Certificados de Empleado Público de ACGISS

TEXTO DIVULGATIVO
(PUBLIC DISCLOSURE STATEMENT – PDS)

Versión: 1.1.4
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 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 empleado se emiten como certificados cualificados personales dentro de la jerarquía de la PKI ACGISS v2 y de acuerdo con la normativa vigente en la AGE relativa a certificados electrónicos de empleado público.

Estos certificados están dirigidos a trabajadores de la Seguridad Social (personal funcionario, laboral o eventual) que ejercen sus funciones en los distintos departamentos de la Seguridad Social.

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

OID (Interno GISS)	2.16.724.1.4.2.2.1.2.1*
OID (Política AGE)	2.16.724.1.3.5.7.2
OID (ETSI EN 319 411-2)	0.4.0.194112.1.0 (QCP-n)

Cada certificado electrónico consta de dos pares de claves, uno para la autenticación y firma y otro para el cifrado de datos, identificados con distintos OIDs:

- **Certificado de autenticación y firma** **OID** **2.16.724.1.4.2.2.1.2.11**
- **Certificado de cifrado** **OID** **2.16.724.1.4.2.2.1.2.12**

Significado del OID interno: joint-iso-itu-t (2) country (16) es (724) adm (1) giss (4) infraestructuras (2) ACGISSv2 (2) SubCA GISS01 (1) Personales (2) PC de empleado público (1)

Las claves de los certificados de empleado 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 empleado son certificados de persona física, emitidos a los trabajadores al incorporarse a su puesto de trabajo en una de las Entidades dependientes de la Secretaría de Estado de la Seguridad Social y son revocados al cesar en sus funciones dentro de ese mismo ámbito.

Los certificados de empleado sirven a los trabajadores de la Seguridad Social para realizar las siguientes tareas en el ejercicio de sus funciones:

- Autenticación de la identidad.
- Firma electrónica de documentos.

- Cifrado de datos y documentos.

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

De acuerdo con el Art. 22 del RD 1671/2009, los certificados de empleado público sólo podrán ser utilizados en el desempeño de las funciones propias del puesto que ocupen o para relacionarse con las Administraciones públicas cuando éstas lo admitan.

Asimismo, estos certificados permiten a los usuarios, en el ámbito de la Seguridad Social, acceder a los servicios para la ejecución de las tareas asignadas para la consecución de los fines de la organización.

3. Límites de uso del certificado

La aceptación de los certificados se produce en el momento de la firma del contrato de emisión por el titular.

Los certificados de empleado delimitan su ámbito de actuación a las gestiones propias de las Administraciones Públicas cuando éstas lo admitan.

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.

Los certificados serán revocados cuando los empleados dejen de prestar sus servicios en la Seguridad Social.

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.

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 2.16.724.1.4.2.2.1.2.1*) 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 empleado.

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.

El titular consiente la publicación, exclusivamente en el ámbito interno, de la parte pública de su certificado para la realización de las funciones propias de la organización.

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 empleado 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.