Disclosure Text (PDS) of the Electronic Time Stamp Qualified Authority Certificate

Index

Electronic seal certificate of Authority Qualified Electronic Time Stamp

INFORMATIVE TEXT - PDS

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

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

General information

Documentary control

Security classification:	Public
Destination entity:	ESFIRMA
Version:	1.6

Version control

Version	Changing parts	Description of the change	Author of the change	Date of change
1.0	Original	Creation of the document	esFIRMA	7/05/2017
1.4		Submissions/Corrections	esFIRMA	7/06/2017
1.5	1.1 -1.3 8.6	Change of name	esFIRMA	6/11/2017
1.6	1.3	Reference to esFIRMA's website is added.	esFIRMA	21/04/2023

1. Contact information

1.1. Responsible organization

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

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

1.2. Contact

For any inquiries, please contact:

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

1.3. Contact for revocation processes

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

ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (ESFIRMA)
CALLE BARI 39 (BINARY BUILDING EDIF.)
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	In accordance with the hierarchy of esFIRMA
0.4.0.194112.1.1	In accordance with the EU policy (QCP-l)

The Qualified Electronic Time Stamp Authority certificates are certificates qualified in accordance with Article 38 and Annex III of Regulation (EU) 910/2014 of the European Parliament and of the Council, of July 23, 2014, and comply with the provisions of the technical regulations identified with the references ETSI EN 319 412-3, ETSI EN 319 421, and ETSI EN 319 422.

These certificates allow the signing of digital evidence of electronic time.

The usage information in the certificate profile indicates the following:

a) The "key usage" field has enabled, and therefore allows us to perform, the following functions:
    a. Compromiso con el contenido (Content commitment, to perform the electronic signature function)
b) In the "extKeyUsage" field, the indication is activated:
    a. timeStamping" to perform the electronic time stamping function.
c) In the "Qualified Certificate Statements" field, the following statement appears:
    a. qCCompliance (0.4.0.1862.1.1), which reports that the certificate is issued as qualified.
d) The "User Notice" field describes the use of this certificate.

2.1. Issuing Certification Authority

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

3. Certificate usage limits

3.1. Usage limits aimed at signatories

The qualified electronic time stamping service provided by ESFIRMA must be used exclusively for the authorized uses in the contract signed between ESFIRMA and the SUBSCRIBER, which are subsequently reproduced (section "obligations of the signatories").

The electronic time stamping service must be used in accordance with the instructions, manuals, or procedures provided by ESFIRMA.

Any law and regulation that may affect the use of the cryptographic tools employed must be complied with.

Inspection, alteration, or reverse engineering measures of ESFIRMA's electronic time-stamping services cannot be adopted without prior express permission.

3.2. Usage limits aimed at verifiers

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

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

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

The certificates have not been designed, cannot be used for and are not authorized for use or resale as equipment for controlling dangerous situations or for uses that require fail-safe performance, such as the operation of nuclear facilities, air navigation or communication systems, or weapon control systems, where a failure could directly result in death, personal injury, or severe environmental damage.

The limits indicated in the various fields of the certificate profiles must be taken into account, visible on the ESFIRMA website https://www.esfirma.com

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

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

4. Obligations of the subscribers

4.1. Key generation

The subscriber authorizes ESFIRMA to generate the private and public keys for the issuance of this certificate.

4.2. Certificate request

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

4.3. Information obligations

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

The subscriber must immediately inform ESFIRMA:

- Of any inaccuracy detected in the certificate once it has been issued.
- Of the changes that occur in the information provided and/or registered for the issuance of the certificate.
- From the loss, theft, misappropriation, or any other type of loss of control of the private key by the custodian.

4.4. Custody obligations

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

To safeguard the personal identification code or any technical support provided by ESFIRMA, the private keys, and, if necessary, the ESFIRMA-owned specifications that are supplied to them.

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

4.5. Obligations of proper use

The certificate must be used exclusively for the authorized uses in the DPC and in any other instruction, manual, or procedure provided to the subscriber.

Any law and regulation that may affect your right to use the cryptographic tools employed must be complied with.

Inspection, alteration, or decompilation measures of the digital certification services provided cannot be adopted.

Additionally:

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

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

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

4.6. Prohibited transactions

It indicates the obligation not to use private keys, certificates, or any other technical support provided by ESFIRMA in carrying out any transaction prohibited by applicable law.

