Disclosure Text (PDS) of certificates issued for Public Administrations

esfirma
Autoridad de certificación

Index

DISCLOSURE TEXT - PDS

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

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

1.1.Documentary control

Safety rating	Public
Version	2.0

1.2.Version control

Version	Changes	Description	Author	Date
1.0	Original	Document creation	esFIRMA	28/04/2016
1.4		Subsanaciones	esFIRMA	07/06/2017
1.5		Change denomination and reference to regulations	esFIRMA	06/11/2017
2.0		Inclusion of all certificates relating to Spanish AAPPPs	esFIRMA	03/06/2020

2. Information

1.1. Responsible organization

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

ESPUBLICO SERVICES FOR THE ADMINISTRATION SA (ESFIRMA)
CALLE BARI 39 (Edif. Binary Building)
50197 - ZARAGOZA
(+34) 976300110

1.2. Contact

For any questions, please contact:

ESPUBLICO SERVICES FOR THE ADMINISTRATION SA (ESFIRMA)
CALLE BARI 39 (Edif. Binary Building)
50197 - ZARAGOZA
(+34) 976300110

1.3. Contact for revocation processes

For any questions, please contact:

ESPUBLICORVICIOS FOR THE ADMINISTRATION 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 to 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 by theETSI EN 319 411-2 refencia.

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

3.2. Public employee certificates under a pseudonym

These certificates allow to identify their holders as personnel in the service of the Public Administration, linking them with it, following the requirements established in article 43.2 of Law 40/2015, of October 1, of the Legal Regime of the Public Sector, for the electronic signature of the staff in the service of thePublicAdministrations, which for public safety reasons will only be identified with the professional identification number or other pseudonym of public employee.

3.3. Card certificates

Certificates using a card operate with a qualified electronic signature creation device, in accordance with Annex II to 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 signer.

3.6. Certificates for advanced signature

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 ternated signaturelificada

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

3.8. Qualified e-seal certificates

These certificates are qualified in accordance with Article 38 and Annex III to 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 identifiedwith the reference ETSI EN 319 411-2.

These certificates allow the identification of their holders as Public Administrations, following the requirements set out in Article 40 of Law 40/2015, of October 1, of the Legal Regime of the PublicSector, 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

Certificateswith the signature function allow the generation of the "advanced electronic seal" that is 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	Company	● 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	Centralized HSM	Company	● 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 (pending qualification)	*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	Company	● 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 under a pseudonymous middle level, for signature	Centralized HSM	Company	● 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 under a high-level pseudonym, for authentication (pending qualification)	*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	Company	● 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	Company	● 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 using the data indicated above.

3.12. Certificate validation

The lists of revoked certificates and OCSP services are located on the esFIRMA website and in the URLs indicated in each of the certificates.

4. Certificate usage limits

4.1. Limits of use for signatories

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

In addition, the signer and the creator of seals are obliged to use the digital certification service in accordance with the instructions, manualor procedures supplied by esFIRMA.

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

The signer and seal manufacturer may not take inspection, alteration or reverse engineering measures of esFIRMA'sdigital certification serviceswithout prior express permission.

4.2. Limits of use for verifiers

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

Similarly, certificates should only be used in accordance with applicable law, especially taking into account theimport and export restrictions that exist at all times.

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

Certificates are not designed, cannot be used and are not authorized for use or resale as hazardous situation control equipment or for use requiring fail-safeactions, such as the operation of nuclear facilities, navigation systems or air communications, or weapons control systems, where a failure could directly lead to death, personal injury or severe environmental damage.

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

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

The provider is not has access to the data on which the use of a certificate can be applied. Therefore, and as a result of this technical impossibility to access the content of the message, it is not possible on the part of esFIRMA to issue any assessment on such content, assuming therefore the subscriber, the signer or the creator of stamps, any responsibility arising from the content associated with the use of a certificate.

Likewise, the subscriber will be attributable toany liability that may arise from the use of the same outside the limits and conditions of use contained in this disclosure text, or in the contracts with the subscribers, as well as any other misuse thereof derived from this section or that may be interpreted as such in accordance with the current legislation.

5. Subscriber obligations

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 thecloud 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 stamp certificates, the subscriber authorizes esFIRMA to generatethekeys, private and public, for use by stamp creators, and requests on his behalf the issuance of the electronic stamp certificate.

5.2. Request for certificates

The Subscriber undertakes to make requests, where necessary, ofthese certificates in accordance with the procedure and, if necessary, the technical components provided by ESFIRMA, in accordance with what is set out in the Certification Practices Statement (DPC) and in the ESFIRMA operationsdocumentation.

