An Indra company

TSA - SIA

Política de Servicio expedición de sellos electrónicos cualificados de tiempo (TSA)

OID: 1.3.6.1.4.1.39131.10.1.6

Versión: 1.6

HISTÓRICO DE CONTROL DE CAMBIOS DEL DOCUMENTO

Revisión	Fecha	Descripción
1.0	22 de octubre de 2015	Primera versión del documento
1.1	18 de febrero de 2017	Se alinea perfil y política de certificación con eIDAS, nuevas normas técnicas y RFCs.
1.2	11 de junio de 2019	Corrección sobre los puntos de distribución de CRLs.
1.3	17 de noviembre de 2020	Revisión erratas. Adecuación a la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
1.4	20 de mayo de 2022	Se incluye nuevo certificado de TSU TSAQC 2022 de SIA
1.5	16 de enero de 2023	Cambio de plantilla y actualización de domicilio social.
1.6	23 de julio de 2025	Adecuación a eIDAS-2 y revisión general de redacción.

Tabla de contenido

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 confianza (TSP), Sistemas Informáticos Abiertos Sociedad Anónima (en adelante SIA), que emite certificados cualificados según:

- Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) nº 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital, en adelante, eIDAS-2.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

En este contexto, se establecen las reglas a emplear por el Servicio de expedición de sellos electrónicos cualificados de tiempo, conforme a la norma ETSI 319 421 "Policy and Security Requirements for Trust Service Providers issuing Time-Stamps", ETSI 319 422 "Time-stamping protocol and time-stamp profiles" y al documento RFC-3161 "Internet X.509 Public Key Infrastructure Time-Stamp Protocol".

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 Confianza 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

Documento	Política de Servicio expedición de sellos electrónicos cualificados de tiempo
Versión	1.6
Estado	Vigente
Fecha de emisión	12/02/2025
Fecha de caducidad	No aplicable

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 / Prestador de Servicios de Confianza, 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 / Prestador cualificado de Servicios de Confianza

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"** (SIA ROOT y SIA ROOT 2025) - Autoridad de Certificación de primer nivel. Esta AC solo emite certificados para sí misma y sus AC Subordinadas, la excepción de la emisión del certificado de validación de OCSP y la emisión de la ARL. Únicamente estará en funcionamiento durante la realización de las operaciones para las que se establece.
- **"AC subordinada"** (SIA SUB01 y SIA SUB01 2025) - Autoridad de Certificación subordinada de "AC raíz". Su función es la emisión de certificados electrónicos, como por ejemplo la emisión del Certificado de Servicio expedición de sellos electrónicos cualificados 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 entidades 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 sellados de tiempo

Un sello emitido por la Autoridad de Sellado de Tiempo de SIA solo puede utilizarse para los fines expresamente permitidos en esta Política y en la correspondiente Declaración de Prácticas de Certificación. Su uso se limita a garantizar la existencia de datos electrónicos en un momento determinado para organismos o entidades con los que se haya formalizado un convenio de certificación.

Los certificados emitidos bajo los criterios de esta política están indicados para soportar firma electrónica avanzada con certificados cualificados, tal y como está definido en los artículos 26 y 27 de eIDAS-2, garantizando lo siguiente para todas las firmas:

a) estar vinculada al firmante de manera única;

b) permitir la identificación del creador de la firma;

c) haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, y

d) estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.

1.4.1 Usos apropiados y permitidos de los sellados de tiempo

El sellado debe 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 sellado, 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 sellados 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 e-mail	psc@sia.es
Dirección postal	Avenida de Bruselas, 35 - 28108 Alcobendas - Madrid (España)
Teléfono	+34 91 307 79 97

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” 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. Los algoritmos de hashes soportados actualmente son SHA-1, SHA-256 y SHA-512.
- 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

El servicio filtra todo acceso mediante una conexión TLS con autenticación mediante certificado de cliente, y contrasta además la dirección IP de origen de las peticiones de sellado. Solo se concede acceso a quienes hayan firmado un convenio con el prestador de servicios de confianza.

