Certification Practices Statement

esFIRMA

Overview

Document control

Security Rating:	Public
Author:	ESFIRMA
Version:	1.18

Formal status

Prepared by:	Reviewed by:	Approved by:
Security Office Date: 26/07/2024	Security Manager Date: 26/07/2024	Security Committee Date: 10/10/2024

Version Control

See	Description of the change	Date
1.0	Document creation	29/04/2016
1.1	Corrections	02/06/2016
1.2	ETSI Review	19/05/2017
1.3	Review of types of certificates	
1.4	Review Certificate Types, Acronyms and Definitions	02/06/2017
1.5	Regulatory reference adjustments, change of name, change of certificates 1.3.2, 1.3.3.1, 1.3.3.2, 1.4.1.8, 3.1.1.8, 4.3.1, 6.1.5, 9.2.1, 9.4, 9.6.2, 9.6.4	06/11/2017
1.6	6.1.1 TSA Duration	20/06/2018
1.7	Correction regarding 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 review of the renewal sections.	13/11/2018
1.9	3.1.1.1 Clarification on the optional second surname. 3.1.1.2 OrganizationIdentifier conditional on CA/Browser Forum Guidelines 3.1.1.4 Adjusting for Typographical Errors in 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 RFC 3647 Alignment 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 Certificate 4.4.3 Moved to 4.4.2 Certificate Publication 4.4.4 Moved to 4.4.3 Notification of Issuance to Third Parties Added 4.6.1 Circumstances for Certificate Renewal Added 4.6.2 Who can request a renewal Added 4.6.3 Certificate Renewal Request Processing Added 4.6.4 Notification of Certificate Reissue to Subscriber Addendum 4.6.5 Conduct Constituting Acceptance of a Renewal Certificate Added 4.6.6 Publication of the renewal certificate by the CA Added 4.6.7 Notification of the issuance of the certificate 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 the 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 the 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 Life Cycle Security Assessment 6.9 moved to 6.8 Time Sources Added 7.1.7 Using the Policy Restrictions Extension Added 7.1.8 Policy, Syntax, and Semantic Qualifiers Added 7.1.9 Processing Semantics for Critical Extension of Certificate Policies Added 7.2.2 CRL and CRL extensions Added 7.3.1 Version Number Added 7.3.2 OCSP Extensions Added 9.4.1 Privacy Plan Added 9.4.2 Information Treated as Private Added 9.4.3 Information Not Considered Private Added 9.4.4 Responsibility to Protect Private Information Added 9.4.5 Notice and Consent to Use of Private Information Added 9.4.6 Disclosure pursuant to judicial or administrative process Added 9.4.7 Other Circumstances of Disclosure of Information 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 Responsibility of Other Participants 9.6.3 moved to 9.7 Disclaimer 9.6.4 moved to 9.8 Limitation of liability in case of 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 Completion Added 9.10.3 Termination and Survivability Effect Added 9.11 Individual notifications and communication with participants Added 9.12 Modifications Added 9.12.1 Amendment Procedure Added 9.12.2 Notification mechanism and deadlines Added 9.12.3 Circumstances in which OID should 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 (FIRMA), certificate of natural person with pseudonym linked to entity (Authentication), certificate of natural person with pseudonym linked to entity (FIRMA)	
1.11	New qualified electronic seal certificates are included The e-Office certificate profile is deleted. Adaptation due to regulatory change (Law 6/2020, of 11 November, regulating certain aspects of electronic trust services). Section 5.8 Termination of the DPC Service adds the detail of how the status information of the certificates is provided beyond their lifetime.	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 of "Registry Administrator" to "Registry Operator". References to CA/B Forum are removed.	10/05/2021
1.13	Modification point 5.8 Termination of Service, in accordance with the Termination Plan Section 4.9.1 is amended to include the end of QSCD certification Modification point 6.5.1, including the end of DCCF certification. Removal of reference to the esFIRMA security document from section 6.6.2 (Management operations) Replacing "security policy" with "information security management system" in section 6.6.2 (Classification and management of information and property) Section 6.9 is added in accordance with ETSI TS 119 431-1: OVR-5.1-02 Point 9.6.4 is modified, including the Certification Chain as a verification point. The integration system with DIR3 is added as a means of verifying the identity of the entity (3.2.2) The verification of the status of certificates in the certification chain is added in section 4.9.6.	18/07/2022
1.14	New TSA Certificate Information	16/03/2023
1.15	Settings, information about TSA and incorporation of non-qualified time stamp	31/03/2023
1.16	New Certificate Profile Element Length Restrictions New European sub-profiles for Natural Persons and Electronic Seal Simplification of sections 3.2.2 and 3.2.3 Section 4.5.3 is added to separate the information and obligations of third parties who rely on certificates. Differences and Considerations Between Certificate Revocation Status Queries Using OCSP and CRL 4.10.1	21/04/2023
1.17	The possibility of transferring the management of the certificates issued to another provider in the event of termination of the service is eliminated from section 5.8.	10/02/2024
1.18	Maximum time is included between identity validation and certificate issuance (section 3.2.3.2) Exceptional proceedings are included in the event that the request for revocation cannot be confirmed in less than 24 hours (section 4.9.5) New section 1.4.3. Issuance of test certificates.	26/07/2024

Index

1. Introduction

1.1 Presentation

This document states esFIRMA's electronic signature certification practices.

The certificates that are issued are the following:

- **Public Employee (FIRMA)**
  - Of Public Employee Middle Level
  - High level Public Employee
- **Public Employee (AUTHENTICATION)**
  - High level Public Employee
- **Of Public Employee with pseudonym (FIRMA)**
  - Of Public Employee Middle Level
  - High level Public Employee
- **Of Public Employee with pseudonym (AUTHENTICATION)**
  - High level Public Employee
- **From a natural person linked to an entity (FIRMA)**
  - From an individual linked to an Intermediate level entity
  - From an individual linked to a High level entity
- **From a natural person linked to an entity (AUTHENTICATION)**
  - From an individual linked to a High level entity
- **From an individual linked to an entity with a pseudonym (FIRMA)**
  - From an individual linked to an Intermediate level entity
  - From an individual linked to a High level entity
- **From a natural person linked to an entity with a pseudonym (AUTHENTICATION)**
  - From an individual linked to a High level entity
- **Organ Seal**
  - 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 the "Statement of Certification Practices" of esFIRMA.

1.2.1 Certificate Identifiers

OID Number	Certificate policies
	Public Employee (FIRMA)
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 – Intermediate Level in HSM*
	Public Employee (AUTHENTICATION)
1.3.6.1.4.1.47281.1.1.5	*Public Employee – High level on card*
	Of Public Employee with Pseudonym (SIGNATURE)
1.3.6.1.4.1.47281.1.3.1	*From EP with Pseudonym – High Level on Card*
1.3.6.1.4.1.47281.1.3.4	*PE with Pseudonym – Intermediate Level in HSM*
	Pseudonymous Public Employee (AUTHENTICATION)
1.3.6.1.4.1.47281.1.3.5	*From EP with Pseudonym – High Level on Card*
	From Individual linked to entity (FIRMA)
1.3.6.1.4.1.47281.1.6.1	*Of PF linked to entity – Qualified e-Signature, on Card*
1.3.6.1.4.1.47281.1.6.4	*Entity-linked PF – Centralized e-Signature*
	From a natural person linked to an entity (AUTHENTICATION)
1.3.6.1.4.1.47281.1.6.5	*Entity-linked PF – on Card*
	From a natural person with a pseudonym linked to an entity (FIRMA)

1.3.6.1.4.1.47281.1.7.1	*From PF with a pseudonym linked to an entity – Qualified e-Signature, on Card*
1.3.6.1.4.1.47281.1.7.4	*De PF with a pseudonym linked to an entity – Firma-e Centralizado*
	From a Person with a pseudonym, linked to an entity (AUTHENTICATION)
1.3.6.1.4.1.47281.1.7.5	*From PF with pseudonym, linked to entity – in Card*
	Organ Seal
1.3.6.1.4.1.47281.1.2.2	*Organ Seal – Intermediate Level in Software*
1.3.6.1.4.1.47281.1.2.4	*Organ Seal – Intermediate Level in HSM*
	Electronic Seal for TSA/TSU
1.3.6.1.4.1.47281.1.5.1	*E-Seal for TSA/TSU in HSM*
1.3.6.1.4.1.47281.1.5.2	*TSA/TSU Qualified e-Seal in HSM*
	Electronic Seal
1.3.6.1.4.1.47281.1.8.2	*Electronic Seal in 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 documents of practices and procedures of esFIRMA, the provisions of this Statement of Practices 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, that issues and manages certificates for final entities, using a Certification Body, or providing other services related to electronic signatures.

ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (FORMERLY 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, page Z-28722, and operating under the trade name esFIRMA, trade 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 11 November, regulating certain aspects of electronic trust services, Organic Law 3/2018, of 5 December, on the Protection of Personal Data and guarantee of digital rights and the ETSI technical standards applicable to the issuance and management of the 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 bodies:

enFIRMA AC root 2

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

Identification data:

CN:	ESFIRMA AC RAIZ 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

SIGNATURE AC AAPP 2

This is the certification authority within the hierarchy that issues certificates to the end entities, and whose public key certificate has been digitally signed by "esFIRMA AC RAÍZ 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 exclusive certificate lifecycle management platform for 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 registration authority for the identity of certificate subscribers.

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

The functions of registering subscribers are carried out by delegation and in accordance with the instructions of the certification service provider, under the terms defined by Regulation (EU) 910/2014, and Law 6/2020, of 11 November, 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 that are the recipients of 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 the esFIRMA certification services:

1. Subscribers to the certification service.
2. Signatories.
3. User parts.

1.3.4 User Parties

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

As a prelude to relying on certificates, users must verify them, as set out in this statement of certification practices and in the corresponding instructions available on the Certification Authority's website.

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 organisational environment, and are identified in the certificates.

The subscriber of the certification service acquires a licence to use the certificate, for its own use – electronic seal certificates – or in order to facilitate the certification of the identity of a specific person duly authorised for various actions in the subscriber's organisational field – electronic signature certificates. In the latter case, this person is identified in the certificate, as provided in the following section.

The subscriber of the certification service is therefore the customer of the certification service provider, in accordance with commercial law, and has the rights and obligations defined by the certification service provider, which are additional and are 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 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, in accordance with the regime of obligations and responsibilities of Regulation (EU) 910/2014, and Law 6/2020, of 11 November, regulating certain aspects of electronic trust services, the digital signature keys for identification and advanced or qualified electronic signature; typically being the holders or members of the administrative bodies, in the electronic signature certificates of the body, the persons in the service of the Public Administrations, in the certificates of public employees or the persons who belong to an entity, in the certificates of linked natural persons.

The signatories are duly authorized by the subscriber and duly identified in the certificate by their name and surnames, 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 of certificates.

1.4.1 Permitted Uses for Certificates

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

High level Public Employee Certificate on Card

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.1.1	In the hierarchy of the CA esFIRMA
0.4.0.194112.1.2	In accordance with QCP-n-qscd policy
2.16.724.1.3.5.7.1	High-level Spanish public employee

The certificates of high-level public employee natural persons 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 in the service of the Administration, body, public law entity or other entity, linking them to it, complying with the requirements established in Article 43 of Law 40/2015, of 1 October, on the Legal Regime of the Public Sector, for the electronic signature of personnel in the service of the Public Administrations.