5.3. Truthfulness of information

The Subscriber is responsible for en being responsible for all information included in their certificate request being accurate, complete for the purpose of the certificate and up to date at all times.

The subscriber must immediately inform ESFIRMA:

- Of any inaccuracies 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. Custodyobligation

The Subscriber undertakes to hold all the information it generates in its activity as a registration entity.

6. Obligations of signers and stamp creators

6.1. Custody obligations custodia

The signer or stamp creator undertakes to guard the personal identification code, private keys, where the card or any other technical support provided by esFIRMA exists and, if necessary, the specifications owned by esFIRMA that are provided to it.

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

6.2. Obligations for correct use

The signer or stamp creator must use the certification service provided by esFIRMA,exclusively for the authorized uses in the DPC and in any other instruction, annual mor procedure provided to thesubscriber.

The signer or stamp creator must comply with any law and regulation that may affect his right to use the cryptographic tools used.

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

The signer or stamp creator must stop using the private key in case of commitment of such clave, revocation, or commitment of the keys of the CA.

The signer or stamp creator shall recognize:

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

b) 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. Transactions prohibidas

The signer or creator of stamps undertakes not to use his/her private keys, certificates, cards or any other technical support provided by esFIRMA in the making of a transaction any prohibited by applicable law.

The digital certification (and electronic time stamping) services provided by ESFIRMA have not been designed or permit their use or resale as hazardous situation control equipment, or for use that requires error-proof actions,such as the operation of nuclear facilities, navigation or air communication systems, air traffic control systems or weapons control systems, in which an error could directly cause death, physical damage or serious media damage.entales graves.

7. Verifier obligations

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 relying on the information contained in that certificate.

In addition, the verifier will recognize that the use of the Registry and certificate revocation schedules (hereinafter referred to as "the LRCs"or "the CRLs")of ESFIRMA, are governed by the ESFIRMA DPC and undertake to comply with the technical, operational and security requirements described in the aforementioned DPC.

7.2. Signature verification requirements

The check will normally be run 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 softwareto verify a digital signature with the algorithms and key lengths authorized in the certificate and/or execute any other cryptographic operation, and establish the certificate chain on which the electronic signature is based to verify, since the electronic signature is verified using this certificate chain.
- It is necessary to ensure that the identified certificate chain is best suited for the electronic signature being verified, since anelectronic signature can be based on more than one certificate chain, and it is the verifier's decisionto ensure the use of the most appropriate chain to verifyit.
- It is necessary to check the revocation status of the certificates in the chain with the information provided to ESFIRMA (with LRCs,forexample) to determine the validity of all certificates in the certificate chain, since an electronic signature can only be considered correctly verified if each and every certificate in the chainis correct and are ineffect.

- 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 the possibility that one of the certificates includes limits of uso that prevent trusting the electronic signature that is 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 firma of all certificates in the chain before relying on the certificate used by the signer or stamp creator..

7.3. Trust in an unverified certificate

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

7.4. Effect of verification

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

7.5. Correct use and prohibited activities

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

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

The digital certification services provided by ESFIRMA have not been designed or permit the use or resale, such as heavy situation control equipmentor for use requiring error-proof actions, such as the operation of nuclear facilities, air navigation or communication systems, air traffic control systems, or weapons control systems, where an error could lead todeath, physical damage or serious environmental damage.

7.6. Indemnity clause

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

- Non-compliance with the obligations of the third party who trusts the certificate.
- Reckless reliance on a certificate, depending on the circumstances.
- Failure to check the status of a certificate, to determine that it is not suspended orrevoked.
- Lack of verification of all insurance measures prescribed in the DCP or other implementing rules.

8. ESFIRMA's obligations

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 ESFIRMA DPC.

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

c) To meet 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, as set out 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, so that it can carry out the checks it deems appropriate.

In the event that ESFIRMA detects errors in the data to be included in the certificates or that justify this data, you can make any changes you deem necessary before issuing the certificate or suspending the issuance process and managing with the subscriber thecorrespondinginformation. In the event that ESFIRMA corrects the data without prior management of the corresponding incident with the subscriber, it must notify the data finally certified to the Subscriber.

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

The above obligations will be suspended in cases where the subscriber acts as registration authority and has the technical elements corresponding to the generation of keys, issuance of certificates and recording of signing devicesto corporate.

8.3. Conservation periods

ESFIRMA archives records for applications for issuance and revocation of certificates for at least 15 years.

