SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA
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

psc.sia.es

TSA - SIA

Política de sellado de tiempo (TSA)

OID: 1.3.6.1.4.1.39131.10.1.6

Versión: 1.0

HISTÓRICO DE CONTROL DE CAMBIOS DEL DOCUMENTO

Revisión	Fecha	Autor	Descripción
1.0	22 de octubre de 2015	SIA	Primera versión del documento

INDICE

RELACION DE TABLAS

1. INTRODUCCIÓN

1.1 Resumen

El presente documento recoge la Política correspondiente al servicio de sellado de tiempo de la Autoridad de Certificación (en adelante AC) del prestador de servicios de certificación, Sistemas Informáticos Abiertos Sociedad Anónima (en adelante SIA), que emite certificados reconocidos según la Ley 59/2003, de 19 de diciembre, de firma electrónica.

En este contexto, se establecen las reglas a emplear por la Autoridad de Sellado de Tiempo, conforme a la norma ETSI TS 102 023 v1.2.2 "Policy requirements for time-stamping authorities" y al documento RFC-3161 "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

Esta política, sirve de guía en la relación entre SIA y las partes conjuntas a los suscriptores de los servicios telemáticos. En consecuencia, todas las partes involucradas tienen la obligación de conocer esta política y ajustar su actividad a lo dispuesto en la misma.

En esta Política se detalla y completa lo estipulado en la Declaración de Prácticas de Certificación (en adelante DPC) del Prestador de Servicios de Certificación de SIA, conteniendo las reglas a las que se sujeta el uso del servicio definido, así como el ámbito de aplicación y las características técnicas.

Esta PC asume que el lector conoce los conceptos básicos de PKI, certificado y firma electrónica, en caso contrario se recomienda al lector que se forme en el conocimiento de los anteriores conceptos antes de continuar con la lectura del presente documento.

1.2 Nombre del documento e identificación

Nombre del documento	Política de sellado de tiempo
Versión del documento	1.0
Estado del documento	Vigente
Fecha de emisión	10/09/2015

Fecha de caducidad	No aplicable
OID	1.3.6.1.4.1.39131.10.1.6
Ubicación de la Política	https://psc.sia.es/
DPC relacionada	Declaración de Prácticas de Certificación de la PKI de SIA OID 1.3.6.1.4.1.39131.10.1.1.1.0 Disponible en https://psc.sia.es/

Tabla 1 – Datos identificación Política de sellado de tiempo

1.3 Entidades y personas intervinientes

Las entidades y personas intervinientes son:

- SIA como Autoridad de Certificación, emisor del certificado de TSA.
- SIA como órgano competente de la Autoridad de Sellado de Tiempo (TSA).
- Los Suscriptores.
- Las Terceras partes aceptantes de los certificados y sellos de tiempo emitidos.

1.3.1 Autoridad de Certificación

SIA actúa como Autoridad de Certificación (AC) relacionando una determinada clave pública con un sujeto o entidad concretos a través de la emisión de certificados electrónicos.

Las Autoridades de Certificación que componen la PKI de SIA son:

- "AC raíz" Autoridad de Certificación de primer nivel. Esta AC solo emite certificados para sí misma y sus AC Subordinadas. Únicamente estará en funcionamiento durante la realización de las operaciones para las que se establece.
- "AC subordinada": Autoridad de Certificación subordinada de "AC raíz". Su función es la emisión de certificados electrónicos, como por ejemplo la emisión del Certificado de Servidor de Sellado de Tiempo (TSA).

1.3.2 Autoridades de Sellado de tiempo

La Autoridad de Sellado de Tiempo, es el elemento de confianza, que actúa como tercera parte vinculando una representación de un dato electrónico a una fecha y hora concretos, garantizando que el dato electrónico existió en un determinado tiempo mediante la expedición de tokens de sellos de tiempo.

1.3.3 Suscriptor

Persona o entidad que solicita los servicios proporcionados por la Autoridad de Sellado de Tiempo. Por medio de un convenio podrán solicitar sellos durante un periodo de tiempo estipulado, o bien si acuerdan otras condiciones de contratación, por ejemplo por volumen de sellos solicitados.

1.3.4 Terceras Partes

Las terceras partes aceptantes, son las personas físicas o jurídicas que deciden aceptar y confiar en un sello de tiempo emitido por la autoridad de sellado de tiempo de SIA. Y como tales, les es de aplicación lo establecido por la presente Política de sellado de tiempo cuando deciden confiar en estos.

