MINISTERIO
DE EMPLEO
Y SEGURIDAD SOCIAL

SECRETARÍA DE ESTADO
DE LA SEGURIDAD SOCIAL

Gerencia de Informática
de la Seguridad Social

Sellado de Tiempo de ACGISS

Política de certificación

V 2.0.2
(Última revisión: Mayo 2017)

Gerencia de Informática de
la Seguridad Social
c/ Doctor Tolosa Latour s/n
28041 Madrid

Control de cambios

Versión	Observaciones	Fecha
1.0	Versión inicial	10-12-2009
1.1	Asignación de los OIDs	15-12-2009
1.2	Modificación de las ramas internas de OIDs de la GISS	02-02-2010
1.2.1	Modificación del perfil de los certificados	07-04-2010
2.0	Revisión completa por actualización de la PKI para su adaptación al Reglamento eIDAS	20-06-2016
2.0.1	Revisión: corrección de erratas y aclaración de redacción.	22-02-2017
2.0.2	Revisiones de redacción	31-05-2017

Índice

1. INTRODUCCIÓN

1.1. Presentación

La Gerencia de Informática de la Seguridad Social (GISS), como Prestador de Servicios de Confianza que emite certificados cualificados, 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 Energía, Turismo y Agenda Digital.

Para su elaboración, se ha seguido el estándar EN 319 421, 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.

1.2. Nombre del documento e identificación

Nombre del documento	Sellado de Tiempo de ACGISS. Políticas y prácticas de certificación
Versión	2.0.2
Estado del documento	Aprobado
Fecha de emisión	31 mayo 2017
OID (Interno GISS)	2.16.724.1.4.2.2.1.3.1
Localización	http://www.seg-social.es/ACGISS

Significado del OID: joint-iso-itu-t (2) country (16) es (724) adm (1) giss (4) infraestructuras (2) ACGISSv2 (2) SubCA GISS01 (1) Servicios Confianza (3) Política TSA (1)

2. DEFINICIONES Y ACRÓNIMOS

2.1. Definiciones

Autoridad de Sellado de tiempo (TSA): Autoridad perteneciente a un Prestador de Servicios de Confianza que proporciona certeza sobre la preexistencia de determinados documentos electrónicos a un momento dado.

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.

Sello de tiempo electrónico: datos en formato electrónico que vinculan otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante;

Sello cualificado de tiempo electrónico: un sello de tiempo electrónico que cumple los requisitos establecidos en el artículo 42 del Reglamento UE nº 910/2014.

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

Tiempo Universal Coordinado (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
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)
TSU	Time-Stamping Unit
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).

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 confianza, 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.

3.4. Comunidad de usuarios y aplicabilidad

Los usuarios del servicio serán principalmente las aplicaciones/sistemas o clientes definidos en el ámbito de la Secretaría de Estado de la Seguridad Social. La TSA se utilizará a través de la Plataforma de Servicios de Seguridad de la GISS.

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

3.5. Limitaciones de uso

El área de actividad de los certificados y servicios de sellado de tiempo está limitada a aplicaciones/sistemas y clientes específicos dentro del ámbito de la Seguridad Social.

Los servicios de TSA generalmente se utilizan para comprobar la existencia de un dato en un momento dado, principalmente en procesos de firma de documentos y en intercambios de datos con otras entidades.

Los servicios se utilizarán de acuerdo a lo establecido en este documento y en los procedimientos internos que sean aplicables.

3.6. Disponibilidad del servicio

Los servicios de la TSA están disponibles 24 horas al día, 7 días a la semana, excepto en el caso de operaciones de contingencia y de mantenimiento.

En caso de fallo de los sistemas de la TSA, la GISS realizará todos los esfuerzos para que el servicio esté inactivo el mínimo tiempo posible. Para este propósito, los sistemas involucrados en la provisión del servicio están replicados y balanceados, lo que permite garantizar la continuidad del mismo.

4. POLÍTICAS Y PRÁCTICAS

4.1. Introducción

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 generales establecidos en la DPC de la ACGISS, así como las diferentes normativas existentes en el ámbito interno de la GISS.

4.2. Obligaciones y responsabilidades

4.2.1. Obligaciones de la TSA

4.2.1.1. Generales

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

- Seguir los procedimientos y directrices especificados en el presente documento de política y DPC de ACGISS.
- 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.
- 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 confianza según lo especificado en la Ley 59/2003 de Firma Electrónica.

4.2.1.2. Obligaciones de la TSA hacia sus suscriptores

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

Se encargará de garantizar la continuidad del 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.
- Mantener la información de los sellos de tiempo, de acuerdo con lo dispuesto en la legislación aplicable.

4.2.2. 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.
- Cumplir los términos y condiciones publicados.
- 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.

