Certificate Practice Statement

esFIRMA

esFIRMA: Prácticas de Certificación

General Information

Document control

Security Category:	Public
Recipient Entity:	ESFIRMA
Version	1.10

Formal Status

Prepared by:	Reviewed by:	Approved by:
Security Office: Date: 02/06/2020	Security Manager Date: 04/06/2020	Security Committee Date: 08/06/2020

Version Control

Ver	Description of change	Date
1.0	Creation of documentation	29/04/2016
1.1	Remedies	02/06/2016
1.2	ETSI Review	19/05/2017
1.3	Review of types of certificates	
1.4	ETSI Review Review of types certificates 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 referring to signing on issuing of software certificates	08/08/2018
1.8	Adaptation for regulatory change (Regulation (EU) 910/2014 and Regulation (EU) 2016/679) and review of renovation sections.	13/11/2018
1.9	3.1.1.1 Second surname optionality clarification. 3.1.1.2 OrganizationIdentifier conditioned to CA/Browser Forum Guidelines 3.1.1.3 Fix OID Description typos 3.1.1.4 EV cert CN optional	14/06/2019
1.10	Clarifications 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 Contact person 1.5.2 moved to 1.5.3 Person determining CPS suitability for the policy "DEFINITIONS ACRONYMS" moved to 1.6 Definitions and acronyms 4.4.2 moved to 4.4.1 Conduct constituting certificate acceptance 4.4.3 moved to 4.4.2 Publication of the certificate by the CA 4.4.4 moved to 4.4.3 Notification of certificate issuance by the CA to other entities Added 4.6.1 Circumstance for certificate renewal Added 4.6.2 Who may request renewal Added 4.6.3 Processing certificate renewal requests Added 4.6.4 Notification of new certificate issuance to subscriber Added 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 certificate issuance by the CA to other entities Added 4.7.2 Who may request certification of a new public key 4.7. moved to 4.7.3 Processing certificate re-keying requests 4.7.3 moved to 4.7.4 Notification of new certificate issuance to subscriber 4.7.4 moved to 4.7.5 Conduct constituting acceptance of a re-keyed certificate 4.7.5 moved to 4.7.6 Publication of the re-keyed certificate by the CA 4.7.6 moved to 4.7.7 Notification of certificate issuance by the CA to other entities 4.11 moved to 4.10 Certificate status services 4.11.1 moved to 4.10.1 Operational characteristics 4.11.2 moved to 4.10.2 Service availability Added 4.10.3 Optional features 4.10 moved to 4.11 End of subscription 6.1.9 moved to 6.1.7 Key usage purposes (as per X.509 v3 key usage field) 6.2.9 moved to 6.2.9 Method of deactivating private key 6.2.10 moved to 6.2.10 Method of destroying private key Added 6.2.11 Cryptographic Module Rating Added 6.4.3 Other aspects of activation data	01/02/2020

	6.6.2.5 moved to 6.6.3 Life cycle security controls 6.9 moved to 6.8 Time-stamping Added 7.1.7 Usage of Policy Constraints extension Added 7.1.8 Policy qualifiers syntax and semantics Added 7.1.9 Processing semantics for the critical Certificate Policies extension Added 7.2.2 CRL and CRL entry extensions 7.2.2 moved to 7.3 OCSP profile Added 7.3.1 Version number(s) 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 deemed private Added 9.4.4 Responsibility to protect private information Added 9.4.5 Notice and consent to use private information Added 9.4.6. Disclosure pursuant to judicial or administrative process Added 9.4.7 Other information disclosure circumstances Added 9.6.2 RA representations and warranties 9.6.2 moved to 9.6.3 Subscriber representations and warranties Added 9.6.4 Relying party representations and warranties 9.6.2 moved to 9.6.5 Representations and warranties of other participants 9.6.3 moved to 9.7 Disclaimers of warranties 9.6.4 moved to 9.8 Limitations of liability 9.6.5 moved to 9.9 Indemnities Added 9.10 Term and termination Added 9.10.1 Term Added 9.10.2 Termination Added 9.10.3 Effect of termination and survival Added 9.11 Individual notices and communications with participants Added 9.12 Amendments Added 9.12.1 Procedure for amendment Added 9.12.2 Notification mechanism and period Added 9.12.3 Circumstances under which OID must be changed 9.6.10 moved to 9.13 Dispute resolution provisions 9.6.7 moved to 9.14 Governing law Added 9.15 Compliance with applicable law Added 9.16 Miscellaneous provisions Added 9.16.1 Entire agreement Added 9.16.2 Assignment 9.6. moved to 9.16.3 Severability Added 9.16.4 Enforcement (attorneys' fees and waiver of rights) 9.6.6 moved to 9.16.5 Force Majeure Added 9.17 Other provisions New certificates are included: public employee certificate (Authentication), public employee certificate with a pseudonym (Authentication), natural person linked to entity certificate (Authentication), natural person linked to entity certificate (SIGNATURE), natural person with pseudonym linked to entity certificate (Authentication), natural person with pseudonym linked to entity certificate (SIGNATURE)	

Index

1. Introduction

1.1. Overview

This document declares the certification practices for the electronic signing esFIRMA.

The certificates issued are the following:

- **De Empleado Público (FIRMA)**
  - De Empleado Público nivel Medio
  - De Empleado Público nivel Alto
- **De Empleado Público (AUTENTICACIÓN)**
  - De Empleado Público nivel Alto
- **De Empleado Público con seudónimo (FIRMA)**
  - De Empleado Público nivel Medio
  - De Empleado Público nivel Alto
- **De Empleado Público con seudónimo (AUTENTICACIÓN)**
  - De Empleado Público nivel Alto
- **De persona física vinculada a entidad (FIRMA)**
  - De persona física vinculada a entidad nivel Medio
  - De persona física vinculada a entidad nivel Alto
- **De persona física vinculada a entidad (AUTENTICACIÓN)**
  - De persona física vinculada a entidad nivel Alto
- **De persona física vinculada a entidad con seudónimo (FIRMA)**
  - De persona física vinculada a entidad nivel Medio
  - De persona física vinculada a entidad nivel Alto
- **De persona física vinculada a entidad con seudónimo (AUTENTICACIÓN)**
  - De persona física vinculada a entidad nivel Alto
- **De Sello de Órgano**
  - De Sello de Órgano nivel Medio
- **De Sede electrónica**
  - De sede electrónica administrativa nivel Medio
- **De Sello electrónico para TSA/TSU**
  - De sello electrónico para TSU en HSM

1.2 Document name and identification

This document is the esFIRMA "Certificate Practice Statement"

1.2.1 Certificate identifiers

Número OID	Políticas de certificados
	De Empleado Público (FIRMA)
1.3.6.1.4.1.47281.1.1.1	*De Empleado Público – Nivel Alto en tarjeta*
1.3.6.1.4.1.47281.1.1.4	*De Empleado Público – Nivel Medio en HSM*
	De Empleado Público (AUTENTICACIÓN)
1.3.6.1.4.1.47281.1.1.5	*De Empleado Público – Nivel Alto en tarjeta*
	De Empleado Público con Seudónimo (FIRMA)
1.3.6.1.4.1.47281.1.3.1	*De EP con Seudónimo – Nivel Alto en Tarjeta*
1.3.6.1.4.1.47281.1.3.4	*De EP con Seudónimo – Nivel Medio en HSM*
	De Empleado Público con Seudónimo (AUTENTICACIÓN)
1.3.6.1.4.1.47281.1.3.5	*De EP con Seudónimo – Nivel Alto en Tarjeta*
	De Persona Física vinculada a entidad (FIRMA)
1.3.6.1.4.1.47281.1.6.1	*De PF vinculada a entidad – Firma-e Cualificada, en Tarjeta*
1.3.6.1.4.1.47281.1.6.4	*De PF vinculada a entidad – Firma-e Centralizada*
	De Persona Física vinculada a entidad (AUTENTICACIÓN)
1.3.6.1.4.1.47281.1.6.5	*De PF vinculada a entidad – en Tarjeta*
	De Persona Física con seudónimo vinculada a entidad (FIRMA)
1.3.6.1.4.1.47281.1.7.1	*De PF con seudónimo vinculada a entidad – Firma-e Cualificada, en Tarjeta*
1.3.6.1.4.1.47281.1.7.4	*De PF con seudónimo vinculada a entidad – Firma-e Centralizada*

	De Persona Física con seudónimo, vinculada a entidad (AUTENTICACIÓN)
1.3.6.1.4.1.47281.1.7.5	*De PF con seudónimo, vinculada a entidad – en Tarjeta*
	De Sello de Órgano
1.3.6.1.4.1.47281.1.2.2	*De Sello de Órgano – Nivel Medio en software*
1.3.6.1.4.1.47281.1.2.4	*De Sello de Órgano – Nivel Medio en HSM*
	De Sede electrónica
1.3.6.1.4.1.47281.1.4.2	*De Sede-e EV – Nivel Medio*
	De Sello electrónico para TSA/TSU
1.3.6.1.4.1.47281.1.5.2	*Timestamp TSA/TSU HSM*

In the event of contradiction between this Declaration of Certificate Practices and other esFIRMA Procedure Documents, the provisions of this Declaration of Practices shall prevail.

esFIRMA conforms to the version 1.6.7 of the Baseline Requirements and 1.7.0 of the Extended Validation Guidelines published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document

This document is structured in accordance with IETF RFC 3647.

1.3 PKI participants

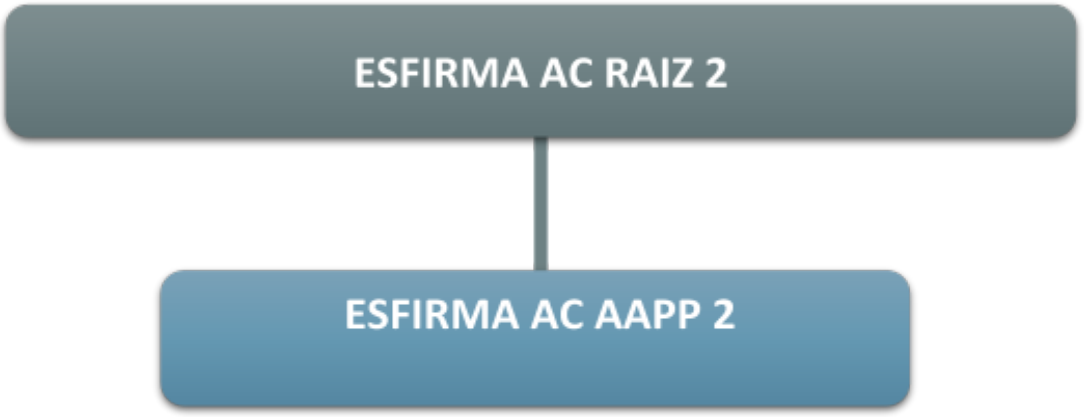
1.3.1 Certification authorities

The certification services provider is the natural or legal person who issues and manages certificates for final entities, using a Certifying Body or providing other services relating to electronic signatures.

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

under Volume 2.649, Folio 215, Sheet Z-28722, and which trades under the commercial name esFIRMA, the commercial name by which it shall be referred throughout this document. It is a certification services provider which acts in accordance with the provisions of the regime of obligations and responsibilities of Regulation (EU) No 910/2014 and the applicable ETSI technical standards for the issuing and management of qualified certificates, primarily ETSI EN 319-411-1 and ETSI EN 319 411-2, for the purpose of facilitating compliance with the legal requirement and international recognition of its services.

To provide the certification services, esFIRMA has established a hierarchy of certification entities:



ESFIRMA AC RAIZ 2

It is the root certification entity of the hierarchy that issues certificates to other certification entities and whose public key certificate has been self-signed.

Identification data:

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

ESFIRMA AC AAPP 2

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

Identification data:

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

1.3.1.3 Electronic Administration Platform

It is the exclusive platform for the management of the life-cycle of the certificate for its request, approval, issuing and revocation.

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

1.3.2 Registration authorities

In general, the certification service provider performs the function of registering the identity of the certificate subscribers.

The certificates subject to this Declaration of Certificate Practices are also registers due to their status as corporate certificates as are the units designated for this function by the subscribers of the certificates such as the Secretariat of the corporation or the personnel department of the Administration given they have access to the authentic registries on the links between the signatories and the subscriber.

The functions of registration of subscribers are carried out by the delegation and agreement with the instructions of the certification services provider, in the terms

defined in Regulation (EU) 910/2014 and under the full responsibility of the certification services provider before third parties.

1.3.3 Subscribers

The final entities are the recipient people and organisations of the issuing services, management and use of digital certificates, for users with electronic identification and signature.

The following shall be final entities of esFIRMA certifications:

1. Certification services subscribers.
2. Signatories.
3. Relying parties.

1.3.4 Relying parties

Relying parties are persons and organisations that receive digital signatures and digital certificates.

As a prior step to trusting the certificates the relying parties must verify them, as established in this declaration of certificate practices and in the corresponding instructions available in the Certification Entity.

1.3.5 Other participants

1.3.5.1 Certification services subscribers.

Certification services subscribers are the public administrators who acquire services from esFIRMA for use in their corporate or organisational sphere, and are identified on the certificates.

The subscribers of the certification service acquire a certificate use license, for their own use - electronic stamp or web authentication certificates - or for the purpose of facilitating the certification of the identity of a specific person duly authorised for different actions in the organisational sphere of the subscriber - electronically signed certificates. In the case of the latter, this person is identified on the certificate in accordance with the following paragraph.

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

1.3.5.2 Signatories

The signatories are the natural persons who exclusively possess or hold under their exclusive control, in accordance with the regime of obligations and responsibilities (EU) 910/2014, the digital signature keys for identification and advanced or qualified electronic signature, it typically being the incumbent persons or members of administrative bodies on the electronic signature of the body, or persons in the service of the Public Administrations on public employment certificates.

The signatories are duly authorised by the subscriber and duly identified on the certificate using their name and surnames and valid tax identification number from the jurisdiction that has issued the certificate or through the corresponding pseudonym of the certificates of this type.

Given the existence of the certificates for different uses of the electronic signature, such as identification, the more generic term “natural person identified on the certificate” is also used, with full respect at all times for compliance with the legislation on electronic signatures in relation to the rights and obligations of the signatory.

1.4 Certificate usage

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

1.4.1. Appropriate certificate uses

The permitted uses indicated in the different certificate profile fields available at https://www.esfirma.com must be taken into account.

SmartCard Empleado Público nivel alto Certificate

This certificate has the following OIDs

1.3.6.1.4.1.47281.1.1.1	In the hierarchy of the EC esFIRMA
0.4.0.194112.1.2	In accordance with the QCP-n-qscd policy
2.16.724.1.3.5.7.1	Senior Level Spanish Public Employee

The certificates of senior level natural person public employees are qualified certificates in accordance with Article 28 and Annex I of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provision of the technical standards identified in relation to ETSI EN 319 411-2.

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

The certificates of senior level natural person public employees function with a secure signature creation device, in accordance with Annex II of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014.

Thus, the certificates of senior level natural person public employee are issued in accordance with high security levels of the profiles of certificates established in point 10 of the document “Electronic Certificate Profiles” of the General Sub-Directorate of Information, Documentation and Publications of the Ministry of Finance and Public Administration.

These certificates ensure the identity of the subscriber and the signatory and allow for the generation of the “qualified electronic signature,” that is, the advanced electronic signature based on a qualified certificate and which has been generated using a qualified device which therefore, in accordance with the provisions of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014, shall have legal effect equivalent to that of a manuscript signature.

It can also be used in applications that do not require the electronic signature equivalent to a written one, such as the applications indicated below:

a) Signing of secure electronic signature.
b) Other digital signature applications.

esFIRMA does not offer secure copy or key recovery services. For this reason, esFIRMA will not respond, in any cases, for loss of any of the encrypted data which cannot be recovered.

The information on uses in the certificate profile indicates the following:

a) The field "key usage" has the following functions activated, which can therefore be performed:
    a. Content commitment (to perform the electronic signature function).

b) In the field "Qualified Certificate Statements" the following declaration 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 informs that the certificate is used exclusively in conjunction with a secure signature creation device.
c) The field "User Notice" describes the use of this certificate.

HSM Empleado Público nivel medio Certificate

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.1.4	In the hierarchy of the EC esFIRMA
0.4.0.194112.1.0	In accordance with the QCP-n-qscd policy
2.16.724.1.3.5.7.2	Intermediate level Spanish public employee

The certificates of intermediate level natural person public employees are qualified certificates in accordance with Article 28 and Annex I of Regulation (EU) No 910/2014

of the European Parliament and of the Council of 23 July 2014 and comply with the provision of technical standards identified in relation to ETSI EN 319 411-2.

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

The certificates of intermediate level natural person public employees are managed on a centralised basis.

The certificates of intermediate level natural person public employees are issued in accordance with high security levels of the profiles of certificates established in point 10 of the document "Electronic Certificate Profiles" of the General Sub-Directorate of Information, Documentation and Publications of the Ministry of Finance and Public Administration.

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

It can also be used in applications that do not require an electronic signature equivalent to a written one, such as the applications indicated below:

a) Signing of secure electronic signature.
b) Other digital signature applications.

esFIRMA does not offer secure copy or key recovery services For this reason, esFIRMA will not respond, in any cases, for loss of any of the encrypted data which cannot be recovered.