2.2 Fuentes de tiempo fiable

Los sistemas de información empleados por SIA garantizan el registro preciso del tiempo en el que se realizan las operaciones. Para ello, el instante temporal utilizado en estos sistemas proviene de una fuente segura y certificada, asegurando la trazabilidad y fiabilidad de los registros.

El servicio de sellado de tiempo (TSA) opera en España y emplea como referencia la señal horaria proporcionada por el Real Instituto y Observatorio de la Armada (ROA), entidad reconocida por el Bureau International des Poids et Mesures (BIPM) y declarada a efectos legales como Patrón Nacional de la unidad de tiempo. Esta señal mantiene y difunde oficialmente la escala Tiempo Universal Coordinado (UTC(ROA)), considerada la base de la hora legal en todo el territorio nacional, conforme al Real Decreto 1308/1992, de 23 de octubre, y reafirmada en la Ley 32/2014, de Metrología.

El sistema de sincronización provee precisión a nivel del microsegundo y está preparado para realizar ajustes de segundo intercalar siempre que la fuente de tiempo fiable notifique la necesidad de dicho ajuste. Dicho ajuste se llevará a cabo durante el último minuto del día en que esté programado que ocurra, conforme a las directrices establecidas por la autoridad de referencia.

La sincronización se realiza a través del Network Time Protocol (NTP), asegurando alineación con UTC(ROA) y garantizando el cumplimiento de los requisitos normativos de precisión y trazabilidad exigidos en ETSI EN 319 421 y ETSI EN 319 422.

2.2.1 Precisión en la emisión de sellos de tiempo

La TSA emite sellados de tiempo con una precisión temporal, manteniendo un desfase permitido inferior a un segundo. Esta precisión se monitoriza de forma constante para evitar desvinculaciones derivadas de latencias anormales en la sincronización con la fuente o desfases en los relojes internos de los equipos. En caso de detectarse una desincronización horaria, se procederá a la suspensión del servicio de sellado de tiempo (no se emitirán sellos de tiempo) hasta que se realice la calibración y se recupere la sincronización del reloj.

Además, se mantiene un registro exacto del momento en que se produce cualquier ajuste de segundo intercalar, garantizando su trazabilidad dentro de la precisión declarada. Dicho registro se almacena junto con los datos de auditoría del sistema y está disponible para su verificación cuando sea necesario, asegurando la conformidad con las regulaciones aplicables.

2.2.2 Registro de eventos de sincronización del reloj

Para garantizar la precisión y trazabilidad del servicio de sellado de tiempo, la TSA de SIA registra todos los eventos relacionados con la sincronización del reloj de la TSU con UTC(ROA). Estos registros permiten auditar y verificar que el servicio opera dentro de los parámetros establecidos y cumple con los requisitos de ETSI EN 319 421.

Se almacenan registros de los siguientes eventos:

- Recalibración normal o sincronización periódica del reloj con UTC.
- Detección de pérdida de sincronización y acciones correctivas tomadas.
- Ajustes de segundo intercalar, incluyendo la fecha y hora exactas en que se aplicaron.
- Fallo o degradación en la precisión del reloj y su recuperación.
- Intentos de modificación no autorizados en la configuración de sincronización.

Cada entrada de registro incluye los siguientes elementos:

- Fecha y hora exactas del evento.

- Número de serie o secuencia de la entrada.
- Identidad del sistema que genera el registro.
- Tipo de evento registrado.

2.3 Generación de claves de la TSA

2.3.1 Generación y almacenamiento de claves

La generación de las claves de firma de la TSU se lleva a cabo en un entorno físicamente seguro, dentro de un HSM certificado FIPS 140-2 Nivel 3, resistentes a manipulaciones intrusivas a nivel de hardware (Tamper Protection), que garantiza la protección frente a accesos no autorizados y evitando cualquier extracción o importación en otros dispositivos criptográficos seguros. Este procedimiento es realizado exclusivamente por personal de confianza del TSA, bajo un modelo de control dual. El acceso y manejo de las claves está estrictamente limitado al personal autorizado, conforme a las políticas y prácticas establecidas en el TSA.