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

Likewise, the certificates of natural persons at a high level public employee are issued in accordance with the high assurance levels of the certificate profiles established in point 10 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 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, so 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, 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 applications listed below:

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

esFIRMA does not offer backup or key recovery services. Therefore, esFIRMA will not be liable under any circumstances 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 electronic signature function)

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 at the middle level in HSM

This certificate has the following OIDs:

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

The certificates of natural persons at the medium level public employee 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 in the service of the Administration, body, public law entity or other entity, linking them to it, complying with the requirements established in Article 43 of Law 40/2015, of 1 October, on the Legal Regime of the Public Sector, for the electronic signature of personnel in the service of the Public Administrations.

The certificates of natural persons at the middle level public employee are managed centrally.

The certificates of natural persons of medium-level public employees are issued in accordance with the average assurance levels of the certificate profiles established in point 10 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 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 applications listed below:

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

esFIRMA does not offer backup or key recovery services. Therefore, esFIRMA will not be liable under any circumstances 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 electronic signature function)

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 CA esFIRMA
0.4.0.2042.1.2	In accordance with NCP+ policy
2.16.724.1.3.5.7.1	High-level Spanish public employee

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

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

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

The certificates of high-level public employee natural persons are issued in accordance with the high assurance levels of the certificate profiles established in point 10 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 backup or key recovery services. Therefore, esFIRMA will not be liable under any circumstances 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 CA esFIRMA

0.4.0.194112.1.1	In accordance with QCP-l policy
2.16.724.1.3.5.6.2	Mid-level Spanish public employee

The 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 with the 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 1 October, on the Legal Regime of the Public Sector.

The medium-level body electronic seal certificates are issued in accordance with the medium assurance levels of the certificate profiles established in point 9 of the document "Electronic Certificate Profiles" of the Secretary of State for Digitalisation 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 backup or key recovery services. Therefore, esFIRMA will not be liable under any circumstances 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 electronic signature function)

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 Organ Seal at the intermediate level in HSM

This certificate has the following OIDs:

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

The 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 with the 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 1 October, on the Legal Regime of the Public Sector.

The electronic seal certificates of the mid-level body are managed centrally.

The medium-level body electronic seal certificates are issued in accordance with the medium assurance levels of the certificate profiles established in point 9 of the document "Electronic Certificate Profiles" of the Secretary of State for Digitalisation 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 backup or key recovery services. Therefore, esFIRMA will not be liable under any circumstances 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 electronic signature function)

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 High Level Pseudonym on Card

This certificate has the following OIDs:

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

The certificates of natural persons of public employees 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 in the service of the Administration, body, public law entity or other entity, linking them to it, complying with the requirements established in Article 43 of Law 40/2015, of 1 October, on the Legal Regime of the Public Sector, for the electronic signature of personnel at the service of the Public Administrations.

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

Likewise, certificates of natural persons public employees with a high level pseudonym are issued in accordance with the high assurance levels of 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 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, so 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 applications listed below:

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

esFIRMA does not offer backup or key recovery services. Therefore, esFIRMA will not be liable under any circumstances 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 electronic signature function)

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 a pseudonym middle level, in HSM

This certificate has the following OIDs:

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

The certificates of natural persons of public employees with a medium 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 in the service of the Administration, body, public law entity or other entity, linking them to it, complying with the requirements established in Article 43 of Law 40/2015, of 1 October, on the Legal Regime of the Public Sector, for the electronic signature of personnel at the service of the Public Administrations.

The certificates of natural persons of public employees with a medium level pseudonym are managed centrally.

The certificates of natural persons of public employees with a medium level pseudonym are issued in accordance with the medium assurance levels of the certificate profiles established in point 11 of the document "Electronic Certificate Profiles" of the 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 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 applications listed below:

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

esFIRMA does not offer backup or key recovery services. Therefore, esFIRMA will not be liable under any circumstances 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 electronic signature function)

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.

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

This certificate has the following OIDs:

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

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

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

These certificates of natural persons who are public employees with a high level pseudonym work with a secure signature creation device, in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council, of 23 July 2014.

The certificates of natural persons of public employees 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 "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 backup or key recovery services. Therefore, esFIRMA will not be liable under any circumstances 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 Qualified Electronic Seal Certificate

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.5.2	In the hierarchy of the CA esFIRMA

0.4.0.194112.1.1	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 TSUs to issue time-stamps when they receive a request under the RFC3161's specifications.

The 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 following feature enabled:
    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. Optional
e) It includes the "privateKeyUsage" extension, which limits the use of the private key, following the recommendations of the ETSI EN 319 421 and ETSI EN 319 422 standards.

Other considerations:

- Controls are established to guarantee the cessation of use of the private key before its expiration of validity.
- In the event of a certificate change, the associated keys will be destroyed as described in the lifecycle.
- Private keys are destroyed after their defined time of use, replacement, revocation, or other causes have expired.

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

TSA/TSU Electronic Seal Certificate

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.5.1	In the hierarchy of the CA esFIRMA
0.4.0.194112.1.1	In accordance with QCP-l policy

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

The keys are generated in support of an HSM device.

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. Content Commitment

g) The "extend key usage" field has the following feature enabled:
   a. TimeStamping

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

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

Other considerations:

- Controls are established to guarantee the cessation of use of the private key before its expiration of validity.
- In the event of a certificate change, the associated keys will be destroyed as described in the lifecycle.
- Private keys are destroyed after their defined time of use, replacement, revocation, or other causes have expired.
- The destruction is carried out in such a way that the private key cannot be recovered, following the procedure established by the manufacturer of the cryptographic module that stores them.
- For long-term validation of the time stamps, the Last CRL issued by esFIRMA may be used following the guidelines provided. At the time of verification, it can be considered valid if, at the time of the timestamp date, the private key was not compromised, the fingerprint algorithm was not collisioned, and the algorithms used were beyond the reach of the cryptographic attacks of the time.

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 CA esFIRMA
0.4.0.194112.1.2	In accordance with 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 work with a secure signature creation device, in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council, of 23 July 2014.

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, so 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, 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 applications listed below:

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

esFIRMA does not offer backup or key recovery services. Therefore, esFIRMA will not be liable under any circumstances 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 electronic signature function)

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. Optional

Certificate of a 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 CA 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 centrally managed.

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 applications listed below:

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

esFIRMA does not offer backup or key recovery services. Therefore, esFIRMA will not be liable under any circumstances 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 electronic signature function)

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. Optional

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 CA esFIRMA
0.4.0.2042.1.2	In accordance with NCP+ policy

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

These certificates work with a secure signature creation device, in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council, of 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 backup or key recovery services. Therefore, esFIRMA will not be liable under any circumstances 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. Optional

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

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.7.1	In the hierarchy of the CA esFIRMA
0.4.0.194112.1.2	In accordance with 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 work with a secure signature creation device, in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council, of 23 July 2014.

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, so 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 applications listed below:

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

esFIRMA does not offer backup or key recovery services. Therefore, esFIRMA will not be liable under any circumstances 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 electronic signature function)

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. Optional

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 CA 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 centrally managed.
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 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 applications listed below:

g) Secure email signature.

h) Other digital signature applications.

esFIRMA does not offer backup or key recovery services. Therefore, esFIRMA will not be liable under any circumstances 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 electronic signature function)

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. Optional

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

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.7.5	In the hierarchy of the CA esFIRMA
0.4.0.2042.1.2	In accordance with NCP+ policy

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

These certificates work with a secure signature creation device, in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council, of 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 backup or key recovery services. Therefore, esFIRMA will not be liable under any circumstances 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. Optional

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 CA 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 backup or key recovery services. Therefore, esFIRMA will not be liable under any circumstances 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 electronic signature function)
   c. Key encryption

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

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

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 CA 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 centrally managed.

esFIRMA does not offer backup or key recovery services. Therefore, esFIRMA will not be liable under any circumstances 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 electronic signature function)

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. Optional

1.4.2 Limits and prohibitions on the use of certificates

Certificates are used for their own function and established purpose, and may not be used for other functions and for other purposes.

Similarly, certificates 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 certificate issuance, renewal, suspension, or revocation, or to sign public key certificates of any kind, or to sign certificate revocation lists (CRLs).

The certificates have not been designed, cannot be used for and are not authorized for use or resale as hazardous situation control equipment or for uses that require fail-safe actions, such as the operation of nuclear facilities, air navigation or communications systems, or weapons 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 https://www.esfirma.com

The use of 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 use for the appropriate legal purposes, and exempts esFIRMA from any liability for this improper use, whether of the signatory or any third party.

esFIRMA has no access authorisation or legal obligation to supervise the data on which the use of a certified key may 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 on said content, therefore the subscriber, the signatory or the person responsible for the custody assumes any responsibility arising from the content associated with the use of a certificate.

Likewise, the subscriber, the signatory or the person responsible for the custody shall be responsible for any liability that may arise from the use of the same outside the limits and conditions of use set out in this DPC, the legal documents binding with each certificate, or the contracts or agreements with the registration entities or their subscribers. as well as any other improper use of the same derived from this section or that may 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 thereof that the company ESPUBLICO makes available to the subscriber.

1.4.3 Issuance of test certificates

esFIRMA issues test certificates under the production hierarchy, in order to carry out technical interoperability tests and allow their evaluation by the supervisory body.

The data contained in the test certificates are fictitious and conform to the guidelines issued by the supervisory body.

These test certificates are not legally valid, so esFIRMA is exempt from any liability as a result of their use by third parties.

1.5 Policy Management

1.5.1 Organization administering the document

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

Registration Identification	Zaragoza Mercantile Registry
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 Building)
50197 - ZARAGOZA
(+34) 976300110

1.5.3 Organisation approving the document

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

The esFIRMA Security Committee, made up of its Chairman, the Information and Service Manager and the esFirma Security Manager, is responsible for approving this Statement of Practice.

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

1.5.4 Document management procedures

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

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

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

The Security Office is responsible for the drafting, maintenance and administration of the DPC, the disclosure 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 is carried out at the request of its head according to the needs that arise.

esFirma may make changes that do not require notification when they do not directly affect the rights of the signatories and subscribers of the certificates or the subscribers of the seals.

When esFirma is going to introduce changes that modify the rights of the signatories and subscribers of the certificates and of the subscribers of seals, it must notify it publicly in order for them to present their comments to the Security Office within 15 days following the publication of future changes.

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

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

1.6 Acronyms and definitions

1.6.1. Acronyms

AC (*or also CA)*	*Certificate 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.* Distinctive name within the digital certificate
ID	National Identity Document
ETSI EN	*European Telecommunications Standards Institute – European Standard.*
EV (for SSL)	*Extended Validation* Extended validation, in SSL certificates.
FIPS	*Federal Information Processing Standard Publication*
HSM	*Hardware Security Module*
IETF	*Internet Engineering Task Force*
NIF	Tax Identification Number
NTP	*Network Time Protocol*
OCSP	*Online Certificate Status Protocol.* Certificate Status Access Protocol
OID	*Object Identifier*. Object Identifier
PDS	*PKI Disclosure Statements* .
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 Persons with a Qualified Signature/Seal Device
RFC	*Request for Comments* RFC Document
RSA	Rivest-Shamir-Adleman. Type of encryption algorithm
SHA	*Secure Hash Algorithm.* Secure Hashing Algorithm
SSL	*Secure Sockets Layer.* A protocol designed by Netscape and turned into 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*
VPN	*Virtual Private Network.* Virtual Private Network

1.6.2 Definitions

Certificate 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 mathematical value publicly known and used for the verification of a digital signature or the encryption of data.*
Private Key	*Mathematical value known only to the Subject/Signer and used for the creation of a digital signature or the decryption of data.* *The private key of the CA will be used for certificate signing and CRL signing.* *The TSA service private key will be used to sign the timestamps.*
CPS	*A 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 to activate the private key*
DCCF	*Qualified signature creation device. Software or hardware element, suitably certified, used by the Subject/Signatory for the generation of electronic signatures, so that cryptographic operations are carried out within the device and their 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 (completeness)* *b) that the person signing the data is who they say they are (identification)* *c) that the person signing the data cannot deny having done so*

	(non-repudiation in origin)
OID	*Unique numerical identifier registered under ISO standardization and referring to a specific object or class of object.*
Key pair	*A set formed by the public and private key, both mathematically related to each other.*
PKI	*A 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 an authorized 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 relies on the digital certificate and uses it as a means of accrediting the authenticity and integrity of the signed document*

2. Publication of information and deposit of certificates

2.1 Certificate deposit

esFIRMA has a Certificate Depository, in which information relating to 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 the control of esFIRMA, esFIRMA will make its best efforts to make the service available again within the period set out 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 Practice Statement.
- PKI Disclosure Statements (PDS), at least in Spanish and English.

