Text Disclosure (PDS) Certificate of Qualified Authority Electronic Time Stamping

Index

Electronic seal Certificate Authority Qualified Time Stamping Electronic

DIVULGATIVE TEXT - PDS

This document contains essential information disclosed in connection with the certification service of the Certification ESFIRMA.

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

Overview

Control Document

Security classification:	Public
Entity Target:	ESFIRMA
Version:	1.5

version Control

version	changing Parties	Description of change	Author of change	Date of change
1.0	Original	document Creation	esFIRMA	07/05/2017
1.4		rectifications	esFIRMA	07/06/2017
1.5	1.1 -1.3 8.6	change name	esFIRMA	6/11/2017

1. Contact information

1.1. Organization responsible

ESFIRMA Certification Entity, hereinafter "ESFIRMA" is an initiative of:

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

1.2. contact

for inquiries, please contact:

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

1.3. contact for revocation process

for inquiries, please contact:

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

2. Type and purpose of the certificate

This certificate has the following OID:

1.3.6.1.4.1.47281.1.5.2	according to the hierarchy of esFIRMA
0.4.0.194112.1.1	according to EU policy (QCP-l)

Stamping Authority certificates qualified electronic time arecertificates qualified in accordance with Article 38 and Annex IIId 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 ETSI EN 319 412-3 references, ETSI EN 319 421 and ETSI EN 319 422.

These certificates enable digital signing of electronic evidence time.

Information uses the certificate profile indicates the following:

a) Field "key usage" is activated, and thus allows usperform the following functions:
    a. Commitment to the content(Contentcommitmentto perform the function of electronic signature)
b) In the "extKeyUsage" field has activated form of the:
    a. "timeStamping" to perform the sealing function electronic time.
c) the "Qualified Certificate Statements" field the following statement
    a. QcCompliance (0.4.0.1862.1.1), which reports that the certificate is issued asqualified:appears.
d) The "User Notice" describes the use of this certificate.

2.1. Certification Authority issuing

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

3. Limits usecertificate

3.1. limits useaddressed to the signatories

must use the service sealing qualified electronic time provided by ESFIRMA solely for authorized in the contract signed between ESFIRMA and the subscriber uses, and subsequently reproduce (section " obligations of the signatories ").

You must use the electronic stamping service time in accordance with the instructions, manuals or procedures provided by ESFIRMA.

Any law and regulation that may affect the use of cryptographic tools you use must be met.

can not take measures inspection, alteration or reverse engineering services electronic seal ESFIRMA time without prior express permission.

3.2. Usage limits directed verifiers

certificates are used to set its own function and purpose, but they mayused for other functions and for other purposes.

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

Certificates can notused 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.

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 in operations that contravene this text Disclosure (PDS), or contracts with subscribers, is considered to misuse the legal purposes, exempting from both ESFIRMA, according to current legislation, any liability for misuse of the certificates carriedthe undersigned or any third party.

also will be attributable tosubscriber any liability that may arise from the use of it off limits and conditions contained in this text disclosure or contracts with subscribers, as well as any other misuse derivative thereof of this section or that could be construed as such according to the law.

4. Subscribers obligations

4.1. Key Generation

Subscriberauthorizes ESFIRMA to generate keys, private and public, to issue this certificate.

4.2. Certificate Request

Subscriber undertakes to make requests, when necessary, these certificates in accordance with the procedure and, if necessary, the technical components supplied by ESFIRMA, in accordance with what is stated in the declaration of practices certification (DPC) and documentation ESFIRMA operations.

4.3. Reporting obligations

The subscriber is responsible for all information contained in your applicationthe certificate is accurate, complete for the purpose of the certificate and be current at all times.

The subscriber must immediately inform ESFIRMA:

- From any inaccuracies detected in the certificate once issued.
- Changes that occur in the information provided and / or registered to issue the certificate.
- Loss, theft, theft, or any other type of loss of control of the private key by the custodian.

4.4. Custodial obligations

The Subscriber shall keep all the information generatedits activity as a Registrar.

A guard the personal identification code or any technical support delivered by ESFIRMA, private keys and, if necessary, specifications ESFIRMA property that are supplied.

In case of loss or theft of the private key certificate, or if suspected that the private key has lost reliability for any reason, such circumstances must be notified immediately ESFIRMA by the subscriber.

4.5. Obligations of proper use

must be used solely for authorized certificate at the DPC uses and any other instructions manual or procedure provided tosubscriber.

