MINISTERIO
DE TRABAJO, MIGRACIONES
Y SEGURIDAD SOCIAL

SECRETARÍA DE ESTADO
DE LA SEGURIDAD SOCIAL

Gerencia de Informática
de la Seguridad Social

Certificados de Empleado Público de ACGISS

Política de certificación

V 2.0.4
(Julio 2019)

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	20-02-2017
2.0.2	Revisión de redacción.	28-04-2017
2.0.3	Cambios debidos a revisión anual interna: corrección de erratas y actualización de Ministerio.	03-08-2018
2.0.4	Revisión anual interna.	31-07-2019

Índice

1. INTRODUCCIÓN

1.1. Presentación

La Seguridad Social, a través de su Autoridad de Certificación ACGISS emitirá certificados electrónicos para sus empleados con el propósito de identificación, firma electrónica y cifrado.

Se trata de certificados cualificados, conformes con la Ley 59/2003 de Firma Electrónica y que tienen en cuenta los requisitos establecidos en el Reglamento UE nº 910/2014, emitidos en una tarjeta criptográfica segura proporcionada por la Seguridad Social.

Estos certificados se emiten como certificados de empleado público, conforme al art. 22 del RD 1671/2009 y a la política de firma y certificados de la Administración General del Estado.

Como parte de la normativa general de certificación de ACGISS, este documento recoge las características específicas de los certificados de empleado público. Las condiciones generales de prestación de servicios de certificación, no dispuestas en esta política, se establecen en la DPC de ACGISS.

Para elaborar su contenido se ha seguido la estructura de la RFC 3647, incluyendo aquellos apartados que resultan específicos para este tipo de certificado.

1.2. Identificación del documento

Nombre del documento	Certificados Empleado. Política de Certificación
Versión	2.0.4
Estado del documento	Aprobado
Fecha de emisión	31 de julio de 2019
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)
Localización	http://www.seg-social.es/ACGISS

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)

1.3. Participantes de la PKI

1.3.1. Autoridades de Registro

Se consideran autoridades de registro:

- Las unidades de personal de la Seguridad Social.
- El Centro de Seguridad de la Información de la GISS, como responsable de las herramientas y componentes de seguridad que permiten la identificación y autenticación de los usuarios y la emisión de certificados de forma telemática.

1.3.2. Suscriptores y usuarios finales

Los certificados de empleado 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.

La Secretaría de Estado de la Seguridad Social tendrá la consideración de suscriptor general de los certificados de empleado. El titular, usuario o responsable de los certificados será el propio empleado.

1.4. Uso de los certificados

1.4.1. Tipos de certificados emitidos

Los certificados de empleado se emiten como certificados personales dentro de la jerarquía de la PKI y de acuerdo con la normativa vigente en la AGE relativa a certificados electrónicos de empleado público de nivel medio.

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**

1.4.2. Usos típicos de los certificados de empleado

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.

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.

Cada par de claves se utilizará exclusivamente para los propósitos para los que se generan.

1.4.3. Aplicaciones prohibidas

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.

1.5. Administración de la política

Según lo establecido en la DPC.

1.6. Definiciones y acrónimos

Según lo establecido en la DPC.

2. REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN

Según lo establecido en la DPC.

De forma complementaria se publicará información relativa a las condiciones de uso y los servicios relacionados con este tipo de certificados en la Intranet de la Seguridad Social.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. Gestión de nombres

3.1.1. Tipos de nombres

Los certificados de empleado público se emiten de acuerdo con la política de firma y certificados de la AGE en lo relativo a la formación y uso de los campos de los certificados.

Con respecto a la gestión de nombres, además de las condiciones establecidas de forma general en la DPC, se aplican los siguientes criterios para la composición del atributo CN (*Common Name*):

- La estructura será: "NOMBRE" (espacio) "PRIMER APELLIDO" (espacio) "SEGUNDO APELLIDO" (espacio) (espacio-guión-espacio) "NIF/NIE"

- Todos los literales aparecerán en mayúsculas y sin tildes y no se incluirán más de un espacio entre cadenas ni caracteres en blanco al principio o al final de éstas.
- Los datos utilizados serán los presentes en las bases de datos oficiales de la Seguridad Social.

