Certificados de Sello Electrónico de ACGISS

TEXTO DIVULGATIVO
(PUBLIC DISCLOSURE STATEMENT – PDS)

Versión: 1.1.3
Vigencia v1: 1 julio 2016 - actualidad
Última revisión: 1 agosto 2019

Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación de ACGISS siguiendo las directrices incluidas en el Anexo A del estándar ETSI EN 319 411-1.

1. Información de contacto

1.1. Organización responsable

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

1.2. 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

1.3. 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

2. Tipo de certificado, validación y uso

2.1. Tipo de certificado

Los certificados de sello electrónico se emiten como certificados de actuación automatizada dentro de la jerarquía de la PKI ACGISSv2 y de acuerdo con la normativa vigente en la AGE relativa a certificados electrónicos de sello electrónico de órgano administrativo.

ACGISS emite dos tipos de certificado de sello electrónico:

- Certificado de nivel medio/sustancial: emitido en soporte SW para su instalación y utilización distribuida en servidores y sistemas de la Seguridad Social que precisen autenticación o firma automatizada.
- Certificado de nivel alto: emitido de forma centralizada en un HSM y utilizable a través de la plataforma de seguridad disponible en la GISS.

Los certificados de sello están dirigidos a los diferentes Órganos o Entidades de la Seguridad Social con rango al menos de Subdirección General, que serán considerados suscriptores o titulares de los certificados.

A continuación se muestra la identificación de las distintas políticas de certificación aplicables:

OID (Interno GISS v2)	2.16.724.1.4.2.2.1.1.1 (nivel medio) 2.16.724.1.4.2.2.1.1.2 (nivel alto)
OID (Política AGE)	2.16.724.1.3.5.6.2 (nivel medio) 2.16.724.1.3.5.6.1 (nivel alto)
OID (ETSI EN 319 411-2)	0.4.0.194112.1.1 (QCP-l) (nivel medio) 0.4.0.194112.1.3 (QCP-l-qscd) (nivel alto)

Significado del OID: joint-iso-itu-t (2) country (16) es (724) adm (1) giss (4) infraestructuras (2) ACGISSv2 (2) SubCA GISS01(1) Actuación Automatizada (1) PC de sello electrónico (1-nivel medio o 2-nivel alto)

Las claves de los certificados de sello son al menos de 2.048 bits y se utilizan algoritmos de firma RSA y algoritmos de hash SHA-256.

2.2. 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.

2.3. Uso de los certificados

Los certificados de sello electrónico se utilizarán para garantizar la identificación y autenticación del ejercicio de las competencias del Órgano o Entidad titular en la actuación administrativa automatizada.

En concreto, la utilización de los certificados de sello atenderá a los usos previstos en la Ley 40/2015 de Régimen Jurídico del Sector Público, el RD 1671/2009 y demás normativa aplicable.

De forma general se podrán realizar con el certificado de sello electrónico actuaciones dirigidas a:

- Autenticación de la identidad del Órgano o Entidad titular.
- Firma electrónica de documentos en el ejercicio de sus funciones.
- Cifrado de datos y documentos en el ejercicio de sus funciones.

3. Límites de uso del certificado

Se acepta el certificado de sello en el momento en que el solicitante recibe la notificación de que se ha realizado correctamente la emisión, sin que se reciba comunicación en contra de rechazo o modificación de los datos en el plazo de 5 días hábiles.

Cada certificado de sello se utilizará exclusivamente por el titular para los fines para los que ha sido emitido.

Las diferentes claves generadas se utilizarán exclusivamente para los propósitos especificados y con arreglo a lo establecido en su política de certificación.

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

4. Obligaciones de los suscriptores

Son obligaciones de los suscriptores/titulares de los certificados:

- Suministrar a las Autoridades de Registro información exacta, completa y veraz en relación con los datos solicitados en los procesos del ciclo de vida de los certificados.
- Notificar cualquier modificación posterior de los datos suministrados.
- Conocer y aceptar las condiciones de emisión y de utilización de los certificados establecidas en la DPC y en las políticas respectivas.
- No utilizar los certificados cuando haya expirado su período de validez o cuando éste haya sido revocado.
- Proteger sus claves privadas tomando las precauciones oportunas para evitar la pérdida, revelación o uso no autorizado.
- Comunicar a la GISS cualquier mal funcionamiento de los certificados o cualquier compromiso de las claves.
- En caso de certificados de sello de nivel alto, generar las claves en HSM certificados como dispositivos cualificados de creación de firmas.

5. Obligación de terceros de comprobar el estado de los certificados

Los terceros que acepten y confíen en los certificados emitidos por ACGISS, deberán:

- Asumir la responsabilidad en la correcta comprobación de la validez y del estado de revocación de los certificados.
- Asumir la responsabilidad en la correcta validación de las firmas electrónicas realizadas con los certificados de ACGISS.
- Conocer las responsabilidades derivadas de la aceptación de los certificados.
- Limitar la aceptación de los certificados a los usos permitidos establecidos en los mismos y en las políticas de certificación aplicables.

6. Limitaciones de responsabilidad

La ACGISS limita su responsabilidad en los términos del artículo 23 de la Ley 59/2003.

La prestación de servicios de certificación se realizará conforme a lo establecido en la normativa de certificación aplicable, utilizando herramientas y prácticas que garanticen la seguridad de los certificados emitidos.

ACGISS no será responsable de los daños y perjuicios ocasionados al firmante o terceros de buena fe, ante incumplimiento de las obligaciones establecidas en la DPC y la PC a los suscriptores, titulares y terceros que aceptan sus certificados.

Adicionalmente, la ACGISS dispone de una garantía de cobertura de su responsabilidad civil suficiente, en los términos previstos en el artículo 20.2 de la Ley 59/2003, de 19 de diciembre.

7. Acuerdos aplicables, DPC y PC

Los acuerdos aplicables al certificado de empleado público son los siguientes:

- DPC y PC específica (OID 2.16.724.1.4.2.2.1.1.1 (nivel medio) y 2.16.724.1.4.2.2.1.1.2 (nivel alto)) que regulan las condiciones de emisión y utilización de los certificados.
- Condiciones generales del servicio incorporadas en el texto de divulgación del certificado o PDS.
- Contrato de emisión de certificados firmado por el solicitante.

8. Política de privacidad

Los datos personales se recaban y tratan atendiendo a los planes de protección aprobados en la Seguridad Social de acuerdo con lo establecido en el Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos (RGPD).

El Prestador no divulga ni cede estos datos personales, excepto en los casos previstos o cuando sea exigible legalmente. La información de registro y la relativa a la generación de los certificados se almacena durante al menos 15 años, de acuerdo con lo establecido en la DPC.

9. Política de reembolso

No aplicable.

10. Legislación aplicable y resolución de conflictos

10.1. Legislación aplicable

La prestación de servicios de certificación 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 y en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

Por otra parte, los certificados de sello se emiten y utilizan según lo indicado en la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público, y en la Política de firma y certificados de la AGE.

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

10.2. 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.

11. 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 cualificado 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.