GOBIERNO DE ESPAÑA
MINISTERIO DE TRABAJO E INMIGRACIÓN

SECRETARÍA DE ESTADO
DE LA SEGURIDAD SOCIAL

GERENCIA DE INFORMÁTICA
DE LA SEGURIDAD SOCIAL

Centro de Calidad, Auditoría y Seguridad

Política y Declaración de Prácticas de Sellado de Tiempo de la TSA de la Gerencia de Informática de la Seguridad Social

CORREO ELECTRONICO

C/ Dr. Tolosa Latour, s/n
24041 MADRID
TEL: 91 390 27 18
FAX: 91 390 51 67

Control de cambios

Versión	Observaciones	Fecha
1.0	Versión inicial	02-02-2010

Índice

1. INTRODUCCIÓN

1.1. Presentación

La Gerencia de Informática de la Seguridad Social (GISS), como Prestador de Servicios de Certificación que emite certificados reconocidos a efectos de la Ley 59/2003 de Firma Electrónica, ofrece también servicios de sellado de tiempo, cuyo objetivo es demostrar que una serie de datos han existido y no se han modificado desde un determinado instante de tiempo.

El presente documento recoge la política y la declaración de prácticas de sellado de tiempo de la TSA (Time-Stamping Authority) de la GISS, e incluye tanto las obligaciones y responsabilidades de todas las partes implicadas como los detalles técnicos y los términos de uso del servicio.

Para garantizar la fiabilidad de dicho servicio, esta política se basa en criptografía de clave pública y certificados X.509 v3 emitidos por la Autoridad de Certificación de la GISS (ACGISS), por lo que en último término estará subordinada a lo dispuesto en su Declaración de Prácticas de Certificación (DPC).

Desde el punto de vista de la legislación actual, el servicio se encuentra inscrito entre los proporcionados por la ACGISS en la página web del Ministerio de Industria, Turismo y Comercio, cumpliendo lo dispuesto en el art. 29.3 de la Ley 11/2007.

1.2. Referencias

Legislación aplicable:

- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, y su Reglamento de desarrollo aprobado por RD 1671/2009.
- Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su reglamento de desarrollo aprobado por el RD 1720/2007.

Para su elaboración se han tenido en cuenta los siguientes estándares en materia de sellado de tiempo:

- ETSI TS 102 023 v1.2.1 “Policy Requirements for time-stamping authorities”
- RFC 3268 “Requirements for time-stamping authorities”
- ETSI TS 101 861 v1.2.1 “Time Stamping Profile”
- RFC 3161 “Internet X.509 Public Key Infraestructure – Time Stamp Protocol (TSP)”
- ETSI SR 002 176 “Algorithms and Parameters for Secure Electronic Signatures”

- ISO/IEC 27002 “Information technology — Security techniques — Code of practice for information security management”

1.3. Nombre del documento e identificación

Nombre del documento	Política y Declaración de Prácticas de Sellado de Tiempo de la TSA de la Gerencia de Informática de la Seguridad Social
Versión	1.0
Estado del documento	Aprobado
Fecha de emisión	02 de febrero de 2010
Localización	www.seg-social.es

1.4. Administración de la política

Los datos de contacto de la organización encargada de la administración de este documento, son los siguientes:

Nombre	Centro de Calidad, Auditoría y Seguridad (Gerencia de Informática de la Seguridad Social)		
Dirección e-mail	giss-ccas.solicitudes@giss.seg-social.es		
Dirección	C/ Albasanz nº 23, 28037 Madrid		
Teléfono	91 390 27 18	**Fax**	91 390 51 67

2. DEFINICIONES Y ACRÓNIMOS

2.1. Definiciones

Autoridad de Sellado de tiempo: Es un Prestador de Servicios de Certificación que proporciona certeza sobre la preexistencia de determinados documentos electrónicos a un momento dado.

Declaración de prácticas de sellado de tiempo: Declaración de prácticas que la TSA emplea en la emisión de los sellos de tiempo.

Plataforma de servicios de seguridad: Infraestructura de la Gerencia de Informática de la Seguridad Social, que incluye funcionalidades relacionadas con la firma electrónica, la custodia de documentos y el sellado de tiempo.

Política de sellado de tiempo: Consiste en una serie de reglas que indican la aplicabilidad de un sello de tiempo a una comunidad o aplicación en particular, con requisitos de seguridad comunes.