Se utilizan además los siguientes campos de identidad administrativa en el "Nombre Alternativo del Sujeto" (*Subject Alternative Name*):

Tipo de certificado **OID 2.16.724.1.3.5.7.2.1**	CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO
Nombre de la entidad suscriptora **OID 2.16.724.1.3.5.7.2.2**	SECRETARIA DE ESTADO DE LA SEGURIDAD SOCIAL
NIF entidad suscriptora **OID 2.16.724.1.3.5.7.2.3**	S2819001E
DNI/NIE del titular **OID 2.16.724.1.3.5.7.2.4**	NIF/NIE DEL EMPLEADO
Nombre de pila del titular **OID 2.16.724.1.3.5.7.2.6**	NOMBRE DEL EMPLEADO
Primer apellido del titular **OID 2.16.724.1.3.5.7.2.7**	PRIMER APELLIDO DEL EMPLEADO
Segundo apellido del titular **OID 2.16.724.1.3.5.7.2.8**	SEGUNDO APELLIDO DEL EMPLEADO

3.2. Validación inicial de la identidad

3.2.1. Prueba de posesión de clave privada

Los pares de claves se generan dentro de la tarjeta criptográfica suministrada por la Autoridad de Registro.

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

3.2.2. Autenticación de la identidad de una persona física

Para la emisión de certificados de empleado público se precisa siempre la personación física del titular en alguna de las oficinas de las Entidades Gestoras y Servicios Comunes de la Seguridad Social.

La autenticación de la identidad del empleado se realizará en las unidades de personal correspondientes en el momento de incorporarse a su puesto de trabajo en una de las Entidades de la Seguridad Social, previa identificación mediante documento nacional de identidad o medio equivalente.

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 de personal. La incorporación a dicho registro se realiza una vez superado el proceso selectivo correspondiente y publicado el nombramiento en el Boletín Oficial del Estado. Este registro se mantiene actualizado de forma que se detecta cualquier cambio en la situación laboral del empleado y, concretamente, el cese de la prestación de servicios en la organización. Toda modificación del registro se mantiene registrada de forma que es posible consultarla en cualquier momento si es necesario.

Los datos del empleado incorporados en el certificado electrónico serán extraídos directamente del registro de personal y de las bases de datos oficiales de la Seguridad Social, de forma que se garantice su autenticidad.

La autenticación de la identidad del empleado en las aplicaciones y herramientas de gestión de certificados se garantiza mediante:

- Control de acceso físico a las instalaciones, mediante tarjeta criptográfica o, en su defecto, autenticación por personal de seguridad, que garantiza su presencia física en las oficinas.
- Control de acceso lógico posterior en el PC con mecanismo de doble factor de autenticación: tarjeta criptográfica y PIN de acceso.
- Sistema integrado de gestión de identidades y autorizaciones para el acceso a las distintas aplicaciones de la Seguridad Social.

3.3. Identificación y autenticación de solicitudes de renovación

3.3.1. 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 en las unidades de personal o mediante el acceso al sistema correspondiente a través de los sistemas de identificación y autorización 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.

3.4. 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. Para solicitar la revocación se requiere la personación física del titular en la unidad de personal respectiva o, si esto no fuera posible, el uso del servicio de revocación remota proporcionado al efecto. En este último caso se requerirá la personación física posterior del titular en la unidad de personal de cara a obtener un nuevo certificado.

4. REQUISITOS OPERACIONALES DEL CICLO DE VIDA DE CERTIFICADOS DE EMPLEADO

4.1. Solicitud de emisión de certificado

4.1.1. Quién puede efectuar una solicitud de certificado de empleado

La petición para la emisión del certificado a un nuevo empleado la realizará la unidad de personal correspondiente a través de la aplicación de registro, previa personación física del titular.

