about the certification service provider and the

applicable Statement of Certification Practices, such as its obligations, powers and responsibilities
    - Information about the certificate.
    - Recognition, by the signatory, of receiving the certificate and acceptance of the aforementioned elements.
    - Regime of obligations of the signatory.
    - Responsibility of the signatory.
    - Method of exclusive imputation to the signatory, of his private key and of his activation data of the certificate, in accordance with the provisions of sections 6.2 and 6.4.
    - The date of the act of delivery and acceptance.
- Obtain the signature, written or electronic, of the person identified in the certificate.

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

4.4.1 Conduct constituting acceptance of the certificate

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

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

In certificates issued on a card, these are sent to the subscriber's certification manager, and the corresponding PINs are directly to the signatory's postal address.

In addition, the acceptance of the certificate by the natural person identified in the certificate occurs by signing the delivery and acceptance sheet, through the Electronic Administration Platform.

4.4.2 Publication of the certificate

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

4.4.3 Notification of the issue to third parties

esFIRMA does not make any notification of the issuance to third parties.

4.5 Using the Key Pair and Certificate

4.5.1 Use by the subscriber or signer

esFIRMA obliges the following:

- Provide esFIRMA with complete and adequate information, in accordance with the requirements of this Declaration of Certification Practices, especially in relation to the acceptance procedure.
- Express your consent prior to the issuance and delivery of a certificate.
- Use the certificate in accordance with section 1.4.
- Where the certificate operates in conjunction with a DCCF, recognise its capacity to produce qualified electronic signatures; that is, equivalent to handwritten signatures, as well as other types of electronic signatures and information encryption mechanisms.
- Be especially diligent in the custody of your private key, in order to avoid unauthorized uses, in accordance with the provisions of sections 6.1, 6.2 and 6.4.
- Communicate to esFIRMA and to any person who believes that they can trust the certificate, without unjustifiable delays:
    - The loss, theft, or potential compromise of your private key.
    - Loss of control over your private key, due to the compromise of activation data (e.g. PIN code) or for any other reason.
    - Inaccuracies or changes in the content of the certificate that the subscriber knows or may know.
- Stop using the private key after the period indicated in section 6.3.2.

- That all the information provided by the signatory that is contained in the certificate is correct.
- That the certificate is used exclusively for legal and authorized uses, in accordance with the Statement of Certification Practices.
- That no unauthorized person has ever had access to the private key of the certificate, and that he is solely responsible for the damages caused by his breach of the duty to protect the private key.
- That the signatory is a final entity and not a certification service provider, and that it will not use the private key corresponding to the public key listed in the certificate to sign any certificate (or any other certified public key format), nor Certificate Revocation List, nor title of certification service provider or in any other case.

4.5.2 Use by the Subscriber

esFIRMA contractually obliges the subscriber to:

- Provide the Certification Body with complete and adequate information, in accordance with the requirements of this Statement of Certification Practices, especially with regard to the acceptance procedure.
- Express your consent prior to the issuance and delivery of a certificate.
- Use the certificate in accordance with section 1.4.
- Communicate to esFIRMA and to any person that the subscriber believes can trust the certificate, without unjustifiable delays:
    - The loss, theft, or potential compromise of your private key.
    - Loss of control over your private key, due to the compromise of activation data (e.g. PIN code) or for any other reason.
    - Inaccuracies or changes in the content of the certificate that the subscriber knows or may know.
    - The loss, alteration, unauthorized use, theft or compromise, where any, of the card.
- Transfer to the natural persons identified in the certificate the fulfillment of the specific obligations of the same, and establish mechanisms to guarantee the effective fulfillment of the same.

- Not to monitor, manipulate or perform acts of reverse engineering on the technical implementation of esFIRMA's certification services, without prior written permission.
- Not to 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 that is contained in the certificate is correct.
- That the certificate is used exclusively for legal and authorized uses, in accordance with the Statement of Certification Practices.
- That no unauthorized person has ever had access to the private key of the certificate, and that he is solely responsible for the damages caused by his breach of the duty to protect the private key.
- That the subscriber is a final entity and not a certification service provider, and that it will not use the private key corresponding to the public key listed in the certificate to sign any certificate (or any other certified public key format), nor Certificate Revocation List, nor title of certification service provider or in any other case.

esFIRMA informs the third party that trusts in certificates that it must assume the following obligations:

- Advise independently on the fact that the certificate is appropriate for the intended use.
- Verify the validity, suspension or revocation of the certificates issued, 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 verified electronic signatures produced on a qualified signature creation device (DCCF) are legally considered 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.
- Keep in mind any limitations on the use of the certificate, regardless of whether it is in the certificate itself or in the contract of the third party that trusts the certificate.

- Keep in mind any precautions set out in a contract or other instrument, regardless of their legal nature.
- Not to monitor, manipulate or perform acts of reverse engineering on the technical implementation of esFIRMA's certification services, without prior written permission.
- Not to compromise the security of esFIRMA's certification services, without prior written permission.

esFIRMA informs the third party that trusts in certificates that it must assume the following responsibilities:

- That you have enough information to make an informed decision in order to trust the certificate or not.
- That you are solely responsible for trusting or not in the information contained in the certificate.
- That you will be solely responsible if you fail to comply with your obligations as a third party that relies on the certificate.

4.6. Renewal of certificates

esFIRMA does not renew certificates. esFirma will issue a new certificate, following the application procedure registered in the Electronic Administration Platform.

4.6.1 Circumstances for the renewal of the certificate

Not applicable.

4.6.2 Who can request a renewal

Not applicable.

4.6.3 Processing of the certificate renewal application

Not applicable.

4.6.4 Notification of new certificate issuance to subscriber

Not applicable.

4.6.5 Conduct constituting acceptance of a certificate of renewal

Not applicable.

4.6.6 Publication of the certificate of renewal by the CA

Not applicable.

4.6.7 Notification of the issuance of the certificate by the CA to other entities

Not applicable.

4.7 Renewal of keys and certificates

4.7.1 Who can request the certificate of a new public key

Not applicable.

4.7.2 Procedure with new identification

Not applicable.

4.7.3 Processing New Certificate Key Requests

esFIRMA will warn the subscriber of the need to proceed with a new personation of the signatory and signature of the acceptance sheet, in those cases in which it is necessary for the legal identification period of 5 years.

Such personation and identification shall be carried out in accordance with paragraph 3.2.

The signature of the acceptance sheet shall be made in accordance with paragraph 4.4.2.

4.7.4 Notification of the issuance of the renewed certificate

It does not apply because there are no renewals.

4.7.5 Conduct constituting acceptance of the certificate

Not applicable.

4.7.6 Publication of the certificate

Not applicable.

4.7.7 Notification of the issue to third parties

esFIRMA does not make any notification of the issuance to third parties.

4.8 Modification of certificates

The modification of certificates shall be treated as a new certificate issue, applying as described in sections 4.1, 4.2, 4.3 and 4.4.