Prestador de servicios de certificación: Persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.

Sellado de tiempo: Asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento

Suscriptor: Persona o entidad que solicita los servicios proporcionados por la Autoridad de sellado de tiempo.

Sello de tiempo: Objeto de datos que une una representación de un dato o documento a un instante de tiempo, estableciendo así la evidencia de que existía antes de ese momento.

Tercera parte que confía en los sellos de tiempo: Persona o entidad que voluntariamente confía en el sello de tiempo y en el certificado electrónico utilizado para su firma, como medio de acreditación de la autenticidad e integridad del documento firmado

Usuario: Engloba a los suscriptores del servicio de sellado de tiempo y a las terceras partes que confían en el mismo.

UTC: También conocido como *tiempo civil*, es el tiempo de la zona horaria de referencia respecto a la cual se calculan todas las otras zonas del mundo.

2.2. Acrónimos

ACGISS	Autoridad de Certificación de la Gerencia de Informática de la Seguridad Social
ASN	Abstract Syntax Notation
DPC	Declaración de Prácticas de Certificación
FIPS	Federal Information Processing Standards
GISS	Gerencia de Informática de la Seguridad Social
HSM	Hardware Security Module
HTTP	Hipertext Transfer Protocol
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization

OID	Object Identifier
RFC	Request for comment
TSA	Autoridad de Sellado de Tiempo (Time-Stamping Authority)
TSP	Protocolo de Sellado de Tiempo (Time-Stamping Protocol)
TSS	Servicio de Sellado de Tiempo (Time-Stamping Service)
TST	Sello de tiempo (Time-Stamp Token)
UTC	Universal Time Coordinated

3. CONCEPTOS GENERALES

3.1. Servicio de sellado de tiempo

El servicio de sellado de tiempo (TSS) está integrado en la Plataforma de Servicios de Seguridad, que tiene como misión cubrir las nuevas necesidades en materia de cifrado, firma, verificación de firmas, validación de certificados, sellado de tiempo y custodia de documentos en el entorno de la Gerencia de Informática de la Seguridad Social (GISS).

A efectos de este documento, en el servicio se pueden distinguir dos funciones principales:
- Prestación del servicio de sellado de tiempo, que se corresponde con la generación de los sellos.
- Gestión del servicio de sellado de tiempo, que incluye las funciones de monitorización y control del servicio, para asegurar que su operación se realiza tal como especifica la TSA.

La funcionalidad de sellado de tiempo está orientada a servicio mediante protocolo HTTP y formato ASN1, cumpliendo con el estándar RFC 3161 del IETF.

3.2. Autoridad de sellado de tiempo

La TSA es la autoridad en la que confían los usuarios (suscriptores y terceras partes que confían) para la emisión de los sellos de tiempo.

La GISS, como prestador de servicios de certificación, se constituye como Autoridad de Sellado de Tiempo en el ámbito de la Secretaría de Estado de la Seguridad Social, proporcionando la infraestructura necesaria para garantizar la seguridad y la precisión del servicio con las exigencias previstas en la legislación vigente.

Como TSA se responsabiliza de todas las acciones relacionadas con la prestación del servicio de sellado de tiempo y asegura el cumplimiento de lo dispuesto en el presente documento.

3.3. Suscriptores

Los suscriptores de este servicio pertenecen a las Entidades Gestoras y Servicios Comunes incluidos dentro del ámbito de la Secretaría de Estado de la Seguridad Social del Ministerio de Trabajo e Inmigración.

No obstante, se podrán realizar convenios de prestación de servicios con otras administraciones o entidades si así se determina.

4. POLÍTICA DE SELLADO DE TIEMPO

4.1. Vista general

Esta política contiene el conjunto de reglas utilizadas para la prestación y control del servicio de sellado de tiempo, además de regular el nivel de seguridad de la TSA.

Para su elaboración, se ha seguido el estándar ETSI TS 102 023, incorporando las exigencias y condiciones tanto de la legislación vigente como de los estándares internacionales, que pueden consultarse en el apartado de referencias de este documento.

