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

Table of Contents

Electronic Stamping Authority Electronic Seal Certificate

INFORMATIVE TEXT - PDS

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

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

General Information

Document control

Safety Rating:	Public
Target entity:	ESFIRMA
Version:	1.7

Version Control

Version	Parts that change	Description of the change	Author of the change	Date of change
1.0	Original	Document creation	esFIRMA	7/05/2017
1.4		Corrections	esFIRMA	7/06/2017
1.5	1.1 -1.3 8.6	Change of name	esFIRMA	6/11/2017
1.6	1.3	A reference to the esFIRMA website has been added.	esFIRMA	21/04/2023
1.7	2 8.6	Reference to BTSP added Reference to dispute resolution procedure added	esFIRMA	05/06/2026

1. Contact Information

1.1. Responsible organization

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

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

1.2. Contact

For any queries, please contact:

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

1.3. Contact for revocation processes

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

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

2. Type and purpose of the certificate

This certificate has the following OIDs and associated declarations of conformity:

- 1.3.6.1.4.1.47281.1.5.2: Own identifier according to the ESFIRMA hierarchy.
- 0.4.0.194112.1.1: EU Policy Identifier (QCP-l)
- 0.4.0.2023.1.1 (itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) best-practices-ts-policy (1): Best Practices Policy Identifier for Timestamps (BTSP).

In accordance with applicable regulatory requirements, ESFIRMA's TSA explicitly supports, supports and includes the BTSP identifier, thereby indicating its formal declaration of conformity with said industry best practice standard.

Electronic Time-Stamping Authority certificates are qualified certificates in accordance with Article 38 and Annex III of Regulation (EU) 910/2014 of the European Parliament and of the Council, of 23 July 2014 and comply with the provisions of the technical regulations identified with ETSI EN 319 412-3 references. 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 activated, and therefore allows us to perform, the following functions:
    a. Content commitment (to perform the electronic signature function)
b) In the "extKeyUsage" field, the following indication is activated:
    a. "timeStamping" to perform the electronic timestamping function.
c) In the "Qualified Certificate Statements" field, the following statement appears:
    a. qCCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.

2.1. Issuing Certificate Authority

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

3. Certificate usage limits

3.1. Usage limits targeting signers

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

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

Any laws and regulations that may affect the use of the cryptographic tools you employ must be complied with.

No inspection, alteration or reverse engineering measures may be taken for ESFIRMA's electronic time-stamping services, without prior express permission.

3.2. Usage limits targeting verifiers

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

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

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

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

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

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

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

4. Obligations of subscribers

4.1. Key generation

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

4.2. Request for certificates

The subscriber undertakes to make requests, when necessary, for these certificates in accordance with the procedure and, if necessary, the technical components supplied by ESFIRMA, in accordance with the provisions of ESFIRMA's statement of certification practices (CPD) and operations documentation.

4.3. Reporting obligations

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

The subscriber must immediately inform ESFIRMA:

- Any inaccuracies detected in the certificate once it has been issued.
- Any changes that occur in the information provided and/or registered for the issuance of the certificate.
- From the loss, theft, theft, 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 the information generated in its 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 specifications owned by ESFIRMA that are supplied to it.

In the event of loss or theft of the certificate's private key, or in the event that it is suspected that the private key has lost reliability for any reason, such circumstances must be immediately notified to ESFIRMA through the subscriber.

4.5. Obligations of correct use

The certificate must be used only for the uses authorized in the DPC and in any other instructions, manuals, or procedures provided to the subscriber.

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

Measures may not be adopted to inspect, alter or decompile the digital certification services provided.

In addition:

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

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

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

4.6. Prohibited transactions

The obligation not to use the private keys, certificates or any other technical support provided by ESFIRMA in the performance of any transaction prohibited by applicable law is indicated.

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

5. Obligations of verifiers

5.1. Informed decision

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

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

5.2. Timestamp Verification Requirements

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

- It is necessary to use the appropriate software for the verification of a timestamp with the algorithms and key lengths authorized in the certificate and/or to execute any other cryptographic operation, and to establish the chain of certificates on which the timestamp to be verified is based, since it is verified using this chain of certificates.
- It is necessary to ensure that the identified chain of certificates is the most suitable for the timestamp being verified, since a timestamp can be based on more than one chain of certificates, and it is the decision of the verifier to ensure that the most appropriate chain is used to verify it.
- It is necessary to check the revocation status of the certificates in the chain with the information provided to 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 current.
- It is necessary to ensure that all certificates in the chain authorize the use of the private key by the certificate subscriber, as there is a possibility that some of the certificates may include usage limits that prevent trusting the timestamp being verified. Each certificate in the chain has an indicator that refers to the applicable conditions of use, for review by verifiers.

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

5.3. Trust in an unverified certificate

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

5.4. Proper Use and Prohibited Activities

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

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

In addition, the verifier undertakes not to intentionally compromise the security of ESFIRMA's public electronic time-stamping or certification services.

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

5.5. Indemnity clause

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

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

ESFIRMA will not be liable under any circumstances for any loss of encrypted information that cannot be recovered.

6. ESFIRMA's obligations

6.1. In relation to the provision of digital certification

ESFIRMA undertakes to:

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

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

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

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

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

6.2. In relation to registration checks

ESFIRMA undertakes to issue certificates based on the data provided by the subscriber, for which it may carry out the checks it deems appropriate.

In the event that ESFIRMA detects errors in the data that must be included in the certificates or that justify this data, it may make the changes it deems necessary before issuing the certificate or suspend the issuance process and manage the corresponding incident with the subscriber. In the event that ESFIRMA corrects the data without prior management of the corresponding incident with the subscriber, it must notify the subscriber of the data finally certified.

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

6.3. Retention periods

ESFIRMA archives the records corresponding to requests for the 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 Disclaimers of Warranties

7.1. ESFIRMA guarantee for digital certification services

ESFIRMA guarantees the subscriber:

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

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

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

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

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

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

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

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

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

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

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

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

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

7.2. Exclusion of Warranty

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

Specifically, ESFIRMA does not warrant any software used by any person to sign, verify signatures, encrypt, decrypt, or otherwise use any digital certificate issued by ESFIRMA, except in cases where there is a written 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 Terms of Service incorporated into the certificate disclosure text or PDS.
- DPC, which regulates the issuance and use of certificates.

8.2. CPD

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

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

8.3. Privacy Policy

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

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

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

However, the subscriber agrees that certain information, personal and otherwise, provided in the certificate application, will be included in its certificates and in the

certificate status check mechanism, and that the aforementioned information will not be confidential, as required by law.

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

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 registration, the protection of access to personal information, and user consent.

Likewise, it is contemplated that the documentation justifying the approval of the application must be kept and duly registered and with guarantees of security and integrity for a period of 15 years from the expiration of the certificate, including all in the event of early loss of validity due to revocation.

8.5. Refund Policy

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

8.6. Applicable law and competent jurisdiction

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

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

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

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

8.7. Accreditations and quality seals

No stipulation.

8.8. Linking to the list of providers

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

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

The clauses of this disclosure text are independent of each other, which is why, if any clause is considered invalid or unenforceable, the rest of the clauses of the PDS will continue to be applicable, unless expressly agreed otherwise by the parties.

The requirements contained in sections 9.6.1 (Obligations and Responsibility), 8 (Compliance Audit) and 9.3 (Confidentiality) of the ESFIRMA DPC will continue to apply after termination of the service.

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

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