4.9 Revocation and suspension of certificates

4.9.1 Causes of revocation of certificates

esFIRMA will extinguish the validity of the electronic certificates by revocation when any of the following causes concur:

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) Violation, by esFIRMA, of the requirements foreseen in the certificate management procedures, established in this Declaration of Certification Practices.
c) Commitment or suspicion of compromise of the security of the key or certificate issued.
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 caused the issuance of the certificate to the natural person identified in the certificate.
   c) Infringement by the applicant of the certificate of the pre-established requirements for the application of the same.
   d) Infringement by the subscriber or by the person identified in the certificate, of their obligations, responsibility and guarantees, established in the corresponding legal document.
   e) The supervening disability or death of the key holder.
   f) The extinction of the legal entity subscribing to the certificate, as well as the end of the authorization of the subscriber to the holder of keys or the termination of the relationship between subscriber and person identified in the certificate.
   g) Subscriber's request for revocation of the certificate, in accordance with section 3.4.

4) Other circumstances:

a) The termination of esFIRMA's certification service, in accordance with the provisions of section 5.8.

b) The use of the certificate that is harmful and continued for esFIRMA. In this case, a use is considered harmful based on the following criteria:
   - The nature and number of complaints received.
   - The identity of the entities submitting the complaints.
   - The relevant legislation in force at all times.
   - The response of the subscriber or the person identified in the certificate to the complaints received.

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

They can request the revocation of a certificate:

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

4.9.3 Revocation request procedures

The request for revocation shall include the following information:

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

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

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

The revocation service is located on the Electronic Administration Platform, in which the signatory and the subscriber manage their certificates.

[2] Ap 6.2.4(a) iii) of ETSI EN 319 411-1

In the event that the recipient of a request for revocation by a natural person identified in the certificate was the subscriber entity once the request was authenticated, it must send a request in this regard to esFIRMA.

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.

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

4.9.4 Temporary deadline for requesting revocation

Requests for revocation will be sent immediately as soon as the cause of revocation is known, and will not exceed 24 hours[3].

4.9.5 Time period for processing the application

The revocation will occur immediately when it is received, within the ordinary hours of operation of esFIRMA, and will not exceed 60 minutes[4].

4.9.6 Obligation to consult information on the revocation of certificates by third parties

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

One method by which the status of certificates can be verified is by consulting the most recent Certificate Revocation List issued by the esFIRMA Certification Authority.

---

3 Ap 6.2.4(a) (vi) of ETSI EN 319 411-1

4 Ap 6.2.4(a) (vii) of ETSI EN 319 411-1

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

- *ROOT CA:*
  - 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 shall 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 of issuance of a new CRL, although a CRL may be issued before the deadline indicated in the previous CRL, to reflect revocations.

The CRL must keep the certificate revoked or suspended until it expires.

4.9.8 Maximum term of publication of CRLs

CRLs are published in the Deposit 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 the certificates, through the OCSP protocol, which allows to know the validity status of the certificates online from the addresses:

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

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

In case of failure of the certificate status checking 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 that trust certificates about the operation of the Certificate Status Information service.

Certificate health check 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 the 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 the revocation of a subordinate CA Certificate.

5 Ap 6.3.10 of ETSI EN 319 411-2

6 Ap 6.3.10(b) of ETSI EN 319 411-2

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

4.9.11 Other forms of certificate revocation information

Alternatively, third parties that trust certificates will be able to verify the revocation status of certificates by consulting the most recent CRLs issued by esFIRMA. These are published on the esFIRMA website, as well as on the web addresses indicated in the certificates.

esFIRMA does not delegate its OCSP responses using OCSP stapling.

4.9.12 Special requirements in case of private key compromise

The commitment 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 media, including on paper.

4.9.13 Causes of 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 the request for suspension

esFIRMA does not perform certificate suspension.

4.9.16 Maximum period of suspension

esFIRMA does not perform certificate suspension.

4.10 Certificate Health Check Services

4.10.1 Operational characteristics of the services

Certificate health check services are provided through a web query interface, on the web 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 deleted.

4.10.2 Availability of services

Certificate health check services are available 24 hours a day, 7 days a week, throughout the year, with the exception of scheduled stops.

Certificate health check services are free to use.

4.10.3 Optional Features

Not applicable.

4.11 Termination of subscription

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

4.12 Deposit and recovery of keys

4.12.1 Key Deposit and Recovery Policy and Practices

esFIRMA does not provide key deposit and recovery services.

4.12.2 Session Key Encapsulation and Retrieval Policy and Practices

No stipulation.

5. Physical, management and operations 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 are located, the systems themselves and the equipment used for the registration and approval of applications, technical generation of certificates and the management of cryptographic hardware.

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

- Physical access controls.
- Protection against natural disasters.
- Fire protection measures.
- Failure of support systems (electronic energy, telecommunications, etc.)
- Collapse of the structure.
- Floods.
- Anti-theft protection.
- Unauthorized exit 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, from operation to contingency, which are duly audited periodically.

The facilities have preventive and corrective maintenance systems with assistance 24h-365 days a year with assistance within 24 hours of the notice.

5.1.1 Location and construction of facilities

Physical protection is achieved by creating clearly defined security perimeters around services. The quality and robustness of the construction materials of the facilities guarantees adequate levels of protection against intrusions by brute force and located in an area of low risk of disasters and allows quick access.

The room where cryptographic operations are performed 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 the services of approval of certificate requests and revocation management, of the commitment caused by unauthorized access to the systems or data, as well as the disclosure of the same

5.1.2 Physical access

The CPD where the CA of esFIRMA is located has the TIER IV qualification.

Physical access to esFIRMA units where certification processes are carried out is limited and protected by a combination of physical and procedural measures. Like this:

- It is limited to expressly authorized personnel, with identification at the time of access and registration of the same, including CCTV filming and its archive.

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

- For access to the rac where the cryptographic processes are located, it is necessary the prior authorization of esFIRMA to the administrators of the hosting service who have the key to open the cage.

5.1.3 Electricity and air conditioning

EsFIRMA's facilities have current stabilizing equipment and a duplicate equipment power supply system with a generator set.

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 an area of low flood risk.

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

5.1.5 Fire prevention and protection

EsFIRMA's facilities and assets have automatic fire detection and extinguishing systems.

5.1.6 Media storage

Only authorized personnel have access to storage media.

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

5.1.7 Waste treatment

The elimination of supports, both paper and magnetic, are carried out through mechanisms that guarantee the impossibility of retrieving the information.

In the case of magnetic media, we proceed to formatting, permanent deletion, or physical destruction of the support, using specialized software that performs a minimum of 3 erasure passes and with variable erasure patterns.

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

5.1.8 Off-premises backup

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

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

5.2 Procedural controls

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

The staff at the service of esFIRMA executes the 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 with the status of reliable:

- **Internal Auditor:** Responsible for compliance with operating procedures. This is an external person to the Information Systems department. The tasks of Internal Auditor are incompatible in time with the tasks of Certification and incompatible with Systems. These functions will be subordinate to the head of operations, reporting both to it and to the technical management.
- **Systems Administrator**: Responsible for the correct functioning of the hardware and software support of the certification platform
- **CA Administrator**: Responsible for the actions to be executed with the cryptographic material, or with the performance of any function that implies 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 activation material of the cryptographic keys, also responsible for the backup and maintenance operations of the CA.

