Certification Practice Statement

esFIRMA

General information

document control

Security Classification:	Public
Target Entity:	ESFIRMA
Version:	1.5

Formal state

Prepared by:	Reviewed by:	Approved by:
security office Date: 06/11/2017	Safety Officer Date: 06/11/2017	Safety Committee Date: 06/11/2017

Version control

Version	Parties change	Description of Change	Author Change	Date of change
1.0	Original	Document creation	esFIRMA	04/29/2016
1.1		rectifications	esFIRMA	02/06/2016
1.2 1.3		ETSI review Review types of certificates	esFIRMA	05/19/2017
1.4		ETSI review Review types of certificates Acronyms and Definitions	esFIRMA	06/02/2017
1.5	1.3.1 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	Settings normative references, change of name, certified change	esFIRMA	06/11/2017

Index

ACRONYMS	
AC (or also CA)	*Certificate Authority* Certification Authority
AR (or also RA)	*Registration Authority* Registration Authority
CPD	Data processing center
CPS (also DPC)	*Certification Practice Statement*. Certification Practice Statement
CRL (or also LRC)	*Certificate Revocation List.* Certificate Revocation List
DN	*Distinguished Name.* distinguished name in the digital certificate
DNI	National identity document
ETSI EN	*European Telecommunications Standards Institute - European Standard.*
EV (SSL)	*Extended Validation* Extended Validation SSL certificates.
FIPS	*Federal Information Processing Standard Publication*
HSM	*Hardware Security Module* Hardware Security Module
IETF	*Internet Engineering Task Force*
NIF	Tax identification number
NTP	*Network Time Protocol* Network Time Protocol.
OCSP	*Online Certificate Status Protocol.* Access protocol status of certificates
OID	*Object Identifier*. Object Identifier
PDS	*PKI Disclosure Statements* PKI Disclosure text.
PIN	*Personal Identification Number*. Number of personal identification
PKI	*Public Key Infrastructure*. Public Key Infrastructure
QSCD (also DCCF)	*Qualified Electronic Signature / Seal Creation Device.* qualified device signature creation / seals
QCP	*Qualified Certificate Policy* Qualified Certificates Policy
PPP-n	*Qualified Certificate Policy-Natural person* Policy for individuals qualified certificates.
PPP-l	*Qualified Certificate Policy-legal person* Policy for legal persons qualified

	certificates.
PPP-n-qscd	*Qualified Certificate Policy-Natural person-qscd* Policy for qualified individuals qualified device certificates signature / seal
PPP-l-qscd	*Qualified Certificate Policy-legal person-qscd* Policy qualified for legal persons with qualified certified device signature / stamp
RFC	*Request for Comments* RFC
RSA	Rivest-Shamir-Adleman. Type of encryption algorithm
SHA	*Secure Hash Algorithm.* Secure Hash Algorithm
SSL	*Secure Sockets Layer.* Protocol designed by Netscape and become standard network, allows transmission of encrypted information between an Internet browser and a server.
TCP / IP	*Transmission Control. Protocol / Internet Protocol*. System protocols defined within the IETF.
TSA	*Time Stamping Authority* Stamping Authority Electronic Time
TSU	*Time Stamping Unit* Time Stamping Unit.
UTC	*Coordinated Universal Time* Coordinated Universal Time
VPN	*Virtual Private Network.* Virtual Private Network

DEFINITIONS	
Certification Authority	*It is responsible for issuing and managing digital certificates.*
Registration Authority	*Entity responsible for the management of applications, identification and registration of applicants for a certificate. You can be part of the Certification Authority or be employed.*
Certificate	*File that associates the public key with some identifying information Subject / Signer and signed by the AC.*
public key	*mathematical value publicly known and used for the verification of a digital signature or data encryption.*
private key	*mathematical value known only by the subject / signer and used for creating a digital signature or decrypting data.* *The private key of the CA will be used for signing certificates and CRL's signature.* *TSA private key service will be used for signing timestamps.*
CPS	*Set of practices adopted by a Certification Authority for the issuance of certificates in accordance with specific certification policy.*
CRL	*File containing a list of certificates that have been revoked over a period of time and is signed by the AC.*
Activation Data	*private data such as PINs or passwords used for the activation of the private key*
DCCF	*Unqualified device signature creation. Software or hardware element, properly certified, employed by the subject / Signer for generating electronic signatures, so that cryptographic operations are performed within the device and its control is guaranteed only by the subject / signatory.*
Digital signature	*The result of the transformation of a message, or any type of data, by the application of the private key in conjunction with known algorithms, thus ensuring:* *a) that the data have not been modified (integrity)* *b) that the person signing the data is who he claims to be (ID)* *c) that the person signing the data can not deny having done so (non-repudiation at origin)*
OID	*A unique numerical identifier registered under the ISO standardization and referring to an object or*

	class specific object.
Key pair	*Assembly consisting of public and private key, both related to each other mathematically.*
PKI	*Set of hardware, software, human resources, procedures, etc., that make up a system based on creating and managing public key certificates system elements.*
Applicant	*In the context of this document, the applicant is an individual empowered with a special power to perform certain procedures on behalf of the entity.*
Subscriber	*In the context of this document the entity that owns the certificate (corporate level)*
Subject / Signer	*In the context of this document, the natural person whose public key is certified by the CA and has, or has access exclusively to a valid private key to generate digital signatures.*
Usuaria part	*In the context of this document, person who willfully trust the digital certificate and uses it as a means of proof of the authenticity and integrity of the signed document*

1. Introduction

1.1.

1.2. Presentation

This document declares certification practices esFIRMA electronic signature.

Certificates that are issued are as follows:

- **Public Employee**
  - Middle level Public Employee
  - High level Public Employee
- **Organ Seal**
  - Seal midlevel Body
- **Public Employee pseudonymous**
  - Public Employee pseudonymous standard level
  - Public Employee pseudonymous High level
- **Electronic Headquarters**
  - Based electronic administrative level Medium
- **Electronic Seal for TSA / TSU**
  - Electronic seal for TSU in Software

1.3. Document name and identification

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

1.3.1. Certificate identifiers

number OID	Certificate Policy
	Public Employee
1.3.6.1.4.1.47281.1.1.1	*Public Employee - High level on card*
1.3.6.1.4.1.47281.1.1.4	*Public Employee - standard level in HSM*
	Organ Seal
1.3.6.1.4.1.47281.1.2.2	*Organ Seal - Standard level software*
1.3.6.1.4.1.47281.1.2.4	*Organ Seal - Level across HSM*
	Public Employee pseudonymous
1.3.6.1.4.1.47281.	*EP pseudonymous - High Level in card*

1.3.1	
1.3.6.1.4.1.47281.1.3.4	*EP pseudonymous - standard level in HSM*
	Electronic Headquarters
1.3.6.1.4.1.47281.1.4.2	*Headquarters-e EV - standard level*
	Electronic Seal for TSA / TSU
1.3.6.1.4.1.47281.1.5.2	*Seal-e for TSA / TSU software*

In case of contradiction between this Certification Practice Statement and other documents esFIRMA practices and procedures, it will prevail in this Statement of Practice.

EsFIRMA fits the current version of the CA / Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates published in http://www.cabforum.org. In the event of any inconsistency between this document and these guidelines, these guidelines supersede this document (8.3 EVCG).

1.4. Participants in certification services

1.4.1. Certification service provider

The certification service provider is the person, whether natural or legal, which issues and manages certificates to end entities using a Certification Body, or provides other services related to electronic signatures services.

ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (FORMER AULOCE SA), hereinafter esPublico, residing at Calle Bari 39 (EDIF. Binary Building), CP 50197, Zaragoza, CIF A-50878842, registered in the commercial register of Zaragoza in volume 2649, folio 215, sheet Z-28722, and operates under the trade name EsFIRMA, trade name which will be used throughout this document to describe it, it is a service provider certification acts in accordance with the provisions of the regime of obligations and responsibilities of Regulation (EU)

910/2014, and the ETSI technical standards applicable to the issuance and management, mainly ETSI EN 319 411-1 qualified certificates and ETSI EN 319 411-2, the to facilitate compliance with legal requirements and recognition internacional their services.

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

1.4.1.1. AC EsFIRMA root

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

Identification data:

	ESFIRMA AC ROOT 2
TO	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
	2017-11-02T12: 52: 43Z
	2042-11-02T12: 52: 43Z
	4,096 bits

1.4.1.2. EsFIRMA AC AAPP

It is the certification body within the hierarchy that issues certificates to end entities, whose public key certificate has been digitally signed by "esFIRMA AC ROOT 2".

Identification data:

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

1.4.1.3. EGovernment platform

It is the platform lifecycle management certificate exclusively for application, approval, issuance and revocation.

For complete information on the functionality of the Platform eGovernment consulting services certification documentation.

1.4.2. registrars

In general, the certification service provider acts as registrar of the identity of subscribers certificates.

They are also registrars certificates subject to this Statement of Certification Practice because of their status as corporate certificates, units designated for this function by subscribers of certificates, as the Secretary of the Corporation or the Department of Personnel Administration since they have authentic records about linking of the signatories to the subscriber.

The logging functions are performed by subscribers delegation and according to the instructions of certification service provider, under the terms defined in Regulation (EU) 910/2014 and under the full responsibility of the service provider certification against To thirds.

1.4.3. end entities

End entities are the persons and organizations broadcasting services, management and use of digital certificates for applications identification and electronic signature.

They will be late certification services esFIRMA the following entities:

1. Certification service subscribers.
2. Signers.
3. Parties users.

1.4.3.1. Certification service subscribers

Service subscribers are government certification that esFIRMA acquired for use in its corporate or organizational level, and are identified in the certificates.

Subscriber certification service acquires a license to use the certificate for your own use - certificates of electronic seal - or in order to facilitate certification of the identity of a duly authorized individual person for various actions at the organizational level subscriber - electronic signature certificates. In the latter case, this figure person identified in the certificate, as provided in the following section.

Subscriber service certification is therefore the client of the service provider certification, according to corporate law, and has the rights and obligations defined by the service provider certification, which are additional and understood without prejudice to the rights and obligations of the signatories, as authorized and regulated by European technical standards for issuing qualified electronic certificates, especially in ETSI EN 319 411-2, sections 5.4.2 and 6.3.4.e)

1.4.3.2. signers

The signatories are individuals who own exclusively or have under their exclusive control, under the regime of obligations and responsibilities of Regulation (EU) 910/2014, digital signature keys for identification and advanced or qualified electronic signature; typically being the incumbent persons or members of the administrative bodies, electronic

signature certificates organ, or people serving the government, in certificates of public employee.

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

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

1.4.3.3. Parties users

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

Prior to trust certificates step, relying parties should check them, as set out in this statement of certification practices and the instructions available on the website of the Certification.

1.5. Use of certificates

This section lists the applications for each certificate type may be used, sets limitations to certain applications and prohibits certain applications certificates.

1.5.1. permitted uses for certificates

Should take into account the permitted uses specified in the various fields of the certificate profiles, visible on the web https://www.esfirma.com

1.5.1.1. Certified Public Employee highest level in card

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.1.1	In the hierarchy of the EC esFIRMA
0.4.0.194112.1.2	According to the QCP-n-qscd policy

2.16.724.1.3.5.7.1	Spanish public employee senior

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

These certificates are issued to public employees to identify them as persons in the service of the Administration, agency or public entity, linking it, fulfilling the requirements Article 43 of Law 40/2015, of 1 October, the Legal Regime of the Public Sector, for the electronic signature of the staff serving the Public Administrations.

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

In addition, certificates of individual public employee high level are issued in accordance with the levels of high assurance profiles certificates set out in paragraph 10 of document "Profiles Electronic Certificates" of the General Bureau of Information, Documentation and Publications Ministry of Finance and Public Administration.

These certificates guarantee the identity of the subscriber and the signer, and allow the generation of "qualified electronic signature"; ie advanced electronic signature based on a qualified certificate and which has been generated using a qualified device, which according to the provisions of Article 25.2 ofRegulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014, will have equivalent legal effect to a firm Handwritten.
.

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

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

EsFIRMA does not offer backup and recovery of keys. Therefore, esFIRMA not respond in any way for any loss of encrypted information that can not be recovered.

Uses information in the certificate profile indicates the following:

a) The field "key usage" is activated, and therefore allows the following functions:
    a. Commitment to the content (Content commitment, to perform the function of electronic signature)

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

1.5.1.2. Certified Public Employee midlevel

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	According to the policy QCP-n
2.16.724.1.3.5.7.2	Spanish public employee midlevel

Individual certificates midlevel government employee are certified qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and give effect to the provisions of the technical regulations identified with reference ETSI EN 319 411 -2.

