

Texto de Divulgación (TSADS) para los Sellos de Tiempo Electrónico



Información general

Control documental

Clasificación de seguridad:	Público
Entidad de destino:	ESFIRMA
Versión:	1.7

Control de versiones

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
1.0	Original	Creación del documento	esFIRMA	7/05/2017
1.4		Subsanaciones	esFIRMA	7/06/2017
1.5	1.1 2.1-2.3	Cambio de denominación	esFIRMA	6/11/2017
1.6	1.3, 3, 3.8	Se añade referencia a web de esFIRMA (1.3). Se añade información sobre disponibilidad del servicio (3.8). Algoritmos de huella resumen (hash) aceptados	esFIRMA	21/04/2023
1.7	3 3.13	Se añade referencia a la BTSP Se añade referencia al procedimiento de resolución de disputas	esFIRMA	05/06/2026

Índice

1.	Acuerdo completo	6
1.1.	Divisibilidad de las cláusulas, supervivencia, acuerdo íntegro y notificación	6
2.	Información de contacto	6
2.1.	Organización responsable	6
2.2.	Contacto	7
2.3.	Contacto para procesos de revocación	7
3.	Tipos y usos de los sellos de tiempo electrónico	7
3.1.	Validación de los certificados	8
3.2.	Suscriptores	9
3.3.	Entidad de Sellado emisora	9
3.4.	Comunidad de usuarios y aplicabilidad	9
3.5.	Límites de uso del certificado	9
3.5.1.	Exactitud de la hora en el sello cualificado de tiempo electrónico.....	9
3.6.	Obligaciones de los suscriptores	10
3.7.	Obligaciones de los verificadores	10
3.7.1.	Decisión informada.....	10
3.7.2.	Requisitos de verificación de la firma electrónica correspondiente al sello cualificado de tiempo electrónico.....	10
3.7.3.	Confianza en una firma electrónica no verificada correspondiente a un sello cualificado de tiempo electrónico	10
	Efecto de la verificación.....	11
3.7.4.		11
3.7.5.	Uso correcto y actividades prohibidas	11
3.8.	Obligaciones de ESFIRMA	11
3.9.	Garantías limitadas y rechazo de garantías.....	12

- 3.9.1. Garantía de ESFIRMA por los servicios de sellado cualificado de tiempo electrónico.....12
- 3.9.2. Exclusión de la garantía12
- 3.10. Acuerdos aplicables y DPC.....12
 - 3.10.1. Acuerdos aplicables12
 - 3.10.2. DPC13
- 3.11. Política de privacidad.....13
- 3.12. Política de reintegro13
- 3.13. Ley aplicable, jurisdicción competente y régimen de reclamaciones y disputas
13
- 3.14. Acreditaciones y sellos de calidad14
- 3.15. Acreditaciones y auditorías de conformidad14

TEXTO DIVULGATIVO - TSADS

Este documento contiene las informaciones esenciales a conocer en relación con el servicio cualificado de sellado de tiempo electrónico de la Entidad de Certificación ESFIRMA.

Este documento sigue la estructura definida en el Anexo B de la norma ETSI EN 319 421-1.

1. Acuerdo completo

El presente documento proporciona declaraciones de alto nivel con respecto al servicio de Sellado cualificado de tiempo electrónico de esFIRMA.

1.1. Divisibilidad de las cláusulas, supervivencia, acuerdo íntegro y notificación

Las cláusulas del presente texto de divulgación son independientes entre sí, motivo por el cual, si cualquier cláusula es considerada inválida o inaplicable, el resto de las cláusulas de esta TSADS seguirán siendo aplicables, excepto acuerdo expreso en contrario de las partes.

Los requisitos contenidos en las secciones de “Obligaciones y responsabilidad”, de “Auditoría de conformidad” y de “Confidencialidad” de la DPC de esFIRMA continuarán vigentes tras la terminación del servicio.