The information on uses in the certificate profile indicates the following:

a) The field "key usage" has the following functions activated, which can therefore be performed:
    a. Content commitment (to perform the electronic signature function)

b) In the field “Qualified Certificate Statements” the following declaration appears:
    a. QcCompliance (0.4.0.1862.1.1), which reports that the certificate is issued as qualified.
c) The field “User Notice” described the use of this certificate.

Certificado de Empleado Público nivel alto en tarjeta para autenticación

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.1.5	En la jerarquía de la EC esFIRMA
0.4.0.2042.1.2	De acuerdo con la política NCP+
2.16.724.1.3.5.7.1	Empleado público español de nivel alto

Estos certificados son certificados emitidos de acuerdo con la política de certificados normalizados (NCP+) y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-1.

Estos certificados se emiten a empleados públicos para identificarlos como personas al servicio de la Administración, organismo, entidad de derecho público u otra entidad, vinculándolos con ésta, cumpliendo los requisitos establecidos en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Estos certificados de persona física empleado público nivel alto, funcionan con dispositivo seguro de creación de firma, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Los certificados de persona física empleado público nivel alto se emiten de acuerdo con los niveles de aseguramiento alto de los perfiles de certificados establecidos en el punto 10 del documento “Perfiles de Certificados electrónicos” de la Subdirección General de Información, Documentación y Publicaciones del Ministerio de Hacienda y Administraciones Públicas.

Estos certificados garantizan la identidad del suscriptor y de la persona indicada en el certificado, y permiten la autenticación de ésta última ante aplicaciones y sitios web.

esFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo "key usage" tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
    a. Firma digital (para realizar la función de autenticación)

b) El campo "User Notice" describe el uso de este certificado.

Software Seal Certificate

This certificate has the following OIDs:

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

Certificates electronically stamped by an intermediate level public body are qualified certificates in accordance with Article 38 and Annex I of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provision of technical standards identified in relation to ETSI EN 319 411-2.

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

Certificates electronically stamped by senior level public bodies are issued in accordance with the intermediate security levels of the profiles of certificates established in point 9 of the document "Electronic Certificate Profiles" of the General

Sub-Directorate of Information, Documentation and Publications of the Ministry of Finance and Public Administration.

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

esFIRMA does not offer secure copy or key recovery services For this reason, esFIRMA will not respond, in any cases, for loss of any of the encrypted data which cannot be recovered.

The information on uses in the certificate profile indicates the following:

a) The field "key usage" has the following functions activated, which can therefore be performed:
    a. Content commitment (to perform the electronic signature function)

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

HSM Seal certificate

This certificate has the following OIDs

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

Certificates electronically stamped by an intermediate level public body are qualified certificates in accordance with Article 38 and Annex I of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provision of technical standards identified in relation to ETSI EN 319 411-2.

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

Certificates electronically stamped by intermediate level public bodies managed on a centralised basis.

Certificates electronically stamped by senior level public bodies are issued in accordance with the intermediate security levels of the profiles of certificates established in point 9 of the document "Electronic Certificate Profiles" of the General Sub-Directorate of Information, Documentation and Publications of the Ministry of Finance and Public Administration.

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

esFIRMA does not offer secure copy or key recover services For this reason, esFIRMA will not respond, in any cases, for loss of any of the encrypted data which cannot be recovered.

The information on uses in the certificate profile indicates the following:

a) The field "key usage" has the following functions activated, which can therefore be performed:
    a. Content commitment (to perform the electronic signature function)

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

SmartCard Public Employee with Pseudonym certificate

This certificate has the following OIDs

1.3.6.1.4.1.47281.1.3.1	In the hierarchy of the EC esFIRMA

0.4.0.194112.1.2	In accordance with the QCP-n-qscd policy
2.16.724.1.3.5.4.1	Spanish Public Employee Senior Level

The certificates of senior level natural person public employees are qualified certificates in accordance with Article 28 and Annex I of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provision of technical standards identified in relation to ETSI EN 319 411-2.

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

The certificates of senior level natural person public employees with pseudonym function with a secure signature creation device, in accordance with Annex II of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014.

Furthermore, certificates issued by senior level natural person public employees with pseudonym are issued in accordance with the high security levels of the profiles of certificates established in point 11 of the document “Electronic Certificate Profiles” of the General Sub-Directorate of Information, Documentation and Publications of the Ministry of Finance and Public Administration.

These certificates allow for the generation of “qualified electronic signature,” that is, the advanced electronic signature based on a qualified certificate and which has been generated using the qualified device, which therefore in accordance with the provisions of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 shall have legal affect equivalent to that of a manuscript signature.

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

a) Signing of secure email.

b) Other digital signature applications.

esFIRMA does not offer secure copy or key recovery services. For this reason, esFIRMA will not respond, in any cases, for loss of any of the encrypted data which cannot be recovered.

The information on uses in the certificate profile indicates the following:

a) The field "key usage" has the following functions activated, which can therefore be performed:
    a. Content commitment (to perform the electronic signature function)

b) In the field "Qualified Certificate Statements" the following declaration appears:
    a. QcCompliance (0.4.0.1862.1.1), which reports that the certificate is issued as qualified.
    b. QcSSCD (0.4.0.1862.1.4), which states that the certificate is used exclusively in conjunction with a secure signature creation device.
c) The field "User Notice" described the use of this certificate.

HSM Public Employee with pseudonym certificate

This certificate has the following OIDs:

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

The certificates of senior level natural person public employees with pseudonym are qualified certificates in accordance with Article 28 and Annex I of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provision of technical standards identified in relation to ETSI EN 319 411-2.

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

The certificates of intermediate level natural person public employees with pseudonym are managed on a centralised basis.

The certificates of natural person public employees, senior level, are issued in accordance with high security levels of the profiles of certificates established in point 11 of the document "Electronic Certificate Profiles" of the General Sub-Directorate of Information, Documentation and Publications of the Ministry of Finance and Public Administration.

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

It can also be used in applications that do not require the electronic signature equivalent to a written one, such as the applications indicated below:

c) Signing of secure email.
d) Other digital signature applications.

esFIRMA does not offer secure copy or key recover services For this reason, esFIRMA will not respond, in any cases, for loss of any of the encrypted data which cannot be recovered.

The information on uses in the certificate profile indicates the following:

a) The field "key usage" has the following functions activated, which can therefore be performed:
    a. Content commitment (to perform the electronic signature function)

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

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

c) The field “User Notice” described the use of this certificate.

Certificado de Empleado Público con seudónimo, nivel alto en tarjeta para autenticación

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.3.5	En la jerarquía de la EC esFIRMA
0.4.0.2042.1.2	De acuerdo con la política NCP+
2.16.724.1.3.5.4.1	Empleado público español con seudónimo de nivel alto

Estos certificados son certificados emitidos de acuerdo con la política de certificados normalizados (NCP+) y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-1.

Estos certificados se emiten a empleados públicos para identificarlos (por medio de un seudónimo) como personas al servicio de la Administración, organismo, entidad de derecho público u otra entidad, vinculándolos con ésta, cumpliendo los requisitos establecidos en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Estos certificados de persona física empleado público con seudónimo nivel alto, funcionan con dispositivo seguro de creación de firma, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Los certificados de persona física empleado público con seudónimo nivel alto se emiten de acuerdo con los niveles de aseguramiento alto de los perfiles de certificados establecidos en el punto 11 del documento “Perfiles de Certificados electrónicos” de la

Subdirección General de Información, Documentación y Publicaciones del Ministerio de Hacienda y Administraciones Públicas.

Estos certificados garantizan la identidad del suscriptor y de la persona indicada en el certificado, y permiten la autenticación de ésta última ante aplicaciones y sitios web.

esFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo “key usage” tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
    a. Firma digital (para realizar la función de autenticación)

b) El campo “User Notice” describe el uso de este certificado.

Web authentication certificate

This certificate has the following OIDs

1.3.6.1.4.1.47281.1.4.2	In the hierarchy of the EC esFIRMA
0.4.0.194112.1.4	In accordance with the QCP-web policy
2.16.724.1.3.5.5.2	Spanish electronic administrative office, intermediate level.

The intermediate level web authentication certificates are qualified certificates in accordance with Article 45 and Annex IV of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standards identified in relation to ETSI EN 319 411-2.

These certificates are issued to public employees to identify them as persons at the service of the Administration, body or public law entity, linking them to this in

accordance with the requirements established in Article 38 of Law 40/2015 of 1 October on the Legal Regime of the Public Sector for the electronic signing of personnel at the service of the Public Administrations.

Intermediate level web authentication certificates are issued in accordance with high security levels of the profiles of certificates established in point 8 of the document "Electronic Certificate Profiles" of the General Sub-Directorate of Information, Documentation and Publications of the Ministry of Finance and Public Administration.

The information on uses in the certificate profile indicates the following:

a) The field "key usage" has the following functions activated, which can therefore be performed:
    a. Digital Signature (for the authentication function)
    b. Key Encipherment (for the management and transport of keys)

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

Electronic stamp TSA/TSU certificate

This certificate has the following OIDs:

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

The certificates of the electronic stamp TSA/TSU are qualified certificates in accordance with Article 38 and Annex III of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of technical standards identified in with reference ETSI EN 319 421 and ETSI EN 319 422.

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

The keys are generated in support of a HSM device.

The information on uses in the certificate profile indicates the following:

a) The field “key usage” has the following functions activated, which can therefore be performed:
    a. Content Commitment
b) The field “extended key usage has the
    a. TimeStamping function activated
c) In the field “Qualified Certificate Statements” the following declaration appears:
    a. QcCompliance (0.4.0.1862.1.1), which states that the certificate is issued as qualified.
d) The field “User Notice” describes the use of this certificate.

Certificado de persona física vinculada, en Tarjeta para firma

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.6.1	En la jerarquía de la EC esFIRMA
0.4.0.194112.1.2	De acuerdo con la política QCP-n-qscd

Estos certificados son cualificados de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados funcionan con dispositivo seguro de creación de firma, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Estos certificados garantizan la identidad del suscriptor y del firmante, y permiten la generación de la "firma electrónica cualificada"; es decir, la firma electrónica avanzada que se basa en un certificado cualificado y que ha sido generada empleando un dispositivo cualificado, por lo cual de acuerdo con lo que establece el artículo 25.2 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, tendrá un efecto jurídico equivalente al de una firma manuscrita.

También se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.
b) Otras aplicaciones de firma digital.

esFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo "key usage" tiene activadas, y por tanto permite realizar, las siguientes funciones:
    a. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)

b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
    a. QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
    b. QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.
c) El campo "User Notice" describe el uso de este certificado.

Certificado de persona física vinculada, centralizado, para firma

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.6.4	En la jerarquía de la EC esFIRMA
0.4.0.194112.1.0	De acuerdo con la política QCP-n

Estos certificados son cualificados de acuerdo con el artículo 28 y el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados son gestionados de forma centralizada.

Estos certificados garantizan la identidad del suscriptor y de la persona indicada en el certificado, y permiten la generación de la "firma electrónica avanzada basada en certificado electrónico cualificado".

También se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.
b) Otras aplicaciones de firma digital.

esFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo "key usage" tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
    a. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)

b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.

c) El campo “User Notice” describe el uso de este certificado.

Certificado de persona física vinculada, en tarjeta para autenticación

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.6.5	En la jerarquía de la EC esFIRMA
0.4.0.2042.1.2	De acuerdo con la política NCP+

Estos certificados son certificados emitidos de acuerdo con la política de certificados normalizados (NCP+) y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-1.

Estos certificados funcionan con dispositivo seguro de creación de firma, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Estos certificados garantizan la identidad del suscriptor y de la persona indicada en el certificado, y permiten la autenticación de ésta última ante aplicaciones y sitios web.

esFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

d) El campo “key usage” tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
    a. Firma digital (para realizar la función de autenticación)

e) El campo “User Notice” describe el uso de este certificado.

Certificado de persona física vinculada, con seudónimo, en Tarjeta para firma

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.7.1	En la jerarquía de la EC esFIRMA
0.4.0.194112.1.2	De acuerdo con la política QCP-n-qscd

Estos certificados son cualificados de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados funcionan con dispositivo seguro de creación de firma, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Estos certificados garantizan la identidad del suscriptor.
Estos certificados garantizan la identidad del firmante por medio de un seudónimo.
Estos certificados permiten la generación de la "firma electrónica cualificada"; es decir, la firma electrónica avanzada que se basa en un certificado cualificado y que ha sido generada empleando un dispositivo cualificado, por lo cual de acuerdo con lo que establece el artículo 25.2 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, tendrá un efecto jurídico equivalente al de una firma manuscrita.

También se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

c) Firma de correo electrónico seguro.
d) Otras aplicaciones de firma digital.

esFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

d) El campo “key usage” tiene activadas, y por tanto permite realizar, las siguientes funciones:
    a. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)

e) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
    a. QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
    b. QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.
f) El campo “User Notice” describe el uso de este certificado.

Certificado de persona física vinculada, con seudónimo, centralizado, para firma

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.6.4	En la jerarquía de la EC esFIRMA
0.4.0.194112.1.0	De acuerdo con la política QCP-n

Estos certificados son cualificados de acuerdo con el artículo 28 y el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados son gestionados de forma centralizada.

Estos certificados garantizan la identidad del suscriptor.
Estos certificados garantizan la identidad del firmante por medio de un seudónimo.
Estos certificados permiten la generación de la “firma electrónica avanzada basada en certificado electrónico cualificado”.

También se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

c) Firma de correo electrónico seguro.
d) Otras aplicaciones de firma digital.

esFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

f) El campo "key usage" tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
    a. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)

g) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
h) El campo "User Notice" describe el uso de este certificado.

Certificado de persona física vinculada, con seudónimo,en tarjeta para autenticación

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.7.5	En la jerarquía de la EC esFIRMA
0.4.0.2042.1.2	De acuerdo con la política NCP+

Estos certificados son certificados emitidos de acuerdo con la política de certificados normalizados (NCP+) y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-1.

Estos certificados funcionan con dispositivo seguro de creación de firma, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Estos certificados garantizan la identidad del suscriptor.
Estos certificados garantizan la identidad del firmante por medio de un seudónimo.
Estos certificados permiten la autenticación de ésta última ante aplicaciones y sitios web.

esFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

i) El campo “key usage” tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
    a. Firma digital (para realizar la función de autenticación)

j) El campo “User Notice” describe el uso de este certificado.

1.4.2 Prohibited certificate uses

The certificates are used for their own function and the established purpose and may not be used in other functions or for other purposes.

Similarly, the certificates must only be used in accordance with applicable law, taking into account the restrictions on the import and export of existing at any time.

The certificates cannot be used to sign requests for the issue, renewal, suspension or revoking of certificates nor to sign public key certificates of any kind nor to sign Certificate Revocation Lists (CRLs).

The certificates have not been designed nor may they be used nor may their use or resale be authorised as control equipment for dangerous situations or for uses that require fail-safe actions such as the functioning of nuclear facilities, navigation systems

or air traffic communication or arms control systems where an error may directly lead to death, personal injury or major environmental damage.

The limits indicated in the different in the different certificate profile fields available at https://www.esfirma.com must be taken into account.

The use of the digital certificates in a manner that does not comply with this CPS and other applicable documentation, in particular the contract signed with the subscriber and the informational texts or PDS shall be considered inappropriate use with all corresponding legal effects and, esFIRMA shall be released from all liability for such inappropriate use on the part of the signatory or any third party.

esFIRMA has no authorisation for access or legal obligation to supervise the data regarding which the use of the certified key can be applied. Therefore, and as a consequence of the technical impossibility of accessing the content of the message, it is not possible for esFIRMA to issue any valuation whatsoever of said content; the subscriber, signatory or person responsible for the custody thereof thus assuming any liability arising from the content relating to the use of the certificate.

Furthermore the subscriber, signatory or the person responsible for the custody thereof shall be liable for any liability that may arise from the use of same beyond the limits and conditions of use contained in this CPS, the legal documents related to each certificate or the contracts or collective agreements with registration entities or with their subscriber, or any other inappropriate use of same arising from this section or which may be interpreted as such based on the applicable legislation.

The certificates are used exclusively from the Electronic Administration Platform or complementary extensions and supplements of same that the company ESPUBLICO make available to the subscriber.

1.5 Policy administration

1.5.1 Organization administering the document

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

(+34) 976300110

Identification Register	Business Registry of Zaragoza
Volume	2649
Folio	215
Sheet	Z-28722:
CIF	A-50.878.842

1.5.2 Contact person

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

1.5.3 Person determining CPS suitability for the policy

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

The Security Committee of esFIRMA, formed by the President of same, the Information Manager and the Manager and service and the Security Manager of esFirma, has the responsibility of approving this Declaration of Practices-

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

1.5.4 CPS approval procedures

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

esFIRMA carries out reviews of this document on at least an annual basis or when it's required by changes in the guides or documents it must comply with.

As defined in the esFIRMA Security Policy, the Security Office: shall be the entity responsible for the maintenance of this document.

The Security Office shall be responsible for the preparation, maintenance and administration of the CPS, the disclosure statements (PDSs), delivery and acceptance sheets and other legal documentation (collective agreements, contracts) of esFirma.

Provided that there exist changes of sufficient importance in the management of certificates defined in this CPS, a new review of this document will be created, which shall be recorded in the initial "version control" panel within the "general information" section.

The action of the Security Office occurs at the request of its manager based on the needs that may arise.

EsFirma may make changes that require no notification where these do not directly affect the rights of the signatories and subscribers of the certificates or the subscribers of the stamps.

When esFirma is to introduce changes that amend the rights of the signatories and subscribers of stamps, it must give public notice of same for the purpose of presenting the comments to the Security Office for the 15 days following publication of future changes.