- **Registry Operator:** Person responsible for approving certification requests made by the subscriber.
- **Security Manager**: Responsible for coordinating, controlling and enforcing the security measures defined by esFIRMA's security policies. It must take care of the aspects related to information security: logical, physical, networks, organizational, etc.
- **Responsible for Information and Service**: Defines the requirements of 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 the validation of certificate requests.
- **Revocation Officer:** Responsible for the operation of changing the status of the certificates.

Persons occupying the above posts 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 manipulation of the custody device of the keys of the root Certification Authority.

5.2.3 Identification and authentication for each function

The people 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 needed for their role, thus ensuring that no person accesses unallocated resources.

Access to resources is done depending on the asset using cryptographic cards and activation codes.

5.2.4 Roles that require separation of tasks

The following tasks are performed by at least two people:

- Issuance and revocation of certificates, and access to the deposit.
- Generation, issuance and destruction of certificates of the Certification Authority.
- Production of the Certification Body.

5.2.5 PKI Management System

The PKI system consists of the following modules:

- Component/management module of the Subordinate Certification Authority.
- Component/management module of the Registration Authority.
- Component/module of request management.
- Key management component/module (HSM).
- Database component/module.
- CRL management component/module.
- OcSP service management component/module.
- Time Stamping Authority (TSA) management component/module

5.3 Personnel controls

5.3.1 History, qualification, experience and authorisation requirements

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

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

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

esFIRMA ensures that the registration staff is reliable to perform the registration tasks.

The Registry Operator has completed a preparation course for the completion of the tasks of validation of the requests.

In general, esFIRMA will remove an employee from its functions of trust when it becomes aware of the existence of the commission of a criminal act that could affect the performance of their functions.
esFIRMA will not assign to a reliable or management site a person who is not suitable for the position, especially for having been convicted of a crime or misdemeanor that affects their suitability for the position.

5.3.2 History investigation procedures

esFIRMA carries out background checks on potential employees before their hiring or access to the job.

esFIRMA obtains the unequivocal consent of the data subject for such prior investigation, and processes and protects all his 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 shall be repeated sufficiently regularly.

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

- Falsehoods in the job application, made by the candidate.
- Very negative or very unreliable professional references in relation to the candidate.

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

5.3.3 Training requirements

esFIRMA trains staff in reliable and managerial positions in the terms established in the Certification Policies. To this end, 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 formed.
- Tasks that the person must perform.
- esFIRMA security policies and procedures. Use and operation of machinery and installed applications.
- Management and processing of incidents and security commitments.
- Business continuity and emergency procedures.
- Management and security procedure in relation to the processing of personal data.

5.3.4 Requirements and frequency of training updates

esFIRMA updates the training of staff according to needs, and frequently sufficient to perform their duties competently and satisfactorily, especially when substantial modifications are made to the certification tasks

5.3.5 Sequence and frequency of job rotation

Not applicable.

5.3.6 Penalties for unauthorized actions

esFIRMA has a sanctioning system, to debug 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 is applicable to the staff.

Disciplinary actions include the suspension and dismissal of the person responsible for the harmful action, in a manner proportionate to the gravity of the unauthorized action.

5.3.7 Professional recruitment requirements

Employees hired to perform reliable tasks sign in advance the confidentiality clauses and operational requirements used by esFIRMA. Any action that compromises the safety of the 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 forecasts carried out in this section, or in other parts of the DPC, will be applied and fulfilled by the third party that performs the functions of operation of the certification services, however, which, the certification body 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 Provision of documentation to staff

The certification service provider shall provide the documentation strictly required by its staff at all times, in order to carry out its work in a competent and satisfactory manner.

5.4 Security audit procedures

5.4.1 Types of Logged Events

esFIRMA produces and records at least the following events related to the security of the entity:

- Turning the system on and off.
- Attempts to create, delete, set passwords or change privileges.
- Login and end attempts.
- Attempts of unauthorized access to the CA system over the network.
- Attempts of unauthorized access to the file system.

- Physical access to logs.
- Changes in system configuration and maintenance.
- Logs of CA applications.
- Turning the AC app on and off.
- Changes in the details of the CA and/or its keys.
- Changes to certificate policy creation.
- 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 lifecycle of the cryptographic module, such as receiving, using, and uninstalling the cryptographic module.
- The activities of firewalls and routers[7]
- The key generation ceremony and key management databases.
- Physical access logs.
- Maintenance and configuration changes of the system.
- Personnel changes.
- Reports of commitments and discrepancies.
- Records of the destruction of material containing key information, activation data or personal information of the subscriber, in case of individual certificates, or of the natural person identified in the certificate, in case of organizational certificates.
- Possession of activation data, for operations with the private key of the Certification Authority.
- Complete reports of physical intrusion attempts on infrastructures that support the issuance and management of certificates.

Registry entries include the following items:

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

[7] Ap 6.4.5(a) of ETSI EN 319 411-1

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

5.4.2 Frequency of processing of audit logs

esFIRMA reviews its logs when there is a system alert motivated by the existence of an incident.

Audit log processing consists of a review of the records that includes verification that the records have not been tampered with, a brief inspection of all log entries, and a deeper investigation of any alerts or irregularities in the records. The actions taken from the audit review are documented.

esFIRMA maintains a system that allows to guarantee:

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

5.4.3 Retention period of audit logs

esFIRMA stores the information of the logs 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:

[8] Ap 6.4.5(a) of ETSI EN 319 411-2

- They are protected from manipulation, deletion or deletion[9] by signing the files that contain them.
- They are stored in flame retardant devices.
- Its availability is protected by storing it in facilities outside the center where the CA is located.

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

5.4.5 Backup Procedures

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

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

5.4.6 Locating the Audit Log Accumulation System

The information of the event audit is collected internally and in an automated way by the operating system, network communications and certificate management software, in addition to the manually generated data, which will be stored by duly authorized personnel. All this makes up the system of accumulation of audit logs.

5.4.7 Notification of the audit event to the cause of the event

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

[9] Ap 7.10(f) of ETSI EN 319 401

5.4.8 Vulnerability scanning

Vulnerability scanning is covered by esFIRMA's audit processes.

Vulnerability analyses should be executed, reviewed and reviewed through an examination of these monitored developments. These analyses should be run daily, monthly and annually.

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

EsFIRMA's security program includes an annual risk assessment.

5.5. Information files

esFIRMA, guarantees that all information relating to certificates is kept for an appropriate period of time, as set out 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 relating to certificates, including contracts with signatories and data relating to their identification and location
- Requests for issuance and revocation of certificates, including all reports relating to the revocation process[10].
- All those specific choices that the signatory or subscriber has during the subscription agreement[11].
- Type of document presented in the certificate application.