La copia de seguridad de las claves se realiza en las mismas condiciones de seguridad en las que fueron creadas, garantizando su integridad y confidencialidad. Antes de almacenarse fuera del HSM, las claves privadas de la TSU son protegidas mediante los mecanismos criptográficos del propio módulo, lo que segura que solo puedan restaurarse en un entorno seguro autorizado. En caso de que una clave de firma de la TSU esté presente en múltiples dispositivos criptográficos por motivos de continuidad operativa, estará siempre vinculada al mismo certificado de clave pública en todos ellos.

De acuerdo con las prácticas comunes, se utilizan los algoritmos criptográficos apropiados para la creación de la clave de firma y la longitud correspondiente de esta. La implementación de controles criptográficos se realiza de acuerdo con las recomendaciones publicadas en ETSI TS 119 312 y está alineada con las guías “07-Criptología de Empleo ENS” y “CCN-STIC 221 - Guía de Mecanismos Criptográficos Autorizados”.

Para garantizar la validez verificable de los sellos de tiempo a largo plazo, la vigencia de las claves de la TSU se define de manera que permita la conservación segura y confiable de los datos sellados, considerando buenas prácticas de seguridad criptográfica.

El período de expiración de las claves de la TSU puede establecerse en el momento de la inicialización del dispositivo criptográfico seguro (HSM) o, alternativamente, mediante el uso de la extensión privateKeyUsagePeriod dentro del certificado de clave pública, garantizando un control preciso de su tiempo de vida.

En todo momento existirá un único par de claves activo en el dispositivo criptográfico para la creación de sellados de tiempo. Este par de claves solo podrá ser accedido y utilizado por la TSA.

La TSU no emitirá sellos de tiempo hasta que su certificado de clave pública de verificación de firma haya sido correctamente cargado en la TSU.

2.3.2 Registro de eventos del ciclo de vida de claves

Todos los eventos críticos relacionados con la **gestión de claves de la TSU** son registrados y almacenados en los sistemas de auditoría de la TSA, garantizando la trazabilidad y seguridad de su ciclo de vida.

Los eventos registrados incluyen:

- Generación de claves y asignación a la TSU.
- Activación y puesta en producción de claves.
- Rotación o reemplazo de claves en caso de actualización o finalización del período de uso.
- Revocación o expiración de claves por motivos operativos o de seguridad.
- Destrucción segura de claves una vez finalizado su período de uso.

Cada evento registrado incluirá los siguientes datos:

- Fecha y hora exacta del evento.
- Identidad del sistema o usuario que realiza la acción.
- Descripción del evento y justificación (si aplica).
- Número de serie o identificador único de la clave afectada.

2.3.3 Registro de eventos del ciclo de vida de certificados

Se mantiene un registro detallado de todos los eventos relacionados con los certificados de la TSU, asegurando su trazabilidad y cumplimiento normativo.

Los eventos registrados incluyen:

- Emisión y activación del certificado de la TSU.
- Renovación periódica, siguiendo los plazos establecidos (cada 5 años).
- Revocación anticipada, en caso de compromiso o incidentes de seguridad.
- Expiración y retiro del certificado, una vez finalizado su uso.

2.4 Monitorización de la capacidad y escalabilidad del servicio

SIA supervisa continuamente la capacidad de su infraestructura para garantizar el rendimiento óptimo del servicio y evitar interrupciones del servicio debido a sobrecargas.

Para ello, se aplican los siguientes controles:

- Monitorización en tiempo real de la carga del sistema, almacenamiento y tráfico de red.
- Sistemas de alertas automáticas que notifican al equipo de operaciones sobre niveles críticos de uso de recursos.
- Evaluaciones periódicas para prever el crecimiento de la demanda y ajustar la capacidad del servicio según sea necesario.
- Generación de informes mensuales que reflejan el estado de la capacidad y permiten la toma de decisiones sobre escalabilidad.