Any laws and regulations that may affect your right to use cryptographic tools used must be met.

It may not adopt measures of inspection or alteration of digital certification services rendered.

addition,

a) that when any certificate is used, and as the certificate has not expired or been suspended or has been revoked, the certificate will be accepted and will be operational.

b) It is not acting ascertification authority and, therefore, agrees notuse the private key corresponding to the public keys contained in the certificates for the purpose of signing any certificate.

c) That if the private key be compromised, its use is immediately and permanently suspended.

4.6. Prohibited transactions

obligation notuse private keys, certificates or any other technical support delivered by ESFIRMA in conducting any transaction prohibited by applicable law is indicated.

Services digital certification (and sealing electronic time) provided by ESFIRMA not designed nor allow their use or resale as control equipment in hazardous situations or for uses requiring actions foolproof, as the operation nuclear facilities, air navigation systems or communication systems, air traffic control or weapons control systems, where an error could directly cause death, serious bodily injury or environmental damage.

5. Obligations of verifiers

5.1. informed decision

ESFIRMA informs the verifier that has access to sufficientto make an informed decision when verifying a certificate and rely on the information contained in the certificate information.

addition, the verifierrecognize that the use registry and Revocation Lists Certificates (hereinafter, "the LRCs" or "CRLs) of ESFIRMA, are governed by the DPC of ESFIRMA and undertake to meet the technical requirements , operational and security described in the DPC saidrequirements.

5.2. verification requirements timestamp

the check will normallyexecuted automatically by the software verifier and, in any case, according to the DPC, with the following

- it is necessary use the appropriate software for verification of a time stamp with the algorithms and key lengths authorized in the certificate and / or perform any other cryptographic operations and establish the certificate chain that the time stamp is based toverified, and it is verified using the certificate chain.

- is necessaryensure that the chain of certificates identified is most suitable for the seal of tiem po is verified, as a time stamp can be based on more than one certificate chain, and isto the verifier make use of the most appropriate network for verification.

- You needcheck the revocation status of certificates in the chain with the information provided toRegister of ESFIRMA (with LRCs, for example) to determine the validity of all certificates in the certificate chain, since only be considered properly verified one time stamp if each and every one of the certificates in the chain are correct and are in force.

- is necessaryensure that all certificates in the chain authorize use of the private key by the signer of the certificate, as therethe possibility that any certificate includes usage limits that prevent trust the time stamp is verified. Each certificate in the chain has an indicator that refers to the conditions of use applicable for review by verifiers.

- Technically necessaryverify the signature of all certificates in the chain before relying on the certificate used for sealing electronic time.

5.3. Trusting a certificate not verified

If the verifier trusts a certificate not verified, will assume all risks of this action.

5.4. Correct use and prohibited activities

The verifier undertakes notuse any information of status of certificates or any other that has been supplied by ESFIRMA, in conducting a prohibited transaction for the law applicable to the said transaction.

The verifier agrees notinspect, interfereor reverse engineer the technical implementation of public services electronic time stamping or certification ESFIRMA without prior written consent.

addition, the verifier undertakes not intentionally compromise the security of public electronic services sealing time or ESFIRMA certification.

Services sealing electronic time and digital certification provided by ESFIRMA not designed or permit the use or resale as control equipment in hazardous circumstances or for uses requiring actions foolproof, as the operation of nuclear facilities, air navigation systems or communication systems, air traffic control, or weapons control systems, where an error could cause death, serious bodily injury or environmental damage.

5.5. Indemnification

The relying party certificate agrees to indemnify ESFIRMA from harm from any acts or omissions resulting in liability, damages or losses, expenses of any kind, including court and legal representation that can incurred by the publication and use of the certificate, when any of the following:

- 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.
- Non-verification of all security measures required by the DCP or other applicable regulations.

ESFIRMA not respond in any way for any loss of encrypted information that can not be recovered.

6. Obligations ESFIRMA

6.1. In connection with the provision of digital certification

ESFIRMA undertakes:

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

b) Run services with technical means and appropriate materials, and personnel that meet the conditions of qualification and experience established in the DPC.

c) Meet the levels of service quality, in accordance with what is established in the DPC, in the technical, operational and safety aspects.

d) Notify the subscriber before, the expiration date of certificates.

e) Release to third persons requesting the certificate status, according to what is stated in the DPC for various services certificate verification.

6.2. Regarding the registry checks

ESFIRMA undertakes issuing certificates based on the data supplied by the subscriber, which may perform checks as appropriate.