Este texto contiene la voluntad completa y todos los acuerdos entre las partes.

Las partes se notifican hechos mutuamente mediante un procedimiento de envío de email a las siguientes direcciones:

- info@esfirma.com, por parte de esFIRMA
- La dirección electrónica, indicada por el suscriptor en el contrato con ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA.

2. Información de contacto

2.1. Organización responsable

La Autoridad de Sellado Cualificado de Tiempo Electrónico de ESFIRMA, en lo sucesivo “ESFIRMA”, es una iniciativa de:

ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (ESFIRMA) CALLE BARI 39 (EDIF. BINARY BUILDING)
--

50197 - ZARAGOZA
(+34) 976300110

2.2. Contacto

Para cualquier consulta, diríjense a:

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

2.3. Contacto para procesos de revocación

El proceso para solicitar la revocación de un certificado se puede consultar en www.esfirma.com. Para cualquier otra consulta al respecto, diríjense a:

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

3. Tipos y usos de los sellos de tiempo electrónico

El servicio de sellado cualificado de tiempo electrónico de esFIRMA se opera bajo la Política de Sellado de Tiempo (TSP) propia de la entidad con el OID: 1.3.6.1.4.1.47281.1.5.2.

De acuerdo con las exigencias normativas vigentes para indicar su declaración de conformidad ante suscriptores y terceros que confían en el servicio, esFIRMA admite, soporta e incluye en las marcas de tiempo emitidas la declaración explícita de conformidad con la **Política de mejores prácticas para marcas de tiempo (BTSP)**,

identificada mediante el OID estándar 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)).

Al incluir este identificador de objeto en la marca de tiempo, la TSA de ESFIRMA declara explícitamente la conformidad del servicio con dicha política de mejores prácticas.

Los sellos de tiempo electrónico declarados como cualificados siguen las indicaciones del Reglamento UE 910/2014 y el certificado de la TSA es expedido bajo la política declarada en ETSI EN 319 411-2.

Los clientes que reciben este servicio de sellado electrónico están obligados a cumplir con lo dispuesto por la normativa vigente, a respetar lo indicado en los contratos firmados con esta Autoridad de Sellado, verificar la corrección de la firma del sello de tiempo, la validez del certificado de la TSA, así como verificar que el hash del sello de tiempo coincide con el que se envió.

Identificadores de objeto (OID) de los algoritmos criptográficos:

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)

Algoritmos de huella resumen (hash) aceptados:

- 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. Validación de los certificados

Las listas de certificados revocados y servicios OCSP se encuentran en la web de esFIRMA y en las URL indicadas en cada uno de los certificados.

3.2. Suscriptores

El Suscriptor es la persona física o jurídica que ha contratado los servicios de sellado de tiempo electrónico de ESFIRMA.

3.3. Entidad de Sellado emisora

Los servicios de sellado cualificado de tiempo electrónico son emitidos por ESFIRMA, identificada mediante los datos indicados anteriormente.

3.4. Comunidad de usuarios y aplicabilidad

Los usuarios del servicio serán principalmente las aplicaciones y/o sistemas de los clientes (personas físicas o jurídicas) que han contratado estos servicios de ESFIRMA.

Los servicios de sellado de tiempo electrónico proporcionados por la TSA de ESFIRMA se incluyen como servicios proporcionados por ESFIRMA, ante el supervisor nacional, cumpliendo las normativas técnicas y legales vigentes.

3.5. Límites de uso del certificado

Los sellos de tiempo electrónico limitan su uso en las aplicaciones y/o sistemas de los clientes (personas físicas o jurídicas) que han contratado estos servicios.

No se utilizarán los sellos de tiempo electrónico para fines distintos de los especificados anteriormente.

3.5.1. Exactitud de la hora en el sello cualificado de tiempo electrónico

El servicio de Sellado Cualificado de Tiempo de ESFIRMA se basa en el uso del protocolo NTP.