4.2. Identificación de la Política de Sellado de Tiempo

Nombre de la política	Política de Sellado de Tiempo de la TSA de la Gerencia de Informática de la Seguridad Social
Versión	1.0
OID	2.16.724.1.4.2.2.1
Localización	www.seg-social.es

Significado del OID: joint-iso-itu-t (2) country (16) es (724) adm (1) giss (4) infraestructuras (2) TSA (2) politica de sello de tiempo (1)

4.3. Comunidad de usuarios y aplicabilidad

Esta política está orientada a cumplir los requisitos para la emisión de sellos de tiempo que tengan la condición de reconocidos, entendiendo como tales aquellos que se emitan en condiciones equivalentes a la emisión de certificados electrónicos reconocidos según la Ley 59/2003 de Firma Electrónica.

Los servicios de sellado de tiempo proporcionados por la TSA de la Seguridad Social, se encuentran inscritos en el Ministerio de Industria, como servicio proporcionado por el prestador de servicios de certificación ACGISS, que cumple los requisitos técnicos y las obligaciones especificadas en la citada Ley.

Los usuarios del servicio serán principalmente las aplicaciones/sistemas o clientes definidos en el ámbito de la Secretaría de Estado de la Seguridad Social, sin perjuicio de otros que puedan autorizarse mediante los correspondientes convenios.

4.4. Conformidad o cumplimiento

Los TST incluirán el identificador de la política de sellado de tiempo, de forma que se garantice la confianza en los sellos de tiempo que se emiten.

La TSA se compromete a cumplir las obligaciones e implementar los controles especificados en esta política y en la declaración de prácticas de sellado de tiempo recogidos en el presente documento.

5. OBLIGACIONES Y RESPONSABILIDADES

5.1. Obligaciones de la TSA

5.1.1. Generales

La Gerencia de Informática de la Seguridad Social, como Prestador de Servicios de Certificación y Autoridad de Sellado de Tiempo, estará obligada a:

- Seguir los procedimientos y directrices especificados en el presente documento de política y declaración de prácticas de sellado de tiempo.
- Proteger las claves privadas empleadas para la emisión de sellos de tiempo de forma que se asegure su confidencialidad e integridad.
- Utilizar productos y sistemas fiables que garanticen la seguridad de los procesos de sellado de tiempo a los que sirven de soporte.
- Mantener y calibrar la referencia temporal utilizada, de forma que se garantice la hora y la fecha incluidas en los sellos que emite.
- Emitir sellos de tiempo con el contenido y la precisión exigidos por la legislación vigente.
- Conservar toda la información y documentación relativa al servicio de sellado de tiempo durante al menos 15 años.

- Publicar y mantener este documento de Política y Declaración de Prácticas de Sellado de tiempo, así como cualquier otra información relevante para los usuarios del servicio.
- Facilitar un servicio de validación de sellos de tiempo, de forma que puedan comprobar su validez las terceras partes que confíen en ellos.
- Responder por los daños y perjuicios causados como prestador de servicios de certificación según lo especificado en la Ley 59/2003 de Firma Electrónica.

5.1.2. Obligaciones de la TSA hacia sus suscriptores

La TSA debe comprometerse a prestar el servicio según los términos y condiciones especificados, fundamentalmente los relativos a la disponibilidad y la precisión del mismo.

Deberá garantizar el acceso permanente al servicio, debiendo planificarse con suficiente antelación las paradas técnicas de mantenimiento que sean necesarias y advirtiendo de ello a los suscriptores utilizando los medios disponibles.

Asimismo, se compromete a:
- Emitir sellos de tiempo según la información proporcionada por los suscriptores y libres de errores de entrada de datos.
- Emitir sellos de tiempo que sean conformes con la normativa vigente, incluyendo el contenido mínimo que pueda exigirse en cada momento.
- Publicar este documento y facilitar cualquier otra información que sea relevante para el suscriptor.
- Custodiar la información de los sellos de tiempo y la información personal proporcionada con las debidas medidas de seguridad, de acuerdo con lo dispuesto en la Ley 15/1999 de Protección de Datos de Carácter Personal y su normativa de desarrollo.

5.2. Obligaciones de los suscriptores

Los suscriptores del servicio de sellado de tiempo tienen la obligación de:
- Seguir los procedimientos y directrices especificados en el presente documento.
- Haber suscrito, en su caso, el correspondiente convenio de prestación de servicios.
- Identificarse y autenticarse de acuerdo con las exigencias especificadas.
- Verificar la firma electrónica de los sellos de tiempo, incluyendo la comprobación de la validez de los certificados empleados.
- Utilizar los sellos de tiempo dentro de los límites y el ámbito descritos en esta política.

