TEXT DIVULGATIVE

apply to

licenses SEAL BODY IN INTERMEDIATE HSM

esfirma
Autoridad de certificación

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

Document Control

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	7/06/ 2017
1.5		Change of name and reference to regulations	esFIRMA	06/11/2017

index

Contact information

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

Contact

For inquiries, please contact:

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

Contact for revocation

for inquiries, please contact:

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

Type and purpose of the certificate seal midlevel organ HSM

This certificate has the following OIDs:

1.3.6.1.4.1.47281.1.2.4	in the hierarchy of the EC esFIRMA
0.4.0.194112.1.1	according to the policy l
2.16.724.1.3.5.6.2	QCP-Spanishmidlevel civil servant

stamp certificates midlevel electronic organ arecertified qualified in accordance with Article 38 and Annex III of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and give effect to the provisions of the regulationst ECHNICAL identified with reference ETSI EN 319411-2.

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

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

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

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

Information uses the certificate profile indicates the following:
Field "key usage" is activated, and thus allows usperform the following functions:

Commitment to the content(Contentcommitmentto perform the function of electronic signature)
DigitalSignature
Key Encipherment

In the "qualified certificate Statements" field the following statement

QcCompliance (0.4.0.1862.1.1), which reports that the certificate is issued as qualified:appears.

The "User Notice" describes the use of this certificate.

Entity issuing certification

certificates midlevel seal body are issued by ESFIRMA, identified by the data above.

Limits usecertificate

limits useaddressed to the signatories

The signatory must use the certification service certificates midlevel seal body provided by ESFIRMA solely for authorized in the contract signed between ESFIRMA and the subscriber uses, and subsequently reproduce (section "obligations of the signatories").

addition, the undersigned agrees to use digital certification service in accordance with the instructions, manuals or procedures provided by ESFIRMA.

The signer of any law and regulation that may affect your right to use cryptographic tools employing meet.

The signer can not take measures inspection, alteration or reverse engineering of digital certification services ESFIRMA without prior permission.

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, or contracts with subscribers, is considered to misuse the legal purposes, exempting from both ESFIRMA, according to the law, any liability for misuse of the certificates carriedthe undersigned or any third party.

ESFIRMA not have access to data that can be applied using a certificate. Therefore, asresult of this technical impossibility to access the content of the message is not possible by ESFIRMA issue any assessment on such content, thus assuming the subscriber, the signatory or the person responsible for the custody, any liability arising from the use of content rigged a certificate.

also will be attributable tosubscriber, the signer or the person responsible for the custody, 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 derivative thereof misuse of this section or that could be construed as such according to the law.

Subscribers obligations

Key Generation

Subscriberauthorizes ESFIRMA to generate keys, private and public, for identification and electronic signatures of the signatories, and calls on behalf certificate issuance stamp midlevel body.

Certificate Request

Subscriber undertakes to perform license applications stamp midlevel body 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.

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 signer.

Custodial obligations

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

Obligations of the creators of stamps

obligations custody

creator seals is obliged to safeguard the personal identification code or any technical support delivered by ESFIRMA, private keys and, if necessary, specifications owned by ESFIRMA that are supplied. Stamp creator is obliged to safeguard the personal identification code (PIN).

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

Correct use obligations

creator seals have to use the certification service certificates midlevel seal provided by ESFIRMA body, solely for authorized purposes in the DPC and any other instructions manual or procedure provided tosubscriber.

The creator of seals has any law and regulation that may affect your right to use cryptographic tools used comply.

The creator of seals may not adopt measures of inspection or alteration of digital certification services rendered.

The creator of stamps recognize:

that when using any certificate, and while the certificate has not expired or has been suspended or has been revoked, the certificate will be accepted and will be operational.

It does not act as certification and, therefore, agrees notuse the private key corresponding to the public keys contained in the certificates for the purpose of signing any certificate.

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

Prohibited transactions

creator seals are obliged notuse their private keys, certificates or any other technical support delivered by ESFIRMA in conducting any transaction prohibited by applicable law.

The digital certification services 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 of facilities nuclear, navigation systems or air communication systems, air traffic control or weapons control systems, where an error could directly cause death, serious bodily injury or environmental damage.

Obligations of verifiers

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:.

verification requirements electronic signature

the check will normally executed automatically by the software tester and, in any case, according to the DPC, the following

it is necessary using the appropriate software to verify a digital signature algorithms and key lengths authorized certificate and / or perform any other cryptographic operations, and establish the certificate chain when the digital signature is based to verify, since the electronic signature is verified using this certificate chain.

is necessaryensure that the chain of certificates identified is the adecuad A for the electronic signature is verified, because an electronic signature may 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 over electronic signature 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 and the signer, since therethe possibility that any certificate includes usage limits that prevent relying on the electronic signature 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 by the signer.

Trusting a certificate not verified

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

Effect of verification

under proper verification of certificates of seal midlevel body in accordance with this informative text, the verifier can rely on the identification and, where appropriate signerpublic key, within the constraints of appropriate use, to generate encrypted messages.

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 ESFIRMA certification services without prior written consent.

addition, the verifier undertakes not intentionally compromise the security of public certification services ESFIRMA.

The digital certification services 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 facilities nuclear, navigation systems or air communication systems, air traffic control, or weapons control systems, where an error could cause death, serious bodily injury or environmental damage.

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.

Indicated certificate enables encryption of documents, content and data messages under the sole responsibility of the signatory. ESFIRMA not respond in any way for any loss of encrypted information that can not be recovered.

Obligations ESFIRMA

Regarding the provision of digital certification

ESFIRMA undertakes:

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 ESFIRMA the DPC.

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

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

Notify the subscriber before, the expiration date of certificates.

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

Regarding the registry checks

ESFIRMA is obliged to issue certificates based on the data supplied by the subscriber, so you can perform the checks it deems appropriate regarding the identity and other personal and additional information from subscribers and, when appropriate, of the signatories.

These checks may include the documentary evidence provided by the signer by the subscriber, if deemed necessary ESFIRMA, and any other documents and relevant information provided by the subscriber and / or the signatory.

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 the signatory.

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.

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.

Limited warranties and warranty disclaimers

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 signer identified in it 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 certificate in accordance with Annex I of the EU Regulation 910/2014 of the European Parliament and of the Council of 23 July 2014.

that in the case of private keys generatedthe subscriber or, where appropriate, physical person identified in the certificate, confidentiality is maintained throughout the process.

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

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.

DPC applicable agreements and

agreements applicable

agreements applicable to certification stamp midlevel body 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, governing the issuance and use of certificates.

DPC

certification services are regulated ESFIRMA technically and operationally 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

Trust rules for longterm signatures

ESFIRMA informs applicants of certificates midlevel seal that does not offer a service guaranteeing the reliability of the electronic signature of a document over time organ.

ESFIRMA recommended for the reliability of the electronic signature of a document over time, using the standards specified in paragraph 7.3 (trust rules for longterm signatures) of the Guide to Implementation of the Technical Standard for Interoperability "Policy Electronic Signature and certificates of the Administration ".

General considerations for rules longevas trusted signatures are collected in subsection IV.3 of the NTI electronic signature.

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.

Privacy Policy

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

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.

refund policy

ESFIRMAnot reimburse the cost of certification service under any circumstances.

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 SERVICES FOR ADMINISTRATIONSA.

An extension of dispute resolution information is available at the Internet address https://www.esfirma.com

Accreditations and quality seals

No stipulation.

Linking with the list of providers

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

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 referral process email to the address info@esfirma.com