2.3 Frequency of publication

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

Changes to the Statement of Certification Practices are governed by the provisions of 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 reading 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 Deposit, 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 that affect security requirements can be detected.

3. Identification and authentication

3.1 Initial registration

3.1.1 Types of names

All certificates contain a distinct 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 Public employee signature certificate, high level, on card

Country (C)	"IS"
Organization (O)	Name ("official" name) of the Administration, body, public law entity or other entity subscribing to the certificate, to which the employee is linked
organizationalUnitName (OU)	ELECTRONIC CERTIFICATE OF PUBLIC EMPLOYEE
organizationIdentifier	Identifier of the organization according to the technical standard ETSI EN 319 412-1
Surname	First and second (optional) surname, according to identity document (DNI/Passport)
Given Name	First name, according to identity document (DNI/Passport)
Serial Number	Employee's DNI/NIE
Common Name (CN)	Name Surname1 Surname2 – Employee's NIF
Type of certificateOID: 2.16.724.1.3.5.7.1.1	QUALIFIED CERTIFICATE OF SIGNATURE OF HIGH-LEVEL PUBLIC EMPLOYEE
Name of the subscribing entityOID: 2.16.724.1.3.5.7.1.2	Name of the subscribing entity
Subscriber NIF OID: 2.16.724.1.3.5.7.1.3	NIF entity subscription
DNI/NIE of the person in charge OID: 2.16.724.1.3.5.7.1.4	DNI or NIE of the person responsible
OID Battery Name: 2.16.724.1.3.5.7.1.6	First name of the certificate maintainer

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, intermediate 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	Identifier of the organization according to the technical standard ETSI EN 319 412-1
Surname	First and second (optional) surname, according to identity document (DNI/Passport)
Given Name	First name, according to identity document (DNI/Passport)
Serial Number	Employee's DNI/NIE
Common Name (CN)	Name Surname1 Surname2 – Employee's NIF
Type of certificateOID: 2.16.724.1.3.5.7.2.1	ELECTRONIC CERTIFICATE OF MID-LEVEL PUBLIC EMPLOYEE
Name of the subscribing entityOID: 2.16.724.1.3.5.7.2.2	Name of the subscribing entity
NIF subscriber entityOID: 2.16.724.1.3.5.7.2.3	NIF subscribing entity
DNI/NIE of the person in charge OID: 2.16.724.1.3.5.7.2.4	DNI or NIE of the person responsible
OID Personal Authentication Number: 2.16.724.1.3.5.7.2.5	NRP or PIN of the Certificate Subscriber's Maintainer
OID Battery Name: 2.16.724.1.3.5.7.2.6	First name of the certificate maintainer
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 Public employee authentication certificate, high level, on card

Country (C)	"IS"
Organization (O)	Name ("official" name) of the Administration, body, public law entity or other entity subscribing to the certificate, to which the employee is linked
organizationalUnitName (OU)	ELECTRONIC CERTIFICATE OF PUBLIC EMPLOYEE
organizationIdentifier	Identifier of the organization according to the technical standard ETSI EN 319 412-1
Surname	First and second (optional) surname, according to identity document (DNI/Passport)
Given Name	First name, according to identity document (DNI/Passport)
Serial Number	Employee's DNI/NIE
Common Name (CN)	Name Surname1 Surname2 – Employee's NIF
Type of certificateOID: 2.16.724.1.3.5.7.1.1	ELECTRONIC CERTIFICATE OF PUBLIC EMPLOYEE WITH A HIGH LEVEL OF AUTHENTICATION
Name of the subscribing entityOID: 2.16.724.1.3.5.7.1.2	Name of the subscribing entity
Subscriber NIF OID: 2.16.724.1.3.5.7.1.3	NIF entity subscription
DNI/NIE of the person in charge OID: 2.16.724.1.3.5.7.1.4	DNI or NIE of the person responsible
OID Battery Name: 2.16.724.1.3.5.7.1.6	First name of the certificate maintainer
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 Certificate of organ seal, intermediate level, in software

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

3.1.1.5 Organ seal certificate, intermediate level, in HSM

Country (C)	"IS"
Organization (O)	Subscriber's name ("official" name)
organizationalUnitName (OU)	ELECTRONIC SEAL
organizationIdentifier	Identifier of the organization according to the technical standard ETSI EN 319 412-1
Serial Number	DNI/NIE of the subscribing organisation
Common Name (CN)	Naming of the system or application of an automatic process.
Type of certificateOID: 2.16.724.1.3.5.6.2.1	MID-LEVEL ELECTRONIC SEAL
Name of the subscribing entity OID: 2.16.724.1.3.5.6.2.2	Name of the subscribing entity
NIF subscriber entityOID: 2.16.724.1.3.5.6.2.3	NIF subscribing entity
System nameOID: 2.16.724.1.3.5.6.2.5	System name

3.1.1.6 Certificate of signature of a public employee with a pseudonym, high level, on a 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	Identifier of the organization according to the technical standard ETSI EN 319 412-1
Pseudonym	Mandatory pseudonym according to ETSI EN 319 412-2 for this type of certificate
Common Name (CN)	Pseudonym and the Agency
Type of certificateOID: 2.16.724.1.3.5.4.1.1	ELECTRONIC CERTIFICATE OF PUBLIC EMPLOYEE WITH A HIGH-LEVEL PSEUDONYM
Name of the subscribing entityOID: 2.16.724.1.3.5.4.1.2	Name of the subscribing entity
NIF subscriber entityOID: 2.16.724.1.3.5.4.1.3	NIF subscribing entity
Pseudonym OID: 2.16.724.1.3.5.4.1.12	Pseudonym used by the signatory and authorized by the subscriber

3.1.1.7 Certificate of signature of public employee with pseudonym, intermediate 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	Identifier of the organization according to the technical standard ETSI EN 319 412-1
Pseudonym	Mandatory pseudonym according to ETSI EN 319 412-2 for this type of certificate
Common Name (CN)	Pseudonym and the Agency

Type of certificateOID: 2.16.724.1.3.5.4.2.1	ELECTRONIC CERTIFICATE OF PUBLIC EMPLOYEE WITH A MID-LEVEL PSEUDONYM
Name of the subscribing entityOID: 2.16.724.1.3.5.4.2.2	Name of the subscribing entity
NIF subscriber entityOID: 2.16.724.1.3.5.4.2.3	NIF subscribing entity
Pseudonym OID: 2.16.724.1.3.5.4.2.12	Pseudonym used by the signatory 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, public law entity or other entity subscribing to the certificate, to which the employee is linked
organizationalUnitName (OU)	ELECTRONIC CERTIFICATE OF PUBLIC EMPLOYEE
organizationIdentifier	Identifier of the organization according to the technical standard ETSI EN 319 412-1
pseudonym	Mandatory Pseudonym according to ETSI EN 319 412-2
Common Name (CN)	Position or position or "PSEUDONYM" – IDENTIFICATION NUMBER – OFFICIAL NAME OF THE ORGANIZATION
Type of certificateOID: 2.16.724.1.3.5.4.1.1	CERTIFICATE OF AUTHENTICATION OF PUBLIC EMPLOYEE WITH PSEUDONYM
Name of the subscribing entityOID: 2.16.724.1.3.5.4.1.2	Name of the subscribing entity
NIF subscriber entityOID: 2.16.724.1.3.5.4.1.3	NIF subscribing entity

3.1.1.9 TSA/TSU Electronic Seal Certificate

Country (C)	"IS"
Organization (O)	Subscriber's name ("official" name)
organizationIdentifier	Identifier of the organization according to the technical standard ETSI 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

Spain Subprofile:

Country (C)	"IS"
Organization (O)	Name ("official" name) of the entity subscribing to the certificate, to which the employee is linked
organizationIdentifier	Identifier of the organization according to the technical standard ETSI EN 319 412-1
Surname	First and second (optional) surname, according to identity document (DNI/Passport)
Given Name	First name, according to identity document (DNI/Passport)
Serial Number	DNI/NIE of the individual
Common Name (CN)	Surname1 Surname2 Name – NIF natural person (SIGNATURE)
OID Certificate Type : 1.3.6.1.4.1.47281.0.7.1	CERTIFICATE OF NATURAL PERSON LINKED TO ENTITY
Name of the subscribing entity OID: 1.3.6.1.4.1.47281.0.7.2	Name of the subscribing entity
Subscriber NIF OID: 1.3.6.1.4.1.47281.0.7.3	NIF entity subscription
DNI/NIE of the person in charge OID : 1.3.6.1.4.1.47281.0.7.4	DNI or NIE of the person responsible
OID Battery Name : 1.3.6.1.4.1.47281.0.7.6	First name of the certificate maintainer
First surname OID: 1.3.6.1.4.1.47281.0.7.7	First surname of the person responsible for the certificate
Second surname OID: 1.3.6.1.4.1.47281.0.7.8	Second surname of the person responsible for the certificate. Optional.
Email OID: 1.3.6.1.4.1.47281.0.7.9	Email of the person responsible for the certificate. Optional.

Europe Subprofile:

Country (C)	Country
Organization (O)	Name ("official" name) of the entity subscribing to the certificate, to which the employee is linked
organizationIdentifier	Identifier of the organization according to the technical standard ETSI EN 319 412-1
Surname	First and second (optional) surname, according to identity document

Given Name	First name, according to identity document
Serial Number	Identity document number of the natural person
Common Name (CN)	Surname1 Surname2 First Name – document number (SIGNATURE)
OID Certificate Type : 1.3.6.1.4.1.47281.0.19.1	PV
Name of the subscribing entity OID: 1.3.6.1.4.1.47281.0.19.2	It corresponds to the organization of the subject
OID Subscribing Entity Identifier : 1.3.6.1.4.1.47281.0.19.3	Corresponds to the subject's organizationIdentifier
OID Controller ID : 1.3.6.1.4.1.47281.0.19.4	DNI or NIE of the person responsible
OID Battery Name : 1.3.6.1.4.1.47281.0.19.6	First name of the certificate maintainer
First surname OID: 1.3.6.1.4.1.47281.0.19.7	First surname of the person responsible for the certificate
Middle Last Name OID: 1.3.6.1.4.1.47281.0.19.8	Second surname of the person responsible for the certificate. Optional.
Unit of the subscribing entity OID: 1.3.6.1.4.1.47281.0.19.10	Corresponds to the subject's OrganizationUnit. Optional

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

Spain Subprofile:

Country (C)	"IS"
Organization (O)	Name ("official" name) of the subscribing entity, to which the employee is linked
organizationIdentifier	Identifier of the organization according to the technical standard ETSI EN 319 412-1
Surname	First and second (optional) surname, according to identity document (DNI/Passport)
Given Name	First name, according to identity document (DNI/Passport)
Serial Number	Employee's DNI/NIE
Common Name (CN)	Surname1 Surname2 First Name – NIF natural person
OID Certificate Type : 1.3.6.1.4.1.47281.0.7.1	CERTIFICATE OF NATURAL PERSON LINKED TO ENTITY

Name of the subscribing entity OID: 1.3.6.1.4.1.47281.0.7.2	Name of the subscribing entity
Subscriber NIF OID: 1.3.6.1.4.1.47281.0.7.3	NIF entity subscription
DNI/NIE of the person in charge OID : 1.3.6.1.4.1.47281.0.7.4	DNI or NIE of the person responsible
OID Battery Name : 1.3.6.1.4.1.47281.0.7.6	First name of the certificate maintainer
First surname OID: 1.3.6.1.4.1.47281.0.7.7	First surname of the person responsible for the certificate
Second surname OID: 1.3.6.1.4.1.47281.0.7.8	Second surname of the person responsible for the certificate. Optional.
Email OID: 1.3.6.1.4.1.47281.0.7.9	Email of the person responsible for the certificate. Optional.