In order to give public notifications of the changes it shall be published in the "documentation" section on the website https://www.esfirma.com

Review of this CPS shall be published on the website of Esfirma once they are approved by the Security Committee of Esfirma.

1.6 Definitions and acronyms

1.6.1 Acronyms

CA	*Certificate Authority*

RA	*Registration Authority*
DPC	Data Processing Centre
CPS	*Certification Practice Statement*.
CRL	*Certificate Revocation List.*
DN	*Distinguished Name.*
DNI	Spanish National Identification Document
ETSI EN	*European Telecommunications Standards Institute – European Standard.*
EV (for SSL)	*Extended Validation*, in SSL certificates.
FIPS	*Federal Information Processing Standard Publication*
HSM	*Hardware Security Module*
IETF	*Internet Engineering Task Force*
NIF	Spanish Tax Identification Number
NTP	*Network Time Protocol*
OCSP	*Online Certificate Status Protocol.*
OID	*Object Identifier.*
PDS	*PKI Disclosure Statements*
PIN	*Personal Identification Number*. Spanish Tax Identification Number
PKI	*Public Key Infrastructure*.
QSCD	*Qualified Electronic Signature/Seal Creation Device.*
QCP	*Qualified Certificate Policy*
QCP-n	*Qualified Certificate Policy-natural person*
QCP-l	*Qualified Certificate Policy-legal person*
QCP-n-qscd	*Qualified Certificate Policy-natural person-qscd*
QCP-l-qscd	*Qualified Certificate Policy-legal person-qscd*
RFC	*Request for Comments* RFC Document

RSA	Rivest-Shamir-Adleman. Type of encryption algorithm
SHA	*Secure Hash Algorithm.*
SSL	*Secure Sockets Layer.* Protocol designed by Netscape and converted into the network standard, it allows for transfer of encrypted information between a web browser and a server.
TCP/IP	*Transmission Control. Protocol/Internet Protocol*.
TSA	*Time Stamping Authority*
TSU	*Time Stamping Unit*
UTC	*Coordinated Universal Time*
VPN	*Virtual Private Network.*

1.6.2 Definitions	
Certificate Authority	*Entity responsible for issuing and managing digital certificates.*
Registration Authority	*Entity responsible for managing requests, identification and registration of certificate requesters. It may form part of the Certificate Authority or be external from same.*
Certificate	*File which links the public key with some identifying data from the Subject/Signatory and is signed by the CA.*
Public key	*Publicly known mathematical value used for verification of a digital signature or data encryption.*
Private key	*Mathematical value known only by the Subject/Signatory and used for verification of a digital signature or data encryption.* *The private key used for the signing of certificates and signing of CRLs* *The private key of the TSA service shall be used for the signing of the time stamps.*
CPS	*Set of practices adopted by a Certificate Authority for the issue of certificates in accordance with a specific certification policy.*
CRL	*File containing a list of certificates which have been revoked in a determined period of time and which is signed by the CA.*
Activation data	*Private data such as PINs or passwords used for the activation of a private key.*
QSCD	*Qualified Signature Creation Device. Software or hardware element, appropriately certified by the Subject/Signatory for the generation of electronic signatures so that cryptographic operations within the device are performed 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 some known algorithms, thus guaranteeing:* *a) that the data have not been modified (integrity)* *b) that the person who signs the data is the person they claim to be (identification)* *c) that the person who signs the data cannot deny that they have done so (non-rejection at source)*

OID	*Unique numeric identifier registered under ISO standardisation and referring to an object or specific class of object.*
Pair of keys	*Pair comprised of the public and private keys, both mathematically interrelated.*
PKI	*Set of hardware, software, HR elements, procedures, etc. which comprise a system based on the creation and management of public key certificate.*
Requester	*In the context of this document, the requester shall be a natural person assigned a special power to carry out certain processes in the name and on behalf of the body.*
Subscriber	*In the context of this document, the legal person who owns the certificate (at corporate level)*
Subject/Signatory	*In the context of this document, the natural person is certified by the CA and has access or exclusive access to a private key valid for generating digital signatures.*
Relying Party	*In the context of this document, a person who voluntarily trusts the digital certificate and uses it as a form of accreditation of the authenticity and integrity of the signed document*

2. Publication of information and deposit of certificates

2.1 Repositories

esFIRMA has access to a Deposit of certificates in which the information relating to the certification services are published:

https://www.esfirma.com

The service is available 24 hours, 7 days a week, and, in the event of a system failure beyond the control of esFIRMA, its shall make its best efforts to ensure the service is available again within the term established in Section 5.7.4 of this CPS.

2.2 Publication of certification information

esFIRMA publishes the following information, in its Deposit:

- The lists of certificates revoked and other information on the revoke status of the certificates.
- The applicable certificate policies.
- The CPS.
- The texts of revelation (PKI Disclosure Statement -PDS), in the Spanish and English language versions at a minimum.

2.3 Time or frequency of publication

The information of the certification services including the policies and the Declaration of Certification Practices is published as soon as it becomes available.

The changes in the Declaration of Certification Practices are governed by the provisions of Section 1.5 of this Document.

The information on the status of the revoking of certificates is published in accordance with the provisions of sections 4.9.7 and 4.9.8 of this Declaration of Certification Practices.

BR and CA/B forum extended validation SSL guidelines are reviewed regularly and this document is aligned with them.

2.4 Access controls on repositories

esFIRMA does not limit reading access to the information established in Section 2.2 but established controls to prevent unauthorised persons from adding, modifying or deleting files from the Deposit , to protect the integrity and authenticity of the information, especially information on revocation status.

esFIRMA uses reliable systems for the Deposit, in such a way that:

- Only authorised persons may make notes and modifications.
- The authenticity of the information can be checked.
- Any technical change that affects the security requirements may be detected.

3. Identification and authentication

3.1 Naming

3.1.1 Types of names

All certificates contain a name designated X.501 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 along with different additional information in the *SubjectAlternativeName* field.

The names contained on the certificates are the following.

Certificate of senior level public employee on card

Country (C)	"ES"
Organization (O)	Name ("official" name) of the Administration, body or public law entity subscribing the certificate, to which the employee is linked
organizationalUnitName (OU)	ELECTRONIC CERTIFICATE OF PUBLIC EMPLOYEE
organizationIdentifier	Identifier of the organization according to technical standard ETSI EN 319 412-1
Surname	First and second(optional) surname according to identification document (DNI/Passport)
First name	First name according to identification document (DNI/Passport)
Serial Number	DNI/NIE of employee
Common Name (CN)	Name Surname1 Surname2 – NIF of employee
Type of certificate OID: 2.16.724.1.3.5.7.1.1	QUALIFIED CERTIFICATE OF SIGNATURE OF SENIOR LEVEL PUBLIC EMPLOYEE
Name of the subscriber entity OID: 2.16.724.1.3.5.7.1.2	Name of the subscriber entity
NIF of the subscriber entity OID: 2.16.724.1.3.5.7.1.3	NIF subscriber entity
DNI/NIE of the manager OID: 2.16.724.1.3.5.7.1.4	DNI or NIE of the manager

First name OID: 2.16.724.1.3.5.7.1.6	First name of certificate manager
First name OID: 2.16.724.1.3.5.7.1.7	First name of certificate manager
Second surname OID: 2.16.724.1.3.5.7.1.8	Second surname of certificate manager. Optional.
Email OID: 2.16.724.1.3.5.7.1.9	Email of certificate manager. Optional.

Certificate of intermediate level public employee on HSM

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

First name OID: 2.16.724.1.3.5.7.2.7	First name of certificate manager
Second surname OID: 2.16.724.1.3.5.7.2.8	Second surname of certificate manager. Optional.
Email OID: 2.16.724.1.3.5.7.2.9	Email of certificate manager. Optional.

Certificate of stamp of intermediate level body on software

Country (C)	"ES"
Organization (O)	Designation ("official" name of the organisation) of the subscriber
organizationalUnitName (OU)	ELECTRONIC STAMP
organizationIdentifier	Identifier of the organization according to technical standard ETSI EN 319 412-1
Serial Number	DNI/NIE of the subscriber organisation
Common Name (CN)	Designation of the system or application of the automatic process.
Type of certificate OID: 2.16.724.1.3.5.6.2.1	INTERMEDIATE LEVEL ELECTRONIC STAMP
Name of the subscriber entity OID: 2.16.724.1.3.5.6.2.2	Name of the subscriber entity
NIF of the subscriber entity OID: 2.16.724.1.3.5.6.2.3	NIF of the subscriber entity
Name of the system OID: 2.16.724.1.3.5.6.2.5	Name of the system
Email OID: 2.16.724.1.3.5.6.2.9	Email of stamp manager

Certificate of stamp of intermediate level body, in HSM

Country (C)	"ES"
Organization (O)	Name ("official" name of the organization) of the subscriber
organizationalUnitName (OU)	ELECTRONIC STAMP
organizationIdentifier	Identifier of the organization according to technical standard ETSI EN 319 412-1
Serial Number	DNI/NIE of the subscriber organisation

Common Name (CN)	Designation of the system or application of the automatic process.
Type of certificate OID: 2.16.724.1.3.5.6.2.1	INTERMEDIATE LEVEL ELECTRONIC STAMP
Name of the subscriber entity OID: 2.16.724.1.3.5.6.2.2	Name of the subscriber entity
NIF of the subscriber entity OID: 2.16.724.1.3.5.6.2.3	NIF of the subscriber entity
Name of the system OID: 2.16.724.1.3.5.6.2.5	Name of the system

Certificate of Senior Level Public Employee with Pseudonym on Card

Country (C)	"ES"
Organization (O)	Name ("official" name) of the Administration, body or public law entity subscribing the certificate, to which the employee is linked
organizationalUnitName (OU)	ELECTRONIC CERTIFICATE OF PUBLIC EMPLOYEE WITH PSEUDONYM
organizationIdentifier	Identifier of the organization according to technical standard ETSI EN 319 412-1
Pseudonym	Obligatory pseudonym in accordance with ETSI EN 319 412-2 for this type of certificate
Common Name (CN)	Pseudonym and the Body
Type of certificate OID: 2.16.724.1.3.5.4.1.1	ELECTRONIC CERTIFICATE OF SENIOR LEVEL PUBLIC EMPLOYEE WITH PSEUDONYM
Name of the subscriber entity OID: 2.16.724.1.3.5.4.1.2	Name of the subscriber entity
NIF of the subscriber entity OID: 2.16.724.1.3.5.4.1.3	NIF of the subscriber entity
Pseudonym OID: 2.16.724.1.3.5.4.1.12	Pseudonym used by the signatory and authorised by the subscriber

Certificate of intermediate public employee with pseudonym on HSM

Country (C)	"ES"

Organization (O)	Name ("official" name) of the Administration, body or public law entity subscribing the certificate, to which the employee is linked
organizationalUnitName (OU)	ELECTRONIC CERTIFICATE OF PUBLIC EMPLOYEE WITH PSEUDONYM
organizationIdentifier	Identifier of the organization according to technical standard ETSI EN 319 412-1
Pseudonym	Obligatory pseudonym in accordance with ETSI EN 319 412-2 for this type of certificate
Common Name (CN)	Pseudonym and the Body
Type of certificate OID: 2.16.724.1.3.5.4.2.1	ELECTRONIC CERTIFICATE OF INTERMEDIATE LEVEL PUBLIC EMPLOYEE WITH PSEUDONYM
Name of the subscriber entity OID: 2.16.724.1.3.5.4.2.2	Name of the subscriber entity
NIF of the subscriber entity OID: 2.16.724.1.3.5.4.2.3	NIF of the subscriber entity
Pseudonym OID: 2.16.724.1.3.5.4.2.12	Pseudonym used by the signatory and authorised by the subscriber

Web authentication certificate EV, intermediate level

Country (C)	"ES"
Organization (O)	Name ("official" name) of the Administration, body or public law entity subscribing the certificate (custody)
localityName	City
organizationalUnitName	Description of type of certificate ELECTRONIC OFFICE
organizationalUnitName	The descriptive name of the office
serialNumber	The NIF of the entity responsible
businessCategory	Category of the organisation: Government Entity
jurisdictionOfIncorporationCountry Name	Jurisdiction
organizationIdentifier	Identifier of the organization according to technical standard ETSI EN 319 412-1, optional and only when allowed by CA/Browser Forum Guidelines.
Common Name (CN)	Domain name (DNS) where the certificate will reside.

Certificate of electronic stamp of TSA/TSU

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

Certificado de autenticación de empleado público, con seudónimo, nivel alto, en tarjeta

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial") de la Administración, organismo, entidad de derecho público u otra entidad suscriptora del certificado, a la que se encuentra vinculada el empleado
organizationalUnitName (OU)	CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
pseudonym	Seudónimo Obligatorio según ETSI EN 319 412-2
Common Name (CN)	Puesto o cargo o "SEUDONIMO" – NUMERO IDENTIFICATIVO - NOMBRE OFICIAL DEL ORGANISMO
Tipo de certificado OID: 2.16.724.1.3.5.4.1.1	CERTIFICADO DE AUTENTICACIÓN DE EMPLEADO PUBLICO CON SEUDONIMO
Nombre de la entidad suscriptora OID: 2.16.724.1.3.5.4.1.2	Nombre de la entidad suscriptora
NIF entidad suscriptora OID: 2.16.724.1.3.5.4.1.3	NIF entidad suscriptora

Certificado de autenticación web EV, nivel medio

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial") de la Administración, organismo o entidad de derecho público suscriptora del certificado (custodio)
localityName	Ciudad
organizationalUnitName	Descripción del tipo de certificado: SEDE ELECTRONICA

organizationalUnitName	El nombre descriptivo de la sede
serialNumber	El NIF de la entidad responsable
businessCategory	Categoría de la organización: Government Entity
jurisdictionOfIncorporationCountry Name	Jurisdicción
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1, opcional y sólo cuando se ajuste a la versión actual de las CA/Browser Forum Guidelines
Common Name (CN)	Nombre de dominio (DNS) donde residirá el certificado. Opcional.

Certificado de sello electrónico de TSA/TSU

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial" de la organización) del suscriptor
organizationalUnitName (OU)	AUTORIDAD DE CERTIFICACIÓN DE ESFIRMA
Serial Number	DNI/NIE de la organización suscriptora
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
Common Name (CN)	Denominación de la TSU

Certificado de firma de persona física vinculada, en tarjeta

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial") de la entidad suscriptora del certificado, a la que se encuentra vinculada el empleado
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
Surname	Primer y segundo(opcional) apellido, de acuerdo con documento de identidad (DNI/Pasaporte)
Given Name	Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte)
Serial Number	DNI/NIE de la persona física
Common Name (CN)	Apellido1 Apellido2 Nombre – NIF persona física (FIRMA)

Certificado de firma de persona física vinculada, en HSM

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial") de la entidad subscriptora, a la que se encuentra vinculada el empleado
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
Surname	Primer y segundo(opcional) apellido, de acuerdo con documento de identidad (DNI/Pasaporte)
Given Name	Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte)
Serial Number	DNI/NIE del empleado
Common Name (CN)	Apellido1 Apellido2 Nombre – NIF persona física

Certificado de autenticación de persona física vinculada, en tarjeta

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial") de la entidad suscriptora del certificado, a la que se encuentra vinculada el empleado
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
Surname	Primer y segundo(opcional) apellido, de acuerdo con documento de identidad (DNI/Pasaporte)
Given Name	Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte)
Serial Number	DNI/NIE del empleado
Common Name (CN)	Apellido1 Apellido2 Nombre – NIF persona física (AUTENTICACION)

Certificado de firma de persona física vinculada, en tarjeta, con seudónimo

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial") de la entidad suscriptora del certificado, a la que se encuentra vinculada el empleado
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
pseudonym	Seudónimo Obligatorio según ETSI EN 319 412-2

Common Name (CN)	Puesto o "SEUDONIMO" – NUMERO IDENTIFICATIVO - NOMBRE ENTIDAD

Certificado de firma de persona física vinculada, en HSM

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial") de la entidad subscriptora, a la que se encuentra vinculada el empleado
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
pseudonym	Seudónimo Obligatorio según ETSI EN 319 412-2
Common Name (CN)	Puesto o "SEUDONIMO" – NUMERO IDENTIFICATIVO - NOMBRE ENTIDAD

Certificado de autenticación de persona física vinculada, en tarjeta, con seudónimo

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial") de la entidad suscriptora del certificado, a la que se encuentra vinculada el empleado
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
Common Name (CN)	Puesto o "SEUDONIMO" – NUMERO IDENTIFICATIVO - NOMBRE ENTIDAD

3.1.2 Need for names to be meaningful

The name contained in the fields *SubjectName* and *SubjectAlternativeName* of the certificates are understandable in natural language, in accordance with the provisions of the previous sections.

3.1.3 Anonymity or pseudonymity of subscribers

Under no circumstances shall pseudonyms be used to identify an entity/company/organization, and in no case shall anonymous certificates be issued, with the exception of where for public security reasons the electronic signature systems can refer only to the professional identification number of the public employee.

3.1.4 Rules for interpreting various name forms

The name formats shall be interpreted in accordance with the law of the country if the subscriber establishment in its own terms.

The field “country” shall always be Spain as the certificates are issued exclusively to the Spanish Public Administrations.

The certificate shows the relation between the natural person and the Administration, body or public law entity with which they are linked, independently of the nationality of the natural person. That is derived from the corporate nature of certificate, of which the corporation is a subscriber and the natural person linked to the authorised person and their use.