5.3. Obligaciones de las terceras partes que confían en los sellos de tiempo

Las partes que confíen en un sello de tiempo emitido por la GISS están obligados a:

- Seguir los procedimientos y directrices especificados en el presente documento.
- Verificar la firma electrónica de los sellos de tiempo, incluyendo la comprobación de la validez de los certificados empleados.
- Aceptar los sellos de tiempo dentro de los límites y el ámbito descritos en esta política.

5.4. Responsabilidades

De forma general, la GISS responderá por los daños y perjuicios que cause a cualquier persona en el ejercicio de su actividad cuando incumpla las obligaciones que le impone la Ley 59/2003 de Firma Electrónica.

Asimismo, asegurará el cumplimiento de las condiciones y requisitos establecidos en el presente documento, quedando exenta de responsabilidad fuera del ámbito y el alcance del servicio de sellado de tiempo y, en concreto, en cuanto a lo que se refiere al contenido de los documentos sellados.

La TSA no será responsable si se produce alguno de los siguientes supuestos:

- Que se superen los límites establecidos por la GISS en cuanto a sus posibles usos o no se utilicen conforme a las condiciones establecidas y comunicadas al suscriptor del servicio.
- Que el suscriptor o las terceras partes que confían en los sellos no verifiquen la firma electrónica de los mismos, incluyendo la vigencia del certificado utilizado.

6. REQUISITOS DE LA AUTORIDAD DE SELLADO DE TIEMPO

6.1. Prácticas de sellado de tiempo y términos y condiciones de uso

6.1.1. Prácticas de sellado de tiempo

Las prácticas de sellado de tiempo detallan la implementación de los controles necesarios para cumplir con la política de sellado de tiempo y garantizar la fiabilidad y confianza del servicio.

Además de las condiciones especificadas en este apartado, serán de aplicación los mecanismos y procedimientos establecidos en la DPC de la ACGISS, así como las diferentes normativas existentes en el ámbito interno de la GISS.

6.1.2. Términos y condiciones de uso del servicio

La TSA debe facilitar a los suscriptores y las terceras partes que confíen en su sello de tiempo, los términos y condiciones de uso relativos a este servicio.

En concreto, contendrá:
- Información de contacto de la TSA.
- Una referencia a la política de sellado de tiempo.
- Al menos un algoritmo hash utilizado para el sellado de tiempo.
- El tiempo de vida esperado de la firma del sello de tiempo.
- La precisión del tiempo del sello respecto a UTC.
- Cualquier limitación en el uso del servicio de sellado de tiempo.
- Las obligaciones del suscriptor.
- Las obligaciones de las terceras partes que confían en los sellos.
- Información sobre cómo verificar el sello de tiempo para que se considere que se puede confiar razonablemente en él y cualquier limitación existente en el período de validez.
- El período de tiempo durante el que la TSA mantiene los eventos asociados al servicio.
- La legislación aplicable para la prestación del servicio.
- Limitaciones de responsabilidad.
- Procedimientos de resolución de conflictos.
- Las auditorías de conformidad con la política.

Los términos y condiciones mencionados serán publicados en la página web de la Seguridad Social, junto con el resto de información relativa al servicio de sellado de tiempo.

6.2. Gestión del ciclo de vida de las claves

6.2.1. Generación de las claves de la TSA

La TSA asegura que las claves utilizadas para el firmado de los sellos de tiempo se generan en circunstancias controladas, en un módulo criptográfico HSM que cumple con el estándar FIPS 140-1 nivel 3 y por personal autorizado.

Además, los algoritmos utilizados para la firma –RSA y SHA-1 - y la longitud de las claves -1024 bits- cumplen con lo especificado en el estándar ETSI SR 002 176.

6.2.2. Protección de la clave privada

La TSA se compromete a proteger las claves privadas, de forma que se mantenga su confidencialidad e integridad.

En concreto, las claves privadas se mantendrán y usarán dentro de un módulo criptográfico que cumpla los requisitos especificados en el apartado anterior y bajo control multipersona.

6.2.3. Distribución de la clave pública de TSA

La clave pública de la TSA estará disponible en la página web de la Seguridad Social en un certificado electrónico emitido por la ACGISS.

