Sellado de Tiempo de ACGISS

TEXTO DIVULGATIVO
(PUBLIC DISCLOSURE STATEMENT – PDS)

Versión: 1.1.3
Vigencia v1: 1 julio 2016 - actualidad
Última revisión: 30 octubre 2020

Este documento contiene las informaciones esenciales a conocer en relación con el servicio de Sellado de tiempo de ACGISS siguiendo las directrices incluidas en el Anexo B del estándar ETSI EN 319 421.

1. Acuerdo completo

El presente documento proporciona declaraciones de alto nivel con respecto al servicio de Sellado de tiempo de ACGISS. No reemplaza ni anula el documento de Política de Sellado de tiempo de ACGISS que se encuentra disponible en http://www.seg-social.es/ACGISS.

2. Información de contacto

2.1. Organización responsable

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

2.2. Contacto

Nombre	Gerencia de Informática de la Seguridad Social		
Dirección e-mail	acgiss.soporte.giss@seg-social.es		
Dirección	C/ Doctor Tolosa Latour s/n 28041 Madrid		
Teléfono	91 390 27 03	**Fax**	91 460 40 72

2.3. Contacto para procesos de revocación

Nombre	Gerencia de Informática de la Seguridad Social		
Dirección e-mail	acgiss.soporte.giss@seg-social.es		
Dirección	C/ Doctor Tolosa Latour s/n 28041 Madrid		
Teléfono	91 390 27 03	**Fax**	91 460 40 72

3. Tipo de certificado, validación y uso

El servicio de sellado de tiempo 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.

La longitud de las claves de los certificados es de 2048 bits. Se utilizan algoritmos de firma RSA y algoritmos de hash SHA-256 para garantizar la seguridad y la autenticidad de los certificados utilizados.

Las claves de sellado de tiempo se generan y utilizan dentro de módulos criptográficos HSM con adecuadas medidas de seguridad que garantizan la protección de las mismas.

3.1. Validación de los certificados

La comprobación del estado de los certificados se podrá realizar por dos métodos diferentes: vía OCSP o mediante descarga de las CRLs. Los sistemas de validación de certificados están disponibles las 24 horas de los 7 días de la semana.

Los sellos de tiempo podrán validarse a través de las herramientas puestas a disposición de los usuarios para la verificación de firmas electrónicas en la Sede Electrónica de la Seguridad Social y en la Intranet corporativa. Asimismo podrá utilizarse la plataforma @Firma de la Administración General del Estado.

3.2. 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.

3.3. 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 confianza ACGISS, que cumple los requisitos técnicos y las obligaciones especificadas en la normativa vigente.

4. Límites de uso

Los certificados de sellado de tiempo delimitan su ámbito de actuación a las aplicaciones/sistemas o clientes definidos en el entorno de la Secretaría de Estado de la Seguridad Social.

De forma general, no se utilizarán los certificados y las claves asociadas para fines distintos de los especificados en el apartado anterior.

No se podrán utilizar los certificados una vez alcanzada su fecha de caducidad ni cuando hayan sido revocados.

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.

En caso de producirse una pérdida de sincronización que impida a la GISS garantizar el valor de tiempo, 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.

Para garantizar la integridad de la información a sellar, se utilizarán algoritmos hash SHA-256 o superiores para la generación de las huellas de los datos en los sellos.

El servicio está disponible 24 horas, 7 días a la semana, excepto para las operaciones de contingencia y mantenimiento.

Toda la información relevante concerniente al funcionamiento de los servicios de sellado de tiempo será mantenida adecuadamente durante 15 años para cumplir con la legislación vigente.

5. Obligaciones de los suscriptores

Los suscriptores del servicio de sellado de tiempo tienen la obligación de:

- Seguir los procedimientos y directrices especificados en la política de certificación.
- 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 la política de certificación.

6. Obligación 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 obligadas a:

- Seguir los procedimientos y directrices especificados en la política de certificación.
- 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 la política.

7. Limitaciones de responsabilidad

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 exento 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.

8. Acuerdos aplicables, DPC y PC

Los acuerdos aplicables al servicio de sellado de tiempo son los siguientes:

- DPC y PC específica (OID 2.16.724.1.4.2.2.1.3.1) que regulan las condiciones de emisión y utilización de los certificados y sellos de tiempo.
- Política best-practices-ts-policy (OID 0.4.0.2023.1.1) definida en el estándar ETSI 319 421.
- Condiciones generales de uso del servicio incorporadas en el texto de divulgación del certificado.

9. Política de privacidad

La ACGISS desarrolla una política de confidencialidad, de acuerdo con la legislación de protección de datos personales vigente en España.

No obstante, cabe señalar que no se tratan datos de carácter personal en la prestación de servicios de sellado de tiempo.

10. Política de reembolso

No aplicable.

11. Legislación aplicable y resolución de conflictos

11.1. Legislación aplicable

La prestación de servicios de sellado de tiempo se realiza conforme a lo establecido en el 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.

Asimismo, se han tenido en cuenta los estándares europeos aplicables en la fecha de aprobación de la normativa de certificación:

- 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.

11.2. Resolución de conflictos

La ACGISS se atiene a los procedimientos generales establecidos para la Administración Pública. La jurisdicción competente será la correspondiente a la resolución de conflictos en las Administraciones Públicas.

Por otra parte, para la resolución de quejas y sugerencias se podrá utilizar el correspondiente buzón disponible en la Sede de la Seguridad Social, así como los procedimientos internos publicados en la Intranet corporativa.

12. Acreditaciones de confianza y auditorías de conformidad

La GISS se encuentra incluida en la lista de prestadores de confianza (TSL) española https://sede.minetur.gob.es/prestadores/tsl/tsl.pdf

Asimismo está registrada como prestador de servicios electrónicos de confianza cualificados en el Ministerio de Economía y Empresa:

http://www.mincotur.gob.es/telecomunicaciones/es-es/servicios/firmaelectronica/paginas/prestadores.aspx

Conforme a lo establecido en el Reglamento UE nº 910/2014, la GISS realizará auditorías bienales de conformidad con dicho Reglamento.