El valor de tiempo en la TSU es trazable hasta un valor de tiempo distribuido por un laboratorio UTC(k), el ROA (Real Observatorio de la Armada) y mantiene la precisión de reloj con por lo menos cuatro fuentes de tiempo STRATUM-1. Si se detecta que el reloj

está desviado respecto a UTC de la precisión especificada (igual o mayor a un segundo), no se emiten sellos de tiempo.

3.6. Obligaciones de los suscriptores

El suscriptor se obliga a:

- Realizar las solicitudes de sellos cualificados de tiempo electrónico de acuerdo con el procedimiento y, si es necesario, los componentes técnicos suministrados por ESFIRMA, de conformidad con lo que se establece en la declaración de prácticas de certificación (DPC) y en la documentación de ESFIRMA.
- Seguir las indicaciones especificadas en la PDS del certificado de TSA de ESFIRMA.
- Verificar las firmas electrónicas de los sellos de tiempos electrónicos, incluyendo la validez del certificado usado.
- Usar los sellos de tiempo electrónicos dentro de los límites y el ámbito descritos en esta TSADS.

3.7. Obligaciones de los verificadores

3.7.1. Decisión informada

El verificador se compromete a cumplir los requisitos técnicos, operativos y de seguridad descritos en la DPC de ESFIRMA.

3.7.2. Requisitos de verificación de la firma electrónica correspondiente al sello cualificado de tiempo electrónico

- La comprobación será ejecutada normalmente de forma automática por el software del verificador y, en todo caso, de acuerdo con la DPC y ésta TSADS.

3.7.3. Confianza en una firma electrónica no verificada correspondiente a un sello cualificado de tiempo electrónico

Si el verificador confía en una firma electrónica correspondiente a un sello cualificado de tiempo electrónico no verificada, asumirá todos los riesgos derivados de esta actuación.

3.7.4. Efecto de la verificación

En virtud de la correcta verificación de los certificados de sello de tiempo electrónico, de conformidad con este texto divulgativo (PDS), el verificador puede confiar en la información suministrada.

3.7.5. Uso correcto y actividades prohibidas

El verificador se obliga a no utilizar ningún tipo de información de estado de los sellos cualificados de tiempo electrónico o de ningún otro tipo que haya sido suministrada por ESFIRMA, en la realización de transacción alguna prohibida para la ley aplicable a la citada transacción.

El verificador se obliga a no inspeccionar, interferir o realizar ingeniería inversa de la implantación técnica de los servicios públicos de certificación de ESFIRMA, sin previo consentimiento escrito.

Adicionalmente, el verificador se obliga a no comprometer intencionadamente la seguridad de los servicios públicos de sellado de tiempo de ESFIRMA.

Los servicios de sellado cualificado de tiempo electrónico prestados por ESFIRMA no han sido diseñados ni permiten la utilización o reventa, como equipos de control de situaciones peligrosas o para usos que requieran actuaciones a prueba de errores, como la operación de instalaciones nucleares, sistemas de navegación o comunicación aérea, sistemas de control de tráfico aéreo, o sistemas de control de armamento, donde un error podría causar la muerte, daños físicos o daños medioambientales graves.

3.8. Obligaciones de ESFIRMA

En relación con la prestación del servicio de sellado cualificado de tiempo electrónico ESFIRMA se obliga a:

- a) Emitir, entregar y administrar los sellos cualificados, de acuerdo con las instrucciones suministradas por el suscriptor, en los casos y por los motivos descritos en la DPC de ESFIRMA.

- b) Ejecutar los servicios con los medios técnicos y materiales adecuados, y con personal que cumpla las condiciones de cualificación y experiencia establecidas en la DPC.
- c) Cumplir los niveles de calidad del servicio, en conformidad con lo que se establece en la DPC, en los aspectos técnicos, operativos y de seguridad.
- d) Mantener disponible el servicio las 24 horas del día, todos los días del año, salvo por circunstancias ajenas u operaciones de mantenimiento, en cuyo caso se realizarán los mejores esfuerzos por asegurar que el servicio se mantenga inactivo el mínimo tiempo posible.