Los certificados irán destinados a los empleados públicos (personal funcionario, laboral o eventual) que presten sus servicios en el ámbito de la Secretaría de Estado de la Seguridad Social.

4.1.2. Proceso de registro y responsabilidades

La unidad de personal será la encargada de comprobar toda la información relativa al trabajador titular del certificado, antes de solicitar su emisión a través de la aplicación de registro.

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.

Asimismo, proporcionará al solicitante antes de la expedición del certificado la información referida en el artículo 18 b) de la Ley 59/2003. Estas condiciones deberán ser firmadas por el titular.

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

4.2. Tramitación de la solicitud de certificado

4.2.1. Realización de las funciones de identificación y autenticación

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 autenticar al titular y comprobar los datos necesarios para la emisión del certificado, según lo establecido en el apartado correspondiente de este documento.

4.2.2. Aprobación o denegación de las solicitudes

Las solicitudes se aprueban por las correspondientes unidades de personal una vez realizadas las acciones anteriores. Se deniegan las solicitudes siempre que no se cumplan las condiciones mínimas establecidas para la identificación y autenticación de la identidad del empleado.

4.3. Emisión de certificados

4.3.1. Acciones de la ACGISS durante el proceso de emisión

Una vez tramitada la solicitud de certificado de empleado público 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.

Los dos pares de claves se generan en el interior de la tarjeta criptográfica.

Tras la generación de las claves, la aplicación de registro envía las claves públicas a la Autoridad de Certificación y ésta la firma junto al certificado y los devuelve a la tarjeta del titular.

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.

4.3.2. Notificación de la emisión al suscriptor/titular

La notificación de la emisión al titular se realiza una vez finalizado el proceso de emisión, mediante la entrega de la tarjeta criptográfica que contiene el certificado. La tarjeta se entrega bloqueada para impedir su utilización hasta la activación por el usuario.

4.4. Aceptación del certificado

4.4.1. Conducta que constituye aceptación del certificado

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

La emisión de certificados de empleado es un requerimiento de la Secretaría de Estado de la Seguridad Social para poder identificar al empleado y facilitar el ejercicio de sus funciones. La Secretaría de Estado acepta por tanto las condiciones y términos de uso establecidos en este documento.

La política de certificación y el resumen de condiciones de uso aplicables serán publicadas adicionalmente en la Intranet de la Seguridad Social para su consulta por los empleados.

4.5. Uso del par de claves y del certificado

4.5.1. Uso por los titulares

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.

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 otras Administraciones Públicas cuando éstas lo admitan.

4.6. Renovación del certificado sin renovación de claves

Según lo establecido en la DPC.

4.7. Renovación de certificado con renovación de claves

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

La renovación de los certificados puede producirse por alguna de las causas establecidas en la DPC y en concreto:

- Pérdida o deterioro del anterior.
- Fin del período de vigencia de los certificados. Esta circunstancia se notificará al titular con tiempo suficiente para que pueda realizar la renovación antes del fin del periodo de vigencia.
- Re-emisión de oficio por parte de la Seguridad Social derivada de una actualización de la infraestructura o de los perfiles de los certificados.

4.7.2. Quién puede solicitar la renovación

Cuando se trate de renovación de certificados sin renovación de tarjetas físicas y se debe a la extinción del período de vigencia o a cambios en la infraestructura o en los perfiles de certificados, el sistema enviará al empleado un aviso para que sea él mismo quien inicie el proceso de renovación de sus certificados.

En el caso de que se tenga que renovar el certificado con renovación de la tarjeta criptográfica o que se produzcan incidencias en el proceso anterior, se seguirá el mismo procedimiento que para la emisión inicial de un certificado.

4.7.3. Tramitación de las peticiones

Antes de realizar la solicitud del certificado se autenticará previamente al empleado, para lo que se utilizarán los sistemas de la GISS existentes para ello, ya detallados en el apartado 2.2.2., con presencia física del mismo en una oficina de la Seguridad Social. La renovación se realizará preferentemente a través de la aplicación desarrollada para ello y disponible en la Intranet de la Seguridad Social.

