Disclosure Text (PDS) of certificates issued to Public Administrations

Table of Contents

INFORMATIVE TEXT - PDS

This document contains the essential information to be known in relation to the certification service of the ESFIRMA Certification Body.

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

1.1. Document control

Safety Rating	PUBLIC
Version	2.2

1.2. Version Control

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

2.2	(1.3)	A reference to the esFIRMA website has been added.	esFIRMA	21/04/2023
2.3		Reference to dispute resolution procedure added	esFIRMA	15/07/2026

2. Information

2.1. Responsible organization

The ESFIRMA Certification Body, hereinafter referred to as "ESFIRMA", is an initiative of:

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

2.2. Contact

For any queries, please contact:

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

2.3. Contact for revocation processes

The process for requesting the revocation of a certificate can be found on www.esfirma.com.
For any further queries, please contact:

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

3. Type and purpose of the certificate

3.1. Qualified certificates of public employee

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

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

3.2. Certificates of public employee with pseudonym

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

3.3. Card certificates

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 of the Council, of 23 July 2014.

3.4. Cloud Certificates

These certificates are centrally managed.

3.5. Certificates for authentication

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

3.6. Advanced Signing Certificates

Certificates with the signature function allow the generation of the "advanced electronic signature" that is based on a qualified certificate without the joint involvement 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 the provisions of Article 25.2 of Regulation (EU) 910/2014 of the European Parliament and of the Council, of 23 July 2014, 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 23 July 2014 and comply with the provisions of the technical regulations 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 1 October, on the Legal Regime of the Public Sector, which will include the tax identification number and the corresponding name, as well as, where appropriate, the identity of the holder in the case of electronic seals of administrative bodies.

3.9. Advanced Seal Certificates

Certificates with the signature function allow the generation of the "advanced electronic seal" that is based on a qualified certificate without the joint involvement 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
Medium-level public employee, for signature	HSM centralized	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 a 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 a medium-level pseudonym, for signature	HSM centralized	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 a 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	HSM centralized	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 Certificate Authority

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

3.12. Validating certificates

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

4. Certificate usage limits

4.1. Usage limits targeting signers

The signatory and the creator of stamps must use the certification service provided by esFIRMA exclusively for the uses authorised in the contract signed between the esFIRMA and the SUBSCRIBER, and which are reproduced below.

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

The signatory and the stamp creator must comply with any laws and regulations that may affect their right to use the cryptographic tools they employ.

The signatory and the stamp creator may not adopt inspection, alteration or reverse engineering measures of esFIRMA's digital certification services, without prior express permission.

4.2. Usage limits targeting verifiers

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

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

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

The certificates have not been designed, cannot be used for and are not authorized for use or resale as hazardous situation control equipment or for uses that require fail-safe actions, such as the operation of nuclear facilities, air navigation or communications systems, or weapons control systems, where a failure could directly lead to death, personal injury or severe environmental damage.

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

The use of digital certificates in transactions that contravene this disclosure text (PDS), or contracts with subscribers, is considered improper use for the appropriate legal purposes, therefore ESFIRMA is exempt, in accordance with current legislation, from any liability for this improper use of the certificates made by the signatory or any third party.

The esFIRMA provider 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 of accessing the content of the message, it is not possible for esFIRMA to issue any assessment on said content, therefore the subscriber, the signatory or the creator of stamps assumes any responsibility arising from the content associated with the use of a certificate.

Likewise, the subscriber will be responsible for any liability that may arise from the use of the same outside the limits and conditions of use set out in this disclosure text, or in the contracts with the subscribers, as well as any other improper use of the same derived from this section or that may be interpreted as such in accordance with current legislation.

5. Obligations of subscribers

5.1. Key generation

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

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

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

5.2. Request for certificates

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 the provisions of ESFIRMA's statement of certification practices (CPD) and operations documentation.

5.3. Veracity of information

The subscriber is responsible for ensuring that all information included in his/her certificate application is accurate, complete for the purpose of the certificate and is up to date at all times.

