

Disclosure Text (TSADS) for Electronic Time Stamps



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 2.1-2.3	Change of name	esFIRMA	6/11/2017
1.6	1.3, 3, 3.8	A reference to the esFIRMA website (1.3) has been added. Added information about service availability (3.8). Accepted hashing algorithms	esFIRMA	21/04/2023
1.7	3 3.13	Reference to BTSP added Reference to dispute resolution procedure added	esFIRMA	05/06/2026

Table of Contents

1. Entire Agreement	6
1.1. Severability of Terms, Survival, Entire Agreement and Notice	6
2. Contact Information	6
2.1. Responsible organization	6
2.2. Contact.....	7
2.3. Contact for revocation processes.....	7
3. Types and Uses of Electronic Time Stamps.....	7
3.1. Validating certificates	8
3.2. Subscribers	8
3.3. Issuing Sealing Entity	9
3.4. User community and applicability	9
3.5. Certificate usage limits	9
3.5.1. Time accuracy on qualified electronic time stamp	9
3.6. Obligations of subscribers	9
3.7. Obligations of verifiers	10
3.7.1. Informed decision.....	10
3.7.2. Electronic signature verification requirements for the electronic timestamp	10
3.7.3. Reliance on an unverified electronic signature corresponding to a qualified electronic time stamp	10
Effect of verification	10
3.7.4.....	10
3.7.5. Proper Use and Prohibited Activities	10
3.8. ESFIRMA's obligations	11
3.9. Limited Warranties and Disclaimers of Warranties	11

3.9.1.	ESFIRMA Guarantee for Qualified Electronic Time Stamping Services	11
3.9.2.	Exclusion of Warranty	12
3.10.	Applicable Agreements and DPCs	12
3.10.1.	Applicable Agreements.....	12
3.10.2.	CPD	12
3.11.	Privacy Policy	13
3.12.	Refund Policy	13
3.13.	Applicable law, competent jurisdiction and regime of claims and disputes.....	13
3.14.	Accreditations and quality seals	13
3.15.	Accreditations and Compliance Audits	13

INFORMATIVE TEXT - TSADS

This document contains the essential information to know in relation to the qualified electronic time stamping service of the ESFIRMA Certification Body.

This document follows the structure defined in Annex B of the ETSI EN 319 421-1 standard.

1. Entire Agreement

This document provides high-level statements regarding esFIRMA's Electronic Time-Stamping qualified service.

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

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

The requirements contained in the "Obligations and Liability", "Compliance Audit" and "Confidentiality" sections of the esFIRMA DPC will continue to apply after the 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 following addresses:

- info@esfirma.com, by esFIRMA
- The electronic address, indicated by the subscriber in the contract with ESPUBLICO SERVICIOS PARA LA ADMINISTRACION S.A.

2. Contact Information

2.1. Responsible organization

The ESFIRMA Electronic Time-Stamping Qualified Authority, 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
--

2.2. Contact

For any queries, please contact:

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

2.3. 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
--

3. Types and Uses of Electronic Time Stamps

ESFIRMA's qualified electronic time-stamping service is operated under the entity's own Time-Stamping Policy (TSP) with the OID: 1.3.6.1.4.1.47281.1.5.2.

In accordance with the regulatory requirements in force to indicate its declaration of conformity to subscribers and third parties who rely on the service, ESFIRMA admits, supports and includes in the issued timestamps the explicit declaration of conformity with the **Best Practice Policy for Timestamps (BTSP)**, identified by the OID standard 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)).

By including this object identifier in the timestamp, ESFIRMA's TSA explicitly declares the service's compliance with said best practice policy.

Electronic time stamps declared as qualified follow the indications of EU Regulation 910/2014 and the TSA certificate is issued under the policy declared in ETSI EN 319 411-2.

Customers who receive this electronic stamping service are obliged to comply with the provisions of current regulations, to respect the provisions of the contracts signed with this Sealing Authority, to verify the correctness of the signature of the time stamp, the validity of the TSA certificate, as well as to verify that the hash of the time stamp matches the one that was sent.

Object identifiers (OIDs) of cryptographic algorithms:

RSA Public Key (1.2.840.113549.1.1.1)

SHA-256 With RSA Encryption (1.2.840.113549.1.1.11)

SHA-512 With RSA Encryption (1.2.840.113549.1.1.13)

EC PublicKey (1.2.840.10045.2.1):

- params: 1.3.132.0.35 (NIST-P521)
- params: 1.3.132.0.34 (NIST-P384)
- params: 1.2.840.10045.3.1.7 (NIST-P256)

ECDSA With SHA-512 (1.2.840.10045.4.3.4)

ECDSA With SHA-384 (1.2.840.10045.4.3.3)

ECDSA With SHA-256 (1.2.840.10045.4.3.2)

Accepted hashing algorithms:

- 2.16.840.1.101.3.4.2.1 Secure Hash Algorithm that uses a 256 bit key (SHA256)
- 2.16.840.1.101.3.4.2.3 Secure Hash Algorithm that uses a 512 bit key (SHA512)

3.1. Validating certificates

The lists of revoked certificates and OCSP services can be found on the esFIRMA website and at the URLs indicated on each of the certificates.