In the certificates issued to Spanish subscribers, the “series number” field must include the NIF of the signatory, for the admission of the certificate for the processes with Spanish administrations.

3.1.5 Uniqueness of names

The name of the subscribers of certificates shall be unique for each esFIRMA certificate.

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

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

- Tax Identification Number (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 (Description field of the certificate).

3.1.6 Recognition, authentication, and role of trademarks

The requesters of certificates will not include names that may constitute an infraction, by the future subscriber, of third party rights.

esFIRMA shall not be obliged to determine in advance that the requester of certificates has the rights to industrial property over the name that appears on the certificate request but in principle shall proceed to certify it.

Furthermore, they shall not act as arbitrator or mediator nor in any other way shall it resolve any dispute whatsoever concerning the propriety of names of persons or organizations, domain names, brand names or commercial names.

However, in the event that a notification is received relating to a conflict of names, in accordance with the legislation of the country of the subscriber, it may take the pertinent actions in order to block or remove the certificate issued.

In any case, the certification services provider reserves the right to reject a request for a certificate due to a conflict of names.

All disputes or conflicts arising from this document shall be resolved definitively through the legal arbitration of an arbitrator within the framework of the Spanish Court of Arbitration, in accordance with its Regulations and Statutes, which is entrusted with the responsibility of administrating arbitration and the designation of the arbitrator or arbitration tribunal. The parties state for the record their commitment to abide by the arbitration judgement dictated in the contractual document which formalises the service.

3.2 Initial identity validation

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

The identity of the natural persons identified in the certificates is validated through the corporate registers of the Administration, body or public law entity which subscribes the certificates. The subscriber, through the administrative certification issued by the Secretary of the Council will produce a certification of the necessary data and will issued to esFIRMA, through the channels it provides, for the registration of the identity of the signatories. When the subscriber does not have a Secretariat, this certification will be issued by the Manager of the designated certification service.

Each Administration, body or public law entity is the data controller of its personal data, with esFIRMA the data processor of said data.

To avoid any conflict of interest the subscriber Public Administrations are independent of the trusted services Provider "esFIRMA" and of the company ESPUBLICO[1].

esFIRMA only accepts document sources from public and official registers.

3.2.1 Method to prove possession of private key

The possession of the private key is demonstrated by virtue of the trusted procedure of delivery and acceptance of the certificate by the signatory from the Electronic Administration Platform upon signing of the acceptance sheet and the use of said platform.

3.2.2 Authentication of organization identity

Public administrations do not require documentation proving the existence of the public administration, body or entity under public law, given that said identity is part of the corporate scope of the General State Administration or other State Public Administrations.

The natural persons with capacity to act in the name of an Administration, body or public law entity subscribing to the certificates may act as representatives of same in relation to the provisions of this CPS, provided that there exists a situation prior legal or voluntary representation between the natural person and the Administration, body

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

or public law entity subscribing the certificates, which demands its recognition on the part of esFIRMA, which shall be done through the following procedure:

1. A secretariat certificate of the plenary session in which they are named legal representative, with the following data:
    a. As representative:
        i. Name and surnames
        ii. Document: NIF of representative
    b. The identification data of the subscriber
        i. Name of the Administration, body or public law entity.
        ii. Information on the extension and validity of the powers of representation of the requester.
        iii. Document: NIF of Administration, body or public law entity
        iv. Document: Documents the serve the prove the extremes cited in a demonstrable manner in accordance with the provisions of the regulations of applicable administrative law and the registration with the corresponding public register if so required.
    c. The data relating to the representation or the capacity to act it hold:
        i. The validity of the representation or capacity to act (start and end date).
        ii. The scope and limits, where applicable, of the representation or capacity to act.
            1. TOTAL. Representation or total capacity.
            2. PARTIAL Representation or partial capacity.
2. A certification services provision contract which esFIRMA will sign (ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA) and the legal representative of the Administration which includes:
3. A protocol which each authorised operator will sign (including their obligations).

Once the documents are electronically signed, the RA functions are activated for the Local Authority Users who appear in the contract as authorised operators to perform this function.

3.2.3 Authentication of individual identity

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

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

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

1. Request of Employee for certificate through the Electronic Administration Platform (with corresponding registration of entering and opening the file)
2. A secretariat or personnel department certificate in which this person's link with the Local Authority is certified.
3. Request signed by the authorised operator of the entity (or legal representative) registering the issue and notifying ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (attaching copy of the certificate and of the request of the employee).

To issue an electronic Stamp certificate the following steps must be followed, through an electronic procedure generating the following documents:

1. Request of the legal representative of the entity which registers the issue and notifying ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA

To issue a web site certificate the following steps must be followed, through an electronic procedure generating the following documents:

1. Request of the legal representative of the entity which registers the issue and notifying ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA.

3.2.3.1 On the certificates

The identification information of the natural persons identified on the certificates is validated comparing the information of the request of the Administration, body or public law entity subscribing the certificates with the registries of the Administration body or public law entity subscribing the certificates with the registers of the Administration, body or public law entity to which they are linked, generated in

accordance with point 3.2 of this CPS ensuring the accuracy of the information to certify.

3.2.3.2 Requirement to appear in person

To request the certificates it is not necessary to appear directly in person as due to the already accredited relationship between the natural person and the Administration, body or public law entity to which they are linked and the fact that this request is made by an operator authorised by the subscriber in the contract.

Nor is it necessary for the signatory to appear directly to accept the certificate since it can be done by means of an advanced electronic signature.
During this process the identity of the natural person identified in the certificate is confirmed

3.2.3.3 Link of the natural person

The documentary justification of the link of a natural person identified in a certificate with the Administration, body or public law entity to which they are linked is provided by the record of same in the Personnel Registries of the Administration, body or public law entity to which the natural person is linked.

3.2.4 Non-verified subscriber information

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

3.2.5 Validation of authority

In order to issue website certificates esFIRMA validates the Applicant's control over the FQDN by confirming the existence of the file “esfirma.com” under the "/.wellknown/pki-validation" directory accessible via HTTP over port 80. The file must contains a Request Token with an hexadecimal encoded octect string obtained from concatenate a challenge with the SHA256 hash of the PKCS#10 CSR used to request the certificate:

token:=HEX(challenge_bytes||SHA256(CSR_bytes))

esFIRMA verify the validity of the token. The token is expired after 12 hours and just after use. The challenge is uniquely linked with the CSR's Certificate Request Info.

esFIRMA maintains a log of which domain validation method, including relevant BR version number, was used to validate every domain.

3.2.6 Criteria for interoperation

esFIRMA has no interoperability relations with other external certification authorities.

esFIRMA does not issue Subordinate CA Certificates to external parties and its issuing CA is not technically constrained.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

esFIRMA does not re-key its certificates. esFirma issues a new certificate following the request procedure registered on the Electronic Administration Platform.

3.3.2 Identification and authentication for re-key after revocation

esFIRMA does not re-key certificates.

3.4 Identification and authentication for revocation request

esFIRMA authenticates the requests and reports pertaining to the revoking of a certificate, verifying that they originate from an authorised person.

The acceptable methods for said verification are the following:

- The sending of a revocation request on the part of a subscriber or natural person identified on the certificate, signed electronically.
- The use of the "identity verification phrase" or other methods of personal authentication, which consists of Information that is only know the natural person identified on the certificate and which allows them to automatically revoke their certificate.
- Appearance in person in the office of the subscriber entity.

- Other means of communication such as telephone, where, in the judgement of esFIRMA, there are reasonable guarantees of the identity of the person requesting the revocation.

esFIRMA does not suspend certificates. Requests to suspend certificates are treated as requests to revoke.

4. Certificate life-cycle operational requirements

4.1 Certificate Application

4.1.1 Who can submit a certificate application

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

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

There is an authorisation of the subscriber so that the requester can submit the request, which is legally implemented through the certificates request sheet subscribed by said requester in the name of the Administration, body or public law entity.

Only subscribers who have demonstrated control over the name of the domain to be included in the Certificate are able to request Website authentication certificates. Control over the domain name will be verified esFIRMA as described in 3.2.5.

4.1.2 Enrollment process and responsibilities

esFIRMA receives requests for certificates lodged by the Administrations, bodies and public law entities.

The requests are implemented through a document in electronic format, completed by the Administration, body or public law entity, the recipient of which is esFIRMA and which includes the data of the persons issuing the certificate. The request will be made by the operator authorised by the subscriber (responsible for certification) and who has been identified in the contract between the subscriber and esFIRMA.

The request should be accompanied by supporting documentation and other circumstances of the natural person identified in the certificate in accordance with the provisions established in Section 3.2.3. It should also be accompanied by a physical

address or other data which allows for the natural person identified in the certificate to be contacted.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

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

If so, esFIRMA verifies the information provided, verifying that the requirements described in Section 3.2 have been met.

The supporting documentation of the approval of the request must be retained and duly registered with guarantees of the security and integrity for the term of 15 years from the expiry of the certificate, even in the case of the early loss of the validity due to revocation, in the case of qualified certificates.

esFIRMA maintain documented procedures that identify and require additional verification activity for High Risk Certificate Requests, phishing or other fraudulent usages, prior to the Certificate's approval querying domain reputation lists and esFIRMA own risk-mitigation criteria.

4.2.2 Approval or rejection of certificate applications

esFIRMA approves the certificate request and proceeds with its issue and delivery, after the request on the Electronic Administration Platform.

In the event of suspicion that the information may not be correct or that it may affect the reputation of the Certification Entity or that of the subscribers, esFIRMA will reject the request or will stop its approval until the complementary checks deemed appropriate are carried out.

In the event that additional checks do not confirm that the information to be verified is correct, esFIRMA shall definitively reject the request.

esFIRMA notifies the requester of the approval or rejection of the request.

esFIRMA may automate the verification procedures to ensure that the information which the certificates will contain is correct and to approve the requests.

CAA checking is not performed when esFIRMA is the DNS Operator (as defined in RFC 7719) of the domain. When esFIRMA is not the DNS Operator the, the DNS's CAA "issue" record value is verified to match "esfirma.com". Certificates are not issued if any record lookup failure occurs.

The esFIRMA's recognized domain names are:

- *.eadministracio.cat
- *.egoitzaelektronikoa.eus
- *.sedelectronica.gal
- *.sedelectronica.es
- *.sedelectronica.com
- *.sedeelectronica.es
- *.sedeelectronica.com
- *.testing.esfirma.com

4.2.3 Time to process certificate applications

esFIRMA attends to the certificate requests in the order they arrive, in a reasonable term and can specify a maximum term guarantees in the certificates issue contract.

The requests are maintained active up to approval or rejection.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Upon approval of the certification request, the certificate is issued in a secure manner 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 in accordance with the procedure indicated in Section 4.4.2 or via the messaging system of the Electronic Administration Platform

Throughout the process, esFIRMA:

- Protects the confidentiality and integrity of the registration data it has available.
- Uses reliable systems and products which are protected against alteration and which ensure technical security and, where applicable, the encryption of the certification processes which they support.
- Generates a pair of keys through a certificate generation procedure securely linked to the key generation procedure.
- Employs a certificate generation procedure that securely links the certificate with the registration information, including the certified public key.
- It ensures that the certificate is issued by systems that use protection against falsification and that guarantee the confidentiality of the keys during the generation process of said keys.
- The certificate includes 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 of issue of the certificate.

4.3.2 Notification to subscriber by the CA of issuance of certificate

esFIRMA notifies the subscriber Administration, body or public law entity of the certificate and the natural person identified on the certificate of the issue of the certificate via the email addresses included on the Electronic Administration Platform.

4.4 Certificate acceptance

Throughout this process, esFIRMA will carry out the following actions:

- Definitively verify the identity of the natural person identified on the certificate with the collaboration of the Administration, body or public law entity in accordance with the provisions of Sections 3.2.2, 3.2.3, and 4.3.1.
- Deliver the delivery acceptance sheet to the natural person identified in the certificate (with the collaboration of the Administration, body or public law

entity in the event that the signatory does not have an electronic DNI), which shall include the following minimum contents:

- Basic information on the use of the certificate, in particular including the information relating to the provision of certification services and the applicable Declaration of Certification Practices and the obligations, powers and responsibilities
- Information relating to the certificate.
- Recognition on the part of the signatory of receipt of the certificate and acceptance of the above elements.
- Regime of obligations of the signatory.
- Responsibility of the signatory.
- Method of exclusive allocation to the signatory of its private key and activation data of the certificate in accordance with the provisions of Sections 6.2 and 6.4.
- The date of the act of delivery and acceptance.

- Obtain the signature, manuscript or electronic, of the person identified on the certificate.

Where necessary, the Administration, body or public law entity collaborates in these processes and must register the above acts in a document and retain the original documents (delivery and acceptance sheets) issuing an electronic copy to esFIRMA along with the originals when esFIRMA requires access to same.

4.4.1 Conduct constituting certificate acceptance

Upon approval of the certification request, the certificate is issued in a secure manner and the signatory is notified of its acceptance via a link sent to the mobile device and/or email address designated by the subscriber in the certificate request or via the messaging system of the Electronic Administration Platform.

On the certificates issued on software, the certificate and keys are managed in a HSM with a control signatory exclusive for its use.

On the certificates issued on card, these are issued to the person responsible for the certification of the subscriber and the corresponding PINs are issued directly to the postal address of the signatory.

Moreover, the acceptance of the certificate on the part of the natural person identified on the certificate is by means of the signing of the delivery and acceptance sheet via the Electronic Administration Platform.

4.4.2 Publication of the certificate by the CA

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

4.4.3 Notification of certificate issuance by the CA to other entities

esFIRMA does not provide any notification to third parties regarding the issue of the certificate.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

esFIRMA requires the following:

- To provide esFIRMA with complete and adequate information in accordance with the requirements of this Declaration of Certification Practices, in particular that pertaining to the acceptance procedure.
- To state its prior consent for the issue and delivery of a certificate.
- To use the certificate in accordance with the provisions of section 1.4.
- When the certificate functions together with a QSCD, recognising the production capacity of qualified signatures it is equivalent to manuscript signatures and other types of electronic signatures and information encryption mechanisms.
- To be particularly diligent in the custody of the private key in order to ensure there is no unauthorised use, in accordance with the provisions of sections 6.1, 6.2 and 6.4.
- To inform esFIRMA and any person who may trust the certificate without any unjustified delays:
    - The loss, theft or potential compromise of the private key.

  - The loss of control of the private key, due to the activation data (for example, the PIN code) being compromised or for any other reason.
  - The inaccuracy or change in the content of the certificate which the subscriber is aware of or may be aware of.
- To cease using the private key for the duration of the period indicated in Section 6.3.2.
- To ensure that the information provided by the signatory contained in the certificate is correct.
- That the certificate is used exclusively for legal and authorised uses in accordance with the Declaration of Certificate Practices.
- To ensure that no unauthorised person has ever had access to the private key of the certificate and that it is the only party responsible for damages due to failure to fulfil its obligation to protect the private key.
- To ensure that the signatory is a final entity and not the certification services provider, and that it will not use the corresponding private key listed on the certificate to sign any certificate whatsoever (or any other format of certified public key), nor the Certificate Revocations List nor the status as services provider or in any other case.

4.5.2 Relying party public key and certificate usage

esFIRMA contractually forces the subscriber to:

- Provide esFIRMA with complete and adequate information in accordance with the requirements of this Declaration of Certification Practices, in particular that pertaining to the acceptance procedure.
- State its prior consent for the issue and delivery of a certificate.
- Use the certificate in accordance with the provisions of section 1.4.
- Inform esFIRMA and any person who may trust the certificate, without any unjustified delays, of any occurrence of the following:
  - The loss, theft or potential compromise of the private key.
  - The loss of control of the private key, due to the compromised of the activation data (for example, the PIN code) or any other reason.
  - The inaccuracy or change in the content of the certificate which the subscriber is aware of or may be aware of.

  - The loss, alteration, unauthorised use, theft or comprise of the card where there is one.
- Inform the natural person identified on the certificate of the specific obligations of same and to establish mechanisms to ensure effective compliance with same.
- Not monitor, change or carry out reverse engineering actions on the technical implementation of the esFIRMA certification services without prior written permission.
- Not compromise the security of the certification services of esFIRMA without prior written permission.
- Ensure that the declarations made in the request are correct.
- Ensure that the information provided by the Subscriber contained in the certificate is correct.
- Ensure that the certificate is used exclusively for legal and authorised uses in accordance with the Declaration of Certificate Practices.
- Ensure that no unauthorised person ever has access to the private key of the certificate and that it is the only party responsible for damages due to failure to fulfil its obligation to protect the private key.
- Ensure that the subscriber is a final entity and not the certification services provider, and that it will not use the corresponding private key listed on the certificate to sign any certificate whatsoever (or any other format of certified public key), nor the Certificate Revocations List nor the status as services provider or in any other case.

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

- To independently seek advice on the fact that the certificate is appropriate for the intended use.
- To verify the validity, suspension or revocation of the certificates issued for which information on the status of the certificates is used.
- To verify all the certificates of the hierarchy of certificates before trusting the digital signature or any of the certificates of the hierarchy
- To recognise that the electronic signatures verified on a Qualified Signature Creation Device have the legal status of qualified signatures, that is, equivalent to manuscript signatures, and that the certificate allows the creation of other types of electronic signatures and encryption mechanisms.