Europe Subprofile:

Country (C)	Country
Organization (O)	Name ("official" name) of the entity subscribing to the certificate, to which the employee is linked
organizationIdentifier	Identifier of the organization according to the technical standard ETSI EN 319 412-1
Surname	First and second (optional) surname, according to identity document
Given Name	First name, according to identity document
Serial Number	Identity document number of the natural person
Common Name (CN)	Surname1 Surname2 First Name – document number
OID Battery Name : 1.3.6.1.4.1.47281.0.19.6	Certificate Maintainer's First Name, corresponds to Given Name
First surname OID: 1.3.6.1.4.1.47281.0.19.7	First surname of the person responsible for the certificate
Middle Last Name OID: 1.3.6.1.4.1.47281.0.19.8	Second surname of the person responsible for the certificate. Optional.

3.1.1.12 Certificate of authentication of linked natural person, on card

Spain Subprofile:

Country (C)	"IS"

Organization (O)	Name ("official" name) of the entity subscribing to the certificate, to which the employee is linked
organizationIdentifier	Identifier of the organization according to the technical standard ETSI EN 319 412-1
Surname	First and second (optional) surname, according to identity document (DNI/Passport)
Given Name	First name, according to identity document (DNI/Passport)
Serial Number	Employee's DNI/NIE
Common Name (CN)	Surname1 Surname2 Name – NIF natural person (AUTHENTICATION)
OID Certificate Type : 1.3.6.1.4.1.47281.0.7.1	CERTIFICATE OF NATURAL PERSON LINKED TO ENTITY
Name of the subscribing entity OID: 1.3.6.1.4.1.47281.0.7.2	Name of the subscribing entity
Subscriber NIF OID: 1.3.6.1.4.1.47281.0.7.3	NIF entity subscription
DNI/NIE of the person in charge OID : 1.3.6.1.4.1.47281.0.7.4	Corresponds to the subject's SerialNumber
OID Battery Name : 1.3.6.1.4.1.47281.0.7.6	First name of the certificate maintainer
First surname OID: 1.3.6.1.4.1.47281.0.7.7	First surname of the person responsible for the certificate
Second surname OID: 1.3.6.1.4.1.47281.0.7.8	Second surname of the person responsible for the certificate. Optional.
Email OID: 1.3.6.1.4.1.47281.0.7.9	Email of the person responsible for the certificate. Optional.

Europe Subprofile:

Country (C)	Country
Organization (O)	Name ("official" name) of the entity subscribing to the certificate, to which the employee is linked
organizationIdentifier	Identifier of the organization according to the technical standard ETSI EN 319 412-1
Surname	First and second (optional) surname, according to identity document
Given Name	First name, according to identity document
Serial Number	Identity document number of the natural person

Common Name (CN)	Surname1 Surname2 First Name – document number (AUTHENTICATION)
OID Battery Name : 1.3.6.1.4.1.47281.0.19.6	Certificate Maintainer's First Name, corresponds to Given Name
First surname OID: 1.3.6.1.4.1.47281.0.19.7	First surname of the person responsible for the certificate
Middle Last Name OID: 1.3.6.1.4.1.47281.0.19.8	Second surname of the person responsible for the certificate. Optional.

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

Spain Subprofile:

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

Europe Subprofile:

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

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

Spain Subprofile:

Country (C)	"IS"

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

Europe Subprofile:

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

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

Spain Subprofile:

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

Europe Subprofile:

Country (C)	Country
Organization (O)	Name ("official" name) of the entity subscribing to the certificate, to which the employee is linked
organizationIdentifier	Identifier of the organization according to the technical standard ETSI EN 319 412-1
pseudonym	Mandatory Pseudonym according to ETSI EN 319 412-2

Common Name (CN)	PSEUDONYM - ENTITY NAME

3.1.1.16 Electronic seal certificate, in software

Spain Subprofile:

Country (C)	"IS"
Organization (O)	Subscriber's name ("official" name)
organizationalUnitName (OU)	ELECTRONIC SEAL
organizationIdentifier	Identifier of the organization according to the technical standard ETSI EN 319 412-1
Serial Number	DNI/NIE of the subscribing organisation
Common Name (CN)	Naming of the system or application of an automatic process.

Europe Subprofile:

Country (C)	Country
Organization (O)	Subscriber's name ("official" name)
organizationIdentifier	Identifier of the organization according to the technical standard ETSI EN 319 412-1
Serial Number	Subscribing Organization Identification (legalPersonSemanticsIdentifier)

3.1.1.17 Electronic seal certificate with centralized management

Spain Subprofile:

Country (C)	"IS"
Organization (O)	Subscriber's name ("official" name)
organizationalUnitName (OU)	ELECTRONIC SEAL
organizationIdentifier	Identifier of the organization according to the technical standard ETSI EN 319 412-1
Serial Number	DNI/NIE of the subscribing organisation
Common Name (CN)	Naming of the system or application of an automatic process.

Europe Subprofile:

Country (C)	Country
Organization (O)	Subscriber's name ("official" name)

organizationIdentifier	Identifier of the organization according to the technical standard ETSI EN 319 412-1
Serial Number	Subscribing Organization Identification (legalPersonSemanticsIdentifier)

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

Under no circumstances may pseudonyms be used to identify an entity/enterprise/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 construed in accordance with the law of the country of establishment of the subscriber, on their own terms.

The "country" field will always be Spain because the certificates are 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 the person authorized to use it.

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

3.1.5 Uniqueness of names

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

A subscriber name that has already been used may not be assigned to a different subscriber, a situation that, in principle, does not have to occur, thanks to the presence of the Tax Identification Number, or equivalent, in the naming scheme.

A subscriber can request more than one certificate as long as the combination of the following values in the request is 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.
- Type of Certificate (Certificate Description Field).

3.1.6 Resolution of naming disputes

Applicants for certificates shall not include names in applications that may infringe the rights of third parties by the future subscriber.

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

And 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, in the event of receiving a notification regarding a name conflict, in accordance with the law of the subscriber's country, it 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 name conflict.

Any controversy or conflict arising from this document shall be definitively resolved by arbitration by law of an arbitrator, within the framework of the Spanish Court of Arbitration, in accordance with its Rules and Statutes, 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 formalises the service.

3.2 Initial identity validation

The identity of the certificate subscribers is established at the time of signing the contract between esFIRMA and the subscriber or prior to the activation of the esFIRMA service, at which 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 by the corporate records of the Administration, body, public law entity or other entity subscribing to the certificates. The subscriber shall produce a certification of the necessary data, and shall send it to esFIRMA, by the means enabled by it, 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 the FIRM in charge of the processing of said data.

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

[1] ETSI EN 319 411-1 Ap 6.2.2.2.q)

3.2.1 Proof of Private Key Possession

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.

3.2.2 Entity identification

In public administrations, documentation accrediting the existence of the public administration, body or entity under public law is not required, since such identity is part of the corporate scope of the General State Administration or other State Public Administrations.

EsFIRMA verifies the existence of each Public Administration, body or entity under 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).

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

Individuals 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 prior situation of legal or voluntary representation between the natural person and the Administration. body, public law entity or other entity subscribing to the certificates, which requires their recognition by esFIRMA, which will be carried out by one of the following procedures:

1. In the event that the person holding the position of Secretary has the power of public faith, the following documents will be collected and verified:
    a. Certificate from the Secretary appointing the legal representative, with the following information:
        i. Name and surname of the legal representative

    ii. Document: NIF of the representative
    iii. CIF of the entity you represent
    iv. Name of the entity you represent
    v. Mailing address of the entity you represent

2. In the event that the person holding the position of Secretary does not have the power of public faith, the following documents will be collected and verified:
    a. A certificate from the Secretary of the appointment of the legal representative containing the following information:
        i. Representative details:
            1. Name and surname of the legal representative
            2. Document: NIF of the representative
        ii. Details of the entity you represent:
            1. CIF
            2. Name
            3. Mailing address
        iii. Information on the validity of the representation
    b. Official documentation that allows accrediting the data relating to the representation or capacity to act held by the legal representative.
    c. All the documents necessary to prove the aforementioned points in a reliable manner in accordance with the provisions of the applicable administrative law regulations, and their registration in the corresponding public registry if required.

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

Once the documents have been signed electronically, the AR functions will be activated for the entity's users who are listed in the contract as operators authorized to perform this function.

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.

The procedure for requesting and generating certificates is carried out through an electronic procedure on the Electronic Administration Platform available to the subscriber and 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. Application by the individual through the Electronic Administration Platform (with its corresponding entry record and opening of the file).
2. A certificate in which the verification Operator certifies the link between the applicant and the entity.
3. Issuance order signed by the Verification and Authorization Operator of the entity, which is registered at the outset and notified to ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (attaching a copy of the certificate and the user's request).

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

1. Order of issuance of the Legal Representative through the Electronic Administration Platform (with its corresponding entry record and opening of file). To submit such an application, the Legal Representative must identify themselves on the platform using electronic identification means, 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.

3.2.3.1 In certificates

The identification information of the natural persons identified in the certificates is validated by comparing the information in 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

Direct physical presence is not required to apply for certificates due to the already accredited relationship between the natural person and the Administration, body, public law entity or other entity to which he or she is linked. This accreditation is reflected in the validation of the request by the Verification Operator authorized by the subscriber, which states the face-to-face and unequivocal identification of the signatory.

To accept the certificate, the direct physical presence of the signatory is not necessary, since this can be done by means of an advanced electronic signature. During this procedure, the identity of the natural person identified in the certificate is confirmed.

The certificate must be issued within a maximum period of 15 calendar days from the validation of the identity of the natural person by the verification and authorization operator. Therefore, if 15 calendar days have elapsed since the verification and authorization operator validates the applicant's identity and orders the issuance, the applicant does not accept their certificate, the process will expire, and the individual must make a new application.

3.2.3.3 Relationship of the natural person

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

3.2.4 Unverified subscriber information

esFIRMA does not include any unverified subscriber information in 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 requests

3.3.1 Validation for routine certificate renewal

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

3.3.2 Identification and Authentication of Renewal After Revocation

esFIRMA does not renew certificates.