The subscriber must immediately inform ESFIRMA:

- Any inaccuracies detected in the certificate once it has been issued.

- Any 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 the information generated in its activity as a registration entity.

6. Obligations of signatories and stamp creators

6.1. Custody obligations

The signatory or creator of stamps undertakes to safeguard the personal identification code, the private keys, when the card or any other technical support provided by esFIRMA and, if necessary, the specifications owned by esFIRMA that are supplied.

In the event of loss or theft of the certificate's private key, or in the event that you suspect that the private key has lost reliability for any reason, such circumstances must be immediately notified to esFIRMA directly or through the subscriber.

6.2. Obligations of correct use

The signatory or creator of seals must use the certification service provided by esFIRMA, exclusively for the uses authorized in the DPC and in any other instructions, manuals or procedures provided to the subscriber.

The signer or creator of stamps has to comply with any laws and regulations that may affect their right to use the cryptographic tools employed.

The signatory or creator of seals may not adopt measures to inspect, alter or decompile the digital certification services provided.

The signer or creator of seals must stop using the private key in the event of a compromise of the private key, revocation, or compromise of the CA keys.

The signatory or creator of stamps will recognize:

a) That when you use any certificate, and as long as the certificate has not expired or been revoked, you will have accepted that certificate and will be operational.

b) That it does not act as a certification authority and, therefore, undertakes 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 signatory or creator of seals undertakes not to use their private keys, certificates, cards or any other technical support provided by esFIRMA in the performance of any transaction prohibited by applicable law.

The digital certification services (and electronic time-stamping services) provided by ESFIRMA have not been designed and do not allow their use or resale as hazardous situation control equipment, or for uses that require error-proof actions, such as the operation of nuclear facilities, air navigation or communication systems, air traffic control systems or arms control systems, where an error could directly cause death, physical damage or serious environmental damage.

7. Obligations of verifiers

7.1. Informed decision

ESFIRMA informs the verifier that it has access to sufficient information to make an informed decision at the time of verifying a certificate and to rely on the information contained in such certificate.

In addition, the verifier shall acknowledge that the use of the ESFIRMA Registry and Certificate Revocation Lists (hereinafter referred to as "the LRCs" or "the CRLs") are governed by the ESFIRMA DPC and undertakes to comply with the technical, operational and security requirements described in the aforementioned DPC.

7.2. Signature Verification Requirements

The verification will normally be carried out automatically by the verifier's 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 to execute any other cryptographic operation, and to establish the chain of certificates on which the electronic signature to be verified is based, since the electronic signature is verified using this chain of certificates.
- It is necessary to ensure that the identified chain of certificates is the most suitable for the electronic signature being verified, since an electronic signature can be based on more than one chain of certificates, and it is the decision of the verifier to ensure that the most appropriate chain is used to verify it.
- It is necessary to check the revocation status of the certificates in the chain with the information provided to ESFIRMA (with LRCs, for example) to determine the validity of all the certificates in the certificate chain, since it can only be used to determine the validity of the certificates in the chain of certificates.

An electronic signature is considered correctly verified if each and every one of the certificates in the chain is correct and current.

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

7.3. Trust in an unverified certificate

If the verifier relies on an unverified certificate, he will assume all the risks arising from this action.

7.4. Effect of verification

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

7.5. Proper Use and Prohibited Activities

The verifier undertakes not to use any type of information on the status of the certificates or any other type that has been provided by ESFIRMA, in the performance of any transaction prohibited by the law applicable to the aforementioned 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.

In addition, the verifier undertakes not to intentionally compromise the security of ESFIRMA's public certification services.

The digital certification services provided by ESFIRMA have not been designed and do not allow the use or resale, as hazardous situation control equipment or for uses that require error-proof actions, such as the operation of nuclear facilities, air navigation or communication systems, air traffic control systems, or weapons control systems. where a mistake could cause death, physical damage or serious environmental damage.

7.6. Indemnity clause

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

- Failure to comply with the obligations of the third party relying on the certificate.
- Reckless reliance on a certificate, in the light of the circumstances.
- Failure to check the status of a certificate, to determine that it is not suspended or revoked.
- Failure to verify all the security measures prescribed in the DCP or other implementing regulations.