1.4 Uso de los sellos de tiempo

Un sello emitido por la Autoridad de sellado de tiempo de SIA sólo puede ser utilizado para los propósitos explícitamente permitidos e indicados en esta Política y en la correspondiente Declaración de Practicas de Certificación, por lo que existen ciertas limitaciones en el uso de estos, dado que se emplean para garantizar la existencia de datos electrónicos en un determinado tiempo de cualquier organismo o entidad con el que se haya formalizado un convenio de certificación.

1.4.1 Usos apropiados y permitidos de los sellos de tiempo

Los sellos deben emplearse para cualquier tipo de documento firmado o no electrónicamente, y para cualquier tipo de objeto digital, inclusive código ejecutable, garantizándose la existencia de dicho contenido en un determinado tiempo.

Otro uso permitido de sello, es para el resellado, es decir, solicitud de un sello sobre otro anteriormente expedido.

1.4.2 Limitaciones y restricciones en el uso de los sellos de tiempo

De forma general según lo establecido en la Declaración de Practicas de Certificación de SIA, y tras aceptar sus condiciones de uso.

De forma específica, cabe reseñar que este sello de tiempo será utilizado por los firmantes en las relaciones que mantengan con terceros que confían, y en conformidad con sus limitaciones de uso.

1.5 Administración de Políticas

1.5.1 Organización responsable

Esta Política es propiedad de SIA.

Nombre	SIA
Dirección correo	info@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. ASPECTOS GENERALES

2.1 Servicio de sellado 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 (TSP)" 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.

Los pasos para generar un sello de tiempo son los siguientes:

- El cliente calcula el hash del documento a sellar.
- El cliente envía una solicitud de sello de tiempo a una URL determinada siguiendo el protocolo RFC 3161, incluyendo el hash del documento a sellar.
- La TSA recibe la petición, revisa si la petición está completa y correcta.
- Si el resultado es correcto, la TSA firma la petición generando un Sello de Tiempo (incluyendo el hash del documento, la fecha y hora obtenida de una fuente fiable y la firma electrónica de la TSA).
- El sello de tiempo se envía de vuelta al Cliente.
- El Cliente debe validar la firma del sello y guardarlo debidamente.
- La TSA mantiene un registro de los sellos emitidos para su futura verificación.

2.1.1 Componentes del servicio

Los dos componentes de la TSA, en que se resumen principalmente la prestación del servicio son:

- TSU, componente del sistema de TSA encargado de proteger y generar los Sellos de Tiempo en nombre de la TSA.
- Fuente de tiempo fiable, que determine el instante de creación de dicho sello de tiempo de manera fehaciente.

2.1.2 Acceso al servicio

Todo acceso al servicio, va a ser filtrado por medio de una conexión TLS con autenticación con certificado de cliente. Y contrastando el direccionamiento IP Origen, dando solamente acceso a aquellos que hayan firmado el convenio con el prestador del servicio.

2.2 Fuentes de tiempo fiable

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.

2.2.1 Precisión en la emisión de sellos de tiempo

La TSA emite sellos 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.

2.3 Generación de claves de la TSA

La TSA de SIA, ha generado sus claves criptográficas bajo el exclusivo control del personal de confianza de la propia Autoridad de Certificación SIA. Para ello, dichas claves han sido creadas dentro de un módulo criptográfico de seguridad hardware (HSM).

De acuerdo con las prácticas comunes se utilizaran los Algoritmos criptográficos apropiados para la creación de la clave de firma y su longitud correspondiente.

3. PROCESO DEL SELLADO DE TIEMPO

3.1 Servicios

La plataforma de TimeStamp está orientada a Servicio mediante protocolo HTTP y formato ASN1; se puede encontrar la siguiente funcionalidad:

Generación de sellos de tiempo en formato ASN1 conforme al RFC3161.