3.9. Garantías limitadas y rechazo de garantías

3.9.1. Garantía de ESFIRMA por los servicios de sellado cualificado de tiempo electrónico

ESFIRMA garantiza al suscriptor que los sellos de tiempo cumplen con todos los requisitos materiales establecidos en la DPC.

ESFIRMA garantiza al tercero que confía en el sello cualificado de tiempo electrónico que la información contenida o incorporada por referencia en el sello es correcta, excepto cuando se indique lo contrario.

Adicionalmente, ESFIRMA garantiza al suscriptor y al tercero que confía en el sello de tiempo la responsabilidad de la Entidad de Certificación, con los límites que se establezcan, sin que en ningún caso ESFIRMA responda por caso fortuito y en caso de fuerza mayor.

3.9.2. Exclusión de la garantía

ESFIRMA rechaza toda otra garantía diferente a la anterior que no sea legalmente exigible.

3.10. Acuerdos aplicables y DPC

3.10.1. Acuerdos aplicables

Los acuerdos aplicables al sello cualificado de tiempo electrónico son los siguientes:

- Contrato de servicios de sellado electrónico, que regula la relación entre esFIRMA y la empresa que ha contratado los sellos cualificados de tiempo electrónico.
- Condiciones generales del servicio incorporadas en el texto de divulgación (PDS) del certificado de la TSA.
- Las condiciones incorporadas en este texto de divulgación-TSADS de los sellos de tiempo electrónico
- DPC, que regulan la emisión y utilización de los certificados cualificados de sello de tiempo electrónico.

3.10.2. DPC

Los servicios de sellado cualificado de tiempo electrónico de esFIRMA se regulan técnicamente y operativamente por la DPC de esFIRMA, por sus actualizaciones posteriores, así como por documentación complementaria.

La DPC y la documentación de operaciones se modifica periódicamente en el Registro y se puede consultar en la página de Internet: <https://www.esfirma.com>

3.11. Política de privacidad

Ver apartado 9.4 de la DPC de esFIRMA

3.12. Política de reintegro

esFIRMA no reintegrará el coste del servicio de sellado en ningún caso.

3.13. Ley aplicable, jurisdicción competente y régimen de reclamaciones y disputas

Las relaciones con esFIRMA se regirán por la ley española en materia de servicios de confianza vigente en cada momento, así como por la legislación civil y mercantil en lo que sea de aplicación.

La jurisdicción competente es la que se indica en la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

En caso de discrepancia entre las partes, las partes intentarán la previa resolución amistosa. A tal fin, las partes deberán dirigir una comunicación a esFIRMA, rellenando la hoja de quejas y sugerencias disponible en la página web de esFIRMA por cualquier medio

de los allí indicados. La reclamación se tramitará de acuerdo con los procedimientos internos para la resolución de quejas, apelaciones y disputas.

Si las partes no alcanzasen un acuerdo al respecto, cualquiera de ellas podrá someter el conflicto a la jurisdicción civil, con sujeción a los Tribunales del domicilio social de ESFIRMA.

3.14. Acreditaciones y sellos de calidad

Sin estipulación.

3.15. Acreditaciones y auditorías de conformidad

ESFIRMA se encuentra incluida en la lista de prestadores de confianza (TSL) española <https://sedediatid.mineco.gob.es/Prestadores/TSL/TSL.pdf>

Asimismo, está registrada como prestador de servicios electrónicos de confianza cualificados en el Ministerio de Asuntos Económicos y Transformación Digital:

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

De acuerdo con lo indicado en el Reglamento UE 910/2014, ESFIRMA realizará auditorías de conformidad cada 2 años.