3.2. Subscribers

The Subscriber is the natural or legal person who has contracted ESFIRMA's electronic time-stamping services.

3.3. Issuing Sealing Entity

The qualified electronic time stamping services are issued by ESFIRMA, identified by the data indicated above.

3.4. User community and applicability

The users of the service will mainly be the applications and/or systems of the customers (natural or legal persons) who have contracted these ESFIRMA services.

The electronic time-stamping services provided by the ESFIRMA TSA are included as services provided by ESFIRMA, before the national supervisor, in compliance with current technical and legal regulations.

3.5. Certificate usage limits

Electronic time stamps limit their use in the applications and/or systems of customers (natural or legal persons) who have contracted these services.

Electronic timestamps will not be used for purposes other than those specified above.

3.5.1. Time accuracy on qualified electronic time stamp

ESFIRMA's Qualified Time Stamping service is based on the use of the NTP protocol.

The time value on the TSU is traceable to a time value distributed by a UTC(k) laboratory, the ROA (Royal Navy Observatory) and maintains clock accuracy with at least four STRATUM-1 time sources. If the clock is detected to be deviated from UTC from the specified accuracy (equal to or greater than one second), no timestamps are issued.

3.6. Obligations of subscribers

The subscriber undertakes to:

- To make requests for qualified electronic time stamps in accordance with the procedure and, if necessary, the technical components supplied by ESFIRMA, in accordance with what is established in the declaration of certification practices

(DPC) and in the documentation of ESFIRMA.

- Follow the instructions specified in the PDS of the ESFIRMA TSA certificate.
- Verify the electronic signatures of electronic time stamps, including the validity of the certificate used.
- Use electronic timestamps within the limits and scope described in this TSADS.

3.7. Obligations of verifiers

3.7.1. Informed decision

The verifier undertakes to comply with the technical, operational and safety requirements described in the ESFIRMA DPC .

3.7.2. Electronic signature verification requirements for the electronic timestamp

- The check will normally be carried out automatically by the verifier's software and, in any case, in accordance with the DPC and TSADS.

3.7.3. Reliance on an unverified electronic signature corresponding to a qualified electronic time stamp

If the verifier relies on an electronic signature corresponding to an unverified electronic qualified time stamp, he will assume all the risks arising from this action.

3.7.4. Effect of verification

By virtue of the correct verification of electronic time-stamp certificates, in accordance with this informative text (PDS), the verifier can rely on the information provided.

3.7.5. Proper Use and Prohibited Activities

The verifier undertakes not to use any type of information on the status of the electronic or any other type of qualified time stamps 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 ESFIRMA's public certification services, without prior written consent.

In addition, the verifier undertakes not to intentionally compromise the security of ESFIRMA's time-stamping utilities.

The qualified electronic time stamping services provided by ESFIRMA have not been designed and do not allow the 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 weapons control systems, where a mistake could cause death, physical harm or serious environmental damage.

3.8. ESFIRMA's obligations

In relation to the provision of the qualified electronic time-stamping service , ESFIRMA undertakes to:

- a) To issue, deliver and administer the qualified stamps, 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) Keep the service available 24 hours a day, every day of the year, except for external circumstances or maintenance operations, in which case the best efforts will be made to ensure that the service remains inactive for the shortest possible time.

3.9. Limited Warranties and Disclaimers of Warranties

3.9.1. ESFIRMA Guarantee for Qualified Electronic Time Stamping Services

ESFIRMA guarantees the subscriber that the time stamps comply with all the material requirements established in the DPC.

ESFIRMA warrants to the relying third party on the qualified electronic time stamp that the information contained in or incorporated by reference into the stamp is correct, except where otherwise indicated.

In addition, ESFIRMA guarantees the subscriber and the third party that relies on the time stamp the responsibility of the Certification Body, within the limits that are established, without ESFIRMA being liable in any case for fortuitous events and in the event of force majeure.

3.9.2. Exclusion of Warranty

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

3.10. Applicable Agreements and DPCs

3.10.1. Applicable Agreements

The agreements applicable to the qualified electronic time stamp are as follows:

- Electronic stamping services contract, which regulates the relationship between ESFIRMA and the company that has contracted the qualified electronic time stamps.
- General Terms of Service incorporated into the TSA certificate disclosure text (PDS).
- The conditions incorporated in this text-disclosure of electronic time stamps
- DPCs, which regulate the issuance and use of qualified electronic time-stamp certificates.

3.10.2. CPD

ESFIRMA's qualified electronic 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>

3.11. Privacy Policy

See section 9.4 of the ESFIRMA DPC

3.12. Refund Policy

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

3.13. Applicable law, competent jurisdiction and regime of claims and disputes

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 ESFIRMA.

3.14. Accreditations and quality seals

No stipulation.

3.15. Accreditations and Compliance Audits

ESFIRMA is included in the Spanish list of trusted providers (TSL) <https://sedediatid.mineco.gob.es/Prestadores/TSL/TSL.pdf>

It is also registered as a qualified electronic trust service provider with the Ministry of Economic Affairs and Digital Transformation:

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

In accordance with the provisions of EU Regulation 910/2014, ESFIRMA will carry out conformity audits every 2 years.