3.4 Identification and authentication of the revocation request

Requests and reports relating to the revocation of a certificate are authentic, verifying that they come from an authorised person.

Acceptable methods for such testing 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 personal authentication methods, which consists of information known only to the natural person identified in the certificate, and which allows you to automatically revoke your certificate.
- Physical appearance at an office of the subscribing entity.
- Other means of communication, such as telephone, when there are reasonable guarantees of the identity of the applicant for the revocation, in the opinion of esFIRMA.

esFIRMA does not place certificate holds. Petitions for suspension are treated as petitions for revocation.

4. Certificate Lifecycle Operation Requirements

4.1 Certificate Application

4.1.1 Legitimacy to request the issuance

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

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

There is an authorization from the subscriber for the applicant to make the request, which is legally instrumented by means of a certificate application form signed by the 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.

Applications are made by means of a document in electronic format, completed by the Administration, body, public law entity or other entity, whose recipient is esFIRMA, which will include the data of the people to whom certificates will be issued. The request will be made by the operator authorised 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 justifying 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 attached that allows the contact of the natural person identified in the certificate.

4.2 Processing the certification application

4.2.1 Performing identification and authentication functions

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

If so, 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 for a period of 15 years from the expiration of the certificate or the end of the service provided, even in the event of early loss of validity due to revocation, as the certificates are qualified.

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

4.2.2 Approval or rejection of the application

esFIRMA approves the request for the certificate and proceeds to its issuance and delivery, following the request that occurs on the Electronic Administration Platform.

In the event 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 will stop its approval until it has carried out the complementary checks it deems appropriate.

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

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

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

4.2.3 Deadline for resolving the application

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

Applications remain active until they are approved or rejected.

4.3 Issuance of the certificate

4.3.1 Actions of the CA during the issuance process

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

During the process, it is SIGNATURE:

- Protects the confidentiality and integrity of the registration data available to you.
- 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 the registration information, including the certified public key.
- It ensures that the certificate is issued by systems that use protection against forgery and that guarantee the confidentiality of the keys during the process of generating those keys.
- It includes in the certificate the information established in Annex 1 of Regulation (EU) 910/2014, in accordance with the provisions of sections 3.1.1 and 7.1.
- Indicates the date and time a certificate was issued.

4.3.2 Notification of the issue to the subscriber

esFIRMA notifies 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 on the Electronic Administration Platform, of the issuance of the certificate.

4.4 Delivery and acceptance of the certificate

During this process, esFIRMA must carry out the following actions:

- Definitively prove 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.
    - Acknowledgement, 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 attribution to the signatory of their private key and certificate activation data, 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 on the certificate.

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

4.4.1 Conduct Constituting Acceptance of the Certificate

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

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

In the case of certificates issued on a card, these are sent to the subscriber's certification manager, and the corresponding PIN is sent 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 notify third parties of the issue.

4.5 Using the Key Pair and Certificate

4.5.1 Use by the Subscriber or Signatory

esFIRMA obliges the following:

- Provide esFIRMA with complete and adequate information, in accordance with the requirements of this Statement of Certification Practices, especially with regard to the acceptance procedure.
- To express their consent prior to the issuance and delivery of a certificate.
- Use the certificate in accordance with the provisions of section 1.4.
- Where the certificate works 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 prevent unauthorized use, in accordance with the provisions of sections 6.1, 6.2 and 6.4.
- Communicate to esFIRMA and to anyone who is believed to be able to rely on the certificate, without unjustifiable delays:
    - The loss, theft, or potential compromise of your private key.
    - Loss of control over your private key, due to 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 Certification Practice Statement.
- That no unauthorized person has ever had access to the certificate's private key, and that he is solely responsible for the damages caused by his breach of duty to protect the private key.
- That the signatory is an end 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), or Certificate Revocation List, certification service provider title, or otherwise.

4.5.2 Use by 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.
- To express their consent prior to the issuance and delivery of a certificate.
- Use the certificate in accordance with the provisions of section 1.4.
- Communicate to esFIRMA and to anyone the subscriber believes can rely on the certificate, without unjustifiable delays:
    - The loss, theft, or potential compromise of your private key.
    - Loss of control over your private key, due to 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, unauthorised use, theft or compromise, where any, of the card.
- To transfer to the natural persons identified in the certificate the fulfilment of their specific obligations, and to establish mechanisms to guarantee their effective compliance.
- Not to monitor, manipulate or perform reverse engineering acts 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 the 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 Certification Practice Statement.
- That no unauthorized person has ever had access to the certificate's private key, and that he is solely responsible for the damages caused by his breach of duty to protect the private key.
- That the subscriber is an end 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), or Certificate Revocation List, certification service provider title, or in any other case.

4.5.3 Use by the Certificate Relying Third Party

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

- Be independently advised about 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 on the status of the certificates.
- Verify all certificates in the certificate hierarchy, before trusting the digital signature or any of the certificates in the hierarchy.
- Recognize that to be considered a qualified certificate you must be included in the national Trusted List.
- 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.
- Be aware of any limitations on the use of the certificate, regardless of whether they are found in the certificate itself or in the contract of the third party relying on the certificate.
- Bear in mind any precautions established in a contract or other instrument, regardless of its legal nature.
- Not to monitor, manipulate or perform reverse engineering acts 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 relying on 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 relying or not on the information contained in the certificate.
- That it will be solely responsible if it fails to comply with its obligations as a third party relying on the certificate.

4.6. Renewal of certificates

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

4.6.1 Circumstances for Certificate Renewal

Not applicable.

4.6.2 Who can request a renewal

Not applicable.

4.6.3 Processing the Certificate Renewal Application

Not applicable.

4.6.4 Notification of new certificate issuance to the subscriber

Not applicable.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not applicable.

4.6.6 Publication of the renewal certificate by the CA

Not applicable.

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

other entities

Not applicable.

4.7 Renewing 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 appearance of the signatory and signature of the acceptance form, in those cases in which this is necessary due to the expiry of the legal identification period of 5 years.

Such appearance and identification shall be carried out in accordance with the provisions of section 3.2.

The signature of the acceptance sheet will be carried out in accordance with the provisions of section 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 issuance to third parties

esFIRMA does not notify third parties of the issue.

4.8 Modifying certificates

The modification of certificates shall be treated as a new issue of certificate, 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 for revocation of certificates

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

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

2) Circumstances affecting key or certificate security:
    a) Compromise of the private key, infrastructure, or systems of the certification service provider that issued the certificate, as long as it affects the reliability of the certificates issued from that incident.
    b) Infringement, by esFIRMA, of the requirements set out in the certificate management procedures, established in this Statement of Certification Practices.
    c) Compromise 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 led to 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, liability and guarantees, established in the corresponding legal document.
   - e) The supervening incapacity or death of the key holder.
   - f) The termination of the legal entity subscribing to the certificate, as well as the end of the subscriber's authorization to the key holder or the termination of the relationship between the subscriber and the person identified in the certificate.
   - g) Subscriber's request for revocation of the certificate, in accordance with the provisions of section 3.4.

4) Other circumstances:
   - a) The termination of the esFIRMA certification service, in accordance with the provisions of section 5.8.
   - b) The use of the certificate that is harmful and continuous for esFIRMA. In this case, a use is considered harmful based on the following criteria:
     - o The nature and number of complaints received.
     - o The identity of the entities that file the complaints.
     - o The relevant legislation in force at any given time.
     - o 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 Standing to request revocation

The following can request the revocation of a certificate:

- The person identified in the certificate, by means of a 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:

- Date of request for revocation.
- Identity of the subscriber or signatory.
- Detailed reason for the request for revocation.

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

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

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

In the event that the recipient of a request for revocation by a natural person identified in the certificate is the subscribing entity, once the request has been authenticated, the latter 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 in status of the revoked certificate.

[2] Paragraph 6.2.4.a) iii) of ETSI EN 319 411-1

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, in order to be used as support and guarantee of acceptance of the requested revocation.

4.9.4 Time limit for requesting revocation

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

4.9.5 Time Frame for Application Processing

Requests for revocation will be effective within a maximum period of 24 hours[4].

If, due to exceptional circumstances, it is not possible to confirm the request for revocation within this period of 24 hours, the revocation will be carried out as soon as possible; and must prepare a report on the circumstances that have prevented the revocation within the established period and the actions to be taken so that this situation is not repeated.

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

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

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

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

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

[4] 6.2.4-03a of ETSI EN 319 411-1

- *CA ROOT:*
    - 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 will need to verify the status of 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 Publication Deadline for CRLs

CRLs are published in the Deposit in a reasonable period immediately after their generation, which in no case exceeds a few minutes.

4.9.9 Availability of Online Certificate Health Check Services

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

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

In the event of failure of the certificate status check systems for reasons beyond the control of esFIRMA, the latter must make its best efforts to ensure that this service remains inactive for the minimum possible time, which may not exceed one day.

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

Certificate health check services are free to use[5].

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

4.9.10 Obligation to consult certificate health check services

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

esFIRMA supports the GET method for OCSP.

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

OCSP responses have a maximum expiration time of 48 hours.

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

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",* logging such requests as part of the esFIRMA security response procedures.

[5] ETSI EN 319 411-2 AP 6.3.10

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

4.9.11 Other forms of certificate revocation information

Alternatively, third parties relying on certificates will be able to check the revocation status of certificates by querying the most recent CRLs issued by esFIRMA. These are published on the esFIRMA website, as well as at the web addresses indicated on the certificates.

esFIRMA does not delegate its OCSP responses using OCSP stapling.

4.9.12 Special requirements in case of private key compromise

The compromise of the esFIRMA private key 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 for suspension of certificates

esFIRMA does not suspend certificates.

4.9.14 Request for suspension

esFIRMA does not suspend certificates

4.9.15 Procedures for the request for suspension

esFIRMA does not suspend certificates.

4.9.16 Maximum Period of Suspension

esFIRMA does not suspend certificates.

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 checked 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.

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

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

4.10.2 Availability of Services

Certificate health check services and time-stamping service are available 24/7, year-round, with the exception of scheduled shutdowns.

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 Key Deposit and Recovery

4.12.1 Key Deposit and Recovery Policy and Practices

esFIRMA does not provide key deposit and recovery services.

4.12.2 Session Key Wrapping and Retrieval Policy and Practices

No stipulation.

5. Physical, management, and operational security controls

5.1 Physical Security Controls

esFIRMA has established physical and environmental security controls to protect the resources of the facilities where the systems 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 device 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 (e-power, telecommunications, etc.)
- Collapse of the structure.
- Floods.
- Theft protection.
- Unauthorised departure of equipment, information, media and applications relating to components used for the services of the certification service provider.

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

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

5.1.1 Location and construction of the facilities

Physical protection is achieved by creating clearly defined security perimeters around services. The quality and robustness of the facility's construction materials ensures adequate levels of protection against brute force intrusions and is located in a low-disaster risk area and allows quick access.

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

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

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

5.1.2 Physical Access

The DPC where the esFIRMA CA is located has a TIER IV rating.

Physical access to the esFIRMA premises 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, including CCTV filming and archiving.

- Access to the rooms is via ID card readers.

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

5.1.3 Electricity and air conditioning

The esFIRMA facilities have current stabilizing equipment and a duplicated electrical supply system with a generator set.

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

5.1.4 Water Exposure

The facilities are located in a low-risk flood zone.

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 the storage media.

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

5.1.7 Waste treatment

The elimination of supports, both paper and magnetic, is carried out by means of mechanisms that guarantee the impossibility of retrieving the information.

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

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

5.1.8 Off-site 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 expressly authorised persons are required for access, deposit or removal of devices.