- To consider, at all times, any limitation of use of the certificate in terms of the certificate itself or in the contract of the third party trusting the certificate.
- To consider, at all times, any precaution established in a contract or in another instrument, regardless of its legal status.
- To not monitor, change or carry out reverse engineering actions on the technical implementation of the esFIRMA certification services without prior written permission.
- To not compromise the security of the certification services of esFIRMA without prior written permission.

4.6 Certificate renewal

esFIRMA does not renew its certificates. Instead, esFirma issues a new certificate following the requirement procedure described in the Electronic Management Platform.

4.6.1 Circumstance for certificate renewal

No Stipulation

4.6.2 Who may request renewal

No Stipulation

4.6.3 Processing certificate renewal requests

No Stipulation

4.6.4 Notification of new certificate issuance to subscriber

No Stipulation

4.6.5 Conduct constituting acceptance of a renewal certificate

No Stipulation

4.6.6 Publication of the renewal certificate by the CA

No Stipulation

4.6.7 Notification of certificate issuance by the CA to other entities

No Stipulation

4.7 Key and certificate renewal

4.7.1 Circumstance for certificate re-key

No Stipulation

4.7.2 Who may request certification of a new public key

No Stipulation

4.7.3 Processing certificate re-keying requests

esFIRMA shall notify the subscriber that the signatory needs to appear in person and sign the acceptance sheet in those cases in which this is required for the reason that the legal five year identification period has elapsed.

Such appearance and identification shall be carried out pursuant the instructions of section 3.2.

The acceptance sheet must be carried out pursuant the instructions of section 4.4.2.

4.7.4 Notification of new certificate issuance to subscriber

No Stipulation since no certificate renewals are carried out.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

No Stipulation

4.7.6 Publication of the re-keyed certificate by the CA

No Stipulation

4.7.7 Notification of certificate issuance by the CA to other entities

esFIRMA does not make any notifications to third parties regarding any issued certificate.

4.8 Certificate modification

Modification of certificates shall be treated as a new issued certificate, and the provisions of sections 4.1, 4.2, 4.3 and 4.4. shall apply.

4.8.1 Circumstance for certificate modification

No Stipulation

4.8.2 Who may request certificate modification

No Stipulation

4.8.3 Processing certificate modification requests

No Stipulation

4.8.4 Notification of new certificate issuance to subscriber

No Stipulation

4.8.5 Conduct constituting acceptance of modified certificate

No Stipulation

4.8.6 Publication of the modified certificate by the CA

No Stipulation

4.8.7 Notification of certificate issuance by the CA to other entities

No Stipulation

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

esFIRMA may revoke a certificate when any of the following scenarios occurs:

1) Circumstances that affect information included on the certificate:
   a) Any of the data included in the relevant certificate have been modified, after issuing the corresponding certificate including such modifications.
   b) It has been found that some of the data included in the certificate request are not accurate.
   c) It has been found that some of the data included in the certificate are not accurate.

2) Other circumstances affecting the key or certificate security:
   a) Compromise of the private key, the infrastructure or the certificate service provider system issuing the certificate, provided that this compromise affects reliability of certificates issued from this incident.
   b) esFIRMA has not complied with the requirements provided in the certificate management procedures as established in the Guidelines for certificate Procedures
   c) The key or issued certificate safety has been compromised or is suspected to be compromised.
   d) Unauthorised access or use by a third party of the private key corresponding to the public key included in the certificate.
   e) Irregular use of the certificate by the natural person identified in the certificate

3) Circumstances that affect the subscriber or the natural person identified in the relevant certificate:
   a) The legal relationship for service provisioning between esFIRMA and the subscriber has ended.
   b) The underlying legal relationship of the original cause for issuing a certificate to the natural person identified on it.
   c) The certificate requester does not comply with the pre-established conditions to make the requirement.
   d) The subscriber or the person identified in the certificate does not comply with their obligations, responsibilities and guarantees as established in the corresponding legal document.
   e) Supervening incapacity or death of the key holder.
   f) Termination of the legal person who is the subscriber of the certificate, as well as termination of the authorisation granted by the subscriber to the

key holder or end of the relationship between the subscriber ant the person identified on the certificate.

g) Request by the subscriber that the certificate is revoked, pursuant section 3.4.

4) Other circumstances:
   a) Suspension of esFIRMA's certificate services, pursuant section 5.8.
   b) Any ongoing use of the certificate that is harmful for esFIRMA. In this case, it is considered that any use that adjusts to the following criteria is harmful for esFIRMA:
      - Nature and number of complaints submitted.
      - The identity of those organizations that submit such complaints.
      - The relevant laws and regulations in force from time to time.
      - The response to these complaints provided by the subscriber or the person identified in the certificate.

4.9.2 Who can request revocation

The following persons may request that a certificate is revoked:

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

4.9.3 Procedure for revocation request

The revocation request must include the following information:

- Revocation request date.
- Identification of the subscriber or the signatory.
- Detailed justification of the revocation request.

The request must be authenticated by esFIRMA, pursuant the requirements established in section 3.4 of this policy, before completing the revocation.

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

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

The revocation service is located in the Electronic Management Platform by means of which the signatory and the subscriber manage their certificates.

In the event that the person to whom a revocation request by a natural person identified in the certificate is addressed is the subscribing organization, this organization, once the request has been authenticated, must address a request in this sense to esFIRMA.

The revocation request shall be processed at its reception; the subscribed and the natural person identified in the certification shall be informed about the change in the status of the revoked certificate.

esFIRMA does not reactivate a certificate that has already been revoked.

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

4.9.4 Revocation request grace period

Revocation request shall be issued immediately as soon as the cause for such revocation is known, and in any case no later than 48 hours[3].

4.9.5 Time within which CA must process the revocation request

Revocation shall be effective no later than 60 minutes after it is received within esFIRMA usual operating hours.

4.9.6 Revocation checking requirement for relying parties

Third parties are bound to verify the status of those certificates that they need to consider reliable.

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

A method to verify the status of certificates is to verify the most recent version of the certificate Revocation List issued by esFIRMA certificate Organization.

Certificate Revocation Lists are published in the Certificate Authority Deposit, as well as in the following website, stated on each certificate:

- *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

4.9.7 CRL issuance frequency (if applicable)

esFIRMA issues a CRL at least every 24 hours whenever a revocation has occurred-

The CRL states the scheduled time at which a new CLR is to be published; however, a new CRL may be published before this time in order to include the latest revocations.

The CRL compulsorily maintains the revoked or suspended certificate to its expiration date.

4.9.8 Maximum latency for CRLs (if applicable)

CRLs are published on the Deposit in a reasonable immediate period after they are generated, which may not exceed a few minutes.

4.9.9 On-line revocation/status checking availability

esFIRMA informs about the revocation status of certificates by means of the OCSP, which allows to verify online the valid status of certificates from the following addresses:

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

In the event that certificate status verification systems fail for reasons that are outside esFIRMA's control, esFIRMA is bound to make its best efforts to ensure that this services is restored as soon as possible, an in any case no later than one day.

esFIRMA provides information to third parties that rely on certificates regarding the certificate status report service operation.

Certificate status verification services are free of charge.

esFIRMA keeps all information on revocation status available once the certificate validity period has elapsed-

4.9.10 On-line revocation checking requirements

Consultation of certificate status, primarily by accessing the OCSP, before considering them reliable shall be compulsory.

esFIRMA supports GET method for OCSP.

esFIRMA updates Online Certificate Status Protocol at least every four days and immediately in regular conditions.

OCSP responses have a maximum expiration time of 48 hours.

For the status of Subordinate CA Certificates esFIRMA update information provided via OCSP at least every six months and within 24 hours after revoking a Subordinate CA Certificate.

If the OCSP responder receives a request for status of a certificate that has not been issued, then the responder respond with a "unknown" status and log such requests as part of esFIRMA security response procedures.

4.9.11 Other forms of revocation advertisements available

Alternatively, third parties relying on certificates may verify the revocation status of such certificates by consulting the most recent CRLs published by esFIRMA. Such CRLs are published in esFIRMA's websites, as well as on those websites stated on the certificates.

esFIRMA does not rely on OCSP stapling to distribute its OCSP responses.

4.9.12 Special requirements re key compromise

Compromise of esFIRMA's private key must be noticed to all certificate services parties, as extensively as possible, my means of sharing this fact on esFIRMA's website as well as, if considered necessary, other media, including paper-based media.

4.9.13 Circumstances for suspension

esFIRMA does not suspend certificates.

4.9.14 Who can request suspension

esFIRMA does not suspend certificates.

4.9.15 Procedure for suspension request

esFIRMA does not suspend certificates.

4.9.16 Limits on suspension period

esFIRMA does not suspend certificates.

4.10 Certificate status services

4.10.1 Operational characteristics

Certificate status verification services are provided through a web enquiry interface at the esFirma website (https://www.esfirma.com).

Verification may also be carried out by accessing the OCSP service in the website stated in section 4.9.9

Revocation entries on a CRL or OCSP Response are not removed in any case.

4.10.2 Service availability

Status verification services are available 24 hours a day, 7 days a week, all year round, with the exception of scheduled outages.

Certificate status verification services are free of charge.

4.11 End of subscription

Once that the validity period of the certificate has elapsed, the service subscription shall be terminated.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

esFIRMA does not provide key deposit and retrieval practices.

4.12.2 Session key encapsulation and recovery policy and practices

No indications.

5. Facility, management and operational controls

5.1 Physical controls

esFIRMA has established physical and environmental safety controls in order to protect resources on those installations where the systems, including both the systems themselves and the equipment used for requesting registration and approval, for technical generation of certificates and for cryptographic hardware management operations.

Specifically, physical and environmental safety policies applicable to certificate generation, cryptographic devices and revocation management services have established provisions for the following scenarios:

- Physical access controls.
- Protection against natural disasters.
- Fire protection measures.
- Failure of supporting systems (electric energy, telecommunications, etc.)
- Structural collapse.
- Floods.
- Protection against theft.
- Unauthorised extraction of equipment, information, supporting hardware and software regarding components used by the certification service provider to provide such services.

These measures apply to those facilities where certificates are generated under full responsibility of esFIRMA, that provides such services from its high security facilities, both its main facilities and, when necessary, its contingent operation facilities, which are audited periodically.

Facilities include corrective preventive maintenance systems which offer support within 24 hours of the notification and 24 hours a day, 365 days a year.

5.1.1 Site location and construction

Physical protection is achieved by creating clearly defined security perimeters with regard to services. Quality and robustness of facility construction materials guarantees an appropriate level of protection against forced instructions and located in a disaster low-risk area which may be easily access.

The Data Treatment Centre where cryptographic operations are to be carried out:

- Has redundant infrastructures.
- Has more than one alternative power and cooling sources in case of emergency.
- Maintenance operations do not require the Centre to be offline at any time.
- Monthly reliability attains 99.995%.

esFIRMA has facilities that physically protect provision of services such as certificate request approval and revocation management from being compromised for reason of unauthorised access to systems or data, and well as from disclosure of such data.

5.1.2 Physical access

The data centre where esFIRMA's Certificate Authority is located holds TIER IV qualification.

Physical access to the esFIRMA facilities where certificate processes are carried out are limited and protected by means of a combination of physical and procedural measures. Therefore:

- It is limited to expressly authorised personnel, who has to be identified at the time they are accessed and their access is recorded, including recording by means of a television closed circuit, which shall be recoded.

- Access to the rooms is monitored by means of ID card readers.

- In order to access the RAC where encryption processes are located, a previous authorisation by esFIRMA to the hosting service administrator that have the key to the jail is needed.

5.1.3 Power and air conditioning

esFIRMA facilities have voltage stabilising equipment, a power feeding system and a redundant engine generator.

Rooms containing computer equipment are provided with temperature control systems and air conditioning.

5.1.4 Water exposures

Facilities are located in a low flood risk area.

Rooms where computer equipment is located have humidity detection systems.

5.1.5 Fire prevention and protection

esFIRMA's assets and facilities have automatic fire detection and extinction systems.

5.1.6 Media storage

Only authorised personnel may access storage hardware.

Information classified in the highest level of security is stored in a safety cabinet outside the facilities of the Data Processing Centre.

5.1.7 Waste disposal

Discarding supports, both paper and magnetic, is carried out by means of mechanisms that guarantee that the information contained by them is impossible to retrieve.

In case of magnetic supports, they are subject to formatting, permanent deleting or physical destruction by means of specific software that performs at least three deletion runs, with different deleting patterns.

Paper documents must be shredded using shredders or stored in specially purposed bins to be subsequently shredded under relevant monitoring.

5.1.8 Off-site backup

esFIRMA has secure external facilities devoted to custody of documents and magnetic and electronic devices separately from the operational centre.

At least two expressly authorised persons are required to access, deposit or retrieve any device.

5.2 Procedural controls

esFIRMA guarantees that its systems are operated in a secure manner. For this purpose, procedures for the functions that affect service provision have been implemented.

esFIRMA's staff executes the relevant administrative and management procedures in compliance with the corresponding security policy.

5.2.1 Trusted roles

Pursuant its security policy, esFIRMA has identified the following roles as positions of trust:

- **Internal Auditor:** Responsible for compliance with operational procedures. The Internal Auditor must be a person external to the Information Systems department. The Internal Auditor's tasks are not compatible in time with Certification tasks or with Systems. Those roles shall be dependent to the Head of Operations, reporting both to the Head of Operations and to the Technical Direction.
- **System Administrator:** Responsible for correct functioning of hardware and software that support the certification platform.
- **CA Administrator:** Responsible for actions to be performed with encryption material or with certain functions that involve activation of private keys of the certification authorities described in this document, or any of the element of those keys.
- **CA Operator:** Required co-responsible, jointly with the CA Administrator, for custody of encrypted keys activation material, as well as responsible of backup operations and CA maintenance.

- **Registration Administrator:** Person in charge of approving all certification request made by the subscriber.
- **Security Manager:** Person in charge coordinating, monitoring and enforcing any security measure defined by esFIRMA's security policies. They shall be responsible for any aspects related to information security: logical, physical, organizational, in networks, etc.

The person in the above function shall be subject to specific investigative and control procedures.

5.2.2 Number of persons required per task

esFIRMA guarantees that at least two persons are to carry out the tasks detailed in the corresponding Certificate Policies. Especially, handling the device where to the root Certificate Authorities' keys are kept.

5.2.3 Identification and authentication for each role

People assigned to each role are identified by the internal auditor, who will ensure that each person carries out the operation assigned to them.

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

Access to any resources is carried out, depending on the relevant asset, by means of encrypted cards and activation codes.

5.2.4 Roles requiring separation of duties

The following tasks need to be carried out by, at least, two different persons:

- Issuing and revoking certificates and accessing the deposit.
- Generating, issuing and destroying certificates by the Certificate Authority.
- Certificate Authority start-up.

5.2.5 PKI Management System

The PKI system is formed by the following modules:

- Component/module for management by the Subordinate Certificate Authority.
- Component/module for management by the Registration Authority.
- Component/module for request management.
- Component/module for key management (HSM)
- Component/module for databases.
- Component/module for CRL management.
- Component/module for management of the OCSP service.
- Component/module for management by the Time Stamping Authority (TSA).

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

All personnel members that carry out tasks corresponding to positions of trust must have joined the production centre at least a year before and must be hired by means of indefinite contracts.

All personnel must be qualified and has been conveniently trained to carry out the operations assigned to them.

The personnel carrying out reliable functions do not have any personal interest that may cause a conflict with the development of the function entrusted to them.

esFIRMA ensures that registration personnel are to be trusted with regard to carry out registration tasks.

The Registration Administrator has completed a training course in order to carry out the tasks corresponding to request validation.

In general terms, esFIRMA shall replace from a position of trust any employee when esFIRMA becomes aware that this employee has committed any unlawful act which may have an impact on the employee's performance.
esFIRMA shall not appoint any non-eligible person to any position of trust or management function, especially when the reason for their non-eligibility is having been convicted by any crime or unlawful act which affects their eligibility to the function.

5.3.2 Background check procedures

esFIRMA performs checks on the history of potential employees before they join the company or their specific function.

esFIRMA must obtain the unequivocal consent of the affected person to carry out such preliminary check, and processes and protects all your personal data pursuant 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.

Such checks shall be subsequently repeated with an appropriate regularity.

All checks shall be subject to the scope authorised by the relevant current laws and regulations. The reasons for which a candidate may be not accepted to reliable positions are the following:

- False data in the job application completed by the candidate.
- Very negative or untrustworthy professional references.

The job offer must include that a preliminary check in the candidate's history shall be performed, mentioning that a refusal to be subject to such check shall cause the corresponding job application to be rejected.

5.3.3 Training requirements

esFIRMA trains the personnel members who exercise position of trusts and management functions until they are sufficiently qualified; a record of such training must be appropriately filed.

Training programmes must be periodically updated and improved. Training programmes must include, 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 needs to complete.
- esFIRMA's security policies and procedures. Use and operation of installed hardware and software.

- Management and processing of incidents and security compromises.
- Emergency and business continuity procedures,
- Management and security procedures regarding personal data treatment.

5.3.4 Retraining frequency and requirements

esFIRMA updates personnel training according to their needs, with sufficient frequency as to allow training to fulfil its role in a competent and satisfactory manner, especially when substantial modifications are carried out on certificate tasks.

5.3.5 Job rotation frequency and sequence

Not applicable.

5.3.6 Sanctions for unauthorized actions

esFIRMA has a system of penalties in order to ensure accountability of unauthorised action. This system must be compliant with current labour regulations and must especially be coordinated with the penalty system included in the collective agreement applicable to the personnel.

