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

Certificados de Empleado Público y de Personal Externo

Políticas de Certificación

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	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

Índice

1. INTRODUCCIÓN

1.1. Presentación

La Seguridad Social, a través de su Prestador de Servicios de Certificación ACGISS emitirá certificados electrónicos para ser usados por sus trabajadores con el propósito de identificación, firma electrónica reconocida y cifrado. Debido a las características diferentes de sus destinatarios, se van a crear dos tipos distintos de certificados:

- Personal Externo.
- Empleados públicos. Tendrán la consideración de "certificado electrónico de empleado público", tal como se define en el Art. 22 del RD 1671/2009.

Se trata de certificados reconocidos a efectos de la Ley 59/2003 de Firma Electrónica, emitidos en un dispositivo seguro de creación de firma proporcionado por la Seguridad Social.

En lo que sigue en este documento, ambos certificados se denominarán "Certificados de Empleados" y únicamente se hará distinción por sus respectivos nombres cuando sea necesario.

Este documento recoge las características específicas de estos dos tipos de certificados.

Para elaborar su contenido se ha seguido la estructura de la RFC 3647, incluyendo aquellos apartados que resultan específicos para estos dos tipos de certificados. La demás información relativa a los procedimientos y condiciones de prestación de servicios de certificación se encuentra en la Declaración de Prácticas de Certificación de la ACGISS.

1.2. Nombre del documento e identificación

Nombre del documento	Certificados Empleado. Política de Certificación
Versión	1.2.1
Estado del documento	Aprobado
Fecha de emisión	07 de abril de 2010
OID	2.16.724.1.4.2.1.4
Localización	www.seg-social.es

Significado del OID: joint-iso-itu-t (2) country (16) es (724) adm (1) giss (4) infraestructuras (2) ACGISS (1) Politica de certificado de empleado (4)

Esta política de de certificación regula una comunidad de usuarios, que obtienen certificados para diversas relaciones administrativas de acuerdo con la Ley 59/2003 y la normativa administrativa correspondiente.

1.3. Participantes de la PKI

1.3.1. Entidades de Registro

El registro de los titulares de los certificados de empleado se realizará en las diferentes unidades de personal de la Seguridad Social.

1.3.2. Usuarios finales

Los Certificados de Empleados están dirigidos a trabajadores de la Seguridad Social, empleados públicos o personal de empresas de servicios, en situación de activo, que ejercen sus funciones en los distintos departamentos de la Seguridad Social.

1.4. Uso de los certificados

1.4.1. Usos típicos de los Certificados de Empleados

Los certificados de empleados 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.

De acuerdo con el Art. 22 del RD 1671/2009, los certificados de empleado 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.

Cada certificado electrónico consta de dos pares de claves, uno para la autenticación y firma y otro para el cifrado de datos. Cada uno de ellos se utilizará exclusivamente para los propósitos para los que se emiten.

1.4.2. Aplicaciones prohibidas

Los Certificados de Empleados 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.

2. IDENTIFICACIÓN Y AUTENTICACIÓN

2.1. Validación inicial de la identidad

2.1.1. Prueba de posesión de clave privada

El par de claves de firma se genera dentro de la tarjeta criptográfica suministrada por la entidad de registro y el de cifrado en la propia Autoridad de Certificación.

La prueba de posesión de las claves privadas de firma se obtiene mediante el envío a la Autoridad de Certificación de las correspondientes claves públicas junto a sus certificados correspondientes para su firma.

2.1.2. Autenticación de la identidad de una persona física

La autenticación del titular del certificado se realiza mediante la personación física ante los órganos de personal respectivos y con la presentación del DNI.

La comprobación de que el titular presta sus servicios en la Seguridad Social, queda garantizada por el hecho de que para la emisión de la tarjeta criptográfica de empleado es necesario estar dado de alta en el registro interno de personal.