5.2 Procedural Controls

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

The staff at the service of esFIRMA executes the administrative and management procedures in accordance with the security policy.

5.2.1 Reliable Features

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 operational procedures. This is a person external to the Information Systems department. The tasks of the Internal Auditor are incompatible in time with the tasks of Certification and incompatible with Systems. These functions will be subordinate to the head of operations, reporting both to it and to the technical management.
- **System Administrator**: Responsible for the correct operation of the hardware and software support of the certification platform
- **CA Administrator**: Responsible for the actions to be carried out with the cryptographic material, or with the performance of any function that involves the activation of the private keys of the certificate authorities described in this document, or any of their elements.
- **CA Operator:** Jointly responsible with the CA Administrator for the custody of cryptographic key activation material, 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**: In charge of coordinating, controlling and enforcing the security measures defined by esFIRMA's security policies. You must be in charge of aspects related to information security: logical, physical, networking, organizational, etc.
- **Information and Service Manager**: Defines the requirements for information and services in terms of security. This role has the ultimate responsibility for the use made of the information and services and therefore for their level of protection.
- **Validation Specialist**: Responsible for the validation of certificate requests.
- **Revocation Officer:** Responsible for the operation of changing the status of the certificates.

The 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 root Certificate Authority keys.

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 he or she is assigned.

Each person only controls the assets necessary for their role, thus ensuring that no one person has access to unallocated resources.

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

5.2.4 Roles Requiring Separation of Duties

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.
- Implementation of the Certification Body.

5.2.5 PKI Management System

The PKI system is made up of the following modules:

- Management component/module of the Subordinate Certification Authority.
- Management component/module of the Registration Authority.
- Request management component/module.
- 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 checks

5.3.1 History, qualifications, experience, and clearance requirements

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

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

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

esFIRMA ensures that registration staff are reliable to perform registration tasks.

The Registry Operator has completed a preparation course for the performance of the tasks of validating the requests.

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

5.3.2 History Investigation Procedures

esFIRMA carries out background checks on potential employees before they are hired or enter the job.

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

The investigation will be repeated with sufficient periodicity.

All checks are carried out to the extent permitted by applicable applicable legislation. 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 submit to a prior investigation, warning that 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 under 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:

- Security principles and mechanisms of the certification hierarchy, as well as the user environment of the person to be trained.
- Tasks that the person must perform.
- esFIRMA's security policies and procedures. Use and operation of installed machinery and applications.
- Management and processing of security incidents and compromises.
- 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 staff training as needed, and with sufficient frequency to perform their duties competently and satisfactorily, especially when substantial modifications are made to certification tasks

5.3.5 Sequence and frequency of job turnover

Not applicable.

5.3.6 Penalties for Unauthorized Actions

esFIRMA has a sanctioning system to clarify the responsibilities arising from unauthorised actions, adapted to the applicable labour 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 severity of the unauthorized action.

5.3.7 Requirements for hiring professionals

Employees hired to perform reliable tasks sign the confidentiality clauses and operational requirements used by esFIRMA in advance. Any action that compromises the security 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 complied with by the third party that performs the functions of operating the certification services, however, the certification body will be responsible in all cases 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 will provide the documentation that its staff strictly needs at all times, in order to carry out their work in a competent and satisfactory manner.

5.4 Security audit procedures

5.4.1 Types of Logged Events

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

- Switching the system on and off.
- Attempts to create, delete, set passwords, or change privileges.
- Login and logout attempts.
- Attempts to gain unauthorized access to the CA system over the network.
- Unauthorized access attempts to the file system.
- Physical access to logs.

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

Registry entries include the following items:

- Date and time of entry.
- Serial number or sequence of the entry, in automatic registrations.
- Identity of the entity entering the record.
- Type of ticket.

[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 signatories or custodians are recorded[8].

5.4.2 Frequency of Audit Log Processing

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

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

esFIRMA maintains a system that allows it to guarantee:

- Sufficient space for log storage
- 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 stored in structured files that can be incorporated into a database for later exploration.

5.4.3 Audit Log Retention Period

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

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

5.4.4 Protecting 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 fireproof devices.
- Their availability is protected by storing them in facilities outside the centre where the CA is located.

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

5.4.5 Backup Procedures

esFIRMA has an appropriate backup procedure so that, in the event 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 for audit logs, making a weekly copy of all logs on an external medium. In addition, a copy is kept in an external custody center.

5.4.6 Locating the Audit Log Accumulation System

Event audit information is collected internally and in an automated manner by the operating system, network communications and certificate management software, as well as manually generated data, which will be stored by duly authorized personnel. All of this makes up the system of accumulating audit trails.

5.4.7 Notification of the audit event to the person causing the event

When the audit log accumulation system logs an event, you do not need 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 Analysis

The vulnerability analysis is covered by esFIRMA's audit processes.

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

The audit data of the systems is 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 ensures that all information relating to certificates is retained 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 registry entities):

- All system audit data (PKI, TSA, and OCSP).
- All data relating to the certificates, including contracts with signatories and data relating to their identification and location
- Requests for the issuance and revocation of certificates, including all reports relating to the revocation process[10].
- Any specific choices that the signatory or subscriber has during the subscription agreement[11].
- Type of document submitted in the certificate application.

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

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

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

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

5.5.2 Record retention period

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

5.5.3 File Protection

esFIRMA protects the file so that only duly authorised persons can gain access to it. The file is protected from viewing, modification, deletion or any other manipulation by storing it on a reliable system.

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

5.5.4 Backup Procedures

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

esFIRMA at a minimum performs daily incremental backups of all your electronic documents and makes full backups weekly for data recovery cases.

In addition, esFIRMA (or the organisations that perform the registration function) keeps a copy of the paper documents in a secure place different from the facilities of the Certification Body itself.

5.5.5 Date and Time Stamping Requirements

The records are dated with a reliable source via NTP.

esFIRMA has a procedure where it describes the configuration of the times of the equipment used in the issuance of certificates.
The time used to record the events in the audit log 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 centralised system for collecting information on the activity of the teams involved in the certificate management service.

5.5.7 Procedures for Obtaining and Verifying Archival Information

esFIRMA has a procedure that describes the process for verifying that the information on file is correct and accessible.

5.6 Key renewal

Before the use of the AC/SUBCA/TSA private key expires, a key change will be made. The old CA/SUBCA and its private key will only be used for CRL signing as long as there are active certificates issued by that CA/SUBCA. A new AC /SUBCA/TSA will be generated with a new private key and a new DN. The TSA's private key will be destroyed.

The change of subscriber passwords is carried out by carrying out a new issuance process.

[12] Paragraph 7.10.d) of ETSI EN 319 401

5.7 Key Compromise and Disaster Recovery

5.7.1 Procedures for managing incidents and commitments

Backups of the following information are stored in storage facilities external to esFIRMA, which are made available in case of compromise or disaster: technical data from certificate requests, audit data and database logs of all certificates issued.

Backups of esFIRMA private keys are generated and maintained in accordance with section 6.2.4

5.7.2 Resource, Application, or Data Corruption

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

5.7.3 Compromise of the entity's private key

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

In case of compromise of the esFIRMA private key, it may be the case that the statuses of the certificates and revocation processes using this key may not be valid[13]. In any case, all active certificates will be revoked, subsequently generating a final CRL that will include all revoked certificates, whether expired or not. The instructions for the validation of a certificate or time stamp will be published on the esFIRMA website.

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

[13] Paragraph 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 incident affects, in the event of replacement of the passwords, the recognitions by different applications and private and public services. A recovery in the effectiveness of the keys in business terms 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 failure to comply with 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 centre 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 stated as such 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 continuous maintenance of the records required to provide evidence of certification in the event of a civil or criminal investigation.

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

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

- It will notify the Ministry of Economic Affairs and Digital Transformation, at least 2 months in advance, of the cessation of its activity and the destination of the certificates, specifying whether the management is transferred and to whom, or if its validity will be extinguished.
- It will also notify the Ministry of Economic Affairs and Digital Transformation of the opening of any bankruptcy proceedings against esFIRMA as well as any other relevant circumstances that may prevent the continuation of the activity.
- It will inform all Signatories/Subscribers, trusted Third Parties and other CA's with which it has agreements or other types of relationship of the termination with a minimum of 6 months' notice.
- It shall revoke any authorisation for subcontracted entities to act on behalf of the CA in the procedure for issuing certificates.
- Destroy or disable the CA's private keys for use.
- 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 have expired, establishing the necessary means to guarantee their long-term conservation.

6. Technical security checks

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The key pair of the intermediate certification authority "ESFIRMA AC AAPP 2" is created by the root certification body "ESFIRMA AC ROOT 2" in accordance with the esFIRMA ceremony procedures, within the high-security perimeter intended for this task.

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

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

ROOT	4,096 bits	25 years
INTERMEDIATE	4,096 bits	13 years
- End-Entity Certificates	2,048 bits	2 years
- TSA Certificate	4,096 bits	5 years (2 years private key)

More information at the following PDS locations:

CERTIFICATE	PDS
Public Employee (FIRMA)	Spanish: https://esfirma.com/doc-pki/PDS-V2.0/PDS-AAPP-ES.pdf English: https://esfirma.com/doc-pki/PDS-V2.0/PDS-AAPP-EN.pdf
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	
Public Employee (AUTHENTICATION)	
Public Employee – High Level 1.3.6.1.4.1.47281.1.1.5	
Of Public Employee with Pseudonym (SIGNATURE)	
From EP with Pseudonym – High Level 1.3.6.1.4.1.47281.1.3.1	
From EP with Pseudonym – Intermediate Level 1.3.6.1.4.1.47281.1.3.4	
Pseudonymous Public Employee (AUTHENTICATION)	
Of Public Employee with Pseudonym – 1.3.6.1.4.1.47281.1.3.5	
Organ Seal	

CERTIFICATE	PDS
Organ Seal – Intermediate Level 1.3.6.1.4.1.47281.1.2.2	
Organ Seal – Centralized Middle Level *1.3.6.1.4.1.47281.1.2.4*	
From Individual linked to entity (FIRMA)	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
Entity-linked PF – Qualified F. 1.3.6.1.4.1.47281.1.6.1	
Entity-linked PF – F. Centralized 1.3.6.1.4.1.47281.1.6.4	
From a natural person linked to an entity (AUTHENTICATION)	
Of PF linked to an entity 1.3.6.1.4.1.47281.1.6.5	
From a natural person with a pseudonym linked to an entity (FIRMA)	
De PF with pseudonym linked to entity – Qualified Signature 1.3.6.1.4.1.47281.1.7.1	
De PF with pseudonym linked to entity – Firma Centralizado 1.3.6.1.4.1.47281.1.7.4	
From a Person with a pseudonym, linked to an entity (AUTHENTICATION)	
From PF with a pseudonym, linked to an entity 1.3.6.1.4.1.47281.1.7.5	
Electronic Seal	
Electronic Seal in 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

CERTIFICATE	PDS
	English: https://esfirma.com/doc-pki/PDS-V1.5/TSADS-EN.pdf
E-Seal for TSA/TSU in HSM 1.3.6.1.4.1.47281.1.5.2	

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

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

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

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

6.1.2 Sending the Private Key to the Signer

In certificates on a secure signature device, the private key is properly protected inside the secure device.

In software certificates, the signatory's private key is created in the computer system used by this signatory when they make the certificate request, so the private key is properly protected inside the signatory'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 sent to the certification service provider comes from a pair of keys generated by that DCCF.[14]

6.1.4 Distribution of the certification service provider's public key

The keys of esFIRMA are communicated to third parties who rely on certificates, ensuring the integrity of the key and authenticating its origin, by publishing them in the Depository.