Disciplinary actions include suspension and dismissal of the person accountable for the harmful action, and must be proportional to the seriousness of the unauthorised action.

5.3.7 Independent contractor requirements

Employees hired to perform tasks corresponding to positions of trust must have previously signed the relevant confidentiality clauses and operations requirements implemented by esFIRMA. Any action which may compromise the security of the accepted process may, once assessed, cause the job contract to be terminated.

In case that all or part of the certificate services are operated by a third party, controls and forecasts made in this section or on other sections of the CPS must be applied and complied with by such third party that performs the relevant operative functions for certificate services. Notwithstanding the above, the Certificate Authority shall be in all cases responsible for its effective execution. Those aspects are materialised by the

legal instrument used to execute the agreement that certification services are to be provided by a third party other than esFIRMA.

5.3.8 Documentation supplied to personnel

The certificate services provider shall supply those documents strictly required by their staff from time to time, so that they are able to perform their work in a competent, satisfactory manner.

5.4 Audit logging procedures

5.4.1 Types of events recorded

esFIRMA generates and keeps records, at least, of the following events related to the security of the institution:

- System switching on and switching off.
- Attempts to create, delete, set up passwords or modify privileges.
- Attempts to log in and log out.
- Attempts at unauthorised access to the CA system through the network.
- Attempts at unauthorised access to the file system.
- Physical access to logs.
- Changes in system maintenance and set-up.
- Registration of CA applications.
- CA system switching on and switching off.
- Changes in CA details and/or keys
- Changes in certificate policy generation.
- Generation of own keys
- Creating and revoking certificates.
- Records of destruction of media containing keys and activation data.
- Events related with the encryption module life cycle, such as reception, use and uninstalling such module.
- Firewall and router activities[4]
- Key generation procedures and key management databases.
- Physical access records.
- System maintenance and system setup changes.
- Changes in personnel.

[4] Sect. 6.4.5.a) vi) of ETSI EN 319 411-1

- Reports on commitments and disagreements.
- Records proving destruction of material including information such as keys, activation data or personal data of subscriber, for individual certifications, or, for corporate certificates, of the natural person identified in the certification.
- Having activation data to carry out actions by means of the private key of the Certificate Authority.
- Complete reports detailing every attempt of physical intrusion in those infrastructures that support issuing and managing certificates.

Registration entries include the following elements:

- Entry date and time.
- Entry serial or sequential number, for automatic registration.
- Identification of the entity that makes the entry.
- Type of entry.

All events related to the preparation of the Qualified Signature Creation Device used by the signatories or custodians[5].

5.4.2 Frequency of processing log

esFIRMA reviews their logs whenever a system alert is triggered by the occurrence of an incident.

Audit record processing involves a review of records which includes a verification that those were not tampered with, a brief inspection of all record entries and a further, in-depth inspection of any alert or irregularity on records. Actions carried out as a consequence the audit inspection are documented.

esFIRMA has a system that allows to guarantee:

- Sufficient space for log storage.
- That log files are not overwritten.
- That stored information includes, at least: type of event, date and time, user that executes the action and result of the operation.

[5] Sect. 6.4.5.a) vi) of ETSI EN 319 411-2

- Log files shall be stored in structured files which may include a database for subsequent exploration.

5.4.3 Retention period for audit log

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

esFIRMA make these audit logs available to its Qualified Auditor upon request.

5.4.4 Protection of audit log

System logs:

- Are protected against unauthorised handling, deletion or removal[6] by means of the signature in the files that include them.
- They are stored in fireproof devices.
- Availability is protected by storing them in facilities which are external to the centre where the CA is located.

Access to log files is restricted to authorised persons. Besides, devices are handled by authorised personnel at all times.
There is an internal procedure describing in detail the management processes for devices including audit logs data.

5.4.5 Audit log backup procedures

esFIRMA has set an appropriate backup procedure so that, in case those relevant files are destroyed or lost, the corresponding log backup copies may be available within a short period of time.

esFIRMA has implemented as secure backup procedure for audit logs, and a copy of all logs in external devices is carried out weekly. Additionally, a copy is kept at external premises.

[6] Sect. 7.10.f) of ETSI EN 319 401

5.4.6 Audit collection system (internal vs. external)

Audit information on events is automatically collected at internal level by the operative system, network communications and certificate management software, as well as manually generated data, and it shall be stored by duly authorised personnel. All the above forms the cumulative system for audit records.

5.4.7 Notification to event-causing subject

When an event is recorded in the cumulative system for audit record, the relevant individual, organization, device or application that triggered the event needs not to be notified.

5.4.8 Vulnerability assessments

Vulnerability analysis is performed as part of esFIRMA's audit processes.

Vulnerability analyses must be executed, revised and reviewed by means of an examination of these monitored events. Such analyses must be carried out on a daily, monthly and annual basis.

System audit data are stored for the purposes of being used in the investigation of any incidence and locate any vulnerabilities.

esFIRMA's security program include an annual Risk Assessment.

5.5 Records archival

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

5.5.1 Types of records archived

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

- All system audit related data (PKI, TSA and OCSP).

- All data regarding certificates, including contracts with signatories and data related to identification and location.
- Requests to issue and revoke certificates, including all reports regarding the revocation process[7].
- All those specific choices that the signatory or the subscriber has available for the duration of the subscription agreement[8].
- Type of document submitted in the certificate request.
- Identity of the Registration Entity that accepts the certificate request.
- Single identification number provided in the previous document.
- All issued or published certificates.
- Issued CRLs or records regarding the status of generated certificates.
- History of generated keys.
- Communications between PKI elements.
- Certificate Policies and Practices
- All audit data identified under section 5.4
- Information regarding certification requests.
- Documents contributed to support certificate requests.
- Information on the certificate life cycles

esFIRMA shall be responsible for correctly filing all this material.

5.5.2 Retention period for archive

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

5.5.3 Protection of archive

esFIRMA protects files in such a manner that only duly authorised persons may be granted access. The file is protected against unauthorised viewing, modification, deletion or any other action by means of storage in a reliable system.

esFIRMA assures correct protection of files by means of assigning qualified personnel to treat such files, and by subsequently storing then in fireproof safety cabinets in external facilities.

---

7 Sect. 6.4.5.h) vi) of ETSI EN 319 411-1

8 Sect. 6.4.5.c) iv) of ETSI EN 319 411-1

5.5.4 Archive backup procedures

esFIRMA has external storage facilities in order to guarantee availability of electronic files copies. Physical documents are stored in safe places with access restricted to authorised personnel.

esFIRMA makes, at least, daily incremental backup copies of all its electronic documents and weekly complete backup copies for data retrieval purposes.

Besides, esFIRMA (or the organizations that carry out registration functions) keeps a copy of the paper document in a safe place outside the Certificate Entity facilities.

5.5.5 Requirements for time-stamping of records

Records are dated by means of a reliable source through NTP.

esFIRMA has set a procedure in which the time setup of devices used for issuing certificates is described.
The time used to record the events in the audit record must be synchronised with the UTC at least once a day[9].

This information does not need to be digitally signed.

5.5.6 Archive collection system (internal or external)

esFIRMA has a centralized system for collecting information with regard to the activities of equipment involved in the certificate management service.

5.5.7 Procedures to obtain and verify archive information

esFIRMA has a procedure describing the process to verify that filed information is correct and accessible.

[9] Sect. 7.10.d) of ETSI EN 319 401

5.6 Key changeover

Before the CA private key expires and is no longer valid for use, such key shall be renewed. The old CA and their private key shall only be used to sign AC while there are active certificates issued by such CA. A new CA shall be generated with a new private key and a new DN.

The change of keys of the subscribed is carried out by means of carrying out a new emission process.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

Backup copies of certain information are stored in external storage facilities outside esFIRMA, which are made available in case of compromise or disaster. This information includes: technical data regarding certificate requests, audit data and database records of all issued certificates.

Backup copies of esFIRMA's private keys are generated and maintained pursuant the established in section 6.2.4.

5.7.2 Computing resources, software, and/or data are corrupted

When an event involving corrupted resources, applications or data occurs, the incidence shall be communicated to safety and the appropriate management procedures, including escalating, investigation and response to the incident, shall start. If necessary, the esFIRMA's procedures applicable to events of compromised keys or recover after disasters.

5.7.3 Entity private key compromise procedures

If esFIRMA’s private key is known or suspected to have been compromised, the procedures for compromised keys shall be activated, leaded by a response team that shall assess the situation and develop an action plan which is to be executed under the approval of the management of the Certificate Authority.

If esFIRMA's private key is compromised, it may be the case that the status of certificates and revocation procedures that have used this key are no longer valid[10].

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

If the root key is compromised it must be considered as a separate case in the contingency and business continuity process. This incidence affects, in case of key replacement, to recognition by different applications and public and private services. Recovery of key efficiency in terms of business shall depend mainly on the duration of such processes. The contingency and business continuity document shall address any purely operational terms so that new keys are available, although not for recognition by third parties.

Any failure in the achievement of goals established by this Contingency Plan shall be treated as reasonably inevitable unless such failure is caused by lack of compliance with the obligations set by the CA to implement those processes.

5.7.4 Business continuity capabilities after a disaster

esFIRMA shall re-establish (suspension and revocation and published information on certificate status) pursuant the Business Continuity Plan.
If necessary, esFIRMA has an alternative data center for operating the certification systems described in the business continuity plan.

Both the revocation management service and the consultation service are considered critical and described as so in esFIRMA business continuity plan.

5.8 CA or RA termination

esFIRMA assures that potential interruptions to subscribed and third parties as a consequence of certificate service provisioning discontinuation shall be minimal, and, in particular, guarantees continuous maintenance of the required records to provide certificate evidence in case of a civil or criminal investigation, by means of having such records deposited with a notary public.

[10] Sect. 6.4.8.g) ii) of ETSI EN 319 411-1

Before completing its services, esFIRMA develops a termination plan including the following provisions:

- Provision of the necessary funds to continue completion of revocation activities.
- Communication to the Ministry for Industry, Energy and Tourism, with at least 2 months' notice, any discontinuation of its activities and the destinations of the relevant certificates, specifying whether its management is transferred and to whom, or whether its validity is to expire.
- Communication to the Ministry for Industry, Energy and Tourism of the opening of any bankruptcy proceedings submitted against esFIRMA as well as any other relevant circumstances which may prevent continuation of activities.
- Information to all Signatories, Subscribers or Third Parties that Rely on Certificates and other CAs with which they have any agreement or business relationship with at least 6 months' notice.
- Revocation of any authorisation to subcontractors to act on behalf of the CA in the certificate issuing procedure.
- Transference of its obligations regarding maintenance of registration information and logs for the period of time stated to subscribers and users, for the purpose of being used as evidence in legal procedures and guaranteeing service continuity.
- Destruction or disable use of CA's private keys.
- Revocation of Time Stamping Units (TSU) certificates.
- Maintenance of active certificates and verification and revocation system until all issued certificates have expired.
- Execution of the necessary tasks to transfer maintenance obligations with regard to registration information and event registration files during the respective periods of time stated to subscribers and to third parties that rely on certificates.

6. Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

The pair of keys of the intermediate Certificate Authority "ESFIRMA AC AAPP 2" is created by the root Certificate Authority "ESFIRMA AC RAIZ 2" pursuant the ceremony procedures implemented by esFIRMA, within the high security perimeter intended for this task.

Activities carried out during the key generation ceremony have been recorded, dated and signed by all participating individuals, in the presence of a CISA Auditor. Such registrations are kept for auditing and monitoring purposes for an appropriate period of time as determined by esFIRMA.

Generation of the key for root certificate and intermediate certificate entities is carried out by means of devices with certifications Common Criteria EAL 4+ or FIPS 140-2 Level 3.

ROOT	4.096 bits	25 years
INTERMEDIATE	4.096 bits	13 years
- Final Entities Certificates	2.048 bits	2 years
- TSA Certificate	4.096 bits	5 years

More information in the following PDS locations:

CERTIFICATE	PDS
Public Employee - SENIOR 1.3.6.1.4.1.47281.1.1.1	SPANISH: https://www.esfirma.com/doc-pki/PDS2/EP2-ALTO-SMARTCARD-ES/ ENGLISH: https://www.esfirma.com/doc-pki/PDS2/EP2-ALTO-SMARTCARD-EN/
Public Employee - MIDDLE 1.3.6.1.4.1.47281.1.1.4	SPANISH: https://www.esfirma.com/doc-pki/PDS2/EP2-MEDIO-HSM-ES/ ENGLISH: https://www.esfirma.com/doc-pki/PDS2/EP2-MEDIO-HSM-EN/
e-PA Stamp –MIDDLE Soft 1.3.6.1.4.1.47281.1.2.2	SPANISH: https://www.esfirma.com/doc-pki/PDS2/SO2-MEDIO-SOFT-ES/ ENGLISH: https://www.esfirma.com/doc-pki/PDS2/SO2-MEDIO-SOFT-EN/

e-PA Stamp –MIDDLE HSM 1.3.6.1.4.1.47281.1.2.4	SPANISH: https://www.esfirma.com/doc-pki/PDS2/SO2-MEDIO-HSM-ES/ ENGLISH: https://www.esfirma.com/doc-pki/PDS2/SO2-MEDIO-HSM-EN/
Pseudonym EP – HIGH 1.3.6.1.4.1.47281.1.3.1	SPANISH: https://www.esfirma.com/doc-pki/PDS2/ES2-ALTO-SMARTCARD-ES/ ENGLISH: https://www.esfirma.com/doc-pki/PDS2/ES2-ALTO-SMARTCARD-EN/
Pseudonym EP – MIDDLE 1.3.6.1.4.1.47281.1.3.4	SPANISH: https://www.esfirma.com/doc-pki/PDS2/ES2-MEDIO-HSM-ES/ ENGLISH: https://www.esfirma.com/doc-pki/PDS2/ES2-MEDIO-HSM-EN/
MIDDLE EV electronic headquarters 1.3.6.1.4.1.47281.1.4.2	SPANISH: https://www.esfirma.com/doc-pki/PDS2/SE2-MEDIO-SOFT-ES/ ENGLISH: https://www.esfirma.com/doc-pki/PDS2/SE2-MEDIO-SOFT-EN/
TSA in HSM 1.3.6.1.4.1.47281.1.5.2	SPANISH: https://www.esfirma.com/doc-pki/PDS2/TS2-ES/ ENGLISH: https://www.esfirma.com/doc-pki/PDS2/TS2-EN/
PV - FIRMA CUALIFICADA 1.3.6.1.4.1.47281.1.6.1	ESPAÑOL: url: https://www.esfirma.com/doc-pki/PDS2/PV-FIRMA-SMARTCARD-ES/ INGLÉS: https://www.esfirma.com/doc-pki/PDS2/PV-FIRMA-SMARTCARD-EN/
PV - FIRMA CENTRALIZADA 1.3.6.1.4.1.47281.1.6.4	ESPAÑOL: https://www.esfirma.com/doc-pki/PDS2/PV-FIRMA-HSM-ES/ INGLÉS: https://www.esfirma.com/doc-pki/PDS2/PV-FIRMA-HSM-ES/
PV - AUTENTICACIÓN 1.3.6.1.4.1.47281.1.6.5	ESPAÑOL: https://www.esfirma.com/doc-pki/PDS2/PV-AUTENTICACION-SMARTCARD-ES/ INGLÉS: https://www.esfirma.com/doc-pki/PDS2/PV-AUTENTICACION-SMARTCARD-EN/
PS2 - FIRMA CUALIFICADA **1.3.6.1.4.1.47281.1.7.1**	ESPAÑOL: https://www.esfirma.com/doc-pki/PDS2/PS2-FIRMA-SMARTCARD-ES/ INGLÉS: https://www.esfirma.com/doc-pki/PDS2/PS2-FIRMA-SMARTCARD-EN/
PS2 - FIRMA CENTRALIZADA 1.3.6.1.4.1.47281.1.7.4	ESPAÑOL: https://www.esfirma.com/doc-pki/PDS2/PS2-FIRMA-HSM-ES/ INGLÉS: https://www.esfirma.com/doc-pki/PDS2/PS2-FIRMA-HSM-EN/
PS2 - AUTENTICACIÓN 1.3.6.1.4.1.47281.1.7.5	ESPAÑOL: https://www.esfirma.com/doc-pki/PDS2/PS2-AUTENTICACION-SMARTCARD-ES/ INGLÉS: https://www.esfirma.com/doc-pki/PDS2/PS2-AUTENTICACION-SMARTCARD-EN/

The signatory's keys may be created by the signatory themselves by means of esFIRMA authorised hardware or software.

esFIRMA only create keys by means of a certified device.

esFIRMA never generates software keys to be sent unsecured to the signatory.

Keys are generated by using the RSA public key with a minimum length of 2048 bits.

6.1.2 Private key delivery to subscriber

In certificates in signature creation secure devices, the private key is duly protected inside such secure device.

In software certificates, the signatory private key is created in the system used by such signatory when they request the relevant certificate. For this reason, the private key is duly protected inside the signatory's computer system.

6.1.3 Public key delivery to certificate issuer

The method for sending the public key to the certificate service provider is PKCS#10, other equivalent encrypted test or any other method approved by esFIRMA.

When keys are generated by means of a DCCF, esFIRMA shall ensure that the public key sent to the certificate services provider is generated from a pair of keys generated by said DCCF[11].

6.1.4 CA public key delivery to relying parties

esFIRMA's keys are communicated to third parties that rely on certificates, ensuring the key’s integrity and authenticating its origin by publishing it in the Deposit.