2.5 Cese de operaciones de la TSU

En caso de finalización del servicio TSA, se aplicarán los siguientes procedimientos para garantizar la seguridad y el cese definitivo de las operaciones de la TSU:

- **Destrucción de claves privadas**: Todas las claves privadas de la TSU serán destruidas de manera irreversible, asegurando que no puedan ser recuperadas ni reutilizadas.
- **Revocación de certificados**: Antes de la expiración de cualquier certificado activo de la TSU, este será revocado, evitando su uso tras el cese del servicio.
- **Prohibición de generación de nuevas claves y emisión de sellos**: Una vez finalizado el servicio TSA, la TSU no generará un nuevo par de claves pública y privada, ni emitirá nuevos tokens de sellado de tiempo, garantizando la terminación completa de sus operaciones.

2.6 Gestión del ciclo de vida del hardware criptográfico

El hardware criptográfico utilizado en la infraestructura del TSA está sujeto a procedimientos internos de gestión de su ciclo de vida que garantizan su seguridad en todas las fases: transporte, almacenamiento, instalación, activación, uso y retirada.

Estos procedimientos establecen controles para evitar cualquier manipulación no autorizada durante el transporte y almacenamiento del hardware criptográfico, asegurando su integridad hasta su instalación. Además, la instalación, activación y duplicación de claves de la TSU en estos dispositivos es realizada exclusivamente por personal de confianza, con control dual en un entorno físicamente seguro.

Asimismo, en el momento de la retirada de un módulo criptográfico, se aplican mecanismos de eliminación segura que imposibilitan la recuperación de las claves privadas almacenadas en su interior.

La gestión del hardware criptográfico se lleva a cabo conforme a los estándares de seguridad aplicables y garantizan la protección de los dispositivos en todo su ciclo de vida.

3. PROCESO DEL SELLADO DE TIEMPO

3.1 Servicios

La plataforma de TimeStamp está orientada a servicios mediante el protocolo HTTPS y utiliza el formato ASN.1 para la estructura de peticiones y respuestas. Ofrece la siguiente funcionalidad:

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

En el caso que las claves o el certificado estén caducados, el servicio de TimeStamp no estará disponible.

3.2 Emisión de peticiones

Los clientes deben enviar sus peticiones a través del protocolo HTTPS, conformando una petición de sellado de tiempo (time-stamping request) en formato ASN.1 y enviarla según corresponda a la URL:

Servicio	URL
TSAQC 2022	https://host:port/tspTSA2022

Tabla 3: URLs del servicio

3.2.1 Formato de petición

El formato de la petición se define en el RFC3161 y debe ser una estructura ASN.1 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 4: Formato emisión de peticiones

3.3 Generación de respuestas

El módulo de TimeStamp, una vez validada la petición, genera una respuesta ASN.1. Para la emisión de la respuesta, es preciso que el certificado esté disponible y se encuentre dentro de su periodo de validez.

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 5: Formato de respuestas

En el campo **extensions** del token se incorpora la información de que se trata de un sellado de tiempo cualificado y emitido conforme al reglamento 2024/1183 (eIDAS-2):

```
-- object identifiers
id-etsi-tsts OBJECT IDENTIFIER ::= {
       itu-t(0)
       identified-organization(4)
       etsi(0)
       id-tst-profile(19422) 1 }

id-etsi-tsts-EuQCompliance OBJECT IDENTIFIER ::= { id-etsi-tsts 1 }

-- statements
 esi4-qtstStatement-1 QC-STATEMENT ::= { IDENTIFIED BY id-etsi-tsts-EuQCompliance }
```

Tabla 6: Extensión para timestamp cualificado

3.3.2 Verificación de un sellado de tiempo

La verificación de un sellado de tiempo emitido por este servicio requiere de las siguientes tareas:

- Verificación de la integridad del sellado. La firma ha de ser correcta.
- Verificación el periodo de validez del certificado. El servicio no emite sellados con el certificado caducado, pero los terceros deben verificar que no se ha empleado un certificado fuera del periodo de validez establecido por la TSA.
- Verificación del estado de revocación del certificado de sellado, así como de las extensiones del mismo que indican que su uso es el de sellado de tiempo.