Por otra parte, la Seguridad Social utiliza procesos de custodia para resellar datos periódicamente y evitar la obsolescencia de los algoritmos. Estos procesos pueden ser utilizados por todos los suscriptores del servicio. Además, los suscriptores podrán llevar a cabo re-firmados adicionales si lo estiman conveniente.

4.2.3. 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.

4.2.4. Responsabilidades

De forma general, el Prestador 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.

4.3. Términos y condiciones de uso del servicio

La TSA facilita a los suscriptores y las terceras partes que confíen en su sello de tiempo, los términos y condiciones de uso relativos al servicio a través de un documento que será publicado en la página web del prestador.

Adicionalmente, se pondrá a disposición 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.

5. GESTIÓN Y OPERACIÓN DE LA TSA

5.1. 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 del Prestador y en concreto, en su DPC.

5.2. Seguridad del personal

Según lo especificado en la DPC.

5.3. Clasificación y gestión de activos

Según lo especificado en la DPC

5.4. 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.

5.5. Gestión del ciclo de vida de las claves

5.5.1. 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 entorno físicamente seguro, en un módulo criptográfico HSM certificado con FIPS 140-2 nivel 3 y CC EAL 4+.

La longitud de la claves de los certificados es de 2048 bits.

Se utilizan algoritmo de firma RSA y algoritmos de hash SHA-256 para garantizar la seguridad y la autenticidad de los certificados utilizados.

El tiempo de vida inicial de las claves y certificados de TSU será de 5 años.

5.5.2. 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 al menos bajo control dual.

5.5.3. 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 auto-firmado por la ACGISS.

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

5.5.4. 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 se comunicará a los usuarios del servicio en aquellos casos en que sea necesario.

5.5.5. Backup de la clave de la TSA

Las claves privadas de TSU son sometidas a procesos de backup, copiadas, almacenadas y recuperadas sólo por personal con perfiles definidos utilizando, al menos, control dual en un entorno físicamente seguro.

El personal y los procedimientos para estas funciones y las medidas de seguridad aplicadas a las copias serán las establecidas en la DPC.

5.5.6. 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. La GISS tiene establecidos procedimientos internos que aseguran la renovación de las claves antes de su fecha de caducidad, lo que impide que se generen TST con una clave privada que haya expirado.

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

5.5.7. 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.

Además, serán de aplicación todos los aspectos de gestión de HSM establecidos en la DPC.

5.6. Sellado de tiempo

5.6.1. 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. En caso de producirse una pérdida de sincronización que impida a la GISS garantizar este valor, se cesará la emisión de sellos de tiempo y se informará a todas las partes afectadas. Los servicios se reanudarán una vez recuperada correctamente la sincronización.

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.

Los sistemas de la TSA rehazarán cualquier intento de emitir sellos de tiempo si la clave privada de firma ha expirado.

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.

5.6.2. Sincronización con UTC

El Real Observatorio de la Armada tiene como misión principal el mantenimiento de la unidad básica de Tiempo en España así como el mantenimiento y difusión oficial de la escala "Tiempo Universal Coordinado" (UTC (ROA)), considerada a todos los efectos como la base de la hora legal en todo el territorio nacional (R. D. 23 octubre 1992, núm. 1308/1992).

El reloj de la TSA de la GISS está sincronizado con el tiempo UTC a través de su conexión con el ROA (Real Observatorio de la Armada) realizada por una parte utilizando la red SARA (Sistema de Aplicaciones y Redes para las Administraciones), con una precisión de menos de 1 segundo. Dicha red dispone de mecanismos avanzados para garantizar la fiabilidad, seguridad, capacidad, calidad de servicio e interoperabilidad de los servicios prestados. Por otra parte, para minimizar las posibilidades de pérdida de sincronismo, se configura también un canal alternativo de sincronización directa con ROA a través de Internet.

Se mantiene la calibración de los relojes de forma que se asegure la precisión declarada, y se protegen contra cualquier amenaza que pueda suponer un cambio del tiempo fuera de dicha calibración.

Asimismo, la TSA asegura que ante cualquier diferencia superior a la establecida entre el tiempo indicado en un sello de tiempo y el tiempo UTC, 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).

5.7. Seguridad física y del entorno

Según lo establecido en la DPC.

5.8. Gestión de la seguridad

Según lo establecido en la DPC.

Además, los sistemas de TSA disponen de mecanismos adicionales para la gestión de la calidad y la seguridad apropiados para los servicios de sellado de tiempo.

5.9. Seguridad de red

Según lo establecido en la DPC.

5.10. Gestión de incidencias

Según lo establecido en la DPC.

5.11. Gestión de evidencias

Según lo establecido en la DPC.

5.12. Gestión de continuidad de negocio

Según lo establecido en la DPC.

Además de lo anterior, existen procedimientos específicos de contingencia para los sistemas de TSA, que garantizan la recuperación de las operaciones en menos de 24 horas y la respuesta ante compromisos de claves de TSU y pérdida de sincronismo.