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

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

6.1.5 Key sizes

The length of the root CA keys is RSA 4096 bits.
The key length of the subordinate CA is RSA 4096 bits.
The length of TSA keys is RSA 4096 bits.
The keys for end-entity certificates are either RSA 2048 or 4096-bit or 256-bit elliptic curve public key 1.2.840.10045.3.1.7 (NIST-P256/secp256r1).

6.1.6 Generation of Public Key Parameters and Quality Check

The public key of the Root CA, subordinate CAs, and subscriber certificates is encoded in accordance with RFC 5280.

Public Key Parameter Quality

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

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

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

6.1.7 Purposes of Using Keys

The key uses for CA certificates are exclusively for signing certificates and CRLs.

The uses of keys for 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 activation of the CA private key. In the case of this DPC, there is a policy of **3 out of 5** people for the activation of the passwords.

Cryptographic devices are physically protected as determined herein.

6.2.3 Private Key Deposit

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

6.2.4 Private Key Backup

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

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

Signer keys in hardware cannot be copied as they cannot leave the cryptographic device.

6.2.5 Private Key Archiving

CA private keys are archived for a period of **10 years** after the issuance of the last certificate. They will be stored in secure fireproof files and in the external custody center. At least two people will be required to recover 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 Certificate Authority are stored encrypted in the esFIRMA production cryptographic modules.

6.2.8 Private Key Activation Method

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

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

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

6.2.9 Private Key Deactivation Method

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

For their 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, the certificate of the public keys associated with them will be revoked.

Devices that have any part of the esFIRMA private keys stored will be physically destroyed or rebooted at a low level. For removal, the steps described in the cryptographic computer administrator's manual will be followed.

Finally, the backups will be securely destroyed.

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

The signatory's hardware keys may be destroyed by means of a special computer application in the premises of the RA or esFIRMA.

6.2.11 Classification of the Cryptographic Module

Cryptographic modules are subject to the engineering controls provided for in the standards outlined 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 carried out 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 your 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.

Likewise, esFIRMA securely generates the 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 Certificate Authorities are protected by the holders of the administrators cards of the cryptographic modules, as stated in the key ceremony document.

The signer of the certificate is responsible for the protection of their private key, with a password that is as complete as possible. The signer must remember this 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 computer controls and audits in order to establish 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 personnel, in the following aspects:

- Operating system security settings.
- Application security settings.
- Correct sizing of the system.
- User and Permissions Settings.
- Log Event Settings.
- Backup and recovery plan.
- Antivirus settings.
- Network traffic requirements.

6.5.1 Specific technical requirements for computer security

Each esFIRMA server includes the following functionalities:

- Access control to SubCA services and privilege management.
- Enforcing separation of duties for privilege management.
- Identification and authentication of roles associated with identities.
- Archiving of subscriber and SubCA history and audit data.
- Audit of security-related events.
- Security self-diagnosis related to SubCA services.
- SubCA key and system 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]

The verification of the 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.

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

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

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

6.5.2 Assessment of the level of IT security

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

6.6 Technical lifecycle controls

6.6.1 System Development Controls

The 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 correctness 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 training and the documents describing the processes are updated after approval by a group for security management. In carrying out this function, it has an annual training plan.

esFIRMA requires by contract, the equivalent security measures 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 catalogued 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 relating to the functions and responsibilities of the personnel involved in the control and handling of elements contained in the certification process.

Media treatment and security

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

System planning

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

Incident and response reports

esFIRMA has a procedure for monitoring incidents and their resolution.

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 are not confidential.

Access system management

esFIRMA makes every reasonable effort 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 using 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 in place to ensure that operations are carried out in compliance with the role policy.
- Each person has an associated role to perform the certification operations.
- The staff of esFIRMA is responsible for their actions through the confidentiality commitment signed with the company.

Certificate Generation

Authentication for the issuance process is carried out by means of a system of n operators for the activation of the esFIRMA private key.

Revocation Management

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

Revocation status

The revocation status application has access control based on certificate or two-factor authentication to prevent attempts to modify the revocation status information.

6.6.3 Life Cycle Security Assessment

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

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

esFIRMA records all the pertinent information of the device to add to the asset catalog.

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

esFIRMA carries out periodic tests to ensure the correct operation of the device.

The cryptographic hardware device is only tampered with by trusted personnel.
The esFIRMA private signing 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 authorised by the security manager and are reflected in the corresponding work reports. These configurations will be made by at least two trusted 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 through the use of firewalls.

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

6.8 Time Sources

esFIRMA has a 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 Observatory of the Navy) 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 signers with the RSA algorithm with a key length of 2048 bits with probable primes using the FIPS 186-4 B.3.6 algorithm and DRBG (Deterministic Random Bit Generator) in Real Random Mode (hardware noise) according to NIST SP 800-90A and continuous testing according to FIPS 140-2. Outside the HSM module, the keys are stored encrypted with the AES-GCM algorithm and a key length of 256 bits. The encryption key is derived from the HSM's user PIN and master key. The HSM master key uses the ECDSA NIST-P256/secp256r1 algorithm (OID 1.2.840.10045.3.1.7) and requires 3 out of 5 cards for activation and it was generated in a high-security initialization ceremony. The user PIN is derived from a server salt with the PBKDF2-SHA1 algorithm. The transport of the SAD (Signature Activation Data) from the SIC (Signature Interaction Component) to the SAM (Signature Activation Module) is protected by AES-GCM with a 256-bit key derived from a key exchange using the ECDH algorithm according to NIST SP 800-56A. The server key is published in the esFirma web repository, section "Remote Signature Security Information". The system allows the generation of electronic signatures with the RSA PKCS#1 v1.5 algorithm, DSA with elliptic curve key and SHA-256 and SHA-512 summary algorithm.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

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

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

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

7.1.1 Version Number

esFIRMA issues X.509 Version 3 certificates

7.1.2 Certificate Extensions

The 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 ID of the signing algorithm is:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption
- 1.2.840.10045.4.3.2 sha256WithECDSA

The object identifier of the public key algorithm is:

- 1.2.840.113549.1.1.1 rsaEncryption
- 1.2.840.10045.3.1.7 NIST-P256/secp256r1
-

7.1.4 Name Formatting

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

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 X.500 "Distinguished Names", which are unique and unambiguous.

7.1.6 Object Identifier (OID) of Certificate Types

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

7.1.7 Using the Policy Restrictions Extension

Not applicable

7.1.8 Policy, Syntax, and Semantic Qualifiers

Not applicable

7.1.9 Processing Semantics for Critical Extension of Certificate Policies

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

7.1.10 Element Length Restrictions

For all profiles, the following maximum character length restrictions are set for the following elements:

Element	Maximum Length esFIRMA	Longitude Base	Norm
2.5.4.42 *(givenName,GN)*	**127**	32000***	RFC5280
2.5.4.10 (organizationName)	**256**	64	RFC5280
2.5.4.11 (organizationalUnitName)	**256**	32	RFC5280
2.5.4.4 (surnames)	**256**	40	RFC5280
2.5.4.3 (commonName,CN)	**400**	64	RFC5280
2.5.4.5 (serialNumber,SN)	32*	32	RFC5280
2.5.4.97 (organizationIdentifier)	**32**	MAX**	X520
2.5.4.65 (pseudonym)	**64***	128	RFC5280
2.5.4.12 (title)	64*	64	RFC5280

*The ETSI standards EN 319 412-2 4.2.4 and ETSI EN 319 412-3 4.2.1 allow exceeding the limits set in RFC 5280 (provided that it is indicated in the DPC) for the subject fields indicated according to the type of certificate (givenName, surname, pseudonym, commonName, organizationName and organizationalUnitName), but not the rest of the fields. The length of these fields is in accordance with RFC 5280.
** MAX indicates that the upper limit is not specified (RFC5280 Appendix B. ASN1 Notes)
32000 ub-name used instead of ub-givenname (16)

The maximum lengths for all other elements are specified in RFC-5280

7.2 Certificate Revocation List Profile

According to the IETF RFC 3280 standard

7.2.1 Version Number

The CRLs issued by esFIRMA are version 2.

7.2.2 CRL and CRL extensions

crlExtensions:

2.5.29.35 (Authority key identifier)

2.5.29.20 (CRL Number)

crlEntryExtensions

2.5.29.21 (ReasonCode)

7.3 OCSP Profile

According to the IETF RFC 6960 standard

7.3.1 Version Number

The 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 start 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 Conformity Audit

esFIRMA carries out a compliance audit annually, in addition to the internal audits it conducts at its own discretion or at any time, due to a suspicion of non-compliance with a 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 greater 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 third-party auditing firm that demonstrates technical competence and experience in computer security, information systems security, and compliance audits of public key certification services, and related elements.

8.3 Auditor's relationship with the audited entity

Auditing companies are of recognised prestige with departments specialised in carrying out computer audits, so there is no conflict of interest that could distort their actions in relation to esFIRMA.

8.4 List of items subject to audit

The audit verifies with respect to this SIGNATURE:

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 are in accordance with what has been agreed by esFIRMA and with the provisions of current regulations.
d) That the entity adequately manages its information systems

In particular, the elements subject to audit will be the following:

a) CA processes, RAs 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 analysed 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 the senior management of esFIRMA who may carry out the following actions:

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

8.6 Handling of audit reports

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

9. Business and Legal Requirements

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fee

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

9.1.2 Certificate Access Fee

esFIRMA has not established any fee for access to the certificates.

9.1.3 Certificate Status Information Access Fee

esFIRMA has not established any fee 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 comply with its obligations, as well as to face the risk of liability for damages, as established in ETSI EN 319 401-1 7.12 c), in relation to the management of the termination of services and cessation plan.

9.2.1 Insurance Coverage

esFIRMA has a guarantee of sufficient coverage of its civil liability, through professional civil liability insurance that complies with the provisions of the regime of obligations and responsibilities of Regulation (EU) 910/2014, and with article 9.3.b) of Law 6/2020, of 11 November, regulating certain aspects of electronic trust services, with a minimum insured 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 guarantee of sufficient coverage of its civil liability, through professional civil liability insurance that complies with the provisions of the regime of obligations and responsibilities of Regulation (EU) 910/2014, and with article 9.3.b) of Law 6/2020, of 11 November, 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 any other personal information obtained for the issuance and maintenance of certificates, except for the information indicated in the following section.
- Private keys generated and/or stored by the certification service provider.
- Transaction logs, including full logs 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 operation plans, such as archiving, monitoring and other similar documents.

- 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 surnames of the natural person identified in the certificate, as well as any other circumstance or personal data of the holder, in the event that it is significant in terms of the purpose of the certificate.
- The email address of the natural person identified in the certificate, or the email address assigned by the subscriber, if significant in terms of the purpose of the certificate.
- The uses and economic limits outlined in the certificate.
- The validity period of the certificate, as well as the date of issue of the certificate and the expiry date.
- The serial number of the certificate.
- The different statuses or situations of the certificate and the start date of each of them, specifically: 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 not listed in the previous section.

9.3.3 Disclosure of Suspension and Revocation Information

See the previous section.

9.3.4 Legal Disclosure of Information

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

Specifically, the records that guarantee the reliability of the data contained in the certificate, as well as the records related to the reliability of the data and those related to the operation[17], will be disclosed if required to provide evidence of the certification in a legal 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 the 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 applicable, of the natural person identified in the certificate, directly to them or to third parties.