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

9. Limited warranties and disclaimer of warranties

9.1. ESFIRMA's 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 Authority.

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

- That certificates meet all the material requirements set forth in the DPC.

- That the revocation services and the use of the warehouse meet all the material requirements set out in the CPD.

ESFIRMA guarantees the third party that trusts the certificate:

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

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

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

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

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

- That the certificate contains the information to be contained in a qualified certificate, in accordance with Annex I to EU Regulation 910/2014.
- That, in the event that it generates the private keys of the subscriber or, where appropriate, the natural person identified in the certificate, its confidentiality is maintained during the process.
- The responsibility of the Certification Authority, with the limits that are established. In no case shall ESFIRMA rspong in fortuitous cases and in case of force majeure.
- The private key of the certification authority used to issue certificates has not been compromised, unless esFIRMA has not communicated otherwise, according to the DPC.
- It has not originated or entered false or erroneous statements in the information of any certificate, nor has it ceased to include necessary information provided by the subscriber and validated by esFIRMA,at the time of issuance of the certificate.
- All certificates meet the formal and content requirements of the DPC, including all applicable and legal requirements.
- It is bound by the operational and security procedures described in the DPC.

9.2. Warranty exclusion

ESFIRMA disclaims any warranty other than the above that is not legally enforceable.

Specifically, ESFIRMA does not warrant any software used by any person to sign, verify signatures, encrypt, decrypt, or otherwise useany digitally certified digitally issued by ESFIRMA, except in cases where there is a written statement to the contrary.

10. Applicable Agreements and CPD

10.1. Applicable agreements

The agreements applicable to this certificate are as follows:

- Contract of certification services, which regulates the relationship between ESFIRMA and the Public Administration /Legal Person that subscribers the certificates.

- General Terms and Conditions of 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 byESFIRMA's DP C, for its subsequent updates, as well as by additional documentation.

The CPD and operations documentation is periodically modified and can be found on the website: https://www.esfirma.com

11. Privacy policy

ESFIRMA may not disclose and may not be required to disclose any confidential information regarding certificates without a specific prior request arising from:

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

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

However, the Subscriber agrees that certain information, personal and otherwise, provided in the certificate request, is included in its certificates and in the certificate status verification mechanism, and that the above information is not confidential, by legal imperative.

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

The processing of such data by third parties by reason of the provision of a service to esFIRMA,among others, by way of example but not limited to, occurs at the marcor an order for the processing referred to in Article28 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 the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), and 33 of Organic Law 3/2018, 5 December, Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD)and by virtue of the GDPR and LOPDGDD requirements , and guarantees the protection of the rights of the data subject.

Comentado [1]: Review

12. Privacy Policy

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

It is also provided that the supporting documentation of the approvalof the application must be kept and duly registered and with guarantees of security and integrity for the period of 15 years from the expiration of the certificate, even in case of an early loss of validity by revocation.

13. Withdrawal policy

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

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

Relations with ESFIRMA will be governed by Spanish law on the subject of beingtrusted vices in force at all times, as well as by civil and commercial legislation in whatever is 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 the prior amicable resolution. To this end, the parties shall send a communication to esFIRMA by any means that it records to the contact address indicated at thecontact information point of thisSDA.

If the parties do not reach an agreement in this regard, either party may submit the dispute to civil jurisdiction, subject to the Courts of the registered office of ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA.

14.1. Accreditations and quality seals

Comentado [2]: Review

EsFIRMA has the qualification "eIDAS-compliant"eIDAS-compliantfor thefollowing services:

a) Service for issuing qualified electronic certificates of electronic signature
   i) Qualified Electronic Certificates of Public Employee
b) Service for issuing qualified electronic certificates of electronic seal
   i) Qualified Certificates of Electronic Seal of the Public Administration
c) Certification service oftwo qualified website authentication electronics
   i) Qualified certificates from Public Administration e-headquarters
d) Time-qualified electronic seal dispatch service

14.2. Linking to the list of providers

EsFIRMA is a qualified provider of certification services so it is 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 Trusted Electronic Services Provider:
https://webgate.ec.europa.eu/tl-browser/#/tl/ES/27

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

The provisions of this Disclosure Text (PDS) are independent of each other, which iswhy, if any clause is held to be invalid or unenforceable, all other provisions of the PDS shall remain applicable, except as otherwise expressly agreed by the parties.

The requirements contained in the"Obligations and Responsibility" sections,” de “ "ConformityAudit"” and "Confidentiality"” of THE SPD of ESFIRMA will remain in force after the termination of the service. “

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

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