Users may access the deposit in order to obtain public keys, and additionally, in applications S/MIME, the data message may contain a certificate chain, and they are, in this manner, distributed to users.

The root CA and subordinate CAs shall be available to users in the esFIRMA’s website.

6.1.5 Key sizes

The length of the keys used by the root Certificate Authority is RSA 4096 bits.

[11] Sect. 6.5.1.b) vi) of ETSI EN 319 411-2

The length of the keys used by the subordinate Certificate Authority is RSA 4096 bits.
The length of the keys used by the TSA is RSA 4096 bits.
The length of the certificates used by the final entity is RSA 2048 bits.

6.1.6 Public key parameters generation and quality checking

The public keys for the Root CA, subordinate CA and subscriber certificates are coded according to RFC 5280.

Quality check of public key generation parameters

- Module Length = 4096
- Key generation algorithm: rsagen1
- Summarizing encryption functions: SHA256

All keys are generated in equipment, as stated in section 6.1.1.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Keys used for CA certificates shall be exclusively used to sign certificates and CRLs.

The use of keys for final entity certificates is exclusively restricted to the purposes of the digital signature and non repudiation.

The use of keys for final entity website authentication certificates is exclusively restricted to digital signature with the extended use of server authentication key (server authentication)

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

With regard to the modules that manage keys used by esFIRMA and electronic signature certificate subscribers, the level required by the standards stated in the previous section is ensured.

6.2.2 Private key (n out of m) multi-person control

A multi-personal control is required to activate the CA's private key. For this specific DPC, there is a policy that requires **3 of 5 persons** to activate the relevant key.

Cryptographic devices are physically protected as established in this document.

6.2.3 Private key escrow

esFIRMA does not store copies of the signatories' private keys

6.2.4 Private key backup

esFIRMA makes a backup copy of the CAs' private key which enable its retrieval in case of disaster, loss or degradation of such copies. Both generation and retrieval of copies require the participation of at least two persons.

Those recovery files are stored in fireproof cabinets and in the external storage centre.

The hardware keys of the signatory may not be copied, since they may not be extracted from the encryption device.

6.2.5 Private key archival

The CA private keys are filed for a **10-year** period after the issuance of the latest certificate. They will be stored in safe fireproof cabinet and in the external storage centre. The collaboration of at least two persons shall be needed to recover the CAs private keys in the initial encryption device.

6.2.6 Private key transfer into or from a cryptographic module

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

6.2.7 Private key storage on cryptographic module

The Certificate Authority private keys are encrypted and stored in esFIRMA's production encryption modules.

6.2.8 Method of activating private key

EsFIRMA's private key is activated by means of execution of the corresponding secure start procedure of the encryption module by the persons described in section 6.2.2.

The CA keys are activated by means of an m of n process.

Activation of Intermediate CA's private keys is managed by means of the same m of n process used for the CA keys.

6.2.9 Method of deactivating private key

In order to disable esFIRMA's private key, the steps described in the administrator manual corresponding to the administrator of the corresponding encryption device shall be followed.

On its part, the signatory must introduce the PIN for a new activation.

6.2.10 Method of destroying private key

Before the keys are destroyed, a revocation of the public key certificates associated to such keys shall be used.

Any devices storing any part of esFIRMA's private keys shall be physically destroyed or rebooted. In order to disable esFIRMA's private key, the steps described in the administrator manual corresponding to the administrator of the corresponding encryption device.

Finally, backup copies shall be destroyed in a secure manner.

Signatory's keys stored in software may be destroyed by deleting them, following the instruction of the application on which they are stored.

Signatory's keys stored in hardware may be destroyed by means of a specific computer application in the premises of the RA or EsFIRMA.

6.2.11 Cryptographic Module Rating

The cryptographic modules are FIPS-140-2 level 3 certified

6.3 Other aspects of key pair management

6.3.1 Public key archival

esFIRMA routinely stores their public keys according to the provisions set forth in section 5.5. of this document.

6.3.2 Certificate operational periods and key pair usage periods

Periods of use for the different keys shall be those established by the duration of the certificate. Once this period has elapsed, the keys may no longer be used.

6.4 Activation data

6.4.1 Activation data generation and installation

Device activation data for devices that protect private keys are generated in compliance with the provisions of section 6.2.2. And key ceremony procedures.

Creation and distribution of such devices must be registered.

Besides, esFIRMA regenerates activation data in a secure manner.

6.4.2 Activation data protection

Activation data for devices that protect private keys of the root and subordinate Certification Authorities are protected by the holders of the administrator cards of encryption modules, as described in the key ceremony documents.

The certificate signatory shall be responsible for protecting their own private key by means of a password which has to be as complete as possible. The signatory must remember such password.

6.4.3 Other aspects of activation data

Not applicable.

6.5 Computer security controls

esFIRMA offers their certificate services by means of reliable systems. esFIRMA has carried out computer controls and audits in order to manage its appropriate computer assets with the required security level for electronic certificate system management.

Used equipment are first set up with the appropriate security profiles by esFIRMA computer systems department staff, in the following aspects:

- Security setup of the operative system.
- Security setup of applications.
- Appropriate system sizing.
- User configuration and authorisation
- Log events setup.
- Backup and retrieval plan.
- AV software setup.
- Network traffic requirements

6.5.1 Specific computer security technical requirements

Each esFIRMA server includes the following functions:

- Access control to SubCA services and privilege management.
- Compulsory task segregation for privilege management.
- Identification and authentication of roles associated to identities.
- Filing the subscriber and SubCA histories and audit data.
- Audit for security related events.
- Security self-diagnosis related to SubCA services.
- Key and SubCA system retrieval mechanisms.

The above described functions are carried out by a combination of operative system, PKI software, physical protection and procedures.

If esFIRMA distributes qualified signature creation devices, it must verify at all times that such devices are certified as DCCF[12].

Verification of DCCF certification is carried out throughout the entire validity period of the relevant certificate[13]. In case that the DCCF is no longer certified as such, esFIRMA shall notify this situation to the users and shall implement a renovation plan for these devices, as described in internal document esFIRMA (esFIRMA_ProcedimientosGenerales_v1r0.pdf)

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

6.5.2 Computer security rating

Registration and certificate authorities applications used by esFIRMA are reliable.

6.6 Life cycle technical controls

6.6.1 System development controls

Applications are developed and implemented by esFIRMA pursuant development and track changes standards.

Applications have their methods to verify integrity and authenticity, as well as the correctness of the version to be employed.

6.6.2 Security management controls

esFIRMA develops activities specifically for training and raising employee awareness with regard to security. Materials used for training and documents describing the relevant processes are updated after their approval by a team devoted to security management. This function is carried out according to an annual training plan.

12 Sect. 6.5.1.a) of ETSI 319 411-2

13 Sect. 6.5.1.c) vi) of ETSI EN 319 411-2

esFIRMA requires, by means of a contract, equivalent security measures to all third party providers involved in certification tasks.

6.6.2.1 Classification and management of information and assets

esFIRMA maintains an inventory of assets and documents and has established a procedure to manage those materials in such a way that its use is guaranteed.

esFIRMA's safety policies detail the information management procedures including its classification according to its confidentiality level.

Documents are classified in four levels: PUBLIC, RESTRICTED, INTERNAL USE and CONFIDENTIAL.

6.6.2.2 Management operations

esFIRMA has implemented an appropriate incident response and management procedure by implement an alert system and generating reports periodically.

esFIRMA's security document develops in detail the incidence management process.

esFIRMA has documented the entire procedure regarding functions and responsibilities of the personnel involved in control and manipulation of elements included in the certification process.

6.6.2.3 Treatment and security of supports

All supports are treated in a secure manner providing the relevant information classification requirements. Supports including sensitive data will be destroyed in a secure manner when they are no longer required.

System planning

esFIRMA's Systems Department has a record of device capacities. Together with the resource control application for each system, a potential resizing may be foreseen.

Incident reporting and response

esFIRMA has a procedure for monitor incidences and their solutions.

Operational procedures and responsibilities

esFIRMA defines those activities which are to be assigned to persons in a position of trust and different from those persons in charge of carrying out daily operations not labelled as confidential.

6.6.2.4 Access system management

esFIRMA shall perform all reasonable efforts to conform that the access system is limited to authorised persons.

In particular:

General CA

- Has controls based on high availability IDS, firewalls, and antivirus software.
- Sensitive data are protected by means of encryption techniques or access control with strong identification.
- esFIRMA has a documented procedure for managing user authorisations and cancellations and the detailed access policies in its security policy.
- esFIRMA has set procedures in order to ensure that operations are completed respecting the role policies.
- Each person is assigned a role to carry out certification operations.
- esFIRMA's personnel shall be responsible for their own acts and are bound by the confidentiality agreement subscribed by them with regard to the company.

Certificate generation

Authentication for the issuing procedure is carried out by means or a m of n operations system aimed at activating esFIRMA's private key.

Revocation management

Revocation shall be carried out by means of strong authentication in applications of an authorised administrator. Log systems shall generate the necessary tests in order to guarantee non-repudiation of the action carried out by the esFIRMA administrator.

Revocation status

Application of revocation status includes access control based in authentications by certificates or two-factor identification in order to prevent any attempts to modify the information on revocation status.

6.6.3 Life cycle security controls

esFIRMA ensures that cryptographic hardware used to sign certificates is not tampered with during transportation by inspecting the delivered material.

Encryption hardware is transferred by means of prepared supports to prevent them from being tampered with.

esFIRMA records all appropriate information with regard to the device in order to add it to the asset catalogue.

Use of encryption hardware for certificate signature requires the use of at least two trusted employees.

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

The encryption hardware device is operated exclusively by reliable personnel.
esFIRMA's private signature key stored in the encryption hardware shall be deleted once that the device has been removed.

Setup of esFIRMA's system, as well as subsequent modifications and updates, is documented and monitored.

esFIRMA has a maintenance agreement regarding to the device. Any change or update is authorised by the security manager and are document in the corresponding work reports. These set-ups must be carried out by at least two reliable persons,

6.7 Network security controls

esFIRMA prevents physical access to network management devices and has established an architecture that classifies generated traffic by security features, thus creating clearly defined network sections. This division is carried out using firewalls.

Confidential information travelling by means of non-secure networks is transferred in an encrypted manner by means of the use of SSL protocols or the VPN system with two-factor authentication.

6.8 Time-stamping

esFIRMA has a procedure for synchronization of coordinated time via NTP. El valor de tiempo en la TSU es trazable hasta una valor de tiempo distribuido por un laboratorio UTC(k) , el ROA (Real Observatorio de la Armada) y mantiene la precisión de reloj con por lo menos cuatro fuentes de tiempo STRATUM-1.

6.9 Engineering controls for encryption modules

Encryption modules are submitted to the engineering controls provided in the standards described in this section.

Key generation algorithms are commonly accepted for using the key to which they correspond.

All encryption operations by esFIRMA are carried out by modules with certifications FIPS 140-2 level

7. Certificate, CRL and OCSP profiles

7.1 Certificate profile

All qualified certificates issued by virtue of this policy are compliant with standard X.509 version 3, RFC 5280, RFC 3739 y ETSI 101 862 "Qualified Certificate Profile".

esFIRMA generate non-sequential Certificate serial numbers greater than zero (0) containing at least 128 bits of output from a CSPRNG.

7.1.1 Version number(s)

esFIRMA issues X.509 Version 3 standards

7.1.2 Certificate extensions

Extensions of certificates are detailed in the profile document accessible from the esFIRMA website https://www.esfirma.com

7.1.3 Algorithm object identifiers

The object identifier for the signature algorithms is:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption

The object identifier for the public key is:

- 1.2.840.113549.1.1.1 rsaEncryption

7.1.4 Name forms

Certificates must include all information considered necessary for use, as determined by the corresponding policy.

Certificate encoding follows the RFC 5280 recommendation "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL)
See Profiles in https://www.esfirma.com

For website authentication Certificates BR guidelines are followed, such as:

- esFIRMA does not include a Domain Name or IP Address in a Subject attribute.
- Subject attributes not contains only metadata such as '.', '-', and ' ' (i.e. space) characters, nor other indication that the value is absent, incomplete, or not applicable.
- extensions:subjectAltName contain only one entry containing a dNSName with the Fully-Qualified Domain Name. esFIRMA verify the Applicant controls the Fully-Qualified Domain Name.
- dNSName comply with the "preferred name syntax", as specified in RFC 1034, thus cannot contain underscore characters.
- subject:commonName (OID 2.5.4.3) is never present.

7.1.5 Name constraints

Names included in certificates are restricted to “Distinguished Names” X.500, which are unique an unequivocal.

7.1.6 Certificate policy object identifier

All certificates include an identifier referring to the certificate policy under which they have been issued, pursuant the structure described in section 1.2.1.

7.1.7 Usage of Policy Constraints extension

Not applicable

7.1.8 Policy qualifiers syntax and semantics

Not applicable

7.1.9 Processing semantics for the critical Certificate Policies extension

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

7.2 CRL profile

Pursuant to standard IETF RFC 3280

7.2.1 Version number(s)

CRLs issued by esFIRMA belong to version 2.

7.2.2 CRL and CRL entry 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

Pursuant to standard IETF RFC 6960.

7.3.1 Version number(s)

OCSPs issued by esFIRMA belong to 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 and other assessments

esFIRMA has communicated the start of its activities as certificate services providers by the Ministry for Industry, and is thus subject to such control reviews that this entity deems necessary.

8.1 Frequency or circumstances of assessment

esFIRMA performs a compliance audit every year, besides any internal audit carried out at their criterion or at any time that lack of compliance with any security measure is suspected.

esFIRMA monitors adherence to this document and strictly control its service quality by performing self audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

8.2 Identity/qualifications of assessor

Audits are carried out by an independent auditing firm that boasts technical competence and expertise in computers security, information systems security and compliance audits for public key certification services, and related elements.

8.3 Assessor's relationship to assessed entity

Auditing companies are widely recognised by department specialised in computing audits, and therefore there is no interest conflict that may undermine its action with regard to esFIRMA.

8.4 Topics covered by assessment

With regard to esFIRMA, the audit verifies that:

a) The company has implemented a management system that ensures quality of the provided service.
b) The company complies with all DPC requirements and other documents linked to issuing different digital certificates.
c) The DPC and all related legal documents is compliant to provisions set by esFIRMA and by the current regulations.
d) The company manages its information systems in an appropriate manner

Particularly, the following elements shall be subject to an audit:

a) CA and RAs processes and related elements.
b) Information systems.
c) Protection of the data processing centre.
d) Documents.

8.5 Actions taken as a result of deficiency

Once that the company management has received the compliance audit report corresponding to the completed audit, detected non-compliances are analysed with the company that has performed the audit, and develops and executes a corrective plan to put an end to those non-compliances.

If esFIRMA is not capable of developing and executing such plan, or if deficiencies detected pose an imminent threat to system security or integrity, they must immediately notify to esFIRMA's senior managers, who may implement the following actions:

- Temporarily discontinue operations.
- Revoking the CA's key and regenerating infrastructure.
- Ending the CA service provisioning.
- Other complementary actions deemed necessary.

8.6 Communication of results

The audit reports are delivered to esFIRMA's senior manager in a maximum term of 15 days after the audit is completed.

9. Commercial and legal requirements

9.1 Fees

9.1.1 Certificate issuance or renewal fees

esFIRMA may establish a fee for issuing their certificates. When this is the case, subscribers shall be appropriately informed.

9.1.2 Certificate access fees

esFIRMA has not established any fee for accessing certificates.

9.1.3 Revocation or status information access fees

esFIRMA has not established any fee for accessing certificate status information

9.1.4 Fees for other services

No indications.

9.1.5 Refund policy

No indications.

9.2 Financial responsibility

esFIRMA has sufficient economic resources to maintain its operations and comply with their obligations, as well as to face any risk of liability for damages, as established by ETSI EN 319 401-1 7.12 c), with regard to management of discontinuation of services and termination plan.

9.2.1 Insurance coverage

esFIRMA has sufficient coverage guarantee for any civil liability issue due to its subscription of a professional civil liability insurance that complies with the standards

set in the obligations and responsibilities set forth in Regulation (UE) 910/2014, with a minimum insurance sum of 3,000,000 euros.

9.2.2 Other assets

No indications.

9.2.3 Insurance or warranty coverage for end-entities

esFIRMA has sufficient coverage guarantee for any civil liability issued by means of its subscription of a professional civil liability insurance that complies with the standards set in the obligations and responsibilities set forth in Regulation (UE) 910/2014, with a minimum insurance sum of 3,000,000 euros.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

The following information must be kept confidential by esFIRMA:

- Certificate request, either approved or refused, as well as any other personal information obtained for issuing and maintaining certificates, with the exception of the information stated in the following section.
- Private keys generated and/or stored by the certificate services provider.
- Records of transactions, including complete records and audit records for transactions.
- Internal and external records created and/or maintained by the Certificate Authority and their auditors.
- Emergency and business continuity plans.
- Security policy and plans
- Operations documents and other operational plans, such as filing, monitoring and other analogous documents.
- All information shall be labelled as “Confidential”

9.3.2 Information not within the scope of confidential information

The following information is considered non-confidential:

- Issued certificates or certificates in process of being issued.