2.2. Identificación y autenticación de solicitudes de renovación

2.2.1. Validación para la renovación rutinaria de certificados

Se distinguen dos casos:

- Renovación de claves sin renovación de la tarjeta física. La identificación y autenticación se realizará mediante el acceso al sistema correspondiente a través del Single Sign-On de la GISS y el uso del certificado de autenticación y firma vigente.
- Renovación de claves con renovación de la tarjeta física. El proceso será el mismo que para la emisión inicial del certificado.

2.3. Identificación y autenticación de la solicitud de revocación

El inicio de una solicitud de revocación se produce:

- De oficio cuando una persona deja de prestar sus servicios en la Seguridad Social o por otras causas estipuladas en la Declaración de Prácticas de certificación.
- Por el titular por compromiso de sus claves o por cualquier otra causa que requiera la expedición de una nueva tarjeta criptográfica. En este caso se requiere la personación física del titular en la unidad de personal respectiva.

3. REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS DE EMPLEADO

3.1. Solicitud de emisión de certificado

3.1.1. Quién puede efectuar una solicitud de certificado de empleado

Según el tipo de certificado, se distingue:

- Certificados electrónicos de empleado público. Podrán solicitarlo los empleados públicos (personal funcionario, laboral o eventual) que presten sus servicios en el ámbito de la Secretaría de Estado de la Seguridad Social.
- Certificados electrónicos de personal externo. Incluye al personal externo al servicio de la Seguridad Social.

La petición para la emisión del certificado la realizará la unidad de personal correspondiente a través de la aplicación de registro existente.

3.1.2. Proceso de registro y responsabilidades

La unidad de personal será la encargada de comprobar toda la información relativa al trabajador que solicita el certificado, antes de solicitar su emisión a través de la aplicación de registro. Para que se

genere la petición del certificado es necesario que se introduzcan en dicha aplicación todos los datos solicitados.

La generación de las claves de firma se realiza internamente en la tarjeta y en presencia del titular, garantizando la confidencialidad de las claves privadas.

La ACGISS garantiza que los datos presentes en los certificados son exactos y completos y que las solicitudes quedan registradas en el sistema central.

3.2. Tramitación de la solicitud de certificado

La solicitud de un certificado de empleado se realiza inicialmente de oficio cuando una persona comienza a trabajar en la Seguridad Social. Se realiza desde la unidad de personal respectiva por un empleado público debidamente autorizado.

Este empleado será el encargado de comprobar los datos del titular necesarios para la emisión del certificado.

Asimismo, proporcionará al solicitante antes de la expedición del certificado la información referida en el artículo 18 b) de la Ley 59/2003.

Finalmente, una vez tramitada la solicitud de certificado de empleado público o personal externo según la situación particular del titular, se procederá a la emisión del certificado y se le hará entrega de la tarjeta criptográfica.

En el caso que el solicitante ya posea un certificado de empleado previo, se procede a revocar el anterior antes de la emisión del nuevo certificado.

3.3. Emisión de certificado

3.3.1. Acciones de la ACGISS durante el proceso de emisión

La generación de los dos pares de claves, firma y cifrado, depende de su naturaleza:

- Los pares de claves de autenticación y firma se generan en el soporte criptográfico que se encuentra en la tarjeta.
- Los pares de claves de cifrado se generan en la AC.

Tras la generación de las claves, la aplicación de registro envía la clave pública de firmado y autenticación a la autoridad de certificación y ésta la firma junto al certificado y los devuelve a la tarjeta del titular.

Respecto al certificado de cifrado, firma su clave pública y copia las dos claves y el certificado en la tarjeta.

Además la ACGISS tiene en cuenta los siguientes aspectos:

- Genera los certificados vinculándolos de forma segura con la información del empleado, tal como aparece en el registro de personal.
- Protege el secreto y la integridad de los datos de registro.
- Incluye en el certificado las informaciones establecidas en el artículo 11 de la Ley 59/2003.
- Garantiza la fecha y la hora en que se expide un certificado.
- Utiliza sistemas y productos fiables que están protegidos contra toda alteración y que garantizan la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
- Se asegura que el certificado es emitido por sistemas que utilicen protección contra falsificación.