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

[11] Ap 6.4.5(c) (iv) of ETSI EN 319 411-1

- Identity of the Registration Entity accepting the certificate request.
- Unique identification number provided by the above document.
- All certificates issued or published.
- Issued CRLs or status records of generated certificates.
- The history of generated keys.
- Communications between PKI elements.
- Certification Policies and Practices
- All audit data identified in section 5.4
- Certification application information.
- Documentation provided to justify certification applications.
- Certificate lifecycle information.

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

5.5.2 Record keeping 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 gain access to it. The file is protected against viewing, modifying, deleting or any other manipulation by storing it in a reliable system.

esFIRMA ensures the correct protection of files by assigning qualified personnel for their treatment and storage in fireproof safe deposit boxes and external facilities.

5.5.4 Backup Procedures

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

esFIRMA at least performs daily incremental backups of all your electronic documents and perform full backups weekly for data recovery cases.

In addition, esFIRMA (or the organizations that perform the registration function) keeps copies of the paper documents in a safe place different from the facilities of the Certification Authority itself.

5.5.5 Date and time stamping requirements

Records are dated with a reliable source via NTP.

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

This information does not need to be digitally signed.

5.5.6 Locating the File System

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

5.5.7 Procedures for obtaining and verifying file 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 CA expires, a key change will be made. The old CA and its private key will only be used for signing CRLs as long as there are active certificates issued by that CA. A new CA will be generated with a new private key and a new DN.

The change of subscriber keys is done by performing a new issuance process.

12 Ap 7.10(d) of the ETSI EN 319 401

5.7 Key Engagement and Disaster Recovery

5.7.1 Incident and commitment management procedures

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

Backups of esFIRMA's private keys are generated and maintained in accordance with 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 communicated to security, and the appropriate management procedures will be initiated, which contemplate scaling, investigation and response to the incident. If necessary, esFIRMA's key compromise or disaster recovery procedures will be initiated.

5.7.3 Entity Private Key Compromise

In case of suspicion or knowledge of the commitment of esFIRMA, the key commitment 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 Entity.

In case of compromise of the private key of esFIRMA it may be the case that the states of the certificates and of the revocation processes using this key, could not be valid[13]. In any case, all active certificates will be revoked, subsequently generating a last CRL in which all revoked certificates will be included, whether they are expired or not. The fingerprint of the latest CRL will be published on the esFIRMA website to validate this information.

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

---

[13] Ap 6.4.8(g) ii) of ETSI EN 319 411-1

The root key compromise case should be taken as a separate case in the contingency and business continuity process. This incidence affects, in case of replacement of the keys, the recognitions by different applications and private and public services. A recovery of the effectiveness of the keys in terms of business will depend mainly on the duration of these processes. The contingency and business continuity document will deal with the purely operational terms so that the new keys are available, 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 if 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 thus 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 the services of the certification service provider and, in particular, ensure a continuous maintenance of the records required to provide evidence of certification in case of civil or criminal investigation, by transferring them to a notarial deposit.

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

- Provide the necessary funds to continue the completion of the revocation activities.

- It will communicate to the Ministry of Economic Affairs and Digital Transformation, at least 2 months in advance, the cessation of its activity and the destination of the certificates specifying if the management is transferred and to whom, or if its validity will be extinguished.
- It will also communicate to the Ministry of Economic Affairs and Digital Transformation, the opening of any bankruptcy proceedings that are followed against esFIRMA as well as any other relevant circumstance that may prevent the continuation of the activity.
- It will inform all Signatories/Subscribers, Trusted Third Parties and other AC's with which it has agreements or other types of relationship of the cessation with a minimum of 6 months in advance.
- It will transfer the management of the certificates with validity to third party providers provided that there is a consent of their holders or, otherwise, proceed to the extinction of their validity (contained in points b) and c) of the communication of point 1.1).
- It will transfer the obligations of ESFIRMA to the new provider that is in charge: of the management of the certificates, the maintenance of the information of registration of the data and the maintenance of the state of the revocation process and of the files of record of events during their respective periods of time, indicated to the subscribers, to the users and to the parties that trust in the certificates.
- The characteristics of the new provider to which ESFIRMA transfers the management of the certificates will be informed.
- Revoke any authorisation to subcontracted entities to act on behalf of the MA in the certificate issuing procedure.
- It will destroy or disable for use the private keys of the CA.
- Time Stamping Unit (TSU) certificates will be revoked.
- All active certificates and the verification and revocation system will be maintained until the extinction of all certificates issued for 15 years. To this end, a final CRL will be issued that will include all revoked certificates, whether or not they are expired, establishing the necessary means to guarantee their long-term conservation.

6. Technical security controls

6.1 Generating and Installing the Key Pair

6.1.1 Key pair generation

The key pair of the intermediate certification authority "ESFIRMA AC AAPP 2" is created by the root certification authority "ESFIRMA AC RAIZ 2" in accordance with the ceremony procedures of esFIRMA, 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 the individuals participating in it, with the presence of a CISA Auditor. These records are kept for audit and follow-up purposes for an appropriate period determined by esFIRMA.

Devices with Common Criteria EAL 4+ or FIPS 140-2 Level 3 certifications are used to generate the root and intermediate certifications.

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

More information at the following PDS locations:

CERTIFICATE	PDS
Of Public Employee (SIGNATURE)	Spanish: https://esfirma.com/doc-pki/PDS-V2.0/PDS-AAPP-ES.pdf English:
Public Employee – High Level 1.3.6.1.4.1.47281.1.1.1	
Public Employee – Medium Level 1.3.6.1.4.1.47281.1.1.4	
Of Public Employee (AUTHENTICATION)	
Public Employee – High Level 1.3.6.1.4.1.47281.1.1.5	
Public Employee with Pseudonym (SIGNATURE)	
Pseudonymous EP – High Level 1.3.6.1.4.1.47281.1.3.1	
Pseudonymous EP – Medium Level 1.3.6.1.4.1.47281.1.3.4	
Public Employee with Pseudonym (AUTHENTICATION)	

CERTIFICATE	PDS
Public Employee with Pseudonym – 1.3.6.1.4.1.47281.1.3.5	https://esfirma.com/doc-pki/PDS-V2.0/PDS-AAPP-EN.pdf
Organ Seal	
Organ Seal – Medium Level 1.3.6.1.4.1.47281.1.2.2	
Organ Seal – Centralized Medium Level *1.3.6.1.4.1.47281.1.2.4*	
From Natural Person linked to 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 – F. Qualified 1.3.6.1.4.1.47281.1.6.1	
From PF linked to entity – F. Centralized 1.3.6.1.4.1.47281.1.6.4	
From Natural Person linked to entity (AUTHENTICATION)	
From PF linked to entity 1.3.6.1.4.1.47281.1.6.5	
Of Natural Person with pseudonym linked to entity (SIGNATURE)	
From PF with pseudonym linked to entity – Firma Calificada 1.3.6.1.4.1.47281.1.7.1	
From PF with pseudonym linked to entity – Firma Centralizado 1.3.6.1.4.1.47281.1.7.4	
Of Natural Person with pseudonym, linked to entity (AUTHENTICATION)	
From PF with pseudonym, linked to entity 1.3.6.1.4.1.47281.1.7.5	
Electronic Seal	
From Electronic Seal to Software 1.3.6.1.4.1.47281.1.8.2	
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
E-Stamp for TSA/TSU at HSM 1.3.6.1.4.1.47281.1.5.2	

The signer's keys can be created by himself using hardware or software devices authorized by esFIRMA.

esFIRMA can create the keys only by means of a certified device.