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:

- RFC 3161 “Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)”.
- ETSI EN 319 421: “Policy and Security Requirements for Trust Service Providers issuing Time-Stamps”.
- ETSI EN 319 422 “Time-stamping protocol and time-stamp token profiles”.
- ETSI EN 319 412-1 “Certificate Profiles; Part 1: Overview and common data structures”.
- ETSI EN 319 412-3 “Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons”.
- ETSI EN 319 412-5 “Certificate Profiles; Part 5: QCStatements”.
- ETSI TS 119 312 “Cryptographic Suites”.

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	OID	Nº de bits	Servicio
sha256WithRSAEncryption	1.2.840.113549.1.1.11	3072	TSAQC 2022

Tabla 7: Indicadores OID de los algoritmos del servicio

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 identificador de objeto (OID) asignado a la presente Política de Certificación (PC) de sellado de tiempo es el siguiente:

Descripción	OID
OID de la política de sellado de tiempo	1.3.6.1.4.1.39131.10.1.6

Este OID debe ser utilizado en la extensión ReqPolicy de las solicitudes de sellado de tiempo. En caso de que no se indique este OID, la Autoridad de Sellado de Tiempo (TSA) rechazará la solicitud y generará el siguiente mensaje de error "*The requested TSA policy is not supported by the TSA*".

Esta Política de Certificación está alineada con lo dispuesto en el apartado 5.2 de la norma ETSI EN 319 421, y cumple con los requisitos de la política BTSP (Best Practices Time-Stamp Policy). En consecuencia, este OID identifica una política que se adhiere a las mejores prácticas de sellado de tiempo establecidas en dicha norma, sin desviaciones, y amplía sus disposiciones de conformidad.

La TSA incluirá este identificador en los sellos de tiempo emitidos y en la declaración de divulgación (TSA Disclosure Statement) que pone a disposición de los suscriptores y terceros confiables, como prueba de conformidad con esta política.

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

Descripción	OID
Política del certificado de sellado de tiempo TSAQC 2022	1.3.6.1.4.1.39131.10.1.25
NCP+	0.4.0.2042.1.2

Tabla 8: OID política de certificados 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 Certificados de Servicio de expedición de sellos electrónicos cualificados de tiempo (TSA)

4.2.1 Certificado de TSU TSA QC 2022

El certificado de clave pública de la TSU ha sido emitido por SIA como una Autoridad de Certificación (CA) cualificada, que opera bajo la norma ETSI EN 319 411-1 y ETSI EN 319 411-2, asegurando su conformidad con los requisitos europeos de confianza en los servicios de sellado de tiempo. Este certificado será renovado a los 5 años.

El TSA especifica la fecha de expiración de las claves privadas y públicas de la TSU dentro de su Declaración de Prácticas de Certificación (DPC), incluyendo los procedimientos operativos y técnicos implementados para la renovación, revocación y eliminación segura de claves, asegurando la continuidad y seguridad del servicio de sellado de tiempo.

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-3072	
Issuer Distinguished Name (Emisor)		
Country (C)	ES	
Organization (O)	SISTEMAS INFORMÁTICOS ABIERTOS SOCIEDAD ANONIMA	

Organizatión Unit (OU)	QUALIFIED CA	
serialNumber	A82733262	
Common Name (CN)	SIA SUB01	
Validity		
No Before	Fecha de emisión del certificado	
No After	Fecha de emisión + <=10 años	
Subject (Asunto)		
Country (C)	ES	
Organizatión (O)	SISTEMAS INFORMÁTICOS ABIERTOS SOCIEDAD ANONIMA	
Organizatión Unit (OU)	QUALIFIED CA	
Organization Identifier (OI)	VATES-A82733262	
Common Name (CN)	TSAQC 2022	
Subject Public Key Info	Clave pública (RSA-3072 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
id-kp-timeStamping	OID: 1.3.6.1.5.5.7.3.8	SI
CRL Distribution Point		
Distribution Point 1	http://psc.sia.es/crlc[N].crl	N es el número correspondiente a la CRL particionada.
Distribution Point 2	http://psc.sia.es/crlc[N].crl	N es el número correspondiente a la CRL particionada.
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 Qualifier ID	Especificación de la DPC	
CPS Pointer	https://psc.sia.es	
User Notice	Certificado de servicio expedición de sellos electrónicos cualificados de tiempo. Condiciones de uso y vías de contacto en: https://psc.sia.es	
Policy Identifier	0.4.0.2042.1.2	
Policy Identifier	1.3.6.1.4.1.39131.10.1.25	

Tabla 9: Perfil Certificado TSAQC 2022

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.