La integridad y autenticidad de dicha clave queda garantizada por la firma de la autoridad de certificación con su certificado raíz.

Cualquier información adicional relativa a la consulta de la vigencia del certificado puede consultarse en la DPC de la ACGISS.

6.2.4. Regeneración de la clave de la TSA

La regeneración de la clave de la TSA se produce, entre otras causas, por la expiración del certificado o cuando se detecte un posible compromiso de las claves.

La emisión de un nuevo certificado no exigirá la comunicación a los usuarios del servicio, que únicamente deben confiar en el certificado raíz de ACGISS, siendo válido cualquier certificado de la TSA válido emitido y firmado por esta autoridad.

6.2.5. Fin del ciclo de vida de la clave de TSA

La TSA garantiza que no se utilizarán las claves fuera de su período de validez. El sistema de generación de TST rechazará cualquier intento de emitir un sello de tiempo con una clave privada que haya expirado.

Cuando una clave privada expire, se pondrán en funcionamiento los procedimientos necesarios para asegurar su renovación, tal como se especifica en la DPC de la ACGISS.

Asimismo, asegurará que las claves privadas serán destruidas de forma segura, evitando la posible recuperación de las mismas.

6.2.6. Gestión de los módulos criptográficos usados para firmar los sellos de tiempo

La TSA vigilará que el hardware criptográfico utilizado para firmar los TST funcione correctamente y tomará las medidas necesarias para evitar su manipulación.

La instalación, activación y posible duplicación de las claves en el módulo criptográfico las realizarán sólo el personal autorizado para ello, dejando constancia de cada una de estas acciones.

La TSA garantiza que las claves privadas de firma que se encuentren dentro de estos módulos serán borradas según los procedimientos seguros existentes, antes de la retirada de los mismos.

Se llevarán a cabo cualesquiera otros análisis y recomendaciones de los fabricantes de los HSM, para asegurar el cumplimiento de los requisitos necesarios para certificar la seguridad adecuada.

6.3. Sellado de tiempo

6.3.1. Sello de tiempo

La TSA se compromete a que la generación de los TST se realiza de forma segura y con el instante de tiempo correcto.

Además del identificador único incorporado en cada TST, se incluirá un identificador de la política de sellado de tiempo, de forma que se puedan conocer las condiciones y directrices aplicables a los sellos de tiempo.

Por otra parte, el valor de tiempo utilizado estará sincronizado con el tiempo UTC con la precisión definida en la legislación aplicable.

El sello de tiempo se firmará con una clave generada exclusivamente a estos efectos, con las medidas de seguridad necesarias para garantizar su validez, tal como se definen en la DPC de la ACGISS.

Se seguirá el protocolo definido en la RFC 3161 “Time Stamp Protocol”, con las restricciones de la norma ETSI TS 101 861 “Time Stamping Profile”. El sello de tiempo se realizará vía HTTP mediante notación ASN1.

6.3.2. Sincronización con UTC

La TSA utiliza una fuente fiable de tiempo, mediante un servidor NTP que se sincroniza con el tiempo UTC a través de una red de satélites GPS.

Se mantendrá la calibración del reloj de forma que se asegure una precisión aceptable para el TSS, y se protegerá contra cualquier amenaza que pueda suponer un cambio del tiempo fuera de dicha calibración.

Asimismo, la TSA asegura que será detectada cualquier diferencia entre el tiempo indicado en un sello de tiempo y el tiempo UTC, y que se informará adecuadamente de estos eventos a todas las partes interesadas. El cálculo de tiempo cumple lo estipulado en las recomendaciones de NTP (Network Time Protocol) y de la BIPM (Oficina Internacional de Pesos y Medidas).

6.4. Operación y mantenimiento de la TSA

6.4.1. Gestión de la seguridad

La TSA asegurará que se aplican los procedimientos administrativos y de gestión definidos internamente en la Gerencia Informática de la Seguridad Social de forma que se garantice la seguridad de los procesos relacionados con la generación de los sellos de tiempo.

La TSA asumirá la responsabilidad por todos los aspectos relacionados con la seguridad en la prestación de los servicios de sellado de tiempo, dentro del alcance de esta política.

Por ora parte, la GISS dispone de áreas especializadas en la seguridad de la información, que serán las encargadas de velar por el cumplimiento de los procedimientos definidos, por la conformidad con la normativa y los estándares existentes (entre otros, la ISO 27002) y por la correcta implantación de todos los controles necesarios.