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

The keys are generated using the RSA public key algorithm, with a minimum length of 2048 bits.

6.1.2 Sending the private key to the signer

In certificates in secure device of creation of signature the private key is properly protected inside said secure device.

In software certificates, the private key of the signer is created in the computer system used by this signer when making the certificate request, so the private key is duly protected inside the signer's computer system.

6.1.3 Sending the Public Key to the Certificate Issuer

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

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

6.1.4 Distribution of the certification service provider's public key

The esFIRMA keys are communicated to third parties who trust certificates, ensuring the integrity of the key and authenticating its origin, through its publication in the Deposit.

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

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

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

6.1.5 Key sizes

The length of the root CA keys is RSA 4096 bits.
The length of the subordinate CA keys is RSA 4096 bits.
The length of the TSA keys is RSA 4096 bits.
The keys for end-entity certificates are RSA 2048 or 4096 bits.

6.1.6 Generating Public Key Parameters and Quality Checking

The public key of the Root CA, subordinate CA, and subscriber certificates is encrypted according to RFC 5280.

Quality of public key parameters

- Module Length = 4096
- Key generation algorithm: rsagen1
- Summary cryptographic functions: SHA256.

All keys are generated in capital goods, as indicated in section 6.1.1.

6.1.7 Purposes of key use

Key uses for CA certificates are exclusively for certificate signing and CRLs.

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

6.2 Private key protection and cryptographic module controls

6.2.1 Cryptographic Module Standards

In relation to the modules that manage esFIRMA keys and the subscribers of electronic signature certificates, the level required by the standards indicated in the previous sections is ensured.

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

A multi-person control is required for the activation of the CA's private key. In the case of this CPD, in particular there is a policy of **3 out of 5** people for the activation of the keys.

Cryptographic devices are physically protected as determined in this document.

6.2.3 Private Key Deposit

esFIRMA does not store copies of the signatories' private keys.

6.2.4 Backing up the private key

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

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

The signer keys on hardware cannot be copied as 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 flame retardant files and in the external custody center. At least two people will need to retrieve the private key from the CAs on the initial cryptographic device.

6.2.6 Entering the Private Key in the Cryptographic Module

Private keys are generated directly in esFIRMA's production cryptographic modules.

6.2.7 Storing Private Keys in Cryptographic Modules

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

6.2.8 Private Key Activation Method

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

The CA keys are activated by a process of m of n.

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

6.2.9 Private Key Deactivation Method

To deactivate the esFIRMA private key, the steps described in the administrator's manual of the corresponding cryptographic computer will be followed.

For its part, the signatory must enter the PIN for the new activation.

6.2.10 Private Key Destruction Method

Prior to the destruction of the keys, a revocation of the certificate of the public keys associated with them will be issued.

Devices that have any part of esFIRMA's private keys stored will be physically destroyed or restarted at a low level. Removal will follow the steps described in the cryptographic computer administrator's manual.

Eventually the backups will be securely destroyed.

The keys of the signatory in software can be destroyed by deleting them, following the instructions of the application that houses them.

The keys of the signer in hardware can be destroyed by a special computer application in the dependencies of the AR or esFIRMA.

6.2.11 Cryptographic Module Classification

Cryptographic modules undergo 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 for which they are intended.

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

6.3 Other aspects of key pair management

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 public and private keys

The periods of use of the keys are those determined by the duration of the certificate, after which they cannot continue to 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 the provisions of section 6.2.2 and the key ceremony procedures.

The creation and distribution of such devices is recorded.

EsFIRMA also securely generates activation data.

6.4.2 Protection of activation data

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 administrator cards of the cryptographic modules, as stated in the key ceremony document.

The signer of the certificate is responsible for the protection of his private key, with a password as complete as possible. The signer must remember that password.

6.4.3 Other aspects of activation data

Not applicable.

6.5. Computer security controls

esFIRMA uses reliable systems to offer its certification services. esFIRMA has carried out it controls and audits in order to establish an adequate management of its IT assets with 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 staff, in the following aspects:

- Operating system security settings.
- Application security settings.
- Correct sizing of the system.
- Configuration of Users and permissions.
- Log event configuration.
- Backup and recovery plan.
- Antivirus settings.
- Network traffic requirements.

6.5.1 Specific technical requirements for IT security

Each esFIRMA server includes the following functionalities:

- Access control to SubCA services and privilege management.
- Imposition of separation of tasks for privilege management.
- Identification and authentication of roles associated with identities.
- Archive of subscriber history and SubCA and audit data.
- Audit of security-related events.
- Self-diagnosis of security related to the services of the SubCA.
- SubCA system and key recovery mechanisms.

The exposed functionalities are performed 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 these devices continue to be certified as DCCF[15].

Verification of DCCF certification is carried out throughout the validity period of the certificate[16]. If the DCCF loses its certification as such, esFIRMA will proceed to revoke the certificates issued in said DCCF, informing the holders of the same.

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

6.5.2 Assessment of the level of IT security

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

6.6 Technical life cycle controls

15 Ap 6.5.1(a) of ETSI 319 411-2

16 Ap 6.5.1.c) of ETSI EN 319 411-2

6.6.1 System development controls

Applications are developed and implemented by esFIRMA in accordance with development and change control standards.

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

6.6.2 Security management controls

esFIRMA develops the necessary activities for the training and awareness of employees in terms of security. The materials used for the training and the descriptive documents of the processes are updated after approval by a group for safety management. In the performance of this function it has an annual training plan.

esFIRMA requires by contract, the security measures equivalent to any external provider involved in the certification work.

Classification and management of information and assets

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

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

The documents are cataloged in four levels: PUBLIC, RESTRICTED, INTERNAL USE and CONFIDENTIAL.

Management operations

esFIRMA has an adequate procedure for managing and responding to incidents, through the implementation of an alert system and the generation of periodic reports.

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

Treatment of supports and security

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

System Planning

EsFIRMA's Systems department keeps track of the equipment's capabilities. Together with the resource control application of each system, a possible resizing can be foreseen.

Incident reports and response

esFIRMA has a procedure for monitoring incidents and resolving them.

Operational procedures and responsibilities

esFIRMA defines activities, assigned to people with a role of trust, other than the people in charge of carrying out daily operations that do not have the character of confidentiality.

Access system management

esFIRMA makes every effort reasonably available to it to confirm that the access system is limited to authorized persons.

In particular:

AC General

- Firewall,antivirus, and IDS-based controls are available in high availability.
- Sensitive data is protected by cryptographic techniques or access controls with strong identification.
- esFIRMA has a documented procedure for managing user registrations and cancellations and an access policy detailed in its security policy.