5.2 Obligaciones de las partes

5.2.1 Obligaciones del Suscriptor del Servicio de Sellado de Tiempo

SIA, como suscriptor del servicio de sellado de tiempo deberá:

- Utilizar los sellos electrónicos de tiempo únicamente en los contextos y condiciones definidos por la presente política y los términos y condiciones del servicio.
- Asegurarse de que los datos enviados para su sellado están correctamente formateados y no contienen errores.
- Abstenerse de manipular, alterar o reinterpretar los sellos de tiempo emitidos.
- Mantener la seguridad y control de los sistemas que generen las peticiones de sellado.
- Notificar sin demora al Prestador cualquier incidente de seguridad o sospecha de mal uso relacionado con el servicio.

5.2.2 Obligaciones de las Partes Confiables (Relying Parties)

Las partes confiables que decidan confiar en un sello de tiempo emitido por este servicio deberán:

- Verificar que el sello de tiempo ha sido firmado por una Autoridad de Sellado de Tiempo válida y que la firma es criptográficamente válida.
- Asegurarse de que la clave utilizada por el TSA no ha sido revocada ni comprometida en el momento de la verificación.
- Consultar y respetar las limitaciones de uso descritas en esta política, en especial aquellas que afecten al ámbito de aplicación o periodo de validez del sello.
- Considerar cualquier otra advertencia o restricción establecida en la documentación oficial del servicio o en acuerdos contractuales asociados.

6. RECUPERACIÓN ANTE DESASTRES Y COMPROMISO DE CLAVE

6.1 Procedimientos de gestión de incidencias y compromisos

SIA ha desarrollado políticas de seguridad y continuidad del negocio que garantizan la gestión eficiente de incidentes y la recuperación de los sistemas en caso de compromisos de seguridad o fallos operativos. Estas políticas incluyen procedimientos para la detección, escalado, investigación y respuesta ante incidentes, asegurando la restauración segura del servicio en el menor tiempo posible.

Cualquier incidente que pueda comprometer la seguridad, la integridad o la precisión del servicio TSA se gestiona conforme a estos procedimientos, asegurando la trazabilidad y comunicación adecuada a las partes interesadas.

6.2 Corrupción en datos, aplicaciones o recursos

Si se detecta un evento que afecte la integridad de los recursos, aplicaciones o datos del TSA, se activarán los procedimientos de gestión de incidentes, siguiendo las políticas de seguridad establecidas.

6.3 Compromiso de claves privadas de la TSU

En caso de sospecha o confirmación del compromiso de las claves privadas de la TSU, SIA activará los procedimientos de gestión de compromiso de claves, en conformidad con las políticas de seguridad, gestión de incidencias y continuidad del negocio.

6.4 Continuidad del negocio después de un desastre

SIA garantiza la restauración de los servicios críticos en conformidad con el Plan de Continuidad de Negocio (BCP), asegurando la vuelta a la operación normal en un plazo máximo de 24 horas tras un evento disruptivo.

6.5 Comunicación de incidentes a suscriptores y partes confiables

En caso de compromiso de claves, posible compromiso o pérdida de calibración, el TSA notificará a todos los suscriptores y partes confiables, proporcionando información sobre la naturaleza del incidente, las medidas adoptadas y las implicaciones para los sellos de tiempo emitidos.

Cuando sea necesario, el TSA pondrá a disposición de las partes confiables información que permita identificar los sellos de tiempo potencialmente afectados, garantizando siempre la protección de la privacidad de los usuarios y la seguridad del servicio.

An Indra company

Persona de contacto
psc@sia.es

Av. de Bruselas, 35
28108 Alcobendas, Madrid
T +34 91 307 79 97

sia.es