3.2 Emisión de peticiones

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 a la URL: http://host:port/tspTSA/inputRequestTSA

3.2.1 Formato de petición

El formato de la petición se define en el RFC3161 y debe ser una estructura ASN1 definida como:

```
TimeStampReq ::= SEQUENCE {
        Version             INTEGER { v1(1) },
        messageImprint      MessageImprint,
        reqPolicy           TSAPolicyId                 OPTIONAL,
        nonce               INTEGER                     OPTIONAL,
        certReq             BOOLEAN                     DEFAULT  FALSE,
        extensions          [0] IMPLICIT Extensions     OPTIONAL }

MessageImprint ::= SEQUENCE {
        hashAlgorithm       AlgorithmIdentifier,
        hashedMessage       OCTET STRING }


TSAPolicyId ::= OBJECT IDENTIFIER
```

Tabla 3 – Formato emisión de peticiones

3.3 Generación de respuestas

El módulo de TimeStamp, una vez validada la petición, genera una respuesta ASN1.

3.3.1 Formato de respuesta

El formato de la respuesta es el siguiente:

```
TimeStampResp ::= SEQUENCE {
        Status                  PKIStatusInfo,
        timeStampToken          TimeStampToken    OPTIONAL
}

PKIStatusInfo ::= SEQUENCE {
        status                  PKIStatus,
        statusString            PKIFreeText       OPTIONAL,
        failInfo                PKIFailureInfo    OPTIONAL
}

PKIStatus ::= INTEGER {
        granted                 (0),
        grantedWithMods         (1),
        rejection               (2),
        waiting                 (3),
        revocationWarning       (4),
        revocationNotification  (5)
}

PKIFailureInfo ::= BIT STRING {
        badAlg                  (0),
        badRequest              (2),
        badDataFormat           (5),
        timeNotAvailable        (14),
        unacceptedPolicy        (15),
        unacceptedExtension     (16),
        addInfoNotAvailable     (17)
        systemFailure           (25)
}

TimeStampToken ::= ContentInfo
        -- contentType is id-signedData as defined in [CMS]
        -- content is SignedData as defined in([CMS])
        -- eContentType within SignedData is id-ct-TSTInfo
        -- eContent within SignedData is TSTInfo

id-ct-TSTInfo OBJECT IDENTIFIER ::= { iso(1) member-body(2)
        us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) ct(1) 4}

TSTInfo ::= SEQUENCE {
        Version                 INTEGER { v1(1) },
        policy                  TSAPolicyId,
        messageImprint          MessageImprint,
        serialNumber            INTEGER,
        genTime                 GeneralizedTime,
        accuracy                Accuracy                OPTIONAL,
        ordering                BOOLEAN                 DEFAULT FALSE,
        nonce                   INTEGER                 OPTIONAL,
        tsa                     [0] GeneralName         OPTIONAL,
```

```
            extensions          [1] IMPLICIT Extensions     OPTIONAL
}

Accuracy ::= SEQUENCE {
            seconds     INTEGER         OPTIONAL,
            millis    [0] INTEGER  (1..999)   OPTIONAL,
            micros    [1] INTEGER  (1..999)   OPTIONAL  }
```

Tabla 4 – Formato de respuestas

4. PERFILES DEL CERTIFICADO

4.1 Perfil de certificado

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 TS 102 023: “Policy Requirements for time-stamping authorities”
- RFC 3161 “Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)”
- ETSI TS 101 861 “Time Stamping Profile”

4.1.1 Número de versión

El certificado sigue el estándar definido X.509 versión 3.

4.1.2 Extensiones del certificado

Los certificados emitidos por SIA de sellado de tiempo, vinculan la identidad de la entidad de sellado de tiempo a una determinada clave pública, sin incluir ningún tipo de atributos en el mismo. Para garantizar la autenticidad y no repudio, toda esta información estará firmada electrónicamente por el prestador de servicios de certificación encargado de la emisión.

Los campos singulares para identificar al certificado de sellado de tiempo son:

- Versión.
- Serial Number.
- Signature.
- Issuer (Emisor).
- Validity.
- Subject (Asunto).
- Subject Public Key Info.

Las extensiones utilizadas en los certificados son:

- Authority Key Identifier.
- Subject Key Identifier.

- KeyUsage. Calificada como crítica.
- ExtKeyUsage.
- CRL Distribution Point.
- Authority Information Access.
- CertificatePolicies.

4.1.3 Identificadores de objeto (OID) de los algoritmos

Identificador del algoritmo criptográfico con Objeto (OID): SHA-256 with RSA Encryption (1.2.840.113549.1.1.11).

4.1.4 Formatos de nombre

Los certificados emitidos por SIA contienen el "distinguished name X.500" del emisor y del titular del certificado en los campos "issuer"" y "subject"" respectivamente.