- esFIRMA has procedures to ensure that operations are carried out in compliance with the role policy.
- Each person has an associated role to perform the certification operations.
- 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 by means of a system m of n operators for the activation of the private key of esFIRMA.

Revocation management

The revocation will be done by strong authentication to the applications of an authorized administrator. The log systems will generate the tests that guarantee the non-repudiation of the action carried out by the esFIRMA administrator.

Revocation status

The revocation status application has access control based on certificate or two-factor identification authentication to prevent attempted modification of revocation status information.

6.6.3 Life cycle security assessment

esFIRMA ensures that the cryptographic hardware used for certificate signing is not manipulated during transport by inspecting the delivered material.

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

esFIRMA records all relevant device information to add to the asset catalog.

Using certificate-signing cryptographic hardware requires the use of at least two trusted employees.

esFIRMA performs periodic test tests to ensure the correct functioning of the device.

The cryptographic hardware device is only manipulated by reliable personnel.

The esFIRMA signature private key stored on 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 device maintenance contract. Changes or updates are authorized by the security officer and are reflected in the corresponding worksheets. These configurations will be done by at least two reliable people.

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 done by using firewalls.

Confidential information that is transferred over unsecured networks is done in encrypted form using SSL protocols or the VPN system with two-factor authentication.

6.8 Time Sources

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

6.9 Signature algorithms and parameters of the centralized signature system

The centralized signing service generates keys for signatories with the RSA algorithm with a key length of 2048 bits with probable primes using the FIPS algorithm 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 master key of the HSM. 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 jump 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 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 web repository of esFirma, section "Remote signature security information". The system allows to generate electronic signatures with the RSA PKCS#1 v1.5 algorithm 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 X.509 version 3, 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 the QCStatements of qualified certificates according to RD (EU) 910/2014.

esFIRMA generates serial numbers of non-sequential certificates 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 extensions of the certificates are detailed in the profile documents that are accessible from the esFIRMA website https://www.esfirma.com

7.1.3 Object Identifiers (OIDs) of algorithms

The object identifier of the signature algorithm is:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption

The object identifier of the public key algorithm is:

- 1.2.840.113549.1.1.1 rsaEncryption

7.1.4 Name Format

The certificates must contain the information that is necessary for their use, as determined by the corresponding policy.

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

7.1.5 Restriction of names

The names contained in the certificates are restricted to "Distinguished Names" X.500, 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 Restrictions Extension

Not applicable

7.1.8 Syntax and semantic policy qualifiers

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 can contain a policy qualifier. See 7.1.6

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 OCSPs 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 beginning of its activity as a provider of certification services by the Ministry of Economic Affairs and Digital Transformation is subject to the control reviews that this body deems necessary.

8.1 Frequency of compliance audit

esFIRMA conducts a compliance audit annually, in addition to the internal audits it conducts at its own discretion or at any time, due to a suspected breach of any security measure.

esFIRMA monitors compliance with this document and strictly controls the quality of its service by conducting self-audits at least quarterly against a randomly selected sample of the largest of a 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 conducted by an independent external audit firm that demonstrates technical competence and expertise in computer security, information systems security, and compliance audits of public key certification services, and related elements.

8.3 Relationship of the auditor with the audited entity

Audit companies are of recognized prestige with departments specialized in carrying out computer audits, so there is no conflict of interest that may distort their performance in relation to esFIRMA.

8.4 List of items subject to audit

The audit verifies with respect to 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 the different digital certificates.
c) That the DPC and other related legal documentation, conforms to what is agreed by esFIRMA and with the provisions of current regulations.
d) That the entity properly manages its information systems

In particular, the elements to be audited shall be the following:

a) CA processes, ARs and related elements.
b) Information systems.
c) Data center protection.
d) Documents.

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

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

If esFIRMA is unable to develop and/or execute such a plan or if the deficiencies found pose an immediate threat to the security or integrity of the system, it must immediately notify esFIRMA's senior management, which may carry out the following actions:

- Cease operations temporarily.
- Revoke the CA key and regenerate the infrastructure.
- Terminate the CA service.
- Other complementary actions that may be necessary.

8.6 Treatment of audit reports

The audit results reports are delivered to esFIRMA's senior management within a maximum period of 15 days after the execution of the audit.

9. Commercial and legal requirements

9.1 Fees

9.1.1 Fee for issuing or renewing certificates

esFIRMA may establish a fee for the issuance of certificates, of which, where appropriate, subscribers will be informed in a timely manner.

9.1.2 Certificate Access Fee

esFIRMA has not established any fees for access to certificates.

9.1.3 Certificate Status Information Access Fee

esFIRMA has not established any fees for access to certificate status information.

9.1.4 Fees for other services

No stipulation.

9.1.5 Withdrawal Policy

No 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 the ETSI EN 319 401-1 7.12 c), in relation to the management of the completion of services and cessation plan.

9.2.1 Insurance coverage

esFIRMA has a sufficient guarantee of coverage of your civil liability, through a professional civil liability insurance that complies with what is indicated in the regime of obligations and responsibilities 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 an insured minimum of 3,000,000 euros.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance coverage for subscribers and third parties relying on certificates

esFIRMA has a sufficient guarantee of coverage of your civil liability, through a professional civil liability insurance that complies with what is indicated in the regime of obligations and responsibilities 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 of 3,000,000 euros.

9.3 Confidentiality of information

9.3.1 Confidential information

The following information is kept confidential by esFIRMA:

- Applications for certificates, approved or denied, as well as all 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 logs, including complete records and audit logs of transactions.
- Internal and external audit records, created and/or maintained by the Certification Body and its auditors.
- Business continuity and emergency plans.
- Security policy and plans.
- Documentation of operations and other operating plans, such as archiving, monitoring and other analogues.

- All other information identified as "Confidential".

9.3.2 Non-confidential information

The following information is considered non-confidential:

- 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 surname 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 depending on 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 uses and economic limits outlined in the certificate.
- The period of validity of the certificate, as well as the date of issue of the certificate and the expiration date.
- The serial number of the certificate.
- The different states or situations of the certificate and the date of the start of each of them, in particular: pending generation and / or delivery, valid, revoked, suspended or expired and the reason that caused the change of status.
- Certificate revocation lists (CRLs), as well as other revocation status information.
- Any other information that is not indicated in the previous section.

9.3.3 Disclosure of Suspension and Revocation Information

See previous section.

9.3.4 Legal Disclosure of Information

esFIRMA discloses confidential information only in the cases provided for by law.

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

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

9.3.5 Disclosure of information at the request of its owner

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

9.3.6 Other Disclosure Circumstances

No 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 related in REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of these 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 by the SUBSCRIBER, who must have obtained them legally 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 status of person in charge of the processing of personal data and, as such, treats the data solely and exclusively for the purposes contained in this Declaration

[17] Section 7.10(c) of the ETSI EN 319 401

of Certification Practices in accordance with the instructions of the person responsible for the treatment, which is the SUBSCRIBER and which are included in the Annex "*Annex 1: For the processing of personal data by ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A. as THE PERSON IN CHARGE OF THE TREATMENT* ", which governs the contract for the provision of the "Gestiona" service 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 in this Declaration of Certification Practices, as well as in the Annex "Annex 1: *For the processing of personal data by ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A. as DATA PROCESSOR*" that governs the contract for the provision of the service "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 rules.