In case ESFIRMA detect errors in the data to be included in the certificates or justifying this data, you can make the necessary changes before issuing the certificate or suspend the issuing process and manage the subscriber corresponding incidence. If ESFIRMA correct data without prior management of relevant incident with the subscriber, you must notify the subscriber data finally certified.

ESFIRMA reserves the right notissue the certificate ifconsiders that the documentary evidence is insufficient for correct identification and authentication of the subscriber and / or domain.

The foregoing obligations shall be suspended in cases where the subscriberacting as a registration authority and has the technical elements corresponding to the key generation, certificate issuance and recording devices corporate signature.

6.3. Retention periods

ESFIRMA file records regarding issuance requests and revocation of certificates for at least 15 years.

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

7. Limited warranties and warranty disclaimers

7.1. Guarantee ESFIRMA by digital certification services

ESFIRMA to subscriberguarantees:

- that 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 DPC.
- That revocation services and use of container materials meet all requirements of DPC.

ESFIRMA warrants to third party trusts the certificate:

- that the information contained or incorporated by reference in the certificate is accurate, unless otherwise indicated.

- If published in the deposit certificates, the certificate has been issued tosubscriber and domain identified herein and that the certificate has been accepted.

- In the approval of the certificate application and issuance of the certificate they have been met all material requirements of DPC.

- 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 qualified electronic seal certificate in accordance with Annex III of the EU Regulation 910/2014 of the European Parliament and of the Council July 23, 2014, and additional instructions for creating qualified time in accordance with Article 42 of the regulation seals.

- That in the event that generates private keys subscriber confidentiality is maintained throughout the process.

- Responsibility for the Certification,the limits established. In any case ESFIRMA liable for unforeseeable circumstances and force majeure.

7.2. Excludingguarantee

ESFIRMA rejects anyother than the above is not legally enforceable guarantee.

Specifically, ESFIRMA does not warrant any software used by anyone to sign, verify signatures, encrypt, decrypt, or otherwise use any digital certificate issued by ESFIRMA form, except in cases where a written declarationthe contrary exists.

8. Agreements and policies

8.1. applicable agreements

agreements applicable to this certificate are:

- certification service contract, which regulates the relationship between ESFIRMA company and underwriter certificates.

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

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

8.2. DPC

certification services and timestamping of ESFIRMA technically and operationally regulated by the DPC of ESFIRMA, for its subsequent updates, as well as additional documents.

The DPC and documentation of operations is changed periodically in the registry and can be found on the website: https://www.esfirma.com

8.3. Privacy policy

ESFIRMA may not disclose or may be required to disclose any confidential information regarding certificates without prior specific request coming from:

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

b) a judicial, administrative or other provided in the legislation order.

However, the Subscriber agrees that certain information, personal and otherwise, provided in the certificate request, be included on the certificates and in the mechanism of checking the status of certificates, and that the above informationnot confidential, bylaw.

ESFIRMA does not give any person the data provided specifically for the provision of certification.

8.4. Privacy Policy

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

It is also contemplated that the 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, including any in case of early loss of effect for revocation .

8.5. refund policy

ESFIRMAnot reimburse the cost of certification service under any circumstances.

8.6. Applicable law and jurisdiction

Relations with ESFIRMA be governed by Spanish law on trust servicesforce at all times, as well as civil and commercial law as applicable.

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

In case of disagreement between the parties, the partiesseek prior amicable settlement. To this end, the parties shall send a communication to esFIRMA by any means allowing the contact address indicated at the point of contact of this PDS.

If the parties failreach an agreementthe matter, either party may refer the dispute to the civil jurisdiction, subject to the courts of the registered office of esPublico SA managementservices.

8.7. Accreditations and quality seals

No stipulation.

8.8. Linking with the list of providers

http://www.minetur.gob.es/telecomunicaciones/es-es/servicios/firmaelectronica/paginas/prestadores.aspx

8.9. Severability, survival, and notification entire agreement

clauses of this text disclosure are independenteach other, why, if any provision is held invalid or unenforceable, the remaining provisions of the PDS continueapply, except expressly agreed by the parties.

The requirements contained in Sections 9.6.1 (Obligations and responsibility), 8 (Compliance Audit) and 9.3 (Confidentiality) of the CPD ESFIRMA will survive termination of service.

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

The parties made are notified each other through a process of sending email to the address info@esfirma.com