4.1.5 Identificador de objeto (OID) de la Política de Certificación

El OID de la presente PC es 1.3.6.1.4.1.39131.10.1.6

Los identificadores de los certificados expedidos para la presenta Política de sellado de tiempo son los siguientes:

Política de sellado de tiempo (TSA)	1.3.6.1.4.1.39131.10.1.6

Tabla 5 – OID política de sellado de tiempo

4.1.6 Sintaxis y semántica de los "PolicyQualifier"

La extensión "Certificate Policies" contiene los siguientes "Policy Qualifiers":

- URL DPC: contiene la URL donde puede obtener la última versión de la DPC y de las Políticas de Certificación asociadas.
- Notice Reference: Nota de texto que se despliega en la pantalla, a instancia de una aplicación o persona, cuando un tercero verifica el certificado.

4.1.7 Tratamiento semántico para la extensión "Certificate Policy"

La extensión "Certificate Policy" permite identificar la política y el tipo de certificado asociado al certificado.

4.2 Certificado de sellado de tiempo (TSA)

Certificado de sellado de tiempo (TSA)		
Nombre atributo	**Valor**	**Observaciones**
Campos x509 v1		
Versión	V3	
Serial Number	Número secuencial único, asignado automáticamente por la AC subordinada emisora	
Signature Algorithm	SHA-256 con RSA-2048	
Issuer Distinguished Name (Emisor)		
Country (C)	ES	
Organization (O)	SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA	
Organizational Unit (OU)	QUALIFIED CA	
Serial Number (serialNumber)	A82733262	
Common Name (CN)	SIA SUB01	
Validity		
Not Before	Fecha de emisión del certificado	
Not After	Fecha de emisión + 3 años	
Subject (Asunto)		
Country (C)	ES	
Organization (O)	SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA	
Organizational Unit (OU)	QUALIFIED CA	
Serial Number (serialNumber)	A82733262	
Common Name (CN)	SIA TSA	

Subject Public Key Info	Clave pública (RSA-2048 Bits), codificada de acuerdo con el algoritmo criptográfico	
Extensiones x509 v3		
Authority Key Identifier	Identificador de la clave pública del emisor	
Subject Key Identifier	Identificador de la clave pública del firmante del certificado	
KeyUsage		Marcado como crítica
Digital Signature	**1 (seleccionado)**	SI
Content Commitment (nonRepudiation)	**1 (seleccionado)**	SI
Key Encipherment	0 (no seleccionado)	
Data Encipherment	0 (no seleccionado)	
Key Agreement	0 (no seleccionado)	
Key Certificate Signature	0 (no seleccionado)	
CRL Signature	0 (no seleccionado)	
EncipherOnly	0 (no seleccionado)	
DecipherOnly	0 (no seleccionado)	
ExtendedKeyUsage		Marcado como crítica
Impresión de fecha	OID: 1.3.6.1.5.5.7.3.8	SI
CRL Distribution Point		
Distribution Point 1	https://psc.sia.es/ac_sub01.crl	
Distribution Point 2	http://psc.sia.es/ac_sub01.crl	
Authority Info Access		
Access Method	id-ad-calssuers	
Access Method	https://psc.sia.es/ac_sub01.crt	
Access Method	Id-ad-ocsp	
Access Location	https://psc.sia.es/ocsp	
Certificate Policies		
Policy Identifier	1.3.6.1.4.1.39131.10.1.6	
Policy Qualifier ID	Especificación de la DPC	

CPS Pointer	https://psc.sia.es	
User Notice	"Certificado de servidor de Sellado de Tiempo. Consulte las condiciones de uso en https://psc.sia.es. Contacto: Avda. de Europa, 2 Alcor Plaza. Edificio B Parque Oeste Alcorcón - 28922 Alcorcón - Madrid"	

Tabla 6 – Perfil certificado

5. OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD

5.1 Tarifas

5.1.1 Tarifas de emisión de sellos de tiempo o renovación

SIA como autoridad de sellado de tiempo (TSA) aplicará a los organismos o entidades las tarifas aprobadas para la prestación de dicho servicio o, en su defecto, las tarifas acordadas en el convenio o encomienda de gestión formalizados para tal efecto.

5.1.2 Política de reembolso

La política de reembolso vendrá detallada, como parte de las tarifas acordadas, en el convenio o encomienda de gestión formalizados para tal efecto.