3.4. Aceptación del certificado

3.4.1. Conducta que constituye aceptación del certificado

El suscriptor acepta el certificado en el momento en que lo desbloquea al acceder con él la primera vez.

3.5. Uso del par de claves y del certificado

3.5.1. Uso por los suscriptores

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

- Firma reconocida de documentos.
- Cifrado de datos y documentos.
- Autenticación de la identidad.

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

Principalmente, los sistemas accedidos pertenecen a la Seguridad Social, aunque se habilita la posibilidad de acceder a otros sistemas de otras Administraciones.

Tal como se dijo anteriormente, el uso de los certificados de empleado estará limitado al desempeño de las funciones propias del puesto que ocupen o para relacionarse con las Administraciones públicas cuando éstas lo admitan.

3.6. Renovación de certificado con renovación de claves

3.6.1. Circunstancias para la renovación con cambio de claves de un certificado

Las claves de autenticación y firma y de cifrado tienen un periodo de vigencia de 36 meses.

3.6.2. Quién puede solicitar la renovación

Cuando se trate de renovación de certificados sin renovación de las tarjetas físicas y se debe a la extinción del período de vigencia, el sistema enviará al empleado un aviso para que sea él mismo quien solicite la renovación de sus certificados.

La solicitud de renovación la realizará el empleado a través de la aplicación desarrollada para ello y disponible en la Intranet de la Seguridad Social.

En el caso de que se tenga que renovar el certificado con renovación de la tarjeta criptográfica, se seguirá el mismo procedimiento que para la emisión inicial de un certificado, es decir, con la personación física del titular en la unidad de personal correspondiente.

3.6.3. Tramitación de las peticiones

Cuando la renovación se realice a través de la aplicación disponible en la Intranet, el usuario se identifica y autentica mediante el uso del Single Sign-On de la Seguridad Social y el certificado de autenticación y firma vigente.

Primeramente la aplicación solicitará la revocación del certificado anterior y a continuación se genera la solicitud de emisión del nuevo certificado.

Cuando se requiera la renovación de la tarjeta, el proceso seguido será el mismo que para la emisión inicial de un certificado.

3.7. Revocación y suspensión de certificados

3.7.1. Causas de revocación de certificados

Además de las causas de revocación especificadas en la Declaración de Prácticas de Certificación de la ACGISS, los certificados de empleado se revocan cuando sus titulares dejan de prestar sus servicios en la Seguridad Social.

3.7.2. Procedimientos de solicitud de revocación

Para proceder a la solicitud de revocación, el suscriptor debe personarse en la unidad de personal correspondiente.

El registrador accede al sistema a través de la aplicación de registro y realiza petición de revocación del certificado.

Un certificado revocado no puede volver a utilizarse; es decir, no puede levantarse la revocación ni anularse de ninguna otra forma.

La revocación de oficio la realiza el personal de las unidades de recursos humanos utilizando la aplicación de registro.

4. CONTROLES DE SEGURIDAD TÉCNICA

4.1. Generación e instalación del par de claves

4.1.1. Generación del par de claves

El par de claves de autenticación y firma se genera internamente en la tarjeta criptográfica del titular, la cual cumple los requisitos de Dispositivo Seguro de Creación de Firma.

El par de claves de cifrado se genera en la Autoridad de Certificación y posteriormente se almacenan también en la tarjeta criptográfica.

4.1.2. Envío de la clave privada al suscriptor

La clave privada se genera en presencia del titular del certificado en la tarjeta criptográfica y no es posible la extracción de la misma. No existe, por tanto, ninguna transferencia de clave privada.

4.1.3. Envío de la clave pública al emisor del certificado

La clave pública se exporta de la tarjeta y es enviada a través de la aplicación de registro a la Autoridad de Certificación para su firma.

4.1.4. Longitud de claves

Las claves de los suscriptores de certificados de Empleado son al menos de 1.024 bits.