Primeramente, se verifican los datos de la tarjeta y la viabilidad de la renovación. Seguidamente la aplicación solicitará la firma de las condiciones de uso del certificado y a continuación, una vez solicitada la revocación del certificado anterior, se genera la solicitud del nuevo certificado. Por último, se almacenan en la tarjeta los nuevos certificados renovados y se informa al usuario de su vigencia.

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

En ambos casos, todos los datos incorporados al certificado serán validados de nuevo contra el registro de personal y las bases de datos de la Seguridad Social para garantizar su actualización.

4.7.4. Notificación de la emisión al suscriptor/titular

Los procedimientos indicados aseguran la notificación al titular una vez realizado el proceso de emisión.

4.8. Modificación de certificados

Según lo establecido en la DPC.

4.9. Revocación y suspensión de certificados

4.9.1. 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.

4.9.2. Legitimación para solicitar la revocación

La revocación del certificado de empleado podrá solicitarla:

- El propio empleado.
- Las unidades de personal correspondientes.
- La ACGISS de oficio.

4.9.3. Procedimientos de solicitud de revocación

Para proceder a la solicitud de revocación por alguna de las causas especificadas en la DPC, el titular debe personarse en la unidad de personal correspondiente. El registrador accede al sistema a través de la aplicación de registro y realiza la petición de revocación del certificado.

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

Cuando no sea posible la personación física en las unidades de personal y se cumplan las condiciones establecidas para ello, la revocación se realizará mediante el uso del servicio de revocación puesto a disposición de los empleados. Será necesario personarse posteriormente en la unidad de personal correspondiente para solicitar la emisión de un nuevo certificado.

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

4.9.4. Plazo máximo de procesamiento de la solicitud de revocación

La solicitud de revocación se realizará de forma inmediata una vez personado el empleado público en las unidades de personal correspondientes.

Las solicitudes no realizadas de forma presencial se procesarán en el mínimo tiempo posible teniendo en cuenta las limitaciones técnicas de los sistemas involucrados. En todo caso se garantiza la atención de las solicitudes dentro de un plazo máximo de 24 horas.

4.10. Servicios de comprobación del estado de los certificados

Según lo establecido en la DPC.

4.11. Finalización de la suscripción

Según lo establecido en la DPC.

4.12. Custodia y recuperación de claves

No se realiza custodia de las claves privadas de los certificados de empleado público, por lo que tampoco es posible la recuperación posterior, siendo necesario en su caso iniciar un nuevo proceso de emisión de certificados.

5. CONTROLES DE SEGURIDAD FÍSICA, GESTIÓN Y OPERACIONES

Según lo establecido en la DPC.

5.1. Procedimientos de auditoría de seguridad

Según lo establecido en la DPC.

En particular, en el caso de certificados de empleado público, serán registrados específicamente los siguientes eventos:

- Datos relacionados con la emisión, renovación y revocación de los certificados de empleado.
- Cambios en las políticas de certificados de empleado.
- Firma de los certificados de empleado.
- Firma de las condiciones de uso por el usuario.
- Otras relacionados con la operación de los sistemas de la infraestructura en la emisión de certificados de empleado.

6. CONTROLES DE SEGURIDAD TÉCNICA

6.1. Generación e instalación del par de claves

6.1.1. Generación del par de claves

Los pares de claves se generan internamente en la tarjeta criptográfica del titular, la cual dispone de las medidas de seguridad suficientes para proteger las claves privadas.

6.1.2. Envío de la clave privada al suscriptor

Las claves privadas se generan en presencia del titular del certificado en la tarjeta criptográfica y no es posible la extracción de las mismas. No existe, por tanto, ningún envío de clave privada al titular.

6.1.3. Envío de la clave pública al emisor del certificado

Las claves públicas se exportan de la tarjeta y son enviadas a través de las aplicaciones de registro o renovación a la Autoridad de Certificación para su firma.

6.1.4. Longitud de claves

Las claves de los suscriptores de certificados de empleado son al menos de 2.048 bits.