9.4.2 Information treated as private

Personal information about an individual that is not publicly available in the Contents of a certificate or CRL is 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 as non-private as it is necessary to provide 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 the regulations on the protection of personal data is protected from loss, destruction, damage, falsification and unlawful or unauthorised processing, in accordance with the requirements set out in this document, which are aligned with the obligations laid down 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 processing of personal data and the free movement of these data and repealing Directive 95/46/EC, and 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 Of Private Information

Before entering into a contractual relationship, the interested parties shall be offered the prior information about the processing of your personal data and exercise of rights, and where appropriate, will obtain the mandatory consent for the differentiated treatment of the main treatment for the provision of the contracted services.

9.4.6 Disclosure pursuant to judicial or administrative proceedings

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 case of termination of the certification service.

9.4.7 Other Disclosure Circumstances

No personal data is transferred to third parties except legal obligation.

9.5 Intellectual Property Rights

9.5.1 Ownership of Certificates and Revocation Information

EsfirmA only 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, at no cost, as long as 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 according to the documentation that links them.

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

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

9.5.2 Ownership of the Declaration of Certification Practices

Only esFIRMA enjoys intellectual property rights over this Statement of Certification Practices.

9.5.3 Ownership of Name Information

The subscriber and, where appropriate, the natural person identified in the certificate, retains all rights, if any, over the brand, product or trade name contained in the certificate.

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

9.5.4 Key Ownership

Key pairs are owned by certificate signers.

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

9.6 Obligations and civil liability

9.6.1 Obligations of the Certification Body "esFIRMA"

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

esFIRMA provides certification services in accordance with this Statement of Certification Practices.

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

The dissemination text document, also called PDS[18], complies with the content of Annex A of the ETSI EN 319 411-1 v1.1.1 (2016-02), a document which can be transmitted by electronic means, using a means of communication lasting over time, and in understandable language.
esFIRMA permanently communicates the changes[19] that occur in its obligations by publishing new versions of its legal documentation on its website https://www.esfirma.com

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

- Requirements to comply with sections 4.5.3, 9.2, 9.6.7, 9.6.8, 9.6.9 and 9.6.10.
- Indication of the applicable policy, indicating that certificates are not issued to the public.
- Statement that the information contained in the certificate is correct, except notification to the contrary by the subscriber.
- Consent for the storage of the information used for the registration of the subscriber and for the transfer of said information to third parties, in case of termination of operations of the Certification Authority without revocation of valid certificates.
- Limits on use of the certificate, including those set out 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

18 "PKI Disclosure Statement", or applicable PKI disclosure statement.

19 Ap 6.2.3.b) of ETSI EN 319 411-1

certificate can reasonably be trusted, which is applicable when the subscriber acts as a third party trusting the certificate.

- How the patrimonial responsibility of the Certification Entity is guaranteed.
- Applicable limitations of liability, including the uses for which the Certification Body accepts or excludes its liability.
- The period for archiving certificate request information.
- Audit log archiving period.
- Applicable dispute resolution procedures.
- Applicable law and competent jurisdiction.
- Whether the Certification Authority has been declared in accordance with the certification policy and, where appropriate, according to which system.

9.6.2. Obligation and responsibility of the RA

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

• Respect the provisions of this CPS and the corresponding PDS.

• Protect their private keys that will serve them for the exercise of their functions.

• Verify the identity of the Subjects/Signatories and Applicants of the certificates when necessary, definitively proving the identity of the Signatory, in case of individual certificates, or of the holder of keys, in case of organizational certificates, in accordance with the provisions of the corresponding sections of this document.

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

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

• Deliver, where appropriate, the corresponding cryptographic device.

• File, for the period provided in current legislation, the documents provided by the applicant or Signatory.

• Respect the provisions of the contracts signed with esFIRMA and with the Subject/Signatory.

• Inform esFIRMA of the causes of revocation, 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 holder of receiving the certificate and, where appropriate, the cryptographic device, and acceptance of said elements.
• Inform the method of exclusive imputation to the holder of the private key and their activation data of the certificate and, where appropriate, of the cryptographic device, in accordance with the provisions of the corresponding sections of this document.
These obligations apply even in the cases of entities delegated by them such as face-to-face verification points (PVP).
Information on subscriber usage and responsibilities is provided through the acceptance of the terms of use prior to the confirmation of the certificate application and by email.

RAs sign a service provision contract with esFIRMA through which esFIRMA delegates the registration functions in the AR, consisting mainly of:
1.- Obligations prior to the issuance of a certificate.
(a) Adequately inform applicants of the signature of their obligations and Responsibilities.
(b) Proper identification of applicants, who must be trained persons or authorized to request a digital certificate.
c) The correct verification of the validity and validity of these data of the applicants and of the Entity, in the event that there is a relationship of linkage or representation.
d) Access the Registration Authority application to manage applications and certificates issued.
2.- Obligations once the certificate has been issued.
a) Sign the contracts for the Provision of Digital Certification Services with the Applicants. In most emissions processes this contract is formalized
by accepting conditions on the web pages that are part of the process of issuance of the certificate, not being able to carry out the issuance without first not having accepted the conditions of use.
b) The maintenance of the certificates during their validity (extinction, suspension, revocation).
(c) To file copies of submitted documentation and contracts properly signed by applicants in accordance with published Certification Policies by esFIRMA and current legislation.
Thus, the AR are responsible for the consequences in case of non-compliance with their registration tasks, and through which they also undertake to respect the internal regulatory rules of the certifying entity esFIRMA (Policies and CPS) which must be perfectly controlled by the RA and which must serve as a reference manual.

In case of claim by a Subject, an Entity, or a user, the CA must provide the proof of diligent action and if it is found that the origin of the complaint lies in an error in the validation or verification of the data, the MA may, by virtue of the agreements signed with the RA, make the responsible RA bear the assumption of the consequences.
Because, although legally the CA is the legal entity responsible to the Subject, an Entity, or User Party, and that for this it has a civil liability insurance, according to the current agreement, the RA has as a contractual obligation "to correctly identify and authenticate the Applicant and, where appropriate, the corresponding Entity", and by virtue of it must respond to esFIRMA of its breaches.
Of course, it is not the intention of esFIRMA to offload the full weight of the assumption of liability to ra for possible damages arising from a failure to comply with tasks delegated to AR. For this reason, as foreseen for the CA, the RA is subject to a control regime that will be exercised by esFIRMA, not only through the controls of archives and procedures of conservation of the archives assumed by the RA through the realization of audits to evaluate among others, the resources used and the knowledge and control of the operating procedures to offer the services of RA.
The same responsibilities shall be assumed by ar ARs by virtue of breaches of the delegated entities such as face-to-face checkpoints (PVP), without prejudice to their right to have an impact against them.