6.4.2. Clasificación y gestión de activos

La GISS realiza cada dos años un análisis de riesgos, siguiendo la metodología MAGERIT y utilizando para ellos la herramienta PILAR del CNN.

De esta forma, se obtiene un inventario de todos los activos existentes, junto con su clasificación en términos de seguridad y los requisitos necesarios para su adecuada protección.

6.4.3. Seguridad del personal

La TSA asegura que todo el personal relacionado con el servicio de sellado de tiempo tiene el conocimiento, la experiencia y la cualificación necesaria para el desempeño de sus funciones.

Asimismo, se documentarán todos los perfiles relacionados con el servicio y se definirán las responsabilidades de cada actor implicado.

Los principales roles identificados relacionados con esta funcionalidad son:
- Responsables de seguridad: encargados de la implementación de las políticas y controles de seguridad así como gestión y revisión de logs.
- Administradores de sistemas: autorizados para instalar, configurar y mantener los sistemas y aplicaciones de confianza de la TSA que soportan las operaciones de certificación.
- Operadores de sistemas: responsables de la gestión diaria de los sistemas y de realizar funciones relacionadas con el sistema de backup y de recuperación
- Auditores: realizan las funciones de supervisión y control del cumplimiento de lo dispuesto en el presente documento.

6.4.4. Seguridad física y del entorno

La GISS dispone de normas y procedimientos para controlar el acceso físico a sus servicios y activos, y protegerlos contra accesos no autorizados, daños, pérdidas, compromiso de su información o interrupción de sus actividades.

Para ello, implementa los controles exigidos por el estándar ISO 27002, incluyendo los relacionados con los módulos criptográficos implicados en el servicio de sellado de tiempo

6.4.5. Gestión de las operaciones

La GISS tiene establecidos procedimientos para la protección de los componentes y la información contra accesos no autorizados, pérdida, código malicioso, etc., así como para la gestión de las incidencias que puedan producirse.

En concreto, tiene implementados controles y procedimientos para la gestión de todas las operaciones y sistemas relacionados con la emisión de sellos de tiempo.

6.4.6. Gestión de acceso a los sistemas

El acceso al sistema de la TSA debe estar limitado a las personas debidamente autorizadas, existiendo controles implementados para evitar el acceso no permitido a la red interna, a las funciones de la TSA y a la información que maneja.

Se dispone de procedimientos para la gestión de los perfiles de usuarios existentes en la plataforma de seguridad de la GISS, y en concreto, en el módulo de sellado de tiempo, otorgando los privilegios

necesarios a cada uno de ellos y controlando las operaciones que realizan por medio de rastros de auditoría y registros de eventos.

6.4.7. Despliegue y mantenimiento de sistemas de confianza

La TSA utiliza sistemas y productos confiables que están adecuadamente protegidos contra modificaciones y alteraciones, allí donde el análisis de riesgos lo determina en base a su criticidad.

Se lleva a cabo un análisis de seguridad de todos los módulos incorporados, así como de cualquier cambio o modificación autorizada que se lleve a cabo.

Asimismo existen procedimientos de control de cambios aplicados a cualquier nueva versión, modificación o ampliación de software.

6.4.8. Compromiso de los servicios de la TSA

La TSA garantiza que en caso de que se produzca un evento de seguridad en los servicios de sellado de tiempo, incluyendo el compromiso de su clave privada o la pérdida de calibración respecto a la UTC, informará por los medios de que disponga a los suscriptores y las terceras partes que confíen en sus sellos.

Estos procedimientos estarán recogidos en el Plan de Continuidad de la ACGISS.

6.4.9. Cese de la TSA

La TSA asegura el mínimo impacto en los suscriptores y terceras partes que confían en sus sellos, en caso de cese de sus servicios de sellado de tiempo, y en particular, garantiza el mantenimiento de la información requerida para verificar la corrección de los sellos de tiempo.

La TSA realizará con una antelación suficiente las siguientes acciones:
- Informar a todos los suscriptores y terceras partes de todo lo relacionado con el cese de actividad.
- Comunicar los mecanismos existentes para mantener los registros de eventos y de auditoría necesarios para demostrar la correcta operación de la TSA por un período razonable.
- Mantener sus obligaciones de hacer disponible la clave pública o sus certificados a terceras partes por un período razonable.
- Eliminar todas las claves privadas, incluyendo las copias de seguridad, evitando su recuperación.