These certificates are issued to public employees to identify them as persons in the service of the Administration, agency or public entity, linking it, fulfilling the requirements Article 43 of Law 40/2015, of 1 October, the Legal Regime of the Public Sector, for the electronic signature of the staff serving the Public Administrations.

Individual certificates midlevel government employee are managed centrally.

Certificates of individual public employee midlevel are issued in accordance with the levels of medium assurance profiles certificates set out in paragraph 10 of document "Profiles Electronic Certificates" of

the General Bureau of Information, Documentation and Publications of the Ministry of Finance and Public Administration.

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

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

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

EsFIRMA does not offer backup and recovery of keys. Therefore, esFIRMA not respond in any way for any loss of encrypted information that can not be recovered.

Uses information in the certificate profile indicates the following:

a) The field "key usage" is activated, and thus allows us to perform the following functions:
    a. Commitment to the content (content commitmentTo perform the function of electronic signature)

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

1.5.1.3. Seal Certificate Authority midlevel software

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.2.2	In the hierarchy of the EC esFIRMA
0.4.0.194112.1.1	According to the policy QCP-l
2.16.724.1.3.5.6.2	Spanish public employee midlevel

Electronic stamp certificates midlevel body are certified qualified in accordance with Article 38 and Annex III of Regulation (EU) 910/2014 of

the European Parliament and of the Council of 23 July 2014 and give effect to the provisions of the technical regulations identified with reference ETSI EN 319 411 -2.

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

Certificates of electronic seal midlevel body are issued in accordance with the levels of medium assurance profiles certificates set out in paragraph 9 of document "Profiles Electronic Certificates" of the General Bureau of Information, Documentation and Publications of the Ministry of Finance and Administration.

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

EsFIRMA does not offer backup and recovery of keys. Therefore, esFIRMA not respond in any way for any loss of encrypted information that can not be recovered.

Uses information in the certificate profile indicates the following:

a) The field "key usage" is activated, and thus allows us to perform the following functions:
    a. Commitment to the content (content commitmentTo perform the function of electronic signature)

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

1.5.1.4. Seal certificate midlevel Organ HSM

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.2.4	In the hierarchy of the EC esFIRMA
0.4.0.194112.1.1	According to the policy QCP-l
2.16.724.1.3.5.6.2	Spanish public employee midlevel

Electronic stamp certificates midlevel body are certified qualified in accordance with Article 38 and Annex III of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and give

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

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

Electronic stamp certificates midlevel body are managed centrally.

Certificates of electronic seal midlevel body are issued in accordance with the levels of medium assurance profiles certificates set out in paragraph 9 of document "Profiles Electronic Certificates" of the General Bureau of Information, Documentation and Publications of the Ministry of Finance and Administration.

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

EsFIRMA does not offer backup and recovery of keys. Therefore, esFIRMA not respond in any way for any loss of encrypted information that can not be recovered.

Uses information in the certificate profile indicates the following:

a) The field "key usage" is activated, and thus allows us to perform the following functions:
    a. Commitment to the content (content commitmentTo perform the function of electronic signature)

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

1.5.1.5. Public Employee Certificate of high level pseudonymous Card

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.3.1	In the hierarchy of the EC esFIRMA
0.4.0.194112.1.2	According to the QCP-n-qscd policy
2.16.724.1.3.5.4.1	Spanish public employee pseudonymous high level

Individual certificates of public employee with top-level pseudonym certificates qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and give effect to the provisions of the technical regulations identified with reference ETSI EN 319 411 -2.

These certificates are issued to public employees to identify (using a pseudonym) as persons in the service of the Administration, agency or public entity, linking it, fulfilling the requirements Article 43 of Law 40/2015, of 1 October, the Legal Regime of the Public Sector, for the electronic signature of the staff serving the Public Administrations.

Individual certificates of public employee pseudonymous high level, work with secure signature creation device, according to Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014.

In addition, certificates of individual public employee pseudonymous high level are issued in accordance with the levels of high assurance profiles certificates set out in paragraph 11 of document "Profiles Electronic Certificates" of the General Bureau of Information, Documentation and publications of the Ministry of Finance and Public Administration.

these certificates allow the generation of "qualified electronic signature"; ie advanced electronic signature based on a qualified certificate and which has been generated using a qualified device, which according to the provisions of Article 25.2 ofRegulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014, will have equivalent legal effect to a firm Handwritten.

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

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

EsFIRMA does not offer backup and recovery of keys. Therefore, esFIRMA not respond in any way for any loss of encrypted information that can not be recovered.

Uses information in the certificate profile indicates the following:

a) The field "key usage" is activated, and therefore allows the following functions:

   a. Commitment to the content (Content commitment, to perform the function of electronic signature)

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

1.5.1.6. Certified Public Employee midlevel pseudonym in HSM

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.3.4	In the hierarchy of the EC esFIRMA
0.4.0.194112.1.0	According to the policy QCP-n
2.16.724.1.3.5.4.2	Spanish public employee pseudonym midlevel

Individual certificates of public employee under a pseudonym midlevel are certified qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and give effect to the provisions of the technical regulations identified with reference ETSI EN 319 411-2.

These certificates are issued to public employees to identify (using a pseudonym) as persons in the service of the Administration, agency or public entity, linking it, fulfilling the requirements Article 43 of Law 40/2015, of 1 October, the Legal Regime of the Public Sector, for the electronic signature of the staff serving the Public Administrations.

Individual certificates of public employee pseudonym midlevel They are managed centrally.

Certificates of individual public employee pseudonymous average level are issued in accordance with the levels of medium assurance profiles certificates set out in paragraph 11 of document "Profiles Electronic Certificates" of the General Bureau of Information, Documentation and Publications Ministry of Finance and Public Administration.

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

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

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

EsFIRMA does not offer backup and recovery of keys. Therefore, esFIRMA not respond in any way for any loss of encrypted information that can not be recovered.

Uses information in the certificate profile indicates the following:

a) The field "key usage" is activated, and thus allows us to perform the following functions:
    a. Commitment to the content (content commitmentTo perform the function of electronic signature)

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

1.5.1.7. Web authentication certificate, midlevel

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	According to the policy QCP-web
2.16.724.1.3.5.5.2	Spanish electronic office administrative midlevel

Web authentication certificates are certificates midlevel qualified in accordance with Article 45 and Annex IV of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and give effect to the provisions of the technical regulations identified with reference ETSI EN 319 411-2.

These certificates are issued to Web addresses to identify them as electronic administrative offices of the Administration, agency or public entity, linking with it, fulfilling the requirements Article 38 of Law 40/2015, of 1 October, the Legal Regime of the Public Sector, for identification and secure communication with citizens.

Certificates for web authentication midlevel are issued in accordance with the levels of medium assurance profiles certificates set out in paragraph 8 of document "Profiles Electronic Certificates" of the General Bureau of Information, Documentation and Publications of the Ministry of Finance and Public Administration.

Uses information in the certificate profile indicates the following:

a) The field "key usage" is activated, and thus allows us to perform the following functions:
    a. Digital Signature (for authentication feature)
    b. Key Encipherment (for management and key transport)

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

1.5.1.8. Electronic Seal certificate TSA / TSU

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	According to the policy QCP-l

Electronic stamp certificates of TSA / TSU are certified qualified in accordance with Article 38 and Annex III of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and give effect to the provisions of the technical regulations identified with reference ETSI EN 319 421 and ETSI EN 319 422.

This certificate allows Time Stamping Units or TSU issuing timestamps when they receive an application under the specifications of RFC3161.

The keys are generated in a qualified support device (HSM).

Uses information in the certificate profile indicates the following:

a) The field "key usage" is activated, and thus allows us to perform the following functions:
    a. content Commitment
b) Field "extend key usage" has enabled the function:
    a. TimeStamping
c) In the "Qualified Certificate Statements" field the following statement appears:
    a. QcCompliance (0.4.0.1862.1.1), which reports that the certificate is issued as qualified.
d) The "User Notice" describes the use of this certificate.

1.5.2. Limits and prohibitions on use of certificates

Certificates are used to set its own function and purpose without usable in other functions and for other purposes.

Similarly, certificates must be used only in accordance with applicable law, especially taking into account the existing import restrictions and export at all times.

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

Certificates are not designed, can not allocate and use or resale is not authorized as control equipment dangerous situations or for uses requiring actions failsafe, as the operation of nuclear facilities, navigation systems or air communications or weapons control systems, where failure could lead directly to death, personal injury or severe environmental damage.

They should take into account the limits in the various fields of the certificate profiles, visible on the web of esFIRMA https://www.esfirma.com

The use of digital certificates so that the DPC and other applicable documents, especially the contract with the subscriber and factual texts or PDS is considered to misuse the legal purposes is breached,

and exempts esFIRMA any liability for misuse, whether the signer or any third party.

EsFIRMA not authorized to access or legal obligation to monitor the information on which can be applied using a certified key. Therefore, as a result of this technical impossibility to access the content of the message is not possible by esFIRMA issue any assessment on such content, thus assuming the subscriber, the signatory or the person responsible for the custody, any liability arising from the use of content rigged a certificate.

It also will be attributable to the subscriber, the signer or the person responsible for the custody, any liability that may arise from the use thereof beyond the limits and conditions set out in this CPS, the binding legal documents with each certificate, or contracts or agreements with the registration authorities or subscribers, as well as any other derivative thereof misuse of this section or that could be construed as such according to the law.

Certificates are used exclusively and only from the Platform eGovernment and add-ons or extensions thereof esPublico the company makes available to the subscriber.

1.6. Policy Administration

1.6.1. Organization administering the document

Security Office ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (esFIRMA)
BARI CALLE 39 (EDIF. Binary Building)
50197 - ZARAGOZA
(+34) 976 300 110

identification Registry	Mercantile Registry of Zaragoza
I take	2649
Folio	215
Sheet	Z-28722
CIF	A-50,878,842

1.6.2. Organization that approves the document

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

The esFIRMA safety committee, composed of the Chair, the Head of Service and Information and Security Officer esFirma, is responsible for the approval of this Practice Statement.

Both functions as members of the Committee are defined in the Security Policy esFirma (esFIRMA_PolíticaSeguridad_v2r0.pdf).

1.6.3. Contact the organization

ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (esFIRMA)
BARI CALLE 39 (EDIF. Binary Building)
50197 - ZARAGOZA
(+34) 976 300 110

1.6.4. Document management procedures

The documentary system and organizational guarantees esFIRMA by the existence and implementation of relevant procedures, proper maintenance of this document and service specifications related thereto.

EsFIRMA performs at least annual reviews of this document.

As defined in the Security Policy esFIRMA (esFIRMA_PolíticaSeguridad_v2r0.pdf), the Security Office shall be the entity responsible for maintaining this document.

Security Bureau responsible for drafting, maintenance and administration of the CPD, the factual texts (PDS), delivery and acceptance sheets, and other legal documents (agreements, contracts, etc.) of esFirma. Whenever there are changes of sufficient importance in the management of certificates defined in this DPC, a new revision of this document, be identified in the initial box "version control" within the section "general information" will be created.

The performance of the Security Office at the request takes its responsibility according to the needs that produzcan.EsFirma can make changes that do not require notification when they do not directly affect the rights of signatories and subscribers of certificates or subscribers seals.

When esFirma will make changes that modify the rights of signatories and subscribers of certificates and subscribers seals must notify publicly in order to submit their comments to the Security Office for 15 days following the publication of future changes .The annual reviews must have upgrade phases for routine consisting of: Phase proposed amendments collection phase analysis, testing and modifications writing comments and approval phase phase PublicationThe department has a logbook where they will be introduced and registered each of the proposals, indicating the date of receipt of the proposal, describing the proposed amendment and the reasons technical and / or legal.Notifying publicly the changes will be published in the section "documentation" on the website https: //www.esfirma.comLas reviews of this DPC will be published on the website of esFirma after being approved by the Board of Directors of Esfirma.

2. Disclosure and deposit certificates

2.1. Deposit (s) Certificate

EsFIRMA has a deposit certificate, in which the information concerning certification services are published.

Such service is available 24 hours a day, 7 days a week and in case of failure of runaway esFIRMA system, it will use its best efforts to ensure that the service is back available within the deadline set in section 5.7.4 of this Certification Practice Statement

2.2. Publication of information of the service provider certification

EsFIRMA publishes the following information in your deposit:

- Certificates issued, when obtained consent of the individual identified in the certificate.
- Certificate revocation lists and other status information revocation of certificates.
- Applicable certificate policies.
- The Certification Practice Statement.
- Disclosure texts (PKI Disclosure Statements - PDS), at least in Spanish and in English.

2.3. Frequency of publication

Information service provider certification, including policies and Certification Practice Statement is published as soon as it is available.

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

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

2.4. Access control

EsFIRMA does not limit read access to the information set out in Section 2.2, but establishes controls to prevent unauthorized persons can add, modify or delete records reservoir to protect the integrity and authenticity of information, especially information status revocation.

EsFIRMA uses reliable systems for the tank, so that:

- Only authorized persons can make entries and changes.
- It can be verified the authenticity of the information.
- Certificates are only available for consultation if the individual identified in the certificate has consented.
- You can any technical changes affecting safety requirements detected.

3. Identification and authentication

3.1. initial registration

3.1.1. Types of names

All certificates contain a distinguished name in the Subject X.501, including a Common Name component (CN =) on the subscriber identity and the individual identified in the certificate, and various additional information in the identity SubjectAlternativeName field.

The names contained in the certificates are as follows.

3.1.1.1. Certificate of public employee, senior, on card

	"IS"
	Name ("official" name) of the Administration, agency or public entity underwriter certificate, which is linked to the employee
	CERTIFIED PUBLIC EMPLOYEE ELECTRONICO
	Organization identifier according to the technical standard ETSI EN 319 412-1
	First and second name, in accordance with identification (ID / Passport)
	Name, according to identity document (ID / Passport)
	DNI / NIE employee
	Name Surname1 Surname2 - NIF employee
	QUALIFIED EMPLOYEE SIGNATURE CERTIFICATE OF PUBLIC HIGH LEVEL
	Name of the Subscriber
	NIF entity subscription
	DNI or NIE responsible
	Name of responsibility for the Certificate

	Surname of the head of certificate
	Second surname of the head of certificate
	Email responsibility for the certificate. Optional.

3.1.1.2. Certificate of public employee, middle level, HSM

	"IS"
	Name ("official" name) of the Administration, agency or public entity underwriter certificate, which is linked to the employee
	CERTIFIED PUBLIC EMPLOYEE ELECTRONICO
	Organization identifier according to the technical standard ETSI EN 319 412-1
	First and second name, in accordance with identification (ID / Passport)
	Name, according to identity document (ID / Passport)
	DNI / NIE employee
	Name Surname1 Surname2 - NIF employee
	CERTIFICATE OF PUBLIC EMPLOYEE OF ELECTRONIC STANDARD LEVEL
	Name of the Subscriber
	NIF subscriber entity
	DNI or NIE responsible

	NRP or PIN responsible for the certificate subscriber
	Name of responsibility for the Certificate
	Surname of the head of certificate
	Second surname of the head of certificate
	Email CERTIFICATE responsible. Optional.

3.1.1.3. Certificate stamp body, mid-level software

	"IS"
	Name ("official" name of organization) subscriber
	SEAL ELECTRONICO
	Organization identifier according to the technical standard ETSI EN 319 412-1
	DNI / NIE of the subscribing organization
	Designation automatic system or application process.
	ELECTRONIC SEAL STANDARD LEVEL
	Name of the Subscriber
	Subscriber NIF
	Second surname responsible Seal

	Email responsible Seal

3.1.1.4. Certificate stamp body, medium level, HSM

	"IS"
	Name ("official" name of organization) subscriber
	SEAL ELECTRONICO
	Organization identifier according to the technical standard ETSI EN 319 412-1
	DNI / NIE of the subscribing organization
	Designation automatic system or application process.
	ELECTRONIC SEAL STANDARD LEVEL
	Name of the Subscriber
	Subscriber NIF
	Second surname responsible Seal

3.1.1.5. Certificate of public employee under a pseudonym, high level, on card

	"IS"
	Name ("official" name) of the Administration, agency or public entity underwriter certificate, which is linked to the employee
	PUBLIC EMPLOYEE CERTIFICATE ELECTRONIC pseudonymous
	Organization identifier according to the technical standard ETSI EN 319 412-1
	mandatory according to ETSI EN 319 pseudonymous 412-2 for such certificates
	Pseudonymous and the Agency

	PUBLIC EMPLOYEE ELECTRONIC CERTIFICATE OF HIGH-LEVEL pseudonymous
	Name of the Subscriber
	Subscriber NIF
	Pseudonym used by the signer and authorized by the subscriber

3.1.1.6. Certificate of public employee under a pseudonym, middle level, HSM

	"IS"
	Name ("official" name) of the Administration, agency or public entity underwriter certificate, which is linked to the employee
	PUBLIC EMPLOYEE CERTIFICATE ELECTRONIC pseudonymous
	Organization identifier according to the technical standard ETSI EN 319 412-1
	mandatory according to ETSI EN 319 pseudonymous 412-2 for such certificates
	Pseudonymous and the Agency
	ELECTRONIC CERTIFICATE PUBLIC EMPLOYEE LEVEL HALF pseudonymous
	Name of the Subscriber
	Subscriber NIF
	Pseudonym used by the signer and authorized by the subscriber

3.1.1.7. EV Web authentication certificate, midlevel

	"IS"
	Name ("official" name) of the Administration, agency or public entity underwriter certificate (custodian)
	City
	Description Certificate Type: Electronic Office
	The descriptive name of the site
	The NIF of the entity responsible
	Organization Category: Government Entity
	Jurisdiction
	Organization identifier according to the technical standard ETSI EN 319 412-1
	Domain name (DNS) where he would spend the certificate.

3.1.1.8. Electronic stamp certificate TSA / TSOR

	"IS"
	Name ("official" name of organization) subscriber
	CERTIFICATION AUTHORITY ESFIRMA
	DNI / NIE of the subscribing organization
	Name of TSU

3.1.2. Meaning of the names

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

3.1.3. Use of anonymous and pseudonymous

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

3.1.4. Interpreting name formats

Names formats construed in accordance with the law of the country in which the subscriber, on their own terms.

The "country" field will always be Spain by certificates issued exclusively to the Spanish government.

The certificate shows the relationship between an individual and the administration, agency or public entity with which it is linked, regardless of the nationality of the individual. This stems from the corporate nature of the certificate, which is subscriber corporation, and the individual linked the person authorized to use.

Certificates issued to subscribers Spanish, the "serial number" field must include the signer NIF, the effect of the admission certificate for performing procedures with the Spanish authorities.

3.1.5. Uniqueness of names

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

You can not assign a subscriber name that has already been used to a different subscriber, a situation which in principle is not to give thanks to the presence of Tax Identification Number, or equivalent, in the naming scheme.

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

- Tax Identification Number (NIF) or other legally valid for the individual identifier.
- Tax Identification Number (NIF) or other legally valid subscriber identifier.
- Type Certificate (Certificate Description field).

3.1.6. Resolution of disputes concerning names

License applicants will not include names in applications that may involve infringement by the prospective subscriber of third party rights.

EsFIRMA not be required to first determine that an applicant has certified industrial property rights over the name in a certificate request, but in principle shall certify it.

It also will not act as arbitrator or mediator, nor in any other way should resolve any dispute concerning the ownership of names of people or organizations, domain names, trademarks or trade names.

However, if you receive a notification concerning a name conflict, according to the country's legislation subscriber, you can take appropriate actions to block or withdraw the certificate issued.

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

Any controversy or dispute arising hereof, shall be finally settled by arbitration law an arbitrator within the framework of the Spanish Court of Arbitration in accordance with its Rules and Regulations, to which the management is entrusted arbitration and the appointment of the arbitrator or arbitral tribunal. The parties state their commitment to comply with the award rendered in the contractual document that formalizes the service.

3.2. Initial validation of identity

The identity of the signers of certificates is fixed at the time of signing the contract between esFIRMA and the subscriber, at which verified the existence of the subscriber, and the supporting documentation provided their identity and cargo and / or condition in which signature, in accordance with the rules specified in administrative law applies.

The identity of individuals identified in the certificate is validated by the corporate records of the Administration, agency or public entity underwriter certificates. The subscriber, by administrative certificate issued by the City Clerk, will produce a certification of the necessary

data and send it to esFIRMA, by means enable it to register the identity of the signatories. When the subscriber does not have Secretariat, this certification will be issued by the Head of certification service designated.

The personal data files each administration, agency or public entity must be registered in Protection Agency corresponding data for each of them, being their responsibility, not that of esFIRMA, which acts as a processor, as it indicated in section 9.4 of this DPC.

To avoid any conflict of interests Public Administrations subscribers are independent entities of the service provider trusted "esFIRMA" and the company esPublico[1].

3.2.1. Proof of possession of private key

Possession of the private key is demonstrated under reliable method of delivery and acceptance by the signer certificate from the Platform eGovernment, to sign the acceptance and use in the platform.

3.2.2. Identity authentication subscriber acting through a representative

Physical capable of acting on behalf of an Administration, agency or public entity underwriter certificates, people can act as their representatives in relation to the provisions of this CPS, provided there is a previous situation of legal representation or voluntary between the individual and the administration, agency or public entity underwriter certificates, which requires recognition by esFIRMA, which will be made by the following procedure:

1. A certificate secretariat in full agreement appointing the legal representative with the following information:
    a. as a representative:
        i. Name and surname
        ii. Document: NIF representative
    b. The subscriber identification data it represents:

1 Ap 6.2.2.q) ETSI EN 319 411-1

i. Name of administration, agency or public entity.
ii. Information on the extent and duration of the powers of representation of the applicant.
iii. Document: Tax Administration, agency or public entity.
iv. Document: Documents used to establish the matters referred irrefutably in accordance with the rules specified in administrative law applies, and registration in the corresponding public register if it is enforceable.

c. The data relating to the representation or the ability to act that shows:
    i. The validity of the performance or capacity of action (start and end).
    ii. The scope and limits, if any, representation or the ability to act:
        1. TOTAL. Performance or capacity.
        2. PARTIAL. Representation or partial capacity.

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

Once electronically signed documents, RA functions will be activated users City Council stated in the contract as authorized operators to perform this function.

3.2.3. Authentication of the identity of an individual

This section describes the test methods of the identity of an individual identified in a certificate.

The procedure for requesting and generate certificates is done through an electronic process tool Platform eGovernment layout Subscriber and signatories.

The electronic procedure for issuing a certificate to an individual will follow these steps and the following documents will be generated:

1. Employee Application Certificate through the e-government platform (with its corresponding check and opening file)
2. A secretarial certificate or personnel department, which certifies that the person is linked to City Hall.
3. Petition signed by authorized by the entity (or legal representative) operator, recorded output and notifies ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA(Attaching a copy of the certificate and the request of the employee).

To issue a certificate of electronic stamp the following steps are followed, through an electronic procedure in which the following documents are generated:

1. Request of the legal representative of the entity that output is recorded and reported to ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA

To issue a certificate See the following steps are followed, through an electronic procedure in which the following documents are generated:

1. Request of the legal representative of the entity that output is recorded and reported to ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA.

3.2.3.1. The certificates

Identifying information of individuals identified in the certificate is validated by comparing the information request of the Administration, agency or public entity underwriter certificates, the Administration records, agency or public entity to which is linked, generated as indicated in section 3.2 of this CPS, ensuring the accuracy of information to be certified.

3.2.3.2. Need for personal presence

Certificate Request

To request certificates direct physical presence due to the already proven relationship between the individual and the administration,

agency or public entity to which it is linked is not required, since this request is made by an authorized operator the subscriber in the contract.

Either direct physical presence of the signer to accept the certificate that cases where a subject already identified previously by virtue of their relationship with the government, agency or public entity concerned is necessary, sign the acceptance by their ID electronic.

Where it is not possible signature by electronic ID, the signer must print the sheet acceptance document for signature before the responsible ID service, which should contrast the identity of the natural person identified in the certificate through their physical presence. During this procedure is irrefutably confirms the identity of the natural person identified in the certificate.

For this reason, it is only necessary to verify in person the identity of the individual signer in case it is not possible acceptance signed by its electronic DNI.

Certificate Renewal
If any of the information from the individual identified in the certificate has changed, you must properly record new information and a full authentication, by personal identification will occur before the authorized subscriber operator, which should contrast the identity of the person physical.

3.2.3.3. Linking individual
The documentary justification for linking an individual identified in a certificate with the Administration, agency or public entity to which it is linked is given by their constancy in Personnel Records Administration, agency or public entity to which he is linked to the individual.

3.2.4. Subscriber unverified information
EsFIRMA does not include any subscriber information not verified certificates.

3.3. Identification and authentication of applications for renewal

3.3.1. Validation for routine recertification

EsFIRMA generally does not renew certificates. Before it expires the request for the issuance of a new certificate is signed.
esFIRMA verifies that the information used to verify identity and other subscriber data and physical person identified in the certificate remain valid.

If any of the information from the individual identified in the certificate has changed, you must properly record new information and a full authentication, in accordance with the provisions of section 3.2 will occur.

3.3.2. Identification and authentication of the request for renewal after prior revocation

Before generating a certificate to a subscriber whose certificate was revoked, esFIRMA verify that the information used at the time to verify identity and other subscriber data and physical person identified in the certificate remains valid, in which case it will apply the provisions of the previous section.

Certificate renewal after revocation is not possible in the following cases:

- The certificate was revoked by erroneous emission at a different person identified in the certificate.
- The certificate was revoked by issuing unauthorized by the natural person identified in the certificate.
- The revoked certificate may contain incorrect or false information.

If any subscriber information or physical person identified in the certificate has changed, the new information is properly recorded and full authentication, in accordance with the provisions of Section 3.2 occurs.

3.4. Identification and authentication of the revocation request

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

Acceptable methods such verification are:

- Sending a request for revocation by the subscriber or individual identified in the certificate electronically signed.
- The use of "identity verification phrase" or other methods of personal authentication, which consists of information known only to the individual identified in the certificate, which allows you to automatically revoke your certificate.
- Physical personación in an office of the Subscriber.
- Other media, such as telephone, when there is reasonable assurance of the identity of the applicant for revocation, according to esFIRMA.

3.5. Authenticating a suspension request

Suspension requests are treated as revocation requests.

4. Operating requirements lifecycle of certificates

4.1. Certificate issuance request

4.1.1. Standi to apply for the issue

Administration, agency or public entity must sign a contract to provide certification services with esFIRMA.

Also, prior to the issuance and delivery of a certificate, a certificate request exists in a sheet certificate request through the electronic administration platform.

There is a subscriber authorization for the applicant to make the application, which is implemented legally by a certificate application form signed by that applicant on behalf of the Administration, agency or public entity.

4.1.2. Procedure high and responsibilities

EsFIRMA receives certificate requests, made by administrations, public agencies or public law.

Applications are implemented through a document in electronic form, completed by the Administration, agency or public entity, whose recipient is esFIRMA, which will include data from persons who shall be issued. The request will be made by the authorized by the subscriber (responsible for certification) and has been identified in the contract between the subscriber and operator esFIRMA.

The application shall be accompanied by supporting documentation of identity and other circumstances of the individual identified in the certificate, in accordance with the provisions of section 3.2.3. also it must include a physical address, or other data that allow physical contact person identified in the certificate.

4.2. Processing the application for certification

4.2.1. Execution of the functions of identification and authentication

Upon receipt of a certificate request, esFIRMA ensures that license applications are complete, accurate and duly authorized, before processing.

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

Supporting documentation for the approval of the application must be preserved and duly registered with guarantees of security and integrity for a period of 15 years from the expiry of the certificate, even if anticipated loss of validity for revocation, when the certificates, qualified.

4.2.2. Approval or rejection of the request

EsFIRMA approves the certificate request and proceeds to its issuance and delivery, after the request occurs in the Platform eGovernment.

In case of suspicion that the information is incorrect or that may affect the reputation of the Certification or subscribers, esFIRMA denied the request, approval or stop until you have made the additional checks it deems appropriate.

If the additional checks no correction information to verify discards, esFIRMA definitely reject the application.

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

EsFIRMA can automate the verification procedures of correcting the information to be contained in the certificates, and approval of applications.

4.2.3. Application deadline for resolving

EsFIRMA attends license applications in order of arrival within a reasonable time, a guarantee may be specified in the contract maximum period of issuing certificates.

Applications remain active until its approval or rejection.

4.3. Issuance of Certificate

4.3.1. CA shares during the issuance process

Following approval of the application for certification is applicable to the issuance of the certificate safely and made available to the undersigned for acceptance by sending a link to the mobile device and / or email address which is designated by the subscriber certificate request in accordance with the procedure referred to in paragraph 4.4.2.

During the process, esFIRMA:

- Protects the confidentiality and integrity of registration data available.
- Use trustworthy systems and products that are protected against modification and ensure the technical safety and, where appropriate, cryptographic certification processes to support those who serve.
- It generates the key pair, using a method of generating certificates securely linked with the procedure of key generation.
- It employs a method of generating certificates securely linking the certificate with the registration information, including certified public key.
- It ensures that the certificate is issued by systems using protection against counterfeiting and to ensure the confidentiality of the key during the process of generating those keys.
- It includes the information on the certificate set out in Annex 1 of Regulation (EU) 910/2014, in accordance with the provisions of Sections 3.1.1 and 7.1.
- Indicates the date and time when a certificate was issued.

4.3.2. Notification of the subscriber issuance

EsFIRMA notifies the issuance of the certificate to the Administration, agency or public entity underwriter certificate, and physical person identified in the certificate through their email addresses, already included in the information of the Platform eGovernment.

4.4. Delivery and acceptance certificate

4.4.1. Responsibilities CA

During this process, esFIRMA must perform the following actions:

- definitely prove the identity of the natural person identified in the certificate, with the collaboration of government, agency or entity of public law in accordance with the provisions of sections 3.2.2, 3.2.3, and 4.3.1.
- Deliver the sheet delivery and acceptance of the certificate to the individual identified in the certificate (with the collaboration of government, agency, or entity of public law in cases where the signer does not have electronic ID), which has the following minimum content:
  - Basic information regarding use of the certificate, including especially information about the service provider and Certification Practice Statement applicable Certification, and their duties, powers and responsibilities
  - Information about the certificate.
  - Recognition by the signer, receiving the certificate and acceptance of said elements.
  - Signer liability regime.
  - Responsibility of the signatory.
  - Method exclusive to the signer, your private key and its certificate activation data, in accordance with the provisions of Sections 6.2 and 6.4 imputation.
  - The date of the ceremony and acceptance.
- Obtain the signature, written or electronic, of the person identified in the certificate.

When necessary, the Administration, agency or public entity contributes to these processes, having documented record the previous acts and retaining said original documents (sheets delivery and acceptance), sending electronic copy to esFIRMA as well as the original when esFIRMA required access to them.

4.4.2. Conduct constituting acceptance of the certificate

Following approval of the application for certification is applicable to the issuance of the certificate safely and notifies the undersigned for acceptance by sending a link to the mobile device and / or email address which is designated by the subscriber certificate request or via the messaging system of the Platform eGovernment.

Certificates issued in software, the certificate and keys are managed on a HSM, arranging the signing of exclusive control of its use.

Certificates issued on card, these are sent to the subscriber responsible for certification and corresponding PINs directly to the postal address of the consignee.

Furthermore, the acceptance certificate for the individual identified in the certificate signature is produced by the sheet delivery and acceptance, by the electronic administration platform.

4.4.3. Publication of the certificate

EsFIRMA publishes the certificate in the tank section 2.1 concerns with relevant safety checks and whenever esFIRMA has the authorization of the natural person identified in the certificate.
EsFIRMA publishes the TSA certificate / TSU on its website.

4.4.4. Notice of the issue to third parties

EsFIRMA takes no notice of the issue to third parties.

4.5. Using the key pair and certificate

4.5.1. Use by the subscriber or signatory

EsFIRMA requires the following:

- EsFIRMA provide complete and accurate information in accordance with the requirements of this Certification Practice Statement, particularly as regards the acceptance procedure.
- Give its prior consent to the issuance and delivery of a certificate consent.
- Use the certificate in accordance with the provisions of section 1.4.
- When the certificate work in conjunction with a DCCF, recognizing its production capacity of qualified electronic signatures; this is equivalent to handwritten signatures as well as other types of electronic signatures and data encryption mechanisms.
- Be especially diligent in keeping your private key, in order to prevent unauthorized use, in accordance with the provisions of Sections 6.1, 6.2 and 6.4.
- EsFIRMA and communicate to anyone who believes may trust the certificate, without unjustifiable delays:
    - Loss, theft, or potential compromise of its private key.
    - Loss of control over your private key, due to the commitment of activation data (eg PIN code) or for any other reason.
    - Inaccuracies or changes to the certificate content that you know or could know the subscriber.
- Stop using the private key the period specified in section 6.3.2 elapsed.

EsFIRMA requires the signer to take responsibility for:

- All information provided by the signer that are contained in the certificate are correct.
- That the certificate is used exclusively for authorized and legal purposes, in accordance with the Certification Practice Statement.
- That no unauthorized person has ever had access to the private key of the certificate, which is solely responsible for

any damage caused by its breach of the duty to protect the private key.

- That the signer is an end entity and not a service provider certification, and who will not use the private key corresponding to the public key listed in the certificate to sign any certificate (or any other format of certified public key) or List certificate revocation or title certification services provider or any other case.

4.5.2. Use by the subscriber

4.5.2.1. Obligations of the certificate subscriber

EsFIRMA contractually obliges the subscriber to:

- Provide the Certification complete and accurate information in accordance with the requirements of this Certification Practice Statement, particularly as regards the acceptance procedure.
- Give its prior consent to the issuance and delivery of a certificate consent.
- Use the certificate in accordance with the provisions of section 1.4.
- EsFIRMA and communicate to anyone who believes that the subscriber can trust the certificate, without unjustifiable delays:
    - Loss, theft, or potential compromise of its private key.
    - Loss of control over your private key, due to the commitment of activation data (eg PIN code) or for any other reason.
    - Inaccuracies or changes to the certificate content that you know or could know the subscriber.
    - Loss, alteration, unauthorized use, theft or compromise, if any, of the card.
- Move individuals identified in the certificate compliance with specific obligations thereof, and establish mechanisms to ensure effective compliance with them.

- Not monitor, manipulate or perform reverse engineer the technical implementation of esFIRMA certification services without prior written permission.
- Not compromise safety certification services provider esFIRMA certification services without prior written permission.

4.5.2.2. Liability Underwriter certificate

EsFIRMA contractually obliges the subscriber to take responsibility for:

- That all statements made in the application are correct.
- All information provided by the subscriber that are contained in the certificate are correct.
- That the certificate is used exclusively for authorized and legal purposes, in accordance with the Certification Practice Statement.
- That no unauthorized person has ever had access to the private key of the certificate, which is solely responsible for any damage caused by its breach of the duty to protect the private key.
- The subscriber is an end entity and not a service provider certification, and who will not use the private key corresponding to the public key listed in the certificate to sign any certificate (or any other format of certified public key) or List certificate revocation or title certification services provider or any other case.

4.5.3. Use by the third party trust certificates

4.5.3.1. Obligations of the relying party certificates

EsFIRMA informs the relying party certificates that it must assume the following obligations:

- Advice independently about the fact that the certificate is appropriate for the intended use.
- Verify the validity, suspension or revocation of certificates issued, for which used information on the status of certificates.

- Verify all certificates in the certificate hierarchy before relying on the digital signature or any certificate of the hierarchy
- Recognize that electronic signatures verified, produced in a qualified signature creation device (DCCF) are legally considered qualified electronic signatures; this is equivalent to handwritten signatures and the certificate allows the creation of other types of electronic signatures and encryption mechanisms.
- Keep in mind any limitations on the use of the certificate, regardless of whether it is in the certificate itself or contract third party that trusts the certificate.
- Keep in mind any precautions established in a contract or other instrument, regardless of its legal status.
- Not monitor, manipulate or perform reverse engineer the technical implementation of esFIRMA certification services without prior written permission.
- Not compromise the safety of services certification esFIRMA without prior written permission.

4.5.3.2. the third party liability trust certificates

EsFIRMA informs the relying party certificates that it must assume the following responsibilities:

- You have enough information to make an informed decision in order to trust the certificate or not.
- Which is solely responsible for trust or not the information contained in the certificate.
- Which shall be solely responsible if you violate its obligations as a third party that trusts the certificate.

4.6. Certificate Renewal

EsFIRMA not perform recertification. Expired certificate a new certificate is issued, following the application procedure registered with the Platform eGovernment.

4.7. Renewing keys and certificates

4.7.1. Causes of renewal of keys and certificates
Does not apply.

4.7.2. New identification procedure

EsFIRMA warn the subscriber to the need for a new personación signer and signature of acceptance sheet in those cases where this is required by the statutory period during identification 5 years.

Such personación and identification shall be in accordance with specified in paragraph 3.2.

The signing of the acceptance sheet shall be in accordance with that specified in paragraph 4.4.2.

4.7.3. Notification of the issuance of the renewed certificate
Does not apply because there was no renewals.

4.7.4. Conduct constituting acceptance of the certificate
Does not apply.

4.7.5. Publication of the certificate
Does not apply.

4.7.6. Notice of the issue to third parties
EsFIRMA not make any notice of the issue to third parties.

4.8. Certificate Modification
The modification of certificates, except the modification of the certified public key, which is considered renewal, will be treated as a new issue of certificate applied as described in Sections 4.1, 4.2, 4.3 and 4.4.

4.9. Revocation and suspension of certificates

4.9.1. Causes certificate revocation
EsFIRMA revoke a certificate when there occurs any of the following causes:

1) Circumstances affecting the information contained in the certificate:

a) Changing any of the data contained in the certificate, after the issuance of the certificate corresponding including modifications.
b) Discovery that any of the data contained in the certificate application is incorrect.
c) Discovery that any of the data contained in the certificate is incorrect.

2) Circumstances affecting the security of the key or certificate:
   a) Commitment of the private key infrastructure or systems certification service provider that issued the certificate, provided that affects the reliability of certificates issued from that incident.
   b) Infringement by esFIRMA, the requirements of management procedures certificate, in this Declaration Certification Practices.
   c) Compromise or suspected compromise security key or certificate issued.
   d) Unauthorized access or use, by a third party private key corresponding to the public key contained in the certificate.
   e) Irregular use of certified physical person identified in the certificate, or lack of diligence in the custody of the private key.

3) Circumstances affecting the subscriber or physical person identified in the certificate:
   a) Completion of the legal relationship between esFIRMA service delivery and subscriber.
   b) Modification or termination of the underlying legal relationship or what caused the issuance of the certificate to the individual identified in the certificate.
   c) Infringement by the certificate applicant preset requirements for the application thereof.
   d) Violation by the subscriber or by the person identified in the certificate, their obligations, liabilities and guarantees established in the relevant legal document.
   e) The incapacity or death of key owner.

f) The termination of the legal person underwriter certificate and authorization to the holder subscriber key or termination of the relationship between subscriber and person identified in the certificate.
g) Subscriber request revocation of the certificate, in accordance with the provisions of section 3.4.

4) Other circumstances:
   a) Termination of service esFIRMA certification in accordance with the provisions of section 5.8.
   b) Using the certificate that is harmful and continued to esFIRMA. In this case, it is considered that a use is harmful in terms of the following criteria:
      - The nature and number of complaints received.
      - The identity of the entities filing complaints.
      - The relevant legislation at all times.
      - The response of the subscriber or of the person identified in the certificate to complaints received.

4.9.2. Standing to request revocation

They may request revocation of a certificate:

- The person identified in the certificate, on request from the subscriber or esFIRMA.
- Subscriber certificate by request to esFIRMA.

4.9.3. Application procedures revocation

The revocation request include the following information:

- Date of application for the revocation.
- Subscriber Identity or Signer.
- Detailed reason for the recall petition.

The application must be authenticated by esFIRMA, in accordance with the requirements of section 3.4 of this policy, prior to revocation.

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

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

The revocation service is in the Platform eGovernment, in which the signer and the subscriber manage their certificates.

If the recipient of a request for revocation by a natural person identified in the certificate was the Underwriter once the request is authenticated must submit a request in this regard to esFIRMA.

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

EsFIRMA nonreactive once the certificate has been revoked.

4.9.4. Temporary revocation application deadline

Revocation requests shall be sent immediately as knowledge of the cause of revocation shall have, and shall not exceed 24 hours[3].

4.9.5. temporary period of application processing

The revocation will occur immediately when received, in the ordinary operation schedule esFIRMA, and shall not exceed 60 minutes[4].

4.9.6. Information consultation obligation certificate revocation

Third parties should check the status of those certificates in which they wish to rely.

A method by which you can verify the certificate status is by consulting the List of Revoked Certificates latest issued by the Certification of esFIRMA.

Revocation Lists Certificates are published in the Repository Certification Body and on the following web addresses, indicated in certificates:

3 Ap 6.2.4.a) vi) ETSI EN 319 411-1
4 Ap 6.2.4.a) vii) ETSI EN 319 411-1

- *CA ROOT:*
  - https://crls2.esfirma.com/acraiz/acraiz2.crl
  - https://crls1.esfirma.com/acraiz/acraiz2.crl
- *CA INTERMEDIATE:*
  - https://crls1.esfirma.com/acaapp/acaapp2.crl
  - https://crls2.esfirma.com/acaapp/acaapp2.crl

4.9.7. Emission frequency of revocation lists certificates (LRCs)
LRC EsFIRMA emits at least every 24 hours and to a reversal occurs.

The LRC indicates the scheduled time of issue of a new LRC, but can be issued before the deadline LRC indicated in the above LRC to reflect reversals.

The LRC maintains compulsorily revoked or suspended certificate until it expires.

4.9.8. maximum period of publication of LRCs
The LRCs are published in the deposit within a reasonable period immediately after generation in any case no more than a few minutes.

4.9.9. Availability of services online checking certificate status

EsFIRMA reports the revocation status of certificates, using the OCSP protocol, which allows the status of validity of the certificates online from directions:

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

In case of failure of systems checking certificate status for reasons beyond the control of esFIRMA, it must make its best efforts to ensure

that this service remains idle the minimum possible time, which may not exceed one day.

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

Services status check of certificates are free to use[5].

EsFIRMA information remains available revocation status past the period of validity of the certificate[6].

4.9.10. Obligation consultation service certificate status checking

It is mandatory to check the status of certificates before relying on them as a priority, by OCSP service access.

4.9.11. Other forms of certificate revocation information

Alternatively, third parties who rely on certificates may consult the esFIRMA deposit certificates, which is available 24 hours a day, 7 days a week on the web:

https://www.esfirma.com

4.9.12. Special requirements if engagement of the private key

The commitment of the private key esFIRMA is notified to all participants in certification services, as far as possible, by publishing this fact on the website of esFIRMA and, if deemed necessary, in other media, even on paper.

4.9.13. Causes suspension of certificates

- EsFIRMA not perform suspension of certificates.

4.9.14. Suspension request

- EsFIRMA not perform suspension of certificates

4.9.15. Procedures for suspension request

EsFIRMA not perform suspension of certificates.

4.9.16. period of suspension

5 Ap 6.3.10 ETSI EN 319 411-2

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

EsFIRMA not perform suspension of certificates.

4.10. Completion of the Subscription

After the period of validity of the certificate, will terminate the service subscription.

EsFIRMA can issue a new certificate ex officio, while subscribers maintain that state.

4.11. Testing services Certificate Status

4.11.1. operational characteristics of services

Services certificate status checking is provided through a web interface consultation, web https://www.esfirma.com

They can also be checked using OCSP service access to web addresses listed in paragraph 4.9.6

4.11.2. Availability of services

Services certificate status checking are available 24 hours a day, 7 days a week, throughout the year, except for scheduled stops.

4.12. Deposit and Key Recovery

4.12.1. Deposit policy and practices and key recovery

EsFIRMA pays no deposit and key recovery.

4.12.2. Encapsulated policy and practices and key recovery session

No stipulation.

5. Physical security controls, management and operations

5.1. Physical security controls

EsFIRMA has established security checkpoints physical and environmental to protect the resources of the facilities where the systems, the systems themselves and the equipment used for operations registration and approval of applications, technical generation of certificates and hardware management cryptographic.

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

- Physical access controls.
- Protection against natural disasters.
- Protective measures against fire.
- Failure of support systems (electronic energy, telecommunications, etc.)
- Collapse of the structure.
- Flooding.
- antitheft protection.
- Output unauthorized equipment, information, media and applications relating to components used for the services of the service provider certification.

These measures are applicable to installations where the certificates are produced under the full responsibility of esFIRMA, which lends from its both mainstream and, where appropriate, operating in contingency high security installations that are properly audited periodically.

Facilities include systems preventive and corrective maintenance fee 24h-365 days a year with the assistance of notice 24 hours.

5.1.1. Location and construction of facilities

Physical protection is achieved by creating clearly defined security perimeters around services. The quality and strength of building

materials facility ensures adequate levels of protection against intrusion by brute force and located in an area of low disaster risk and allows quick access.

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

- It has redundancy in its infrastructure.
- It has several alternative sources of power and cooling in an emergency.
- Maintenance operations do not require the Centro is offline at any time.
- 99.995% reliability monthly

EsFIRMA has facilities to physically protect the provision of services approval of applications for certificates and revocation management, commitment caused by unauthorized access to systems or data access and disclosure thereof

5.1.2. physical access

The CPD where AC EsFIRMA has the TIER IV qualification ranks.

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

- It is limited to authorized personnel with identification at the time of access and registration thereof, including filming by CCTV and file.

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

- To access the rac where are located cryptographic processes required prior authorization from esFIRMA administrators hosting service that have the key to open the cage.

5.1.3. Electricity and air conditioning

EsFIRMA facilities have stabilizing machines current and a power supply system with a generator duplicate equipment.

The rooms housing IT equipment have temperature control systems with air conditioners.

5.1.4. Exposure to water

The facilities are located in an area of low risk of flooding.

Rooms where computers are housed have a moisture detection system.

5.1.5. Fire prevention and protection

The facilities and assets esFIRMA have automatic detection systems and fire fighting.

5.1.6. Storage Media

Only authorized personnel have access to the storage media.

Information highest classification level is stored in a safe outside the premises of Data Processing Center.

5.1.7. Waste treatment

Removal of media, both paper and magnetic, are performed by mechanisms that guarantee the impossibility of information retrieval.

In the case of magnetic media, it proceeds to formatting, deletion permanent, or physical destruction of the support, using specialized software to perform a minimum of 3 erasing past patterns and variable deletion.

For paper documents, paper shredders or arranged to effect later be destroyed under control.

5.1.8. Backup offsite

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

at least two persons expressly authorized to access, deposit or withdrawal of devices are required.

5.2. Controls procedures

EsFIRMA ensures that their systems operate safely, for which it has established and implemented procedures for functions that affect the provision of services.

The staff serving esFIRMA runs the administrative and management according to the security policy procedures.

5.2.1. reliable features

EsFIRMA identified, according to its security policy, the following functions or roles provided reliable:

- **Internal Auditor responsible for compliance with operating procedures. This is an external person to the Department of Information Systems. Internal Auditor tasks are incompatible in time with the certification tasks and incompatible systems. These functions will be subordinated to the head of operations, reporting to this as to the technical direction.**
- **Systems Manager: Responsible for the proper functioning of hardware and software platform support certification**
- **CA administrator: Responsible for the actions to execute cryptographic material, or performing any functions involving activation of the private keys of certificate authorities described herein, or any of its elements.**
- **CA Operator: Responsible necessary in conjunction with CA Manager custody of material activation of cryptographic keys, also responsible for backup operations and maintenance of the AC.**
- **Registration Manager: Person responsible for approving the certification requests made by the subscriber.**

- **Security Manager: Responsible for coordinating, controlling and enforcing security measures defined by esFIRMA security policies. Should be responsible for aspects related to information security: logic, physics, networking, organizational, etc.**

Persons occupying previous posts are subject to investigation procedures and specific control.

5.2.2. Number of people per task

EsFIRMA guarantees at least two people to perform tasks that are stated in the corresponding Certification Policy. Especially in handling the escrow device key Authority root and intermediate Certification.

5.2.3. Identification and authentication for each function

People assigned for each role are identified by the internal auditor will ensure that each person performs the operations for which it is assigned.

Each person only controls the assets necessary for its role, ensuring that no person access unallocated resources.

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

5.2.4. Roles requiring separation of duties

The following tasks are performed at least two people:

- Issuance and revocation of certificates, and access to the reservoir.
- Generation, transmission and destruction of certificates of the Certification.
- Production start of the Certification.

5.2.5. PKI management system

The PKI system consists of the following modules:

-component / management module Subordinate Certification Authority.

-component / management module Registration Authority.

-component / management module applications.
-component / key management module (HSM).
-component / module database.
-component / CRL management module.
-component / management module OCSP service.
- Component / management module Time Stamping Authority (TSA)

5.3. Personnel controls

5.3.1. History requirements, qualifications, experience and authorization

All personnel performing tasks classified as reliable, takes at least a year working on the production site and has fixed labor contracts.

All staff are qualified and have been duly trained to perform operations that have been assigned.

Staff in positions of trust have no personal interests that conflict with the development of the role that has been entrusted.

EsFIRMA ensures that personnel record is reliable for registration tasks.

Registration Manager has completed a course of preparation for the tasks of validation requests.

Overall, esFIRMA withdraw from their duties trust an employee when knowledge of the existence of the commission of any criminal act that could affect the performance of its functions it has.

EsFIRMA not assign a reliable site management or a person who is not suitable for the position, especially for having been convicted of a crime or misdemeanor affecting their suitability for the position. For this reason, previously an investigation is carried out, to the extent permitted by applicable law, on the following aspects:

- Studies, including alleged degree.

- Previous work up to five years, including professional references and check that the alleged work actually performed.
- Delinquencies.

5.3.2. Investigation procedures history

EsFIRMA, before hiring a person or it accesses the job, performs the following tests:

- References of work in recent years
- Profesional references
- Studies, including alleged degree.

EsFIRMA obtain the unequivocal consent of the affected to such previous research, and processes and protects all your personal data in accordance with Law 15/1999, of 13 December, Protection of Personal Data and Royal Decree 1720/2007, of 21 December, approving the Regulation implementing Law 15/1999 of 13 December on protection of personal data is approved.

The research will be repeated with sufficient frequency.

All checks are performed to the extent permitted by applicable law. The reasons that can lead to reject the candidate for a reliable post are:

- Untruths in the work request, made by the candidate.
- very negative professional or very unreliable in relation to the candidate references.

The application for the job are informed about the need to undergo a preliminary investigation being noticed that the refusal to submit to the investigation result in rejection of the application.

5.3.3. Training requirements

EsFIRMA reliable way to staff and management positions until they reach the necessary qualifications, maintaining file such training.

Training programs are updated and improved regularly.

Training includes at least the following contents:

- Principles and mechanisms security certification hierarchy and the user environment of the person to form.
- Tasks to be performed by the person.
- Policies and safety procedures EsFIRMA. Use and operation of machinery and installed applications.
- Management and processing incidents and security commitments.
- Business continuity procedures and emergency.
- Process management and security regarding the processing of personal data.

5.3.4. Frequency and requirements Retraining

EsFIRMA updated staff training according to the needs, and with sufficient frequency to perform their duties competently and satisfactorily, especially when substantial modifications are made to the certification tasks

5.3.5. Sequence and frequency of labor turnover

Not applicable.

5.3.6. Penalties for unauthorized actions

EsFIRMA has a disciplinary system to debug the responsibilities arising from unauthorized actions appropriate to the applicable labor legislation and, in particular, coordinated with the disciplinary system of the collective agreement that is applicable to staff.

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

5.3.7. Hiring professional requirements

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

In the event that all or part of the certification services are operated by a third party, controls and forecasts made in this section or in other parts of the DPC, will be applied and enforced by the third party to perform the functions of operation certification services, however, which, the certification shall be liable in any case of actual implementation. These aspects are concretized in the legal instrument used to arrange the provision of certification services by third parties other than esFIRMA.

5.3.8. Providing documentation staff

The certification service provider shall provide the documentation required strictly personal at all times in order to perform their job competently and satisfactorily.

5.4. Procedures security audit

5.4.1. Types of events recorded

EsFIRMA produces and keeps track, at least, of the following events related to the security of the entity:

- On and off the system.
- Attempts creation, deletion, setting passwords or change privileges.
- Attempts start and end of session.
- Unauthorized access attempts to the AC system via the network.
- Attempts of unauthorized access to the file system.
- Physical access to the logs.
- Configuration changes and system maintenance.
- Records of AC applications.
- On and off the application of the AC.
- Changes in the details of the AC and / or their keys.
- Changes in policy making certificates.
- Generation own keys.
- Creation and revocation of certificates.
- Destruction of records containing media keys, activation data.

- Events related to the lifecycle of cryptographic module, such as receipt, use and uninstall it.
- Activities firewalls and routers[7]
- The key generation ceremony databases and key management.
- Physical access records.
- Maintenance and system configuration changes.
- Personnel changes.
- Commitments and reports discrepancies.
- Records of destruction of material containing key information, activation data or personal subscriber information, if individual certificates, or the natural person identified in the certificate, if certificates of organization.
- Possession of activation data for operations with the private key of the Certification.
- complete physical intrusion attempts in infrastructure that support the issuance and certificate management reports.

Log entries include the following elements:

- Date and time of entry.
- Serial number or sequence input in automated registrations.
- Identity of the entity that enters the record.
- Input type.

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

5.4.2. Treatment frequency of audit records

EsFIRMA review their logs when an alert system motivated by the existence of some incident occurs.

Processing records audit includes a review of records including verification that they have not been tampered with, a brief inspection

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

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

of all log entries and further investigation of any alerts or irregularities in the logs. The actions from the audit review are documented.

EsFIRMA maintains a system which ensures:

- enough space for storing logs
- The log files are not rewritten.
- The information stored includes at least: type of event, date and time, user running the event and result of the operation.
- The log files are saved in structured can incorporate a DB files for later examination.

5.4.3. Retention period for audit logs

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

5.4.4. Protection of audit logs

The system logs:

- They are protected from manipulation, deletion or removal[9] by signing files containing them.
- They are stored in fireproof devices.
- its availability is protected through storage in external AC center where facility is located.

Access to log files is reserved only to authorized persons. Also, devices are handled at all times by authorized personnel.

An internal procedure which processes management devices containing audit log data are detailed.

5.4.5. Backup procedures

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

EsFIRMA has implemented a secure backup procedure of audit logs, making a copy of all logs weekly external media. Additionally copy is kept in custody outside center.

9 Ap 7.10.f) ETSI EN 319 401

5.4.6. Location storage system audit logs

Information audit events is collected internally and automated by the operating system, network communications and software certificate management, as well as by manually generated data to be stored by the authorized personnel. All this makes up the storage system audit logs.

5.4.7. Audit event notification to cause the event

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

5.4.8. Vulnerability scan

Vulnerability analysis is covered by audit processes EsFIRMA.

Vulnerability analysis must be performed, reviewed and revised by you through an examination of these monitored events. These analyzes must be performed daily, monthly and annually.

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

5.5. File information

EsFIRMA ensures that all information relating to the certificates is retained for an appropriate period of time as set out in section 5.5.2 of this policy.

5.5.1. Types of records archived

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

- All audit data system (PKI, TSA and OCSP).
- All data relating to certificates, including contracts with signatories and data relating to their identification and location
- Applications for issuance and revocation of certificates, including all reports relating to revocation process[10].

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

- All those specific choices that the signer or subscriber available during the subscription agreement[11].
- Type of document presented in the license application.
- Identity Registration Authority accepts the certificate request.
- Unique identification number provided by the previous document.
- All certificates issued or published.
- CRLs issued or state records generated certificates.
- History generated keys.
- Communications between the elements of the PKI.
- Policies and Practices Certification
- All audit data identified in section 5.4
- Applications for certification information.
- Documentation provided to justify applications for certification.
- Information Lifecycle certificate.

EsFIRMA is responsible for the correct file of all this material.

5.5.2. Record retention period

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

5.5.3. File protection

EsFIRMA protects the file so that only duly authorized persons can gain access to it. The file is protected viewing, modification, deletion or any other tampering by storage in a reliable system.

EsFIRMA ensures proper protection of files by assigning qualified personnel for treatment and storage boxes Fireproof security and external facilities.

5.5.4. Backup procedures

EsFIRMA has a center external storage to ensure availability of file copies of electronic files. Physical documents are stored in safe places restricted to authorized personnel only.

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

EsFIRMA backs least daily incremental backup of all your electronic documents and perform weekly full backups in case of data recovery.

In addition, esFIRMA (or organizations conducting registration function) keeps copies of paper documents in a safe place different facilities own Certification Authority.

5.5.5. Sealing requirements datetime

Records are dated with a reliable source via NTP.

EsFIRMA has a procedure describing the setting times of the equipment used in issuing certificates.
The time used to record audit log events should be synchronized with the UTC, at least once a day[12].

It is not necessary that this information is digitally signed.

5.5.6. File system location

EsFIRMA has a centralized system of information gathering activity of the teams involved in the service certificate management.

5.5.7. Procedures for obtaining and verifying information file

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

5.6. Key Renewal

Prior to using the private key of the CA expires, it will be made a change key. The former AC and its private key is used only for signing CRLs while there are active certificates issued by this AC. a new AC with a new private key and a new DN is generated.

The rekeying subscriber is performed by performing a reissue process.

5.7. Key commitment and disaster recovery

5.7.1. Incident management procedures and commitments

12 Ap 7.10.d) ETSI EN 319 401

They are stored backups of the following information on facilities external storage esFIRMA, which are made available in the event of compromise or disaster: technical data request certificates, audit data and records database of all certificates issued .

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

5.7.2. Corruption resources, applications or data

When an event happens corruption resources, applications or data, the incidence will communicate safety and appropriate management procedures, which provide scaling, investigation and response to the incident will begin. If necessary, the procedures engagement key or esFIRMA disaster recovery will begin.

5.7.3. Commitment of the private key of the entity

In case of suspicion or knowledge of the commitment esFIRMA, procedures engagement key, led by a response team to assess the situation, develop an action plan, to be implemented under the approval of the management of the entity they will be activated certification.

Where compromise of the private key of esFIRMA may be the case that the states of certificates and revocation processes using this key might not be valid[13].

EsFIRMA has developed a contingency plan to recover critical systems, if necessary in alternate data center.

For the root key commitment should be taken as a separate case in the process of contingency and business continuity. This issue affects, in case of replacement of the keys to different applications and awards for private and public services. A recovery of the effectiveness of the keys in terms of business will mainly depend on the duration of these processes. The document contingency and business continuity treat

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

purely operational terms so that new keys are available, not its recognition by third parties.

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

5.7.4. Business continuity after a disaster

EsFIRMA restore critical services (suspension and revocation, and publishing certificate status information) in accordance with the contingency plan and continuity of existing business restoring normal operation of the above services in the following disaster 24 hours.

EsFIRMA has an alternative center if necessary for the operation of certification schemes described in business continuity planning.

5.7.5. Revocation management

Both management service revocations as consultation service are considered critical services and thus contained in the Plan contingency and business continuity planning of esFIRMA

5.8. Termination of service

EsFIRMA ensures that potential disruptions to subscribers and third parties are minimal as a result of the cessation of services of the service provider certification and, in particular, ensure continued maintenance of records required to provide evidence of certification in case of civil research or criminal, by transfer to a notarial deposit.

Before finishing services, esFIRMA develops a plan termination, with the following provisions:

- It will provide the necessary funds (liability insurance) to continue the completion of activities revocation.
- It shall inform the Ministry of Industry, Energy and Tourism, with a minimum of 2 months, the cessation of its activity and the fate of certificates specifying whether management is transferred and to whom, or if their application is extinguished.

- It shall also the Ministry of Industry, Energy and Tourism, the opening of insolvency proceedings any action taken against esFIRMA and any other relevant circumstances that may prevent the continuation of the activity.
- inform all Signatories / Subscribers, relying party and other AC's with which it has agreements or other cessation relationship with a minimum of 6 months.
- It will revoke any authorization to outsourced entities to act on behalf of the AC in the process of issuing certificates.
- It will transfer its obligations regarding the maintenance of registration information and logs for the period of time given to subscribers and users in order to serve as evidence in legal proceedings and to ensure continuity of service.
- It will destroy or disable for use private CA key.
- certificates of Time Stamping Units (TSU) will be revoked
- Remain active certificates and revocation verification system and to the extinction of all certificates issued.
- It will execute the tasks necessary to transfer the obligations to maintain registration information and event log files during the respective time periods indicated to the subscriber and third parties who trust certificates.

6. Technical security controls

6.1. Generation and installation of key pair

6.1.1. Key pair generation

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

Activities during the key generation ceremony are recorded, dated and signed by all individuals involved in it, with the presence of a CISA Auditor. Such records are guarded for auditing and monitoring for an appropriate period determined by esFIRMA.

For the generation of the key entities root and intermediate certification devices certifications Common Criteria EAL 4+ and FIPS 140-2 Level 3 are used.

ROOT	4,096 bits	25 years
INTERMEDIATE	4,096 bits	13 years
- End entity certificates	2,048 bits	2 years

More information in the following locations PDS:

Public employee - ALTO 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 - MEDIUM 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/
Seal-e AAPP - HALF 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/
Seal-e AAPP - HALF 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/
Username EP - ALTO 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/
EP Login - AVERAGE 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/

EV Electronic Office MEDIUM 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/

6.1.1.1. Key pair generation signer

Signer Keys can be created for himself by hardware devices or software authorized by esFIRMA.

EsFIRMA can create keys only by a DCCF.

EsFIRMA never generates keys in software to be sent to the signer.

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

6.1.2. Sending the signer's private key

Certificates Secure signature creation device private key is properly protected inside of the safe device.

Software certificate private key of the signer is created in the computer system using this signer when you make the certificate request, so that the private key is properly protected inside the computer system of the signatory.

6.1.3. Sending the public key to certificate issuer

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

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

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

6.1.4. Distribution of public key certification service provider

EsFIRMA keys are communicated to third parties who rely on certificates, ensuring the integrity of the key and authenticating their origin, through publication in the tank.

Users can access the repository for public keys, and additionally, in applications S / MIME, the data message may contain a certificate chain, which thus is distributed to users.

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

6.1.5. Key sizes

The length of the keys of the Root Certification Authority is 4096 bits.
The length of the keys to subordinate Certification Entity is 4096 bits.
The length of the keys to the TSA is 4096 bits.
Keys end-entity certificates are 2048 bits.

6.1.6. Generation of public key parameters

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

6.1.7. Quality Check public key parameters

- Module Length = 4096
- key generation algorithm: rsagen1
- Cryptographic Functions Summary: SHA256.

6.1.8. Key generation in software or in equipment

All keys are generated in equipment, according to what indicated in section 6.1.1.

6.1.9. Key Usage Purposes

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

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

6.2. Protection of the private key

6.2.1. Standards cryptographic modules

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

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

a multi-person for the activation of the private key of the AC control is required. In the case of the CPD, in particular there is a policy of 3 to 5 people for activation key.

Cryptographic devices are protected physically as determined herein.

6.2.3. Private key deposit

EsFIRMA does not store copies of private keys of the signatories.

6.2.4. Back up the private key

EsFIRMA performs backup copy of the CA private keys that make recovery possible disaster, loss or deterioration thereof. Both generation copy recovery as it takes at least two people participation.

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

Signer Keys in hardware can not be copied because they can not leave the cryptographic device.

6.2.5. Private key file

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

The subscriber can store keys in software delivered during the period of the certificate. Then you must destroy them before they sure have no information encrypted with the public key.

Only if encryption certificates, the subscriber can store the private key long as they need. In this case esFIRMA also keep a copy of the private key associated with the certificate encryption.

6.2.6. Entering the private key in the cryptographic module

Private keys are generated directly in the cryptographic modules esFIRMA production.

6.2.7. Method of activating private key

Private keys of the Certification are stored encrypted cryptographic modules esFIRMA production.

6.2.8. Method of deactivating private key

EsFIRMA private key is activated by running the corresponding procedure safe start of the cryptographic module, for the persons listed in section 6.2.2.

The CA key is activated by a process of m n.

Activation of private keys Intermediate AC is managed with the same process n m of the CA key.

6.2.9. Method of destroying private key

For deactivating private key esFIRMA will follow the steps outlined in the corresponding crypto Administrator Manual.

Meanwhile the signer must enter the PIN for the new activation.

6.2.10. Classification of cryptographic modules

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

They are physically destroyed or reset to low level devices that have stored anywhere esFIRMA private keys. For removal will follow the steps in the administrator's cryptographic equipment manual.

Eventually they are destroyed safely backups.

Signer Keys software may be destroyed by deleting them, following the instructions on the application that houses them.

Signer Keys in hardware may be destroyed by a special computer application at the offices of RA or esFIRMA.

6.3. Other aspects of key pair management

6.3.1. The public key file

EsFIRMA filed their public keys routinely, according to the provisions in section 5.5 of this document.

6.3.2. Periods of use of public and private keys

Periods of use of the keys are determined by the duration of the certificate, after which they can not continue to be used.

As an exception, the private decryption key can continue being used even after the expiry of the certificate.

6.4. Activation data

6.4.1. Generation and installation of activation data

Activation data devices that protect esFIRMA private keys are generated in accordance with the provisions of section 6.2.2 and key procedures ceremony.

The creation and distribution of such devices is recorded.

It also generates safely esFIRMA activation data.

6.4.2. Activation Data Protection

Activation data devices that protect private keys Authorities root and subordinate certification are protected by cards holders administrators of cryptographic modules, as stated in the document key ceremony.

The signer of the certificate is responsible for protecting your private key with password as complete as possible. The signer must remember the password.

6.5. Computer security controls

EsFIRMA uses reliable systems to provide its certification services. EsFIRMA has made computer controls and to establish their proper management with the level of security required in the management of electronic certification systems audit IT assets.

The used equipment is initially configured with the appropriate security profiles by staff EsFIRMA systems in the following aspects:

- Security settings of the operating system.
- Configuring application security.
- correct sizing of the system.
- Users and permissions settings.
- Configuration Event Log.
- Backup and recovery plan.
- antivirus settings.
- Network traffic requirements.

6.5.1. Specific computer security technical requirements

Each server EsFIRMA includes the following features:

- Access control services SubCA and privilege management.
- Imposition of separation of duties for managing privileges.
- Identification and authentication of roles associated with identities.
- Subscriber history file and SubCA and audit data.
- Audit events related to security.
- Self-diagnosis of safety related services SubCA.
- Key recovery mechanisms and SubCA system.

The exposed functionality are performed by a combination of operating system, PKI software, physical protection and procedures.

In case esFIRMA distribute qualified signature creation devices, verify at all times that these devices remain certified as DCCF[15].

Verification DCCF certification is done throughout the period of validity of the certificate[16]. If the DCCF lost its certification as such, esFIRMA notify users of this fact and implement a plan for renewal of these devices as outlined in the internal document esFIRMA General Procedures (esFIRMA_ProcedimientosGenerales_v1r0.pdf)

6.5.2. Assessing the level of security

Applications Certification Authority registration and employed by esFIRMA are reliable.

6.6. Technical controls lifecycle

6.6.1. System development controls

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

Applications have methods for verifying the integrity and authenticity, as well as correcting the version to use.

6.6.2. Security management controls

EsFIRMA develops the precise activities for training and employee awareness of security. The materials used for training and documents describing the processes are updated after approval by a group for safety management. In performing this function it has an annual training plan.

EsFIRMA required by contract security measures equivalent to any outside vendor involved in the certification tasks.

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

6.6.2.1. Classification and management of information and goods
EsFIRMA maintains an inventory of assets and documentation and process for managing this material to ensure its use.

The esFIRMA security policy detailing procedures where management information is classified according to their level of confidentiality.

The documents are classified into three levels: UNCLASSIFIED, CONFIDENTIAL internal use.

6.6.2.2. Management operations
EsFIRMA has a suitable process management and incident response, by implementing an alert system and generating periodic reports.

In the security document esFIRMA develops in detail the process of incident management.

EsFIRMA has documented the whole process on the roles and responsibilities of personnel involved in the control and manipulation of elements contained in the certification process.

6.6.2.3. Treatment and safety brackets

All supports are treated safely in accordance with the requirements of the classification of information. Media containing sensitive data are destroyed safely if they will not again be required.

System Planning
The esFIRMA Systems department keeps track of the capabilities of the equipment. Together with the application resource control each system can provide a possible downsizing.

Reports of incidents and response
EsFIRMA has a procedure for issue tracking and resolution where answers and an economic evaluation which involves the resolution of the incident are recorded.

Operational procedures and responsibilities
EsFIRMA defined activities assigned to individuals with a role of trust, other than those responsible for performing daily operations that do not have character of confidentiality.

6.6.2.4. Access Management System
EsFIRMA makes all efforts that are reasonably available to confirm that the system access is limited to authorized persons.

In particular:

AC General
- It is available based firewalls, antivirus and IDS high availability controls.
- Sensitive data are protected by cryptographic techniques or access controls with strong identification.
- EsFIRMA has a documented procedure for managing high and low users and policy outlined in its security policy access.
- EsFIRMA has procedures to ensure that operations are conducted in compliance policy roles.
- Everyone has a role to perform associated operations certification.
- EsFIRMA staff is responsible for his actions by the confidentiality agreement signed with the company.

Certificate generation
Authentication for the emission process is performed by a system of n m operators for activating the private key esFIRMA.

Revocation management
The revocation will be made by stronger application of an authorized administrator authentication. Systems generate test logs that guarantee non-repudiation of the action taken by the administrator esFIRMA.

Revocation status

State application revocation offers access control based on authentication certificates or dual factor identification to avoid the attempt to change the status information of the revocation.

6.6.2.5. Lifecycle management of cryptographic hardware
EsFIRMA ensures that the cryptographic hardware used for signing certificates is not handled during transport by inspecting the delivered material.

The cryptographic hardware moves onto prepared supports to avoid any manipulation.

EsFIRMA records all relevant device information to add to the catalog of assets.

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

EsFIRMA test performs periodic tests to ensure proper operation of the device.

The cryptographic hardware device is manipulated only by reliable personnel.
Private esFIRMA signing key stored in the cryptographic hardware will be removed once the device is removed.

The system configuration esFIRMA and modifications and updates are documented and controlled.

EsFIRMA has a maintenance contract device. Changes or updates are authorized by the security officer and are reflected in the minutes of corresponding work. These settings are made at least two reliable people.

6.7. Network security controls

EsFIRMA protects the physical access to network management devices, and has an architecture that directs traffic generated based on its safety features, creating clearly defined network sections. This division is performed by using firewalls.

Confidential information is transferred by unsecure networks, is performed through encrypted using SSL protocols or VPN authentication system with double factor.

6.8. Engineering controls Cryptographic Module

Cryptographic modules are subjected to engineering controls under the standards indicated throughout this section.

The key generation algorithms used are commonly accepted to use the key to which they are intended.

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

6.9. Time sources

EsFIRMA has a procedure coordinated timing synchronization via NTP.

7. Profiles of certificates and CRLs

7.1. Certificate profile

All qualified certificates issued under this policy meet the standard X.509 version 3, RFC 3739 and ETSI 101 862 "Qualified Certificate Profile".

7.1.1. Version number

EsFIRMA X.509 Version 3 certificates issued

7.1.2. Certificate extensions

Extensions certificates are detailed in documents profiles that are accessible from the website of esFIRMA https://www.esfirma.com

Thus it is allowed to maintain more stable versions of the CPD and detach them from frequent adjustments profiles.

7.1.3. Object Identifiers (OID) algorithms

The object identifier of the signature algorithm is:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption

The object identifier of the public key algorithm is:

- 1.2.840.113549.1.1.1 rsaEncryption

7.1.4. Name format

Certificates must contain the information which are necessary for use as determined by the appropriate policy.

7.1.5. Restriction names

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

7.1.6. Object identifier (OID) of the types of certificates

All certificates include an identifier certificate policy under which they were issued, according to the structure defined in section 1.2.1

7.2. Profile of certificate revocation list

7.2.1. Version number

CRLs are issued by esFIRMA version 2.

7.2.2. OCSP profile

According to the IETF RFC 6960 standard

8. Compliance audit

EsFIRMA announced the beginning of its activity as a service provider certification by the Ministry of Industry and is subject to control checks that the agency deems necessary.

8.1. Frequency of compliance audit

EsFIRMA conducts a compliance audit annually, plus internal audits carried out at its own discretion or at any time because of a suspected breach of any security measure.

8.2. Identification and qualification of auditor

The audits are conducted by an external independent audit firm demonstrating technical competence and experience in computer security, security of information systems and compliance audits certification service public key, and related items.

8.3. Auditor relationship with the audited entity

Audit firms are renowned specialized departments in conducting IT audits, so there is no conflict of interest that may undermine its performance in relation to esFIRMA.

8.4. List of items audited

Audit verifies about esFIRMA:

a) The entity has a management system which ensures the quality of the service.
b) The entity meets the requirements of the CPD and other documentation related to the issuance of the various digital certificates.
c) The DPC and other related legal documentation, complies with esFIRMA agreed and set out in the regulations.
d) The entity manages properly its information systems

In particular, the elements audited are:

a) Processes AC, ARs and related elements.
b) Information systems.
c) Protection data processing center.
d) Documents.

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

Once received by the direction the report of the compliance audit conducted, analyzed, with the firm that has carried out the audit found shortcomings and develops and implements a corrective plan which overcomes these deficiencies.

If the esFIRMA is unable to develop and / or implement the plan or if the deficiencies pose an immediate threat to the security or integrity of the system, shall immediately notify the senior management of esFIRMA you can perform the following actions:

- Cease operations temporarily.
- Revoke the CA key infrastructure and regenerate.
- Terminate the service of AC.
- Other complementary actions needed.

8.6. Treatment of audit reports

Reports audit results are delivered to senior management of esFIRMA within a maximum period of 15 days following the execution of the audit.

9. commercial and legal requirements

9.1. rates

9.1.1. Rate of issue and renewal of certificates

EsFIRMA can establish a fee for the issuance or renewal of licenses, which, where appropriate, to subscribers shall be informed.

9.1.2. Access fee certificates

EsFIRMA has not established a fee for access to certificates.

9.1.3. Access fee certificate status information

EsFIRMA has not established a fee for access to certificate status information.

9.1.4. Rates for services

No stipulation.

9.1.5. Refund Policy

No stipulation.

9.2. Financial capability

EsFIRMA have sufficient financial resources to maintain its operations and meet its obligations and to address the risk of liability for damages, as stated in ETSI EN 319 401-1 7.12 c) in relation to the management the termination of services and cessation plan.

9.2.1. Insurance Coverage

EsFIRMA has a guarantee sufficient cover for its civil liability through insurance professional liability that meets indicated in the regime of obligations and responsibilities of Regulation (EU) 910/2014, with a guaranteed minimum of 3,000,000 euros.

9.2.2. Other assets

No stipulation.

9.2.3. Insurance coverage for subscribers and others who rely on certificates

EsFIRMA has a guarantee sufficient cover for its civil liability through insurance professional liability that meets indicated in the regime of obligations and responsibilities of Regulation (EU) 910/2014, with a guaranteed minimum of 3,000,000 euros.

9.3. confidentiality

9.3.1. confidential information

The following information is kept confidential by esFIRMA:

- Applications for licenses, approved or denied, and any other personal information obtained for the issuance and maintenance of certificates, except the information listed in the following section.
- Private keys generated and / or stored by the provider of certification services.
- Transaction logs, including full records and audit trails of transactions.
- Records of internal and external audit, created and / or maintained by the Certification and its auditors.

- Business continuity plans and emergency.
- Political and security plans.
- Documentation remaining operations and operation plans, such as file, monitoring and the like.
- All other information identified as "Confidential".

9.3.2. no confidential information

The following information is considered non-confidential:

- Certificates issued or pending issue.
- Subscriber linking to a certificate issued by the Certification Authority.
- The first and last name of the individual identified in the certificate, and any other circumstance or personal data of the holder, in the event that is significant depending on the purpose of the certificate.
- The email address of the individual identified in the certificate, or the email address assigned by the subscriber, in the event that is significant depending on the purpose of the certificate.
- Uses and economic limits outlined in the certificate.
- The period of validity of the certificate and the date of issue of the certificate and the expiration date.
- The serial number of the certificate.
- Different states or conditions of the certificate and the date of commencement of each, specifically: pending generation and / or delivery, valid, revoked, suspended or expired and the reason that caused the status change.
- The certificate revocation lists (LRCs) as well as the remaining revocation status information.
- The information contained in deposits certificates.
- Any other information that is not indicated in the previous section.

9.3.3. Information Disclosure suspension and revocation

See above section.

9.3.4. Legal Disclosure

EsFIRMA disclose confidential information only in cases provided by law.

Specifically, records that support the reliability of the data contained in the certificate and records relating to the reliability of data and related operational[17]They will be disclosed if required to provide evidence of certification in legal proceedings even without the consent of the certificate subscriber.

EsFIRMA indicate the circumstances in the privacy policy under Section 9.4.

9.3.5. Information Disclosure request of the holder

EsFIRMA included in the privacy policy under Section 9.4, requirements to permit the disclosure of subscriber information and, where appropriate, the individual identified in the certificate directly to them or to others.

9.3.6. Other information disclosure circumstances

No stipulation.

9.4. Personal data protection

EsFIRMA undertakes to comply with the regulations on protection of personal data, with appropriate security measures as listed in Organic Law 15/1999 on Protection of Personal Data, and Royal Decree 1720/2007 of development of that Law.

EsFIRMA obtains personal data in files for data capture by the subscriber, who must have obtained them legally pertoque who, as provided in the regulations on electronic signature and protection of personal data.

EsFIRMA has the status of the processor while not decide on the purpose, content and use of treatment of such personal data, while the SUBSCRIBER is responsible for the file.

17 Paragraph 7.10.c) ETSI EN 319 401

EsFIRMA use the data contained in their files, solely for the purposes set out in this Certification Practice Statement.

Also esFIRMA has developed a privacy policy, according to the Organic Law 15/1999, of 13 December, Protection of Personal Data, and documented in this Certification Practice Statement aspects and safety procedures the security document in compliance with the regime of obligations and responsibilities of Regulation (EU) 910/2014 and articles 82 and 88 of Royal Decree Royal Decree 1720/2007 of 21 December,which the regulation implementing the Organic Law 15/1999 of 13 December 1999 on the protection of personal data is approved. This Certification Practice Statement has therefore considering security document.

EsFIRMA not disclose nor gives personal information, except as provided in sections 9.3.2 to 9.3.6 of, and section 5.8, on termination of the certification service.

Confidential information in accordance with the regulations on protection of personal data is protected from loss, destruction, damage, forgery and illegal or unauthorized processing in accordance with the requirements set forth herein, compliance with the obligations established by Royal Decree 1720/2007 of 21 December, by which the Regulation implementing Law 15/1999, of 13 December 1999 on the protection of personal data is approved.

9.5. Intellectual Property Rights

9.5.1. Property of certificates and revocation information

Only esFIRMA enjoys intellectual property rights on certificates issued, without prejudice to the rights of subscribers, holders of keys and others, which grant non-exclusive license to reproduce and distribute certificates, free of charge, as long as the reproduction is full and does not alter any element of the certificate, and is necessary in relation to digital signatures and / or encryption systems within the scope of use of the certificate, and according to the documentation that links them.

In addition, the certificates issued by esFIRMA contain a legal notice concerning the ownership thereof.

The same rules are applicable to the use of the information of certificate revocation.

9.5.2. Property Certification Practice Statement

EsFIRMA only enjoys intellectual property rights on this Certification Practice Statement.

9.5.3. Proprietary information on names

Subscriber and, where appropriate, the individual identified in the certificate, retains all rights to exist thereof on the brand, product or trade name contained in the certificate.

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

9.5.4. Key Property

Key pairs are owned by the signatories of certificates.

When a key is broken up into parts, all parts of the key are the property owner of the key.

9.6. Obligations and Liability

9.6.1. Obligations of the Certification "esFIRMA"

EsFIRMA guarantees under its full responsibility, which meets all the requirements of DPC, are solely responsible for compliance with the procedures, even if part or all of the operations are outsourced externally.

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

Prior to the issuance and delivery of the certificate to the subscriber, esFIRMA informs the subscriber of the terms and conditions for the use

of the certificate, its price and its limitations of use by a subscriber agreement incorporates by reference the factual texts (PDS) of each of the acquired licenses.

The text document disclosure, also called PDS[18]Meets the content of Annex A of ETSI EN 319 411-1 v1.1.1 (2016-02) document which can be transmitted electronically using a durable means of communication in time and in understandable language.
EsFIRMA communicates permanently changes[19] that occur in its obligations by publishing new versions of its legal documents on its Web https://www.esfirma.com

EsFIRMA links subscribers, key holders and relying parties certified by the text of disclosure or PDS, written and understandable language, with the following minimum content:

- Requirements to comply with the provisions in sections Error: not the source of reference, 4.5.3, 9.2, 9.6.7, 9.6.8, 9.6.9 and 9.6.10 was found.
- Indication of the applicable policy, indicating that certificates are not issued to the public.
- Statement that the information in the certificate is correct, unless otherwise notified by the subscriber.
- Consent to the publication of the deposit certificate and third party access to it.
- Consent for storing information used for subscriber registration and for the transfer of such information to others, upon termination of operations without the Certification Revocation valid certificates.
- Certificate usage limits, including those set out in section 1.4.2
- Information on how to validate a certificate, including the requirement to check the status of the certificate, and the conditions under which it can reasonably rely on the

18 "PKI Disclosure Statement", or PKI disclosure statement applicable.
19 Ap 6.2.3.b) ETSI EN 319 411-1

certificate, which applies when the subscriber acts as a third party that trusts the certificate.

- How the liability of the Certification is guaranteed.
- Limitations of liability, including the uses for which the Certification accept or exclude its liability.
- Period information file license applications.
- Period audit log file.
- applicable dispute resolution procedures.
- Applicable law and jurisdiction.
- If the Certification has been declared in conformity with the certification policy and, where appropriate, according to which system.

9.6.2. Guarantees offered to subscribers and relying parties certificates

EsFIRMA in the documentation that links with subscribers and relying parties certificates, established and rejects guarantees, and limitations of liability.

EsFIRMA at least guarantees the subscriber:

- No factual errors in the information contained in the certificates, known or made by the Certification Body.
- No factual errors in the information contained in the certificates, due to lack of due diligence in the management of the license application or creating it.
- Certificates meet all material requirements of the Certification Practice Statement.
- That revocation services and use of the Deposit meet all material requirements of the Certification Practice Statement.

EsFIRMA at least ensure the third party that trusts the certificate:

- That the information contained or incorporated by reference in the certificate is accurate, unless otherwise indicated.
- If published in deposit certificates, the certificate has been issued to the subscriber identified herein and that the certificate has been accepted in accordance with section 4.4

- In the approval of the certificate application and issuance of the certificate they have been met all material requirements of the Certification Practice Statement.
- The speed and security in the provision of services, especially services revocation and deposit.

Additionally, esFIRMA guarantees the subscriber and relying party certificate:

- The certificate contains the information which must contain a certificate skilled, in accordance with Annex 1 of Regulation (EU) 910/2014.
- That in the case of private keys generated by the subscriber or, where appropriate, physical person identified in the certificate, confidentiality is maintained throughout the process.
- Responsibility for the Certification, within the limits established.

9.6.3. Rejection of other guarantees

EsFIRMA disclaims all other warranties not legally required, except those referred to in section 9.6.2.

9.6.4. Limitation of Liability

EsFIRMA limits its liability according to that established the system of obligations and responsibilities of Regulation (EU) 910/2014.

9.6.5. Indemnity clauses

9.6.5.1. Indemnification Subscriber

EsFIRMA included in the contract with the subscriber, a clause whereby the subscriber agrees to indemnify the Certification of any damage from any acts or omissions resulting in liability, damages or losses, expenses of any kind, including judicial and legal representation that may be incurred by the publication and use of the certificate, when any of the following causes:

- False or misleading statement made by the user of the certificate.

- User Error certificate to provide details of the application, if the act or omission brokered fraud or negligence regarding the Certification or anyone who trusts the certificate.
- Negligence in protecting the private key, the use of a reliable system or maintaining the necessary precautions to prevent the compromise, loss, disclosure, modification or unauthorized use of that key.
- Employment by the subscriber of a name (including common names, email address and names domain), Or other information in the certificate that infringes intellectual property of others.

9.6.5.2. Indemnification of third party trusts the certificate

EsFIRMA included in the text of disclosure or PDS, a clause by which the relying party certificate agrees to indemnify the Certification of any damage from any acts or omissions resulting in liability, damage or loss, expenses of any kind, including court and legal representation that may be incurred by the publication and use of the certificate, when any of the following causes:

- Breach of the obligations of the third party trusts the certificate.
- reckless confidence in a certificate, under the circumstances.
- Failure to check the status of a certificate, to determine which is not suspended or revoked.

9.6.6. fortuitous event and force majeure

EsFIRMA included in the text or PDS disclosure clauses that limit their liability in unforeseeable circumstances and force majeure.

9.6.7. applicable law

EsFIRMA states in the subscriber agreement and the text of disclosure or PDS, as that applicable to the provision of services, including law policy and certification practice, is the Spanish Law.

9.6.8. Severability clauses, survival, entire agreement and notification

EsFIRMA states in the subscriber agreement, and the text of disclosure or PDS, severability clauses, survival, entire agreement and notification:

- Under the severability clause, the invalidity of a clause does not affect the rest of the contract.
- Under clause survival, certain rules remain in force after the completion of the regulatory service legal relationship between the parties. To this end, the Bank Sailing Certification that at least the requirements contained in Sections 9.6.1 (Obligations and responsibility), 8 (Compliance Audit) and 9.3 (Confidentiality), remains in force after termination of service and conditions emission / use.
- Under the entire agreement clause it means that the regulatory legal service document contains the full will and all agreements between the parties.
- Under clause notification procedure by which the parties mutually reported facts be established.

9.6.9. Jurisdiction clause

EsFIRMA states in the subscriber agreement and the text of disclosure or PDS, a provision of competent jurisdiction, indicating that international jurisdiction is for the Spanish judges.

Territorial and functional jurisdiction shall be determined under the rules of private international law and procedural law rules that may apply.

9.6.10. Conflict resolution

EsFIRMA states in the subscriber agreement, and the text of disclosure or PDS, mediation procedures and conflict resolution applicable.