The digital certification services (and electronic time stamping services) provided by ESFIRMA have not been designed nor allow their use or resale as equipment for controlling hazardous situations, or for uses that require fail-safe actions, such as the operation of nuclear facilities, air navigation or communication systems, air traffic control

systems, or weapon control systems, in which an error could directly cause death, physical harm, or serious environmental damage.

5. Obligations of the verifiers

5.1. Informed decision

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

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

5.2. Time stamp verification requirements

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

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

- It is necessary to ensure that the identified certificate chain is the most suitable for the time stamp being verified, since a time stamp can be based on more than one

certificate chain, and it is the verifier's decision to ensure the use of the most suitable chain to verify it.

- It is necessary to check the revocation status of the certificates in the chain with the information provided to the ESFIRMA Registry (with LRCs, for example) to determine the validity of all the certificates in the certificate chain, since a time stamp can only be considered correctly verified if each and every one of the certificates in the chain are correct and in force.

- It is necessary to ensure that all certificates in the chain authorize the use of the private key by the certificate subscriber, since there is the possibility that some of the certificates include usage limits that prevent trust in the time stamp being verified. Each certificate in the chain has an indicator that refers to the applicable usage conditions, for review by the verifiers.

- It is necessary to technically verify the signature of all the certificates in the chain before trusting the certificate used for the electronic time stamping.

5.3. Trust in an unverified certificate

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

5.4. Proper use and prohibited activities

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

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

Additionally, the verifier is obliged not to intentionally compromise the security of the electronic time stamping and certification services of ESFIRMA.

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

5.5. Indemnity clause

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

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

ESFIRMA will not be responsible in any case for any loss of encrypted information that cannot be recovered.

6. Obligations of ESFIRMA

6.1. In relation to the provision of digital certification

ESFIRMA undertakes to:

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

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

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

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

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

6.2. In relation to the checks of the registry

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

In the event that ESFIRMA detects errors in the data that must be included in the certificates or that justify this data, it may make the changes it deems necessary before

issuing the certificate or suspend the issuance process and manage the corresponding incident with the subscriber. In the event that ESFIRMA corrects the data without prior management of the corresponding incident with the subscriber, it must notify the subscriber of the finally certified data.

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

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

6.3. Retention periods

ESFIRMA archives the records corresponding to the requests for issuance and revocation of certificates for at least 15 years.

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

7. Limited warranties and warranty disclaimers

7.1. ESFIRMA's guarantee for digital certification services

ESFIRMA guarantees to the subscriber:

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

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

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

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

ESFIRMA guarantees to the third party that trusts the certificate:

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

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

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

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

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

- That the certificate contains the information that a qualified electronic seal certificate must contain, in accordance with Annex III of the European Parliament and Council Regulation EU 910/2014 of July 23, 2014, and with the additional indications for the creation of qualified time seals in accordance with Article 42 of this same Regulation.

- That, in the event that it generates the subscriber's private keys, their confidentiality is maintained during the process.

- The responsibility of the Certification Entity, within the limits that are established. In no case will ESFIRMA be responsible for fortuitous events and in cases of force majeure.

7.2. Exclusion of warranty

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

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

8. Agreements and policies

8.1. Applicable agreements

The agreements applicable to this certificate are as follows:

- Certification services contract, which regulates the relationship between ESFIRMA and the company subscribing to the certificates.

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

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

8.2. DPC

The certification and time-stamping services of ESFIRMA are technically and operationally regulated by the DPC of ESFIRMA, by its subsequent updates, as well as by complementary documentation.

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

8.3. Privacy policy

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

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

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

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

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

8.4. Privacy policy

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

Likewise, it is considered that the supporting documentation for the approval of the application must be preserved and properly registered, with security and integrity guarantees for a period of 15 years from the expiration of the certificate, even in case of early loss of validity due to revocation.

8.5. Refund policy

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

8.6. Applicable law and competent jurisdiction

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

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

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

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

8.7. Accreditations and quality seals

Without stipulation.

8.8. Linking with the list of providers

https://sedeaplicaciones.minetur.gob.es/Prestadores/

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

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

The requirements contained in sections 9.6.1 (Obligations and liability), 8 (Compliance audit) and 9.3 (Confidentiality) of the ESFIRMA DPC will remain in force after the termination of the service.

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

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