- Subscribers are linked to certificates issued by the Certificate Authority.
- The name and surname(s) of the natural person identified in the certificate, as well as any other circumstance or personal data of the holder, when it is relevant for the purposes of the certificate.
- The e-mail address of the natural person identified in the certificate, or the e-mail address assigned by the subscriber, in case that it is relevant for the purposes of the certificate.
- Uses and economic limits stated in the certificate.
- The validity period of the certificate, as well as its issue date and expiry date.
- The serial number of the certificate.
- The different status or situations of the certificate and the starting date for each of them, particularly: pending generation and/or delivery, valid, revoked, suspended or expired and the justification for such change of status.
- The certificate revocation lists (CRLs), as well as any other information about revocation status.
- Any other information not included in the above sections.

9.3.3 Responsibility to protect confidential information

See section above.

9.3.4 Legal disclosure of information

esFIRMA disseminates confidential information only in legally considered cases.

Specifically, records that support certificate data reliability, as well as records related to data reliability and operational procedures [14] may be disclosed when required as evidence of certification in a legal procedure, even without the consent of the certificate subscriber.

esFIRMA shall state these circumstances in the privacy policy included in section 9.4

[14] Sect. 7.10.c) of ETSI EN 319 401

9.3.5 Disclosure of information at the request of its holder.

esFIRMA includes, pursuant the privacy policy included in section 9.4, prescriptions to allow disclosure of subscriber information and, when appropriate, of the natural person identified in the certificate, directly to the same persons or to third parties.

9.3.6 Other circumstances on which information may be disseminated.

No indications.

9.4 Privacy of personal information

esFIRMA hereby undertakes to comply with standards on personal data protection, with the corresponding security measures as described 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.

esFIRMA obtains personal data included in the data collection files by the SUBSCRIBER, whom must have obtained them legally from the appropriate person, under the conditions foreseen in the standards on electronic signature and personal data protection.

esFIRMA shall be considered as the personal data processor, and, as such, shall processes data exclusively for the purposes stated in these Guidelines for Certification Procedures, pursuant the indications of the data controller, that is, the SUBSCRIBER, which are included in Annex *"Annex 1: On personal data treatment by ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A. acting as DATA PROCESSOR*", governed by the "Gestiona" service provisioning agreement executed by the SUBSCRIBER and ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A.

9.4.1 Privacy plan

esFIRMA has developed a privacy policy, pursuant 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 has documented both in these Guidelines for Certification Procedures and in *"Annex 1: On personal data treatment by ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A. acting as DATA PROCESSOR"*, governed by the "Gestiona" service provisioning agreement executed by the SUBSCRIBER and ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A., all aspects, procedures, and organizational and security measures in compliance with the obligations and responsibilities regime established by REGULATION (EU) No 910/2014 and REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons.

9.4.2 Information treated as private

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

9.4.3 Information not deemed private

Personal information about an individual available in the contents of a certificate or CRL, is considered as non-private because it is necessary to provide the contracted service, without prejudice to the rights corresponding to the holder of personal data under the LOPD / GDPR

9.4.4 Responsibility to protect private information

Pursuant the regulations on personal data protection, confidential information is protected from loss, destruction, damage, forging and unlawful or unauthorised processing pursuant the provisions of this documents, which are consistent with obligations provided 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.

9.4.5 Notice and consent to use private information

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

9.4.6 Disclosure pursuant to judicial or administrative process

esFIRMA does not disseminate nor assign personal data, except in the cases provided by sections 9.3.2 to 9.3.6, and by section 5.8, in case of termination of the certification service.

9.4.7 Other information disclosure circumstances

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

9.5 Intellectual property rights

9.5.1 Property of certificates and revocation information

esFIRMA shall be the exclusive holder of intellectual property rights on the certificates issued by it, notwithstanding the rights of subscriber, key holders and third parties which have been granted a non-exclusive license to copy and disseminate certificates at no cost, provided that they are copied in full and without alteration of any element of the certificate, and that such copy is necessary with regard to digital signatures and/or encryption system with the certificate's use scope, and pursuant the documents that bind them.

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

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

9.5.2 Holder of the Declaration of Certificate Practices.

Only esFIRMA shall hold any intellectual property rights whatsoever over these Guidelines for Certification Procedures.

9.5.3 Property of information related to names

The subscriber, and, when appropriate, the natural person identified in the certificate, shall retain all rights, when any, in the brand, product or commercial name included in the certificate.

The subscriber shall own the name included in the certificate, formed by the information stated under section 3.1.1.

9.5.4 Key ownership

Pairs of keys shall be owned by the signatory of certificates.

When a key is fractioned in parts, all key parts shall be owned by the key owner.

9.6 Representations and warranties

9.6.1 CA representations and warranties

Under its entire responsibility, esFIRMA guarantees that it complies with all the requirements established in the DPC, and shall be the sole responsible for the compliance of described procedures, even when all or part of the operations are assigned to third party contractors.

esFIRMA provides its certification services pursuant these Guidelines for Certification Procedures.

Before issuing and delivering the relevant certificate to the subscriber, esFIRMA informs the subscriber on the terms and conditions regarding certificate use, price and use limitations by means of a subscriber agreement which includes, by means of reference, the statement of disclosure (PDS) for each acquired certificate.

The statement of disclosure document, also called PDS PDS[15], complies with the contents of annex A of ETSI EN 319 411-1 v1.1.1 (2016-02), a document which may be transferred by electronic means using a durable communications means in time, and an easily understood language.

15 "PKI Disclosure Statement" or statement of disclosure of the applicable PKI.

esFIRMA shall notify in a final manner any change[16] in their obligations with regard to publishing new versions of their legal documents in their website https://www.esfirma.com

esFIRMA links subscribers, key holders and third parties that rely on certificates by means of such statement of disclosure or PDS, in an easily understandable language, with the following minimum contents:

- Prescriptions to comply the provisions of sections: 4.5.3, 9.2, 9.6.7, 9.6.8, 9.6.9 y 9.6.10.
- Indication of applicable policies, listing those certificates that may not be issued to the public.
- Statement that information included in such certificate is correct, unless the subscriber states otherwise by means of a notification.
- Consent for storing information used for subscriber registration and for assigning such information to third parties in case of termination of operations of the Certificate Authority without revocation of valid certificates.
- Certificate use limits, including those established in section 1.4.2.
- Information on the certificate validation method, including the requirement to check the certificate status and the conditions that assure that such certificate is reasonably reliable, which shall apply when the subscriber acts as a third party that relies on the certificate.
- Manner to guarantee financial liability of the Certificate Authority.
- Applicable liability limits, including those uses by which the Certificate Authority accepts or precludes any liability.
- Certificate request information storage term.
- Audit records storage term
- Applicable procedures to dispute settling.
- Applicable legislation and jurisdiction
- Whether the Certificate Authority has been declared compliant with the certification policy and, when appropriate, with which case.

[16] Sect. 6.2.3.b) vi) of ETSI EN 319 411-1

9.6.2 RA representations and warranties

The RA's are the entities delegated by the CA to carry out the tasks of registration and approval of certificate applications, therefore the RA also binds itself in the terms defined in the Certification Practices for the issuance of certificates, mainly:

- Respect the provisions of this PSC and the corresponding Certification Policy.
- To protect their private keys that will be used for 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 case of individual certificates, or of the key holder, in case of organization certificates, according to what is established in the corresponding sections of this document.
- Verify the accuracy and authenticity of the information provided by the Applicant
- Provide the Signatory, in case of individual certificates, or the future Key Holder, in case of

keys, in case of organisation certificates, access to the certificate.

- Deliver, where appropriate, the corresponding cryptographic device.
- To file, for the period of time stipulated in the legislation in force, 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 are known.
- Provide basic information about the policy and use of the certificate, including

especially information on Camerfirma and the Declaration of Practice of

Applicable certification, as well as its obligations, powers and responsibilities.

- Provide information about the certificate and the cryptographic device.
- Collect information and evidence from the holder of receiving the certificate and, if applicable, the cryptographic device, and acceptance of such elements.
- Report the method of exclusive allocation to the private key holder and its certificate and cryptographic device activation data, if applicable, as stated in the corresponding sections of this document.

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

Information on subscriber use and responsibilities is provided through the

acceptance of the terms of use prior to confirmation of the certificate request and by e-mail.

The RA sign a service provision contract with esFIRMA by means of which

esFIRMA delegates the registration functions to the RAs, consisting essentially of:
1.- Obligations prior to the issuance of a certificate.
a) Adequately inform the applicants of the signing of their obligations and responsibilities
b) The proper identification of applicants, who must be trained or authorized to request a digital certificate.
c) The correct verification of the validity and validity of these data of the applicants and of the Entity, in the event that there is a relationship of relationship or representation.
d) Access the Registration Authority application to manage applications and Certificates issued
2.- Obligations once the certificate is issued.
a) Sign the Digital Certification Services Provision contracts with the Applicants In most of the emissions processes this contract is formalized by accepting conditions on the web pages that are part of the process of issuance of the certificate, and the issuance cannot be made without first accepting the conditions of use.
b) The maintenance of certificates during their validity (extinction, suspension, revocation).
c) File copies of the documentation submitted and the contracts duly signed by applicants in accordance with published Certification Policies by esFIRMA and current legislation.
Thus, the RAs are responsible for the consequences in case of non-compliance with their registration tasks, and through which they undertake to also respect the internal regulatory standards of the certification body esFIRMA (Policies and CPS) which must be perfectly controlled by part of the RA and that should serve as a reference manual.
In case of claim by a Subject, an Entity, or a user, the CA must provide the evidence of the diligent action and if it is found that the origin of the claim lies in an error in the validation or verification of the data, the CA may, by virtue of the agreements signed with the RA, make the RA responsible bear the assumption of the consequences.
Because, although the CA is legally the legal person responsible in front of the Subject, an Entity, or User Party, and that for this it has a civil liability insurance, according to the current agreement and the binding Policies, the RA has as a contractual obligation " correctly identify and authenticate the Applicant and, where appropriate, the Entity that corresponds ", and by virtue of this, he must respond to the SIGNATURE of his breaches.

Of course, it is not the intention of esFIRMA to download the full weight of the assumption of responsibility to the RA regarding the possible damages whose origin would come from a non-fulfillment of the tasks delegated to the RA. For this reason, as foreseen for the CA, the RA is subject to a control regime that will be exercised by esFIRMA, not only through the file controls and archiving procedures 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 assume the RAs due to breaches of the delegated entities such as face-to-face verification points (PVP), without prejudice of their right to impact against them.

9.6.3 Subscriber representations and warranties

esFIRMA, in the document that links it with subscribers and third parties relying in certificates, establishes and rejects any applicable guarantees and liability limitations.

esFIRMA, at the very minimum, guarantees the subscriber that:

- Information included in the relevant certificates is free from material errors which are known or made by the Certificate Authority.
- Information included in the relevant certificates are free from material errors due to lack of due diligence when processing the certificate request or creating the certificate itself.
- Certificates comply with all material requirements established in the Guidelines for Certification Procedures.
- Certificates comply with all material requirements established in the Guidelines for Certification Procedures.

esFIRMA, at the very least, shall guarantee the third party relying on the certificate that:

- All information included or incorporated by means of reference in the certificate is correct, except when stated otherwise.
- Approval of certificate requests and issuing of certificates shall be subject to all material requirements established on the Guidelines for Certification Procedures.
- Services are provided in a secure and secure manner, especially revocation services.

Additionally, esFIRMA guarantees the subscriber and the third party that the certificate is, in its opinion, reliable:

- That the certificate includes all information that needs to be included in any qualified certificate, pursuant annex 1 of Regulation (EU) 910/2014.
- That, in case that the private keys of the subscriber or other natural person included in the certificate are generated, their confidentiality is maintained throughout the process.
- The liability assigned to the Certificate Authority, considering any applicable limits.

9.6.4 Relying party representations and warranties

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

- Verify the validity of the certificates before performing any operation based on them. esFIRMA has several mechanisms to perform this check
- such as access to revoked certificate lists or online consultation services such as OCSP.
- Know and be subject to the guarantees, limits and responsibilities applicable in the acceptance and use of the certificates in which you trust, and accept to abide by them.
- Check the validity of the qualification of a firm associated with a certificate issued by esFIRMA, verifying that the certification authority that has issued the certificate is published in the trust list of the corresponding national supervisor.

9.6.5 Representations and warranties of other participants

No Stipulation

9.7 Disclaimers of warranties

According to the current legislation, the responsibility of esFIRMA and its RA does not extend to those cases in which the misuse of the certificate has its origin in conduct attributable to the Subject, and the User Party by:

- Failure to provide adequate information, initially or subsequently as as a result of changes in circumstances reflected in the certificate

- The electronic data processing system, when its inaccuracy could not be detected by the provider of the certification services
- Negligence with respect to the preservation of signature creation data and their confidentiality.
- Not having requested revocation of the electronic certificate data in case of doubt about the maintenance of confidentiality
- Having used the signature after the expiry of the period of validity of the certificate e-mail
- Exceeding the limits stated in the electronic certificate.
- In conduct attributable to the User Party if it acts negligently, that is
- when it does not check or take into account the restrictions in the certificate regarding its possible uses and limit on the amount of transactions; or when it does not take into account the validity status of the certificate
- Of the damages caused to the Subject or third parties who rely on the inaccuracy of the data contained in the electronic certificate, if these have been accredited to him by means of a public document, registered in a public registry if this is required.
- An inadequate or fraudulent use of the certificate in case the Subject/Holder has assigned or has authorized its use in favor of a third person by virtue of a business mandate or power of attorney, being the exclusive responsibility of the Subject/Holder the control of the keys associated with your certificate.

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

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

9.8 Limitations of liability

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

9.9 Indemnities

See section 9.2

9.10 Term and termination

9.10.1 Term

See section 5.8

9.10.2 Termination

See section 5.8

9.10.3 Effect of termination and survival

See section 5.8

9.11 Individual notices and communications with participants

Any notification concerning this CPS shall be made by e-mail or
by registered mail to any of the addresses referred to in section 1.5.2.

9.12 Amendments

9.12.1 Procedure for amendment

The CA reserves the right to modify this document for technical reasons or to reflect any changes in procedures that have occurred due to legal or regulatory requirements (eIDAS, CA/B Forum, 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 update will be published annually. These updates will be reflected in the version table at the beginning of the document.

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

9.12.2 Notification mechanism and period

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

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

9.12.3 Circumstances under which OID must be changed

Not stipulated

9.13 Dispute resolution provisions

esFIRMA has set forth, both in the subscriber agreement and in the disclosure statement or PDS, the relevant applicable procedure for mediation and dispute settlement.

9.14 Governing law

esFIRMA has set forth, both in the subscriber agreement and in the disclosure statement or PDS, a competent jurisdiction clause, stating that international legal competence is to be assigned to the Spanish courts.

Territorial and functional competence shall be established pursuant the provisions of applicable private international laws and procedural law.

9.15 Compliance with applicable law

See 9.14

9.16 Miscellaneous provisions

9.16.1 Entire agreement

The subscribers and relay parties who rely on the Certificates assume in full the contents of this Certification Policy and Practice Statement

9.16.2 Assignment

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

9.16.3 Severability

esFIRMA has set forth, both in the subscriber agreement and in the disclosure statement or PDS, clauses regarding severability, survival of the agreement, entire agreement and notification practices.

- Pursuant the severability clause, lack of validity of a clause shall not affect the rest of the agreement.
- Pursuant the survival clause, certain rules shall survive after the termination of the legal relationship between the parties that governs the service provision. For this purpose, the Certificate Authority ensures that at least the requirements included in sections 9.6.1 (Obligations and liability), 8 (Compliance audit) and 9.3 (Confidentiality) shall still be valid after termination of service and the general conditions for issuance and use.
- Pursuant the entire agreement clause, it shall be understood that the legal document that governs the service represents the entire will and all the agreements between the parties.
- By virtue of the notification clause, the procedure by which parties notify each other of any relevant fact shall be established.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

esFIRMA may seek compensation and attorney's 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 to esFIRMA to enforce the same provisions later or the right to enforce any other provision of this CPS. To be effective, any waiver must be in writing and signed by esFIRMA

9.16.5 Force Majeure

In its disclosure statement or PDS, clauses that limit liability in the event of acts of God or force majeure.

9.17 Other provisions

9.17.1 Subscriber's indemnity

esFIRMA includes, in the subscriber agreements, a clause by virtue of which the subscriber undertakes to keep the Certificate Authority harmless from all damage from any act or omission that causes any liability, damage or loss, expenses of any kind, including any legal and judicial fees, arisen from the issuing and use of the certificate under any of the following circumstances:

- False or erroneous information provided by the certificate user.
- Certificate user error when providing the requested data, when such erroneous act or omission were carried out with negligence of wilful misconduct with respect to the Certificate Authority or any other person relying in the certificate.
- Negligent behaviour with respect to protecting the private key, using a reliable system or maintaining the necessary precautions to prevent the necessary measures to prevent compromise, loss, disclosure, modification or unauthorised use of such key.
- Inclusion in the certificate of names (including common names, e-mail addresses and domain names) or other information that violate intellectual property rights or industrial property rights of third parties.

9.17.2 Indemnity clause for third parties that rely on the certificate

esFIRMA includes, in disclosure statement or PDS, a clause by virtue of which the third party relying in the certificate undertakes to keep the Certificate Authority harmless from all damage from any act or omission that causes any liability, damage or loss, expenses of any kind, including any legal and judicial fees, arising from issuing and using the certificate under any of the following circumstances:

- Indemnity clause for third parties that rely on the certificate
- Negligent reliance in a certificate, given the circumstances.
- Lack of verification of the status of a certificate in order to ensure that is not suspended or revoked.