Sistemas Informáticos Abiertos, S.A.
Avenida de Europa, 2
Alcor Plaza Edificio B
Parque Oeste, Alcorcón 28922
Alcorcón - Madrid (España)
Telf: (34) 902 480 580 Fax: (34) 91 641 95 13

www.sia.es

PDS – Sellado de Tiempo

Texto divulgativo del Servicio de expedición de sellos electrónicos cualificados de tiempo (TSA)

Fecha: 20/05/2022

SI-0013/2006 STI-01/2008

INDICE

RELACION DE TABLAS

1. ACUERDO COMPLETO

El presente documento recoge la información relativa al Servicio de expedición de sellos electrónicos cualificados de tiempo del Prestador de Servicios de Confianza SIA a un alto nivel. Para la definición de este texto divulgativo, se han seguido las indicaciones de la norma ETSI 319 421 anexo B.

Este documento, no reemplaza a la Política del Servicio de expedición de sellos electrónicos cualificados de tiempo (PC) ni la Declaración de Practicas de certificación (DPC) de SIA, las cuales se encuentran accesibles en la propia WEB del Prestador de Servicios de Confianza (TSP).

Los OID de dichas PC y DPC indicadas anteriormente se corresponden a:

Nombre del documento	OID asignado
Política de Servicio expedición de sellos electrónicos cualificados de tiempo	1.3.6.1.4.1.39131.10.1.6
Declaración Prácticas Certificación (DPC)	1.3.6.1.4.1.39131.10.1.1.1.0

Tabla 1 – OID de PC y DPC de SIA

2. INFORMACIÓN DE CONTACTO

2.1 Organización responsable

Este texto divulgativo es propiedad de SIA.

Nombre	SIA
Dirección correo	psc@sia.es
Dirección postal	Avenida de Europa, 2 Alcor Plaza Edificio B Parque Oeste Alcorcón 28922 Alcorcón - Madrid (España)
Teléfono	+34 902 480 580

Tabla 2 – Organización responsable

2.2 Persona de contacto

Contacto	psc@sia.es
Dirección correo	psc@sia.es
Dirección postal	Avenida de Europa, 2 Alcor Plaza Edificio B Parque Oeste Alcorcón 28922 Alcorcón - Madrid (España)
Teléfono	+34 902 480 580
URL	https://psc.sia.es

Tabla 3 – Persona de contacto

3. TIPOS Y USO DE LOS SELLOS ELECTRONICOS CUALIFICADOS DE TIEMPO

El sellado de tiempo es un mecanismo on-line que permite demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo. Este protocolo se describe en el RFC 3161 "Internet X.509 Public Key Infrastructure Time-Stamp Protocol" y está en el registro de estándares de Internet.

Una Autoridad de Sellado de Tiempo actúa como tercera parte de confianza testificando la existencia de dichos datos electrónicos en una fecha y hora concretos y normalmente se apoya en un software generador de tokens de tiempo.

3.1 Detalle de los certificados empleados

Se ha tenido en cuenta los siguientes estándares y normas europeas en la definición de los certificados de sellado de tiempo emitidos por los sistemas de SIA:

- ETSI EN 319 421: "Policy and Security Requirements for Trust Service Providers issuing Time-Stamps"
- RFC 3161 "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)"
- ETSI EN 319 422 "Time-stamping protocol and time-stamp token profiles"
- ETSI EN 319 412-2 [2] "Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons"
- ETSI EN 319 412-3 [3] "Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons"
- ETSI TS 119 312 "Cryptographic Suites"

El certificado sigue el estándar definido X.509 versión 3. Vinculando la identidad del sellado de tiempo a una determinada clave pública, garantizando la autenticidad y el no repudio.

El identificador del algoritmo criptográfico con Objeto (OID): SHA-256 with RSA Encryption (1.2.840.113549.1.1.11) de 2048 Bits para TSAQC.

El identificador del algoritmo criptográfico con Objeto (OID): SHA-256 with RSA Encryption (1.2.840.113549.1.1.11) de 3072 Bits para TSAQC 2022.

Para validar los certificados empleados en los sellos de tiempo, SIA dispone de un servicio de validación por OCSP y descarga de CRLs, disponibles 24 x 7.

3.2 Formato de emisión de los sellos

La plataforma de TimeStamp está orientada a Servicio mediante protocolo HTTP y formato ASN1 generando sellos de tiempo conforme al RFC3161.