4.1.5. Usos admitidos de las claves

El contenido de los campos relativos a los usos permitidos de las claves para ambos tipos de certificado es el siguiente:

KeyUsage	digitalSignature (80): Certificados de firma keyEncipherment (20): Certificados de cifra
ExtKeyUsage	Email Protección Client Authentication

4.2. Protección de la clave privada

4.2.1. Estándares de módulos criptográficos

La protección de las claves privadas de los certificados de empleado se realiza a través de la tarjeta criptográfica donde reside.

4.2.2. Repositorio de la clave privada

La custodia de las claves privadas de los certificados la realizan los empleados titulares de los mismos.

En el caso de las claves privadas de autenticación y firma, en ningún caso se podrán almacenar en la Autoridad de Certificación, Entidad de Registro ni ningún otro elemento de la infraestructura de la PKI.

Las claves privadas de autenticación y firma se encuentran almacenadas en la tarjeta criptográfica, de manera que no es posible su extracción fuera de la misma.

Las claves privadas de cifrado se almacenan de forma segura en la Autoridad de Certificación.

4.2.3. Backup de la clave privada

No es posible realizar una copia de seguridad de las claves privadas de autenticación y firma asociadas a los certificados de empleado, ya que las claves no pueden ser exportadas fuera de la tarjeta.

La copia de seguridad de las claves privadas de cifrado siguen los mismos procedimientos que el resto de la información almacenada por la Autoridad de Certificación, definidos en la Declaración de Prácticas de Certificación.

4.2.4. Método de activación de la clave privada

La activación de las claves y del certificado requiere la introducción de una clave personal de acceso (PIN) del titular, que debe permanecer bajo su exclusivo conocimiento.

4.2.5. Método de desactivación de la clave privada

Cuando la aplicación que utilice el certificado de Empleado finalice la sesión, será necesaria nuevamente la introducción del PIN.

4.3. Otros aspectos de gestión del par de claves

4.3.1. Periodos de utilización de las claves pública y privada

Los periodos de utilización de las claves públicas y privadas son de 3 años, es decir, igual a los períodos de validez de los certificados.

4.4. Datos de activación

4.4.1. Generación e instalación de los datos de activación

El dato de activación de las claves de los certificados de empleado, consiste en una clave personal (PIN) de la tarjeta que lo contiene.

4.4.2. Protección de los datos de activación

Sólo el titular del certificado conoce la clave personal de acceso o PIN, siendo por tanto el único responsable de la protección de los datos de activación de sus claves privadas.

5. PERFILES DE CERTIFICADOS

5.1. Perfil de certificado

El perfil de los certificados de Empleado son los siguientes:

5.1.1. Certificado de Empleado Público

Campos Certificados Empleado Público	
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: **O=”Denominación Entidad emisora, OU=”Nombre de la entidad emisora”, emisora”,C=Es** **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= ‘’Apellido1” “ Apellido2” “Nombre” – “NIF”, OU=”Código Agrupación”, OU=”EMPLEADO PUBLICO”, OU=ACGISS,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	digitalSignature (80): Certificados de firma keyEncipherment (20): Certificados de cifra
Extkeyusage	Email Protección

	Client Authentication
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= CRL<n>,ou=SGI,o=Seg-Social,c=ES**