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

6.1.5. 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:

- Uso de las claves (Key Usage):

Certificado de autenticación y firma	
KeyUsage	Digital Signature Content Commitment
Certificado de cifrado	
KeyUsage	KeyEncipherment DataEncipherment

- Uso extendido de las claves (Extended Key Usage):

Certificados de autenticación y firma y cifrado	
ExtKeyUsage	Email Protección Client Authentication

6.2. Protección de la clave privada

6.2.1. 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. Esta tarjeta dispone de mecanismos de seguridad para garantizar la correcta custodia de las claves.

6.2.2. Repositorio de la clave privada

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

Las claves privadas de autenticación y firma se encuentran almacenadas en la tarjeta criptográfica, de manera que no es posible la extracción fuera de la misma. En ningún caso se podrán almacenar en la Autoridad de Certificación, Autoridad de Registro ni ningún otro elemento de la infraestructura de la PKI.

6.2.3. 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.

6.2.4. 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.

6.2.5. Método de desactivación de la clave privada

La clave privada se desactiva al extraer la tarjeta del lector. Además, cuando la aplicación que utilice el certificado de empleado finalice la sesión, será necesaria nuevamente la introducción del PIN.

6.3. Otros aspectos de gestión del par de claves

Según lo establecido en la DPC.

6.4. Datos de activación

6.4.1. 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, elegida por su titular en el momento de desbloquear la tarjeta por primera vez. El desbloqueo de la tarjeta se realiza en su puesto de trabajo una vez identificado utilizando los sistemas de autenticación y autorización de la Seguridad Social.

6.4.2. 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.

6.5. Controles de seguridad informática

Según lo establecido en la DPC.

6.6. Controles técnicos del ciclo de vida

Según lo establecido en la DPC.

6.7. Controles de seguridad de red

Según lo establecido en la DPC.

6.8. Sellado de tiempo

Según lo establecido en la DPC.

7. PERFILES DE CERTIFICADOS

7.1. Perfil de certificado

CAMPO	DESCRIPCIÓN	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.	GISS01
1.4.6. Serial Number	Número único de identificación de la entidad de certificación	Q2827003A
1.4.7. Common Name (CN)	Nombre común del certificado de la CA subordinada	SUBCA GISS01
1.5. Validity		
1.5.1. Not Before	Fecha inicio validez YYMMDDHHMMSSZ	YYMMDDHHMMSSZ
1.5.2. Not After	Fecha fin validez YYMMDDHHMMSSZ	YYMMDDHHMMSSZ
1.6. Subject		
1.6.1. Country (C)	ES	ES
1.6.2. Organization (O)	Denominación "oficial" de Administración suscriptora del certificado.	SECRETARIA DE ESTADO DE LA SEGURIDAD SOCIAL
1.6.3. Organizational Unit (OU)	Tipo de certificado	CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO
1.6.4. Organizational Unit (OU)	Subdivisión interna según categoría del certificado	PERSONALES
1.6.5. Organizational Unit (OU)	Subdivisión interna a efectos de gestión	Dos dígitos asignados automáticamente
1.6.6. Serial Number	NIF/NIE del titular	IDCES-"NIF/NIE"

1.6.7. Surname	Primer y segundo apellido y DNI	"PRIMER APELLIDO" (espacio) "SEGUNDO APELLIDO" (espacio-guión-espacio) "NIF/NIE"
1.6.8. Given Name	Nombre de pila	"NOMBRE"
1.6.9. Common Name (CN)	Nombre del titular	"NOMBRE" (espacio) "PRIMER APELLIDO" (espacio) "SEGUNDO APELLIDO" (espacio) (espacio-guión-espacio) "NIF/NIE"
1.7. Subject Public Key Info	Clave pública del certificado	(RSA 2048 bits)
2. X.509v3 Extensions		
2.1. Authority Key Identifier		
2.1.1. KeyIdentifier	Identificador de clave pública del emisor. Path de identificación	*Automático*
2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde esa clