Disclosure Text (PDS) of the certificates issued for Public Administrations

Index

INFORMATIVE TEXT - PDS

This document contains the essential information to know in relation to the certification service of the Certification Entity ESFIRMA.

This document follows the structure defined in Annex A of the ETSI EN 319 411-1 standard, in accordance with the indications of section 4.3.4 of the ETSI EN 319 412-5 standard.

1.1. Documentary control

Security classification	PUBLIC
Version	2.2

1.2. Version control

Version	Changes	Description	Author	Date
1.0	Original	Document creation	esFIRMA	04/28/2016
1.4		Submissions/Corrections	esFIRMA	07/06/2017
1.5		Change of name and reference to regulations	esFIRMA	06/11/2017
2.0		Inclusion of all certificates related to Spanish public administrations	esFIRMA	03/06/2020
2.1		Review of Law 6/2020	esFIRMA	08/04/2021

2.2	(1.3)	Reference to esFIRMA's website is added.	esFIRMA	21/04/2023

2. Information

2.1. Responsible organization

The Certification Authority ESFIRMA, hereinafter "ESFIRMA", is an initiative of:

ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (ESFIRMA)
CALLE BARI 39 (BINARY BUILDING EDIF.)
50197 - ZARAGOZA
(+34) 976300110

2.2. Contact

For any inquiries, please contact:

ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (ESFIRMA)
CALLE BARI 39 (BINARY BUILDING EDIF.)
50197 - ZARAGOZA
(+34) 976300110

2.3. Contact for revocation processes

The process to request the revocation of a certificate can be found at www.esfirma.com. For any other inquiries on this matter, please contact:

ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (ESFIRMA)
CALLE BARI 39 (BINARY BUILDING EDIF.)
50197 - ZARAGOZA
(+34) 976300110

3. Type and purpose of the certificate

3.1. Qualified public employee certificates

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

These certificates allow the identification of their holders as personnel serving the Public Administration, linking them to it, following the requirements established in article 43 of Law 40/2015, of October 1, on the Legal Regime of the Public Sector, for the electronic signature of personnel serving Public Administrations.

3.2. Certificates of public employee with pseudonym

These certificates allow their holders to be identified as personnel serving the Public Administration, linking them to it, as allowed by Article 43.2 of Law 40/2015, of October 1, on the Legal Regime of the Public Sector, for the electronic signature of personnel serving the Public Administrations, personnel who, for reasons of public security, will only be identified with the professional identification number or another public employee pseudonym, as indicated in Annex I, section c) of Regulation (EU) 910/2014 of the European Parliament and of the Council, of July 23, 2014, and Article 6.1.a) of Law 6/2020, of November 11, regulating certain aspects of electronic trust services.

3.3. Certificates in card

The certificates that use a card work with a qualified electronic signature creation device, in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and the Council, dated July 23, 2014.

3.4. Certificates in the cloud

These certificates are managed in a centralized way.

3.5. Certificates for authentication

Certificates with the identification function guarantee the identity of the subscriber and the signer.

3.6. Certificates for Signature advanced

Certificates with the signature function allow the generation of the "advanced electronic signature" which is based on a qualified certificate without the joint participation of a qualified signature creation device.

3.7. Certificates for qualified signature

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

3.8. Qualified electronic seal certificates

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

These certificates allow their holders to be identified as Public Administrations, following the requirements established in article 40 of Law 40/2015, of October 1, on the Legal Regime of the Public Sector, which will include the tax identification number and the corresponding denomination, as well as, if applicable, the identity of the holder in the case of electronic seals of administrative bodies.

3.9. Seal certificates advanced

Certificates with the signature function allow the generation of the "advanced electronic seal" based on a qualified certificate without the joint participation of a qualified signature creation device.

3.10. Types of certificates

Certificate	Support	Profile	OIDs
High-level public employee, for signature	Card	Signature	• 1.3.6.1.4.1.47281.1.1.1 • 0.4.0.194112.1.2 • 2.16.724.1.3.5.7.1
Public employee middle level, for signature	Centralized HSM	Signature	• 1.3.6.1.4.1.47281.1.1.4 • 0.4.0.194112.1.0 • 2.16.724.1.3.5.7.2
High-level public employee, for authentication	*Card*	*Autent*	• *1.3.6.1.4.1.47281.1.1.5* • *0.4.0.2042.1.2* • *2.16.724.1.3.5.7.1*

Certificate	Support	Profile	OIDs
Public employee with high-level pseudonym, for signature	Card	Signature	• 1.3.6.1.4.1.47281.1.3.1 • 0.4.0.194112.1.2 • 2.16.724.1.3.5.4.1

Public employee with medium level pseudonym, for signature	Centralized HSM	Signature	• 1.3.6.1.4.1.47281.1.3.4 • 0.4.0.194112.1.0 • 2.16.724.1.3.5.4.2
Public employee with high-level pseudonym, for authentication	*Card*	*Autent*	• *1.3.6.1.4.1.47281.1.3.5* • *0.4.0.2042.1.2* • *2.16.724.1.3.5.4.1*

Certificate	**Support**	**Profile**	**OIDs**
Electronic seal, Medium level	Software	Signature	• 1.3.6.1.4.1.47281.1.2.2 • 0.4.0.194112.1.2 • 2.16.724.1.3.5.6.2
Electronic seal, medium level, centralized	Centralized HSM	Signature	• 1.3.6.1.4.1.47281.1.2.4 • 0.4.0.194112.1.2 • 2.16.724.1.3.5.6.2

3.11. Issuing Certification Authority

These certificates are issued by ESFIRMA, identified by the data indicated above.

3.12. Validation of the certificates

The lists of revoked certificates and OCSP services can be found on the esFIRMA website and at the URLs indicated in each of the certificates.

4. Certificate usage limits

4.1. Usage limits aimed at signatories

The signer and the seal creator must use the certification service provided by esFIRMA exclusively for the authorized uses in the contract signed between esFIRMA and the SUBSCRIBER, which are reproduced subsequently.

Likewise, the signer and the seal creator are obliged to use the digital certification service in accordance with the instructions, manuals, or procedures provided by esFIRMA.

The signer and the seal creator must comply with any law and regulation that may affect their right to use the cryptographic tools they employ.

The signer and the seal creator cannot adopt inspection, alteration, or reverse engineering measures of esFIRMA's digital certification services, without prior express permission.

4.2. Usage limits aimed at verifiers

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

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

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

The certificates have not been designed, cannot be used for and are not authorized for use or resale as equipment for controlling dangerous situations or for uses that require fail-safe performance, such as the operation of nuclear facilities, air navigation or communication

systems, or weapon control systems, where a failure could directly result in death, personal injury, or severe environmental damage.

The limits indicated in the various fields of the certificate profiles must be taken into account, visible on the ESFIRMA website.

The use of digital certificates in operations that contravene this disclosure text (PDS), or the contracts with subscribers, is considered improper use for the appropriate legal purposes, thus exempting ESFIRMA, according to current legislation, from any responsibility for this improper use of the certificates carried out by the signer or any third party.

The provider esFIRMA does not have access to the data on which the use of a certificate can be applied. Therefore, and as a consequence of this technical impossibility to access the content of the message, it is not possible for esFIRMA to issue any assessment on said content, thus assuming the subscriber, the signer, or the creator of seals, any responsibility arising from the content associated with the use of a certificate.

Likewise, the subscriber will be liable for any responsibility that may arise from the use of it outside the limits and conditions of use set forth in this disclosure text, or in the contracts with the subscribers, as well as for any other improper use of it derived from this section or that may be interpreted as such according to current legislation.

5. Obligations of the subscribers

5.1. Key generation

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

In cloud certificates, the subscriber authorizes the signer to generate their private and public keys, and requests, on behalf of the signer, the issuance of the certificate to esFIRMA.

In electronic seal certificates, the subscriber authorizes esFIRMA to generate private and public keys for use by seal creators and requests the issuance of the electronic seal certificate on their behalf.

5.2. Certificate request

The subscriber undertakes to make requests, when necessary, for these certificates in accordance with the procedure and, if necessary, the technical components supplied by ESFIRMA, in accordance with what is established in the certification practice statement (CPS) and in the ESFIRMA operations documentation.

5.3. Truthfulness of the information

The subscriber is responsible for ensuring that all information included in their certificate request is accurate, complete for the purpose of the certificate, and up-to-date at all times.

The subscriber must immediately inform ESFIRMA:

- Of any inaccuracy detected in the certificate once it has been issued.
- Of the changes that occur in the information provided and/or registered for the issuance of the certificate.

5.4. Custody obligations

The subscriber undertakes to safeguard all information generated in their activity as a registration entity.

6. Obligations of signatories and seal creators

6.1. Obligations of custody

The signer or seal creator is obliged to safeguard the personal identification code, the private keys, when applicable the card or any other technical support provided by esFIRMA, and, if necessary, the esFIRMA-owned specifications that are supplied to them.

In case of loss or theft of the private key of the certificate, or if you suspect that the private key has lost reliability for any reason, these circumstances must be immediately reported to esFIRMA directly or through the subscriber.

6.2. Obligations of proper use

The signer or seal creator must use the certification service provided by esFIRMA, exclusively for the authorized uses in the DPC and in any other instruction, manual, or procedure supplied to the subscriber.

The signer or creator of seals must comply with any law and regulation that may affect their right to use the cryptographic tools employed.

The signer or seal creator may not adopt measures for inspection, alteration, or decompilation of the digital certification services provided.

The signer or seal creator must stop using the private key in case of compromise of said key, revocation, or compromise of the CA's keys.

The signer or creator of seals will acknowledge:

a) That when using any certificate, and as long as the certificate has not expired or been revoked, they will have accepted said certificate and it will be operational.

b) That it does not act as a certification entity and, therefore, is obliged not to use the private keys corresponding to the public keys contained in the certificates for the purpose of signing any certificate.

6.3. Prohibited transactions

The signer or seal creator undertakes not to use their private keys, certificates, cards, or any other technical support provided by esFIRMA in carrying out any transaction prohibited by applicable law.

The digital certification services (and electronic time stamping services) provided by ESFIRMA have not been designed nor allow their use or resale as equipment for controlling hazardous situations, or for uses that require fail-safe actions, such as the operation of nuclear facilities, air navigation or communication systems, air traffic control systems, or weapon control systems, in which an error could directly cause death, physical harm, or serious environmental damage.

7. Obligations of the verifiers

7.1. Informed decision

ESFIRMA informs the verifier that it has access to sufficient information to make an informed decision when verifying a certificate and trusting the information contained in said certificate.

Additionally, the verifier will recognize that the use of the Registry and the Certificate Revocation Lists (hereinafter, "the LRCs" or "the CRLs) of ESFIRMA, are governed by the DPC of ESFIRMA and undertakes to comply with the technical, operational, and security requirements described in the aforementioned DPC.

7.2. Signature verification requirements

The verification will usually be carried out automatically by the verifier software and, in any case, in accordance with the DPC, with the following requirements:

- It is necessary to use the appropriate software for the verification of a digital signature with the algorithms and key lengths authorized in the certificate and/or perform any other cryptographic operation, and establish the certificate chain on which the electronic signature to be verified is based, since the electronic signature is verified using this certificate chain.

- It is necessary to ensure that the identified certificate chain is the most suitable for the electronic signature that is verified, since athe electronic signature It can be based on more than one certificate chain, and it is the verifier's decision to ensure the use of the most suitable chain to verify it.
- It is necessary to verify the revocation status of the certificates in the chain with the information provided a ESFIRMA (with LRCs, for example) to determine the validity of all the certificates in the certificate chain, since it can only be considered correctly verified an electronic signature if each and every one of the certificates in the chain are correct and valid.

- It is necessary to ensure that all certificates in the chain authorize the use of the private key by the certificate subscriber, as there is the possibility that some of the certificates include usage limits that prevent trust in the electronic signature that is verified. Each certificate in the chain has an indicator that refers to the applicable usage conditions, for review by the verifiers.
- It is necessary to technically verify the signature of all the certificates in the chain before trusting the certificate used by the signer or creator of seals.

7.3. Trust in an unverified certificate

If the verifier trusts an unverified certificate, they will assume all risks arising from this action.

7.4. Verification effect

By virtue of the correct verification of these certificates, in accordance with this informative text (PDS), the verifier can trust the identification and, where appropriate, the public key of the signer.

7.5. Proper use and prohibited activities

The verifier undertakes not to use any type of certificate status information or any other type provided by ESFIRMA, in carrying out any transaction prohibited by the law applicable to said transaction.

The verifier undertakes not to inspect, interfere with, or reverse engineer the technical implementation of ESFIRMA's public certification services, without prior written consent.

Additionally, the verifier is obliged not to intentionally compromise the security of ESFIRMA's public certification services.

The digital certification services provided by ESFIRMA have not been designed nor allow the use or resale, as control equipment for dangerous situations or for uses that require fail-safe actions, such as the operation of nuclear facilities, air navigation or communication systems,

air traffic control systems, or weapon control systems, where an error could cause death, physical harm, or serious environmental damage.

7.6. Indemnity clause

The third party that relies on the certificate agrees to hold ESFIRMA harmless from any damage arising from any action or omission resulting in liability, damage or loss, expense of any kind, including legal and attorney fees that may be incurred, for the publication and use of the certificate, when any of the following causes occur:

- Failure to comply with the obligations of the third party who relies on the certificate.
- Reckless trust in a certificate, given the circumstances.
- Failure to verify the status of a certificate to determine that it is not suspended or revoked.
- Lack of verification of all prescribed security measures in the DCP or other applicable regulations.

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

8. Obligations of ESFIRMA

8.1. In relation to the provision of digital certification

ESFIRMA undertakes to:

a) Issue, deliver, manage and revoke certificates, in accordance with the instructions provided by the subscriber, in the cases and for the reasons described in the DPC of ESFIRMA.

b) Execute services with the appropriate technical and material means, and with personnel who meet the qualification and experience conditions established in the DPC.

c) Comply with the service quality levels, in accordance with what is established in the DPC, in technical, operational, and security aspects.

d) Notify the subscriber, in advance, of the expiration date of the certificates.

e) Communicate to third parties who request it, the status of the certificates, in accordance with what is established in the DPC for the different certificate verification services.

8.2. In relation to the checks of the registry

ESFIRMA is committed to the issuance of certificates based on the data provided by the subscriber, for which it may carry out the checks it deems appropriate.

In the event that ESFIRMA detects errors in the data that must be included in the certificates or that justify this data, it may make the changes it deems necessary before issuing the certificate or suspend the issuance process and manage the corresponding incident with the subscriber. In the event that ESFIRMA corrects the data without prior management of the

corresponding incident with the subscriber, it must notify the subscriber of the finally certified data.

ESFIRMA reserves the right not to issue the certificate when it considers that the documentary justification is insufficient for the correct identification and authentication of the subscriber.

The previous obligations will be suspended in cases where the subscriber acts as a registration authority and has the technical elements corresponding to key generation, certificate issuance, and recording of corporate signature devices.

8.3. Retention periods

ESFIRMA preserves the information related to the services provided in accordance with Article 24.2.h) of Regulation (EU) 910/2014 of the European Parliament and of the Council, of July 23, 2014, for at least 15 years from the expiration of the certificate or the completion of the service provided.

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

9. Limited warranties and warranty disclaimers

9.1. ESFIRMA's guarantee for digital certification services

ESFIRMA guarantees to the subscriber:

- That there are no errors of fact in the information contained in the certificates, known or made by the Certification Authority.

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

- That the certificates comply with all the material requirements established in the DPC.

- That the revocation services and the use of the repository comply with all the material requirements established in the DPC.

ESFIRMA guarantees to the third party that trusts the certificate:

- That the information contained or incorporated by reference in the certificate is correct, except when indicated otherwise.

- In the case of certificates published in the repository, that the certificate has been issued to the subscriber identified in it and that the certificate has been accepted.

- That in the approval of the certificate request and in the issuance of the certificate, all material requirements established in the DPC have been met.

- The speed and security in the provision of services, especially in the revocation and deposit services.

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

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

9.2. Exclusion of warranty

ESFIRMA rejects any other warranty different from the previous one that is not legally enforceable.