Extensiones (continuación)	
Certificate Policies	Politicas de certificación se establece la directiva del certificado y la Información de las practicas de Certificación Identificador de directiva OID 2.16.724.1.4.2.1.4 CPS Pointer URL – Calificador de directiva http://www.seg-social.es/Internet_1/Sede/Certificadosdigital47735/ACGISS/index.htm User Notice URL – Condiciones de Uso http://www.seg-social.es/Internet_1/Sede/Certificadosdigital47735/ACGISS/index.htm
Authority Info Access	Método de acceso a la publicación de las CRLs URL OCSP/LDAP https://ocsp.seg-social.gob.es/responder
QcCompilance	Indicación de Certificado Reconocido **QcCompilance** OID “Especifico de Certificado Reconocido” **QCEuRententionPeriod** Período retención de información :**15 años**
SubjectAlternateNames	Identificador alternativo para los usuarios: Dirección del directorio: OID:1.3.6.1.4.1.14862.1.4.4.2.1=”**Empleado Público**” OID:1.3.6.1.4.1.14862.1.4.4.2.2=”**ACGISS**” OID: 1.3.6.1.4.1.14862.1.4.4.2.3=”**NIF Entidad Subscriptora”** OID**:** 1.3.6.1.4.1.14862.1.4.4.2.6=”**Nombre Responsable Certificado**” OID:1.3.6.1.4.1.14862.1.4.4.2.7= “**Apellido1**” OID:1.3.6.1.4.1.14862.1.4.4.2.8 = “**Apellido2**” OID:1.3.6.1.4.1.14862.1.4.4.2.4 “**DNIE/NIE Responsable Certificado**”

5.1.2. Certificado de Personal Externo

Campos Certificados Personal Externo

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: **O=”Denominación Entidad emisora, OU=”Nombre de la entidad emisora”, emisora”,C=Es** **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= ‘’Apellido1” “ Apellido2” “Nombre” – “NIF”, OU=”Código Agrupación”, OU=”PERSONAL EXTERNO”, OU=ACGISS,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	digitalSignature (80): Certificados de firma keyEncipherment (20): Certificados de cifra
Extkeyusage	Email Protección Client Authentication
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= CRL<n>,ou=SGI,o=Seg-Social,c=ES**

Extensiones (continuación)	
Certificate Policies	Politicas de certificación se establece la directiva del certificado y la Información de las practicas de Certificación Identificador de directiva OID 2.16.724.1.4.2.1.4 CPS Pointer URL – Calificador de directiva http://www.seg-social.es/Internet_1/Sede/Certificadosdigital47735/ACGISS/index.htm User Notice

	URL – Condiciones de Uso http://www.seg-social.es/Internet_1/Sede/Certificadosdigital47735/ACGISS/index.htm
Authority Info Access	Método de acceso a la publicación de las CRLs URL OCSP/LDAP https://ocsp.seg-social.gob.es/responder
QcCompilance	Indicación de Certificado Reconocido **QcCompilance** OID "Especifico de Certificado Reconocido" **QCEuRententionPeriod** Período retención de información :**15 años**
SubjectAlternateNames	Identificador alternativo para los usuarios: Dirección del directorio: OID:1.3.6.1.4.1.14862.1.4.4.2.1="**Personal Externo**" OID:1.3.6.1.4.1.14862.1.4.4.2.2="**ACGISS**" OID: 1.3.6.1.4.1.14862.1.4.4.2.3="**NIF Entidad Subscriptora"** OID**:** 1.3.6.1.4.1.14862.1.4.4.2.6="**Nombre Responsable Certificado**" OID:1.3.6.1.4.1.14862.1.4.4.2.7= "**Apellido1**" OID:1.3.6.1.4.1.14862.1.4.4.2.8 = "**Apellido2**" OID:1.3.6.1.4.1.14862.1.4.4.2.4 "**DNIE/NIE Responsable Certificado**"

6. REQUISITOS COMERCIALES Y LEGALES

6.1. Obligaciones y responsabilidad civil

6.1.1. Suscriptores

Los suscriptores de los certificados de empleado emitidos por ACGISS están obligados a:

a. Si el usuario detectara algún error en los datos almacenados en las bases de datos de personal deberá advertirlo inmediatamente al departamento de Recursos Humanos (RRHH) de su Organismo.

b. Comunicar igualmente al departamento de RRHH cualquier variación en los datos personales a fin de ser corregidos en las Bases de Datos de Personal, Confidencialidad y actualizar si fuera necesario los certificados contenidos en la tarjeta.

c. Realizar un uso adecuado del certificado en base a las competencias y facultades atribuidas por el cargo, puesto de trabajo o personal externo al servicio de la Seguridad Social.