9.3.6 Other Circumstances of Disclosure of Information

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 set out in REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. and in Organic Law 3/2018, of 5 December, 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 legally obtained them from the appropriate party, under the conditions provided for in the regulations on electronic signatures and on the protection of personal data.

esFIRMA has the status of processor of personal data and, as such, processes the data solely and exclusively for the purposes contained in this Statement of Certification Practices in accordance with the instructions of the data controller, which is the SUBSCRIBER and which are included in Annex "*Annex 1: For the processing of personal*

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

data by ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A. in its capacity as PROCESSOR", 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 5 December, on the Protection of Personal Data and guarantee of digital rights, and has documented in this Statement 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. in its capacity as DATA PROCESSOR"* which governs the contract for the provision of the "Manage" service between the SUBSCRIBER and ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A., the aspects, procedures and security and organizational measures in compliance with the regime of obligations and responsibilities contained in the previous regulations.

9.4.2 Information Treated as Private

Personal information about an individual that is not publicly available on 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 non-private as it is necessary for the provision of the contracted service, without prejudice to the rights corresponding to the owner of the personal data under the LOPD/GDPR 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 established in this document, which are aligned with the obligations provided for in REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to processing of personal data and the free movement of these data and repealing Directive 95/46/EC, and Organic Law 3/2018, of 5 December, on the Protection of Personal Data and guarantee of digital rights.

9.4.5 Notice and Consent to Use of Private Information

Prior to entering into a contractual relationship, the interested parties shall be offered the

prior information about the processing of their personal data and exercise of rights, and where appropriate, they will obtain the mandatory consent for the differentiated treatment of the main processing for the provision of the contracted services.

9.4.6 Disclosure pursuant to judicial or administrative process

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

9.4.7 Other Circumstances of Disclosure of Information

Personal data is not transferred to third parties unless legally obliged.

9.5 Intellectual Property Rights

9.5.1 Ownership of Certificates and Revocation Information

Only esFIRMA has 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 licence to reproduce and distribute certificates, free of charge, provided that the reproduction is complete and does not alter any element of the certificate, and is necessary in relation to digital signatures and/or encryption systems within the scope of use of the certificate. and in accordance with the documentation that links them.

In addition, 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 Statement of Certification Practices

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

9.5.3 Ownership of Name Information

The subscriber and, where applicable, 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 the certificate signers.

When a key is broken 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.

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 relating to the use of the certificate, its price and its limitations of use, by means of a subscriber agreement that incorporates by reference the disclosure texts (PDS) of each of the certificates acquired.

The disclosure text document, also called PDS, complies with the content of Annex A of ETSI EN 319 411-1 v1.1.1 (2016-02), a document which can be transmitted by electronic means, using a means of communication that is durable over time, and in understandable language.

esFIRMA permanently communicates any changes[18] that occur in its obligations by publishing new versions of its legal documentation on its website https://www.esfirma.com

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

- 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, unless otherwise notified by the subscriber.
- Consent to the storage of the information used for the subscriber's registration and to the transfer of such information to third parties, in the event of termination of operations of the Certification Body without revocation of valid certificates.
- Certificate usage limits, 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 certificate can reasonably be trusted, which is applicable when the subscriber acts as a relying third party on the certificate.
- The manner in which the financial liability of the Certification Body is guaranteed.

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

- Applicable limitations of liability, including the uses for which the Certification Body accepts or excludes its liability.
- Period of archiving of certificate request information.
- Audit log archiving period.
- Applicable Dispute Resolution Procedures.
- Applicable law and competent jurisdiction.
- Whether the Certification Body has been declared compliant with the certification policy and, if applicable, in accordance with which system.

9.6.2. RA Obligation and Responsibility

The ARs are the entities delegated by the CA to carry out 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 in the exercise of their functions.
- Verify the identity of the Subjects/Signatories and Applicants of the certificates when necessary, definitively accrediting the identity of the Signatory, in the case of individual certificates, or of the key holder, in the case of organization 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 the 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.
- Archive, for the period provided for 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 for 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 Declaration of Practices of Applicable certification, as well as its obligations, powers and responsibilities.
- Provide information about the certificate and the cryptographic device.
- To collect information and evidence from the holder of receiving the certificate and, where appropriate, the cryptographic device, and acceptance of such elements.

- Inform the holder of the private key and their activation data of the certificate and, where appropriate, the cryptographic device of the exclusive imputation method, 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 the face-to-face verification points (PVP).

Information about subscriber usage and responsibilities is provided through the Acceptance of the use clauses prior to the confirmation of the request for the certificate and by email.

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

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

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

b) The adequate identification of the applicants, who must be qualified or qualified persons.

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 relationship of relationship or representation.

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

2.- Obligations once the certificate has been issued.

a) To sign the contracts for the Provision of Digital Certification Services with the applicants. In most issuance processes, this contract is formalized by accepting conditions on the websites that are part of the process

of issuance of the certificate, and the issuance cannot be carried out without first having accepted the conditions of use.

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

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

Thus, the RAs are responsible for the consequences in the event of non-compliance with their registration tasks, and through which they also undertake to respect the internal regulatory rules of the certifying body esFIRMA (Policies and CPS) which must be perfectly controlled by the RAs and which must serve as a reference manual.

In the event of a 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 CA may, by virtue of the agreements signed with the RAs, make the responsible RA bear the assumption of the consequences.

Because, although the CA is legally responsible to the Subject, an Entity, or User Party, and that for this purpose it has civil liability insurance, according to the current agreement, the RA has a contractual obligation to "correctly identify and authenticate the Applicant and, where appropriate, the corresponding Entity", and by virtue of this it must respond to this SIGNATURE for its breaches.

Of course, it is not the intention of esFIRMA to unload the entire burden of the assumption of responsibility to the RAs in terms of possible damages whose origin would come from a breach of the tasks delegated to the RAs. For this reason, as provided 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 for the conservation of the archives assumed by the RA through the performance of audits to evaluate, among others, the resources used and the knowledge and control of the operating procedures to offer the RA services.

The same responsibilities must be assumed by the RA by virtue of breaches of the delegated entities such as On-site Verification Points (PVPs), without prejudice to their right to have repercussions against them.

9.6.3 Assurances Offered to Subscribers and Third Parties Relying on Certificates

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

esFIRMA, at the very least, guarantees the subscriber:

- That there are no factual errors in the information contained in the certificates, known or made by the Certification Body.
- 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 established in the Statement of Certification Practices.
- That the revocation services and the use of the Deposit comply with all the material requirements set forth in the Statement of Certification Practices.

esFIRMA, at a minimum, will guarantee the third party relying on 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 Statement of Certification Practices have been met.
- The speed and security in the provision of services, especially revocation services.

In addition, esFIRMA guarantees the subscriber and the third party that relies on the certificate:

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

9.6.4 Liability and liability of third parties

It shall be the obligation of the User Party to comply with the provisions of the regulations in force and, in addition:

- Verify the validity of the certificates and the entire certification chain, before carrying out any operation based on them. esFIRMA has various mechanisms to carry out this verification, such as access to lists of revoked certificates or OCSP online consultation services.
- Know and be bound by and agree to be bound by the warranties, limits and responsibilities applicable to the acceptance and use of the certificates on which you rely.
- Check the validity of the qualification of a signature associated with a certificate issued by esFIRMA by verifying that the certificate authority that issued the certificate is published on the trusted list of the corresponding national supervisor.

9.6.5 Liability 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, such as
- as a result of changes in the circumstances reflected in the electronic certificate, when its inaccuracy could not be detected by the certification service provider
- Negligence with regard to the retention of signature creation data and its confidentiality.
- Not having requested revocation of the data of the electronic certificate in case of doubt about the maintenance of confidentiality
- Have used the signature after the validity period of the electronic certificate has expired
- Exceed the limits that appear in the electronic certificate.

- In conduct attributable to the User Party if the User acts negligently, i.e. when it fails to check or take into account the restrictions contained in the certificate as to its possible uses and limit on the amount of transactions; or when it does not take into account the validity status of the certificate
- Damages caused to the Subject or third parties entrusted to them due to 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 required.
- An inappropriate or fraudulent use of the certificate in the event that the Subject/Holder has assigned it or has authorized its use in favor of a third person by virtue of a legal transaction such as the mandate or power of attorney, being the exclusive responsibility of the Subject/Holder to control the keys associated with their certificate.

esFIRMA and its RAs will not be liable 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
- Due to 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 for revocation.
- By the content of the messages or documents signed or digitally encrypted.
- For the non-recovery of documents encrypted with the Subject's public key.

9.8. Limitation of Liability for Transaction Losses

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

9.9. Compensation

See section 9.2

9.10. Term and Completion

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 SPC shall be made by email 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 amend this document for technical reasons or to reflect any changes in procedures that have occurred due to legal requirements, regulations (eIDAS, National Supervisory Bodies, etc.) or as a result of work cycle optimization. Each new version of this CPS replaces all previous versions, which remain, however, applicable to certificates issued while those versions were in force and until the first expiration date of those certificates. At least one annual update will be published. These updates will be reflected in the version box at the beginning of the document.

Changes that may be made to this CPS do not require notification unless they directly affect the rights of the Subjects/Signatories of the certificates, in which case they may submit their comments to the organization of the administration of the policies within 15 days of publication.

9.12.2 Notification mechanism and deadlines

All proposed changes to this policy will be immediately published on the esFIRMA website. In this same document there is a section of changes and versions where you can find out about the changes that have occurred since its creation and the date of these modifications.

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 relying, affected Third Parties may submit their comments to the policy administration organization within 15 days of receiving the notification.

9.12.3 Circumstances in which the OID should be changed

Not stipulated

9.13 Dispute resolution procedure

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

9.14. Applicable legislation

esFIRMA establishes, in the subscriber agreement 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 who rely on the Certificates fully assume the content of this Statement of Certification Practices and Policies

9.16.2 Allocation

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

9.16.3 Separability

esFIRMA establishes, in the subscriber agreement, and in the disclosure text 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 continue to be in force after the termination of the legal relationship regulating the service between the parties. To this end, 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), continue after the termination of the service and the general conditions of issuance/use.
- By virtue of the clause of the entire agreement, 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 the facts.

9.16.4 Compliance (Attorneys' Fees and 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 eliminate the right of esFIRMA to enforce the same provisions later or the right to enforce
any other provision of this SPC. 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 Entity harmless from any damage arising from any action or omission that results in liability, damage or loss, expenses of any kind, including legal and legal representation expenses 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 by the user of the certificate when providing the application data, if the action or omission involved intent or negligence with respect to the Certification Body or any person relying on the certificate.
- Negligence in protecting the private key, employing a trusted system, or maintaining precautions necessary to prevent unauthorized compromise, loss, disclosure, modification, or use of the private key.
- Use by the subscriber of a name (including common names, e-mail address and domain names), or other information in the certificate, that infringes the 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 relying on the certificate undertakes to hold the Certification Body harmless from any damage arising from any action or omission resulting in liability, damage or loss, expenses of any kind, including legal and legal representation expenses 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 reliance on a certificate, in the light of the circumstances.

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

The third party relying on the certificate undertakes to hold ESFIRMA harmless from any damage arising from any action or omission resulting in liability, damage or loss, expenses of any kind, including legal and legal representation expenses 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 reliance on a certificate, depending on the circumstances.
- Failure to check the status of a certificate, to determine that it is not
is suspended or revoked.
- Failure to verify all the security measures prescribed in the
DCP or other applicable rules.

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