9.6.3 Warranties offered to subscribers and third parties relying on certificates

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

esFIRMA, at a minimum, guarantees the subscriber:

- That there are no factual errors in the information contained in the certificates, known or made by the Certification Authority.
- That there are no factual errors in the information contained in the certificates, due to lack of due diligence in the management of the certificate application or in the creation of the certificate.
- That the certificates comply with all the material requirements set forth in the Declaration of Certification Practices.
- That the revocation services and use of the Deposit comply with all the material requirements set forth in the Declaration of Certification Practices.

esFIRMA, at a minimum, will guarantee to the third party that trusts in the certificate:

- That the information contained or incorporated by reference in the certificate is correct, except where otherwise indicated.
- That in the approval of the certificate application and in the issuance of the certificate, all the material requirements established in the Declaration of Certification Practices have been met.
- Speed and security in the provision of services, especially revocation services.

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

- That the certificate contains the information to be contained by a qualified certificate, in accordance with Annex 1 to Regulation (EU) 910/2014.
- That, in the event that it generates the private keys of the subscriber or, where appropriate, natural person identified in the certificate, its confidentiality is maintained during the process.
- The responsibility of the Certification Body, with the limits that are established.

9.6.4 Obligation and liability of third parties

It will be the obligation of the User Party to comply with the provisions of 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 several mechanisms to carry out this verification, such as access to lists of revoked certificates or OCSP online consultation services.
- Know and be subject to the guarantees, limits and responsibilities applicable in the acceptance and use of the certificates in which it trusts, and agree to be bound by 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 trusted list of the corresponding national supervisor.

9.6.5 Obligation and responsibility of other participants

Not stipulated

9.7. Disclaimer of Warranty

According to current legislation, the liability of esFIRMA and its RAs does not extend to those cases in which the improper use of the certificate has its origin in conduct attributable to the Subject, and to the User Party for:

- Failure to provide adequate information, initially or subsequently as
- as a result of changes in the circumstances reflected in the electronic certificate, where its inaccuracy could not be detected by the certification service provider
- Have incurred negligence with respect to the retention of signature creation data and its confidentiality.
- Not have requested revocation of the data of the electronic certificate in case of doubt about the maintenance of confidentiality
- Have used the signature after the expiration of the period of validity of the electronic certificate
- Exceed the limits set out in the electronic certificate.
- In conduct attributable to the User Party if it acts negligently, that is, when it does not check or take into account the restrictions contained in the certificate regarding its possible uses and limit the amount of the transactions; 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 trust by the inaccuracy of the data contained in the electronic certificate, if these have been accredited by means of a public document, registered in a public registry if it is required.
- An inappropriate or fraudulent use of the certificate in case the Subject / Holder has transferred it or has authorized its use in favor of a third person by virtue of a legal business such as the mandate or power of attorney, being the sole responsibility of the Subject / Holder the control of the keys associated with their certificate.

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

- State of War, natural disasters or any other case of Force Majeure.
- For the use of the certificates as long as it exceeds the provisions of 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.

- For the damage caused in the period of verification of the causes of revocation.
- By the content of digitally signed or encrypted messages or documents.
- For the non-recovery of documents encrypted with the subject's public key.

9.8. Limitation of Liability in Case of Transaction Losses

The maximum limit that ESFIRMA allows in the economic transactions carried out is 0 (zero) euros.

9.9. Indemnities

See section 9.2

9.10. Term and Termination

9.10.1 Term

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 notice regarding this CPS shall be made by e-mail or by registered mail addressed to any of the addresses referred to in the contact details section 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, regulatory requirements (eIDAS, National Supervisory Bodies, etc.) or as a result of the optimization of the work cycle. Each new version of this CPS replaces all previous versions, which remain, however, applicable to certificates issued while those versions were in effect 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 box at the beginning of the document.
Changes that may be made to this CPS do not require notification unless it directly affects the rights of the Subjects/Signatories of the certificates, in which case they may submit their comments to the policy management organization within 15 days of publication.

9.12.2 Notification mechanism and time limits

All proposed changes to this policy will be immediately published on the esFIRMA website. In this same document there is a section of changes and versions where you can know the changes produced since its creation and the date of said modifications.
The changes to this document are communicated to those third party bodies and companies that issue certificates under this CPS as well as to the corresponding auditors. In particular, changes in this CPS will be notified to the National Supervisory bodies.

Signatories/Subscribers and trusted third parties affected may submit their comments to the policy management organization within 15 days of receipt of the notification.

9.12.3 Circumstances in which the OID must be changed

Not stipulated

9.13 Dispute resolution procedure

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

9.14. Applicable law

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

9.15. Compliance with Applicable Law

See point 9.14

9.16. Other provisions

9.16.1 Entire Agreement

The Holders and third parties that trust the Certificates assume in full the content of this Declaration of Certification Practices and Policies

9.16.2 Allocation

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

9.16.3 Separability

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

- Under the severability clause, the invalidity of a clause will not affect the rest of the contract.
- Under the survival clause, certain rules will remain in force after the termination of the legal relationship regulating the service between the parties. For this purpose, the Certification Body ensures that, at least the requirements contained in sections 9.6.1 (Obligations and responsibility), 8 (Compliance audit) and 9.3 (Confidentiality), remain in force after the termination of the service and the general conditions of issuance / use.
- By virtue of the full agreement clause, it will be understood that the legal document regulating the service contains the complete will and all the agreements between the parties.

- The notification clause shall establish the procedure by which the parties notify each other of facts.

9.16.4 Compliance (Attorneys' Fees and Duty Waiver)

esFIRMA may seek compensation and attorneys' fees from a party for damages, losses and expenses related to the conduct of such party. The fact that esFIRMA does not enforce a provision of this CPS does not remove the right of esFIRMA to enforce the same provisions below 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 text of disclosure or PDS, clauses that limit its liability in fortuitous event 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 hold the Certification Body harmless from any damage arising from any action or omission resulting in liability, damage or loss, expense of any kind, including judicial and legal representation 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 user of the certificate.
- Error of the user of the certificate when providing the data of the application, if in the action or omission there was intent or negligence with respect to the Certification Authority or to any person who trusts the certificate.
- Negligence in the protection of the private key, in the use of a reliable system or in maintaining the necessary precautions to avoid the compromise, loss, disclosure, modification or unauthorized use of said key.
- Use by the subscriber of a name (including common names, email address and domain names), or other information in the certificate, which infringes intellectual or industrial property rights of third parties.

9.17.2 Indemnity clause of third party relying on the certificate

esFIRMA includes in the text of disclosure or PDS, a clause by which the third party that trusts in the certificate undertakes to hold the Certification Body harmless from any damage arising from any action or omission that results in liability, damage or loss, expense of any kind, including judicial and legal representation 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 relying on the certificate.
- Reckless confidence in a certificate, depending on the circumstances.
- Failure to check the status of a certificate, to determine that it is not suspended or revoked.