En caso de un compromiso de la clave privada de TSU, al menos la ACGISS:

- Informará a los suscriptores y usuarios del compromiso.
- Revocará el certificado de TSA y publicará la correspondiente lista de revocación.

- Planificará la generación de un nuevo certificado de TSA para evitar la pérdida de servicio, siempre que no existan problemas de seguridad para ello.
- Investigará las causas del compromiso y tomará medidas adecuadas para evitar que se repitan.

En caso de una pérdida de sincronización, al menos la ACGISS:

- Parará la emisión de sellos de tiempo.
- Informará a los suscriptores y usuarios de la pérdida de sincronismo.
- Re-establecerá el servicio lo más rápidamente posible.

5.13. 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.
- Revocar los certificados de TSA.
- Eliminar todas las claves privadas, incluyendo las copias de seguridad, evitando su recuperación.

Además, deberá comunicar al organismo supervisor el cese de servicios y los mecanismos que pondrá a disposición de los usuarios para comprobar la validez de los sellos de tiempo emitidos.

5.13.1. 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.

Los controles técnicos del ciclo de vida de los sistemas involucrados serán los establecidos en la DPC.

5.13.2. 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.

5.13.3. 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 mantenida para permitir la restauración de los servicios y, en particular, para proporcionar las evidencias necesarias en procedimientos legales. Estas actuaciones estarán en funcionamiento durante 15 años para cumplir con la legislación vigente.

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.

5.14. Conformidad o cumplimiento

Esta política está orientada a cumplir los requisitos para la emisión de sellos de tiempo que tengan la condición de cualificados, emitidos teniendo en cuenta los requisitos establecidos en el Reglamento UE nº 910/2014.

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.

6. CARACTERISTICAS TÉCNICAS DEL SERVICIO

6.1. Resumen del perfil del certificado de sello de tiempo

CAMPO	CONTENIDO	VALORES
1. X.509V1		
1.1. Versión	V3	2
1.2. Serial Number	Nº identificativo único	*Automático*
1.3. Signature Algorithm	Tipo de algoritmo. OID 2.16.840.1.101.3.4.2	SHA256RSA
1.4. Issuer Distinguished Name		
1.4.1. Country (C)	ES	ES
1.4.2. Organization (O)	Denominación oficial del prestador	TESORERIA GENERAL DE LA SEGURIDAD SOCIAL
1.4.3 Organizational Unit (OU)	Unidad Organizativa responsable de la emisión	GERENCIA DE INFORMATICA DE LA SEGURIDAD SOCIAL
1.4.4. Locality (L)	Localización	MADRID
1.4.5. Organizational Unit (OU)	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado.	GISS01
1.4.6. Serial Number	Número único de identificación de la entidad de certificación	Q2827003A
1.4.8. Common Name (CN)	Nombre común del certificado de la CA subordinada	SUBCA GISS01

1.6. Subject		
1.5.1. Country (C)	ES	ES
1.5.2. Organization (O)	Denominación del suscriptor	SECRETARIA DE ESTADO DE LA SEGURIDAD SOCIAL
1.5.5. Organizational Unit (OU)	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado.	SERVICIOS DE CONFIANZA
1.5.6. Serial Number	Número único de identificación de la entidad	S2819001E
1.5.7. Common Name (CN)	Denominación del certificado	TSA AUTORIDAD DE SELLADO DE TIEMPO
1.6 Subject Public Key Info	Clave pública del sello codificada	(RSA 2048 bits)
2. X.509v3 Extensions		
2.3. Key Usage		
2.3.1. Digital Signature		"1"
2.3.2. Content Commitment		"1"
2.4 Extended Key Usage		
2.4.1. Impresión de fecha	1.3.6.1.5.5.7.3.8	"1"
2.5. Qualified Certificate Statements	Política de certificados cualificados (OID 0.4.0.1862.1.1)	
2.6. Certificate Policies	OID asociado a la PC de ACGISS y URL de política.	2.16.724.1.4.2.2.1.3.1
2.7. Subject Alternative Name	Correo electrónico de contacto	acgiss.soporte.giss@seg-social.es
2.8. Issuer Alternative Name	Correo electrónico de contacto	acgiss.soporte.giss@seg-social.es
2.9. cRLDistributionPoint	Punto de distribución nº1	http://crl.seg-social.gob.es/ac_sub.crl
2.10. Authority Info Access	dirección web del OCSP URL acceso a certificado SUBCA	http://ocsp.seg-social.gob.es/ http://www.seg-social.es/ACGISS/Certs/SUBCA_GISS01

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

6.2.1. 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.

6.2.2. 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 }
```

7. REFERENCIAS

Legislación aplicable:

- 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.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

- Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público.
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

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

- ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
- ETSI EN 319 422 Profiles for TSP Providing Time-stamping Services.
- RFC 3268 “Requirements for time-stamping authorities”
- RFC 3161 “Internet X.509 Public Key Infraestructure – Time Stamp Protocol (TSP)”