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

8. ESFIRMA's obligations

8.1. In relation to the provision of digital certification

ESFIRMA undertakes to:

a) To issue, deliver, administer and revoke certificates, in accordance with the instructions provided by the subscriber, in the cases and for the reasons described in the ESFIRMA DPC.

b) To carry out the 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 levels of quality of service, in accordance with what is established in the DPC, in the technical, operational and safety 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 registration checks

ESFIRMA undertakes to issue 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 incident

corresponding to the subscriber, 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 foregoing obligations shall be suspended in cases where the subscriber acts as the registration authority and has the technical elements corresponding to the generation of keys, issuance of certificates and recording of corporate signature devices.

8.3. Retention periods

ESFIRMA retains information relating 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 23 July 2014, for at least 15 years from the expiry of the certificate or the end 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 Disclaimers of Warranties

9.1. ESFIRMA guarantee for digital certification services

ESFIRMA guarantees the subscriber:

- That there are no factual errors in the information contained in the certificates, known or made by the Certification Body.

- That there are no factual errors in the information contained in the certificates, due to a lack of due diligence in the management of the certificate application or in the creation of the certificate.

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

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

ESFIRMA guarantees to the third party that relies on the certificate:

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

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

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

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

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

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

9.2. Exclusion of Warranty

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

Specifically, ESFIRMA does not warrant 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 declaration to the contrary.

10. Applicable Agreements and DPCs

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 subscribing to the certificates.

- General Terms of Service incorporated into this Certificate Disclosure or PDS text.

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

10.2. CPD

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

The CPD and the documentation of operations are periodically modified and can be consulted on the website: https://www.esfirma.com

11. Privacy Policy

ESFIRMA cannot disclose and cannot be compelled to disclose any confidential information regarding certificates without a prior specific request from:

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

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

However, the subscriber agrees that certain information, personal and otherwise, provided in the certificate application, will be included in its certificates and in the certificate status check mechanism, and that the aforementioned information will not be confidential, as required by law.

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

The processing of such data by third parties for the purpose of providing a service to esFIRMA, including but not limited to, takes place 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 to the free movement of this data and repealing Directive 95/46/EC (General Data Protection Regulation), and 33 of Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD) and by virtue of which it is in accordance 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 registration, the protection of access to personal information, and user consent.

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

13. Refund Policy

ESFIRMA will not reimburse the cost of the certification service under any circumstances.

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

Relations with ESFIRMA will be governed by Spanish law on trust services in force at all times, as well as by civil and commercial legislation as applicable.

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

In the event of a discrepancy between the parties, the parties shall attempt a prior amicable settlement. To this end, the parties must send a communication to esFIRMA, filling in the complaint and suggestion form available on the esFIRMA website by any of the means indicated therein. The complaint will be handled in accordance with internal procedures for the resolution of complaints, appeals and disputes.

If the parties do not reach an agreement in this regard, either of them may submit the dispute to civil jurisdiction, subject to the Courts of the registered office of ESFIRMA.

14.1. Accreditations and quality seals

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

a) Service for the issuance of qualified electronic certificates for electronic signatures
b) Service for the issuance of qualified electronic certificates with an electronic seal
c) Service for the issuance of qualified electronic certificates for website authentication
d) Time-qualified electronic stamp issuance service

14.2. Linking to the list of providers

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

EsFIRMA is included in the "Trust List" of the European Union as a qualified Provider of Trusted Electronic Services:
https://webgate.ec.europa.eu/tl-browser/#/tl/ES/27

14.3. Severability of Terms, Survival, Entire Agreement and Notice

The provisions 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, unless expressly agreed otherwise by the parties.

The requirements contained in the "Obligations and Liability", "Compliance Audit" and "Confidentiality" sections of ESFIRMA's DPC will remain in force after termination of the service.

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

The parties notify each other of the facts by means of a procedure sent by email to the address info@esfirma.com