Specifically, ESFIRMA does not guarantee any software used by any person to sign, verify signatures, encrypt, decrypt, or otherwise use any digital certificate issued by ESFIRMA, except in cases where there is a written statement to the contrary.

10. Applicable agreements and DPC

10.1. Applicable agreements

The agreements applicable to this certificate are as follows:

- Certification services contract, which regulates the relationship between ESFIRMA and the Public Administration/Legal Entity subscriber of the certificates.

- General conditions of the service incorporated in this Certificate disclosure text or PDS.

- DPC, which regulates the issuance and use of certificates.

10.2. DPC

ESFIRMA's certification services are technically and operationally regulated by ESFIRMA's DPC, by its subsequent updates, as well as by complementary documentation.

The DPC and the operations documentation are periodically modified and can be consulted on the Internet page: https://www.esfirma.com

11. Privacy policy

ESFIRMA cannot disclose nor can it be compelled to disclose any confidential information regarding certificates without a prior specific request coming from:

a) The person with respect to whom ESFIRMA has the duty to maintain confidential information, or

b) A judicial, administrative order, or any other order provided for in the current legislation.

However, the subscriber agrees that certain information, both personal and otherwise, provided in the certificate request, be included in their certificates and in the certificate status verification mechanism, and that the aforementioned information is not considered confidential, due to legal imperative.

ESFIRMA does not transfer to any person the data specifically provided for the certification service.

The processing of such data by third parties for the purpose of providing a service to esFIRMA, among others, merely by way of illustration but not limitation, occurs within the framework of a processing order referred to in Article 28 REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), and 33 of the Organic Law 3/2018, of 5 December, on Personal Data Protection and guarantee of digital rights (LOPDGDD) and, by virtue thereof, complies with the requirements of the GDPR and the LOPDGDD, and guarantees the protection of the rights of the data subject.

12. Privacy policy

ESFIRMA has a privacy policy in section 9.4 of the DPC, and specific privacy regulation in relation to the registration process, the confidentiality of the registry, the protection of access to personal information, and user consent.

The information referred to in section 7.3 is kept for the indicated periods, duly registered and with guarantees of security and integrity.

13. Refund policy

ESFIRMA will not refund the cost of the certification service in any case.

14. Applicable law, competent jurisdiction, and claims and disputes regime

The relationships with ESFIRMA will be governed by the Spanish law on trust services in force at any given time, as well as by civil and commercial legislation where applicable.

The competent jurisdiction is the one indicated in Law 1/2000, of January 7, on Civil Procedure.

In case of discrepancy between the parties, the parties will attempt prior amicable resolution. To this end, the parties must send a communication to esFIRMA by any means that leaves a record to the contact address indicated in the contact information point of this PDS.

If the parties do not will reach an agreement on the matter, any of them may submit the conflict to civil jurisdiction, subject to the Courts of the registered office of ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA.

14.1. Accreditations and quality seals

EsFIRMA has the "eIDAS-compliant" qualification for the following services:

a) Qualified electronic signature certificates issuance service
b) Qualified electronic seal certificate issuance service
c) Qualified electronic certificate issuance service for website authentication
d) Qualified electronic time stamp issuance service

14.2. Linking with the list of providers

EsFIRMA is a qualified provider of certification services, which is part of the List of Qualified Providers (TSL) maintained by the national supervisor and can be obtained at the following address:
https://sedeaplicaciones.minetur.gob.es/Prestadores/

EsFIRMA is included in the European Union's "Trust List" as a Qualified Provider of electronic trust services:
https://webgate.ec.europa.eu/tl-browser/#/tl/ES/27

14.3. Divisibility of clauses, survival, entire agreement, and notification

The clauses of this disclosure text (PDS) are independent of each other, which is why, if any clause is considered invalid or unenforceable, the rest of the clauses of the PDS will continue to be applicable, except for an express agreement to the contrary by the parties.

The requirements contained in the sections ofObligations and responsibilities, “Compliance audit and “Confidentiality The DPC of ESFIRMA will remain valid after the termination of the service.

This text contains the complete will and all agreements between the parties.

The parties mutually notify each other of facts through a procedure shipment email to the address info@esfirma.com