Además, deberá comunicar al Ministerio de Industria, Turismo y Comercio el cese de actividad y los mecanismos que pondrá a disposición de los usuarios para comprobar la validez de los sellos de tiempo emitidos.

6.4.10. Conformidad con los requisitos legales

La TSA de la GISS actúa de conformidad con lo establecido en la Ley 59/2003 de Firma Electrónica, cumpliendo los requisitos exigidos para prestadores de servicios de certificación que expiden certificados reconocidos.

Asimismo, se garantiza el cumplimiento de lo dispuesto en el resto de la legislación vigente, en particular de la Ley Orgánica 14/1999 de Protección de Datos de Carácter Personal, y su Reglamento de desarrollo aprobado por el RD 1720/2007.

6.4.11. Registro de información relativa a los servicios de sellado de tiempo

Toda la información relevante concerniente al funcionamiento de los servicios de sellado de tiempo será almacenada al menos durante 15 años, en particular, para proporciona la evidencia necesarias en procedimientos legales.

Se documentarán los tipos de eventos y la información registrados. Entre otros, se incluirán todos los eventos relativos a la gestión de claves y la sincronización y calibración del reloj.

Toda la información y los eventos registrados se protegerán adecuadamente para evitar su manipulación y mantener la confidencialidad requerida.

6.5. Esquema organizativo

La Autoridad de Sellado de Tiempo se encuentra incluida dentro de la jerarquía de certificación de la ACGISS.

Toda la información relativa a la prestación de servicios de certificación de la GISS está disponible en la página web de la Seguridad Social, y en concreto, en su DPC.

7. CARACTERISTICAS TÉCNICAS DEL SERVICIO

7.1. Perfil del certificado de la TSA

El perfil del certificado de la TSA es el siguiente:

Campos Certificado TSA	
version	**v3**
serialNumber	Identifica un certificado de forma única.
signature	Algoritmo usado por la AC para firmar digitalmente el certificado. **sha1WithRSAEncryption**
issuer	Autoridad de certificación que emite los certificados, con la siguiente nomenclatura: **OU=SGI,O=Seg-Social,C=ES**
Not Before ***Not After***	Intervalo de tiempo en el que la AC garantiza la validez del certificado. Expresado con una fecha de inicio de validez y fecha fin de validez. **36 meses**
Subject	Relaciona la identidad de un usuario con su correspondiente clave pública. Se expresa como Distinguished Name (DN). **cn=SIAVAL SELLADO TSA, ou=Maquinas, ou=SILCON, o=Seg-social, c=ES**
Subject Public Key Info	Algoritmo: RSA Encryption Longitud de Clave: **RSA (1024)**
Extensiones	
authorityKeyIdentifier	Derivada de la aplicación del algoritmo SHA-1 sobre la clave pública de la AC.
subjectKeyIdentifier	Derivada de la aplicación del algoritmo SHA-1 sobre la clave pública del usuario.
keyUsage	Firma Digital (80): Certificados de firma
ExtKeyusage	Impresión de Fecha (1.3.6.1.5.5.7.3.8) Marcado como **crítico**
privateKeyUsagePeriod	Período de uso de la clave privada de firma. Sólo en certificados de firma.
CRLDistributionPoint	CRL donde se busca la información de revocación de un certificado. Se expresa como DN: **cn= CRL1153,ou=SGI,o=Seg-Social,c=ES** **ldap://ldap.seg-social.es/cn=CRL1153,ou=SGI,o=Seg-social,c=ES?certificateRevocationList**

7.2. Proceso de petición y emisión de un sello de tiempo

7.2.1. Proceso para la emisión de un sello de tiempo

Los pasos necesarios para generar un sello de tiempo son los siguientes:
- El cliente calcula el hash del documento a sellar.
- Posteriormente, 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 y revisa si está completa y correcta.
- Si es 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.

7.2.2. Formato de las peticiones y respuestas

Los clientes deben enviar sus peticiones a través del protocolo HTTP, conformando una *time-stamping request* en formato ASN1 y enviarla a la URL:

http://host:port/tspTSA/inputRequestTSA

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 }
```

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 }
```