Los clientes deben enviar sus peticiones a través del protocolo http, conformando una petición de sellado de tiempo (time-stamping request) en formato ASN1 y enviarla según corresponda a la URL:

- http://host:port/tspTSA/inputRequestTSA
- http://host:port/tspTSA2022/inputRequestTSA

4. LIMITES DE USO DEL CERTIFICADO

La TSA cuenta con acceso a una fuente de tiempo que garantice la fiabilidad en el proceso de obtención del instante temporal empleado en la creación del sello de tiempo. Para ellos la TSA de SIA está conectada con una fuente de tiempo “stratum 1”, a través del protocolo NTP. Esta fuente de tiempo provee precisión a nivel del microsegundo utilizando sincronización con sistemas vía satélite.

La TSA emite sellados de tiempo con una precisión de tiempo contando con un desfase permitido por debajo del segundo. Esta precisión esta monitorizada constantemente para evitar desvinculaciones derivadas de latencias anormales en la sincronización con la fuente o desfases en los relojes internos de los equipos.

El tiempo durante el cual se mantienen los registros de eventos por parte del prestador de servicios de confianza para emplearlos como evidencias en caso necesario, será el estipulado por la legislación vigente aplicable.

5. OBLIGACIONES DE LOS SUSCRIPTORES

Las obligaciones de los suscriptores serán las estipuladas en los convenios o contratos firmados por parte del prestador de servicios de confianza y las personas o entidades que solicitan los servicios proporcionados por la Autoridad de Sellado de Tiempo.

Se podrá ampliar la información respecto a este apartado en la PC y DPC indicados en el apartado 1 del presente documento.

6. OBLIGACIÓN DE LAS TERCERAS PARTES QUE CONFIAN EN EL SERVICIO DE EXPEDICIÓN DE SELLOS ELECTRÓNICOS CUALIFICADOS DE TIEMPO

Las terceras partes que confíen en los sellos electrónicos cualificados de tiempo de SIA, tendrán lo obligación de conocer los detalles de la policita que aplica a este servicio de expedición. Pudiendo verificar por medios de validación de OCSP y descarga de CRLs indicados, la validez del estado de los certificados de clave pública de la TSU.

Se podrá ampliar la información respecto a este apartado en la PC y DPC indicados en el apartado 1 del presente documento.

7. LIMITACIONES DE RESPONSABILIDAD

Las limitaciones de responsabilidad de los suscriptores serán las estipuladas en los convenios o contratos firmados por parte del prestador de servicios de confianza y las personas o entidades que solicitan los servicios proporcionados por la Autoridad de Sellado de Tiempo.

Se podrá ampliar la información respecto a este apartado en la PC y DPC indicados en el apartado 1 del presente documento.

8. ACUERDOS APLICABLES, DPC Y PC

La PC y DPC ya indicadas detallaran los acuerdos aplicables, al igual que en los convenios o contratos firmados por parte del prestador de servicios de confianza y las personas o entidades que solicitan los servicios proporcionados por la Autoridad de Sellado de Tiempo.

Se podrá ampliar la información respecto a este apartado en la PC y DPC indicados en el apartado 1 del presente documento.

9. POLÍTICA DE PRIVACIDAD

El prestador de servicios de confianza SIA, aplica la política de protección de datos personales vigente en España. Incorporando a un fichero registrado en la Agencia de Protección de Datos especifico del TSP.

Toda la información recabada será almacenada por el TSP según lo estipulado por la legislación vigente aplicable.

10. POLÍTICA DE REEMBOLSO

La política de reembolso será la estipulada en los convenios o contratos firmados por parte del prestador de servicios de confianza y las personas o entidades que solicitan los servicios proporcionados por la Autoridad de Sellado de Tiempo.

Se podrá ampliar la información respecto a este apartado en la PC y DPC indicados en el apartado 1 del presente documento.

11. LEGISLACIÓN APLICABLE Y RESOLUCIÓN DE CONFLICTOS

11.1 Legislación aplicable

La normativa aplicable al presente documento, así como a las distintas PC, y a las operaciones que derivan de ellas, es la siguiente:

- Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (en adelante eIDAS) y por el que se deroga la Directiva 1999/93/CE.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

11.2 Resolución de conflictos

Para la resolución de cualquier conflicto que pudiera surgir en relación con este documento, las PC o el instrumento Jurídico vinculante, las partes, con renuncia a cualquier otro fuero que pudiera corresponderles a los Tribunales de Justicia de Madrid.

12. ACREDITACIONES DE CONFIANZA Y AUDITORIAS DE CONFORMIDAD

Conforme a lo establecido en el Reglamento eIDAS y la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, el Prestador de Servicios de Confianza SIA se encuentra incluido en:

- TSL; Lista de Prestadores de Confianza Española.
- Portal de Prestadores de Servicios de Confianza del Organismo Supervisor.

Así mismo, el TSP SIA cuenta con el Informe de evaluación de la conformidad en el marco del reglamento (UE) nº 910/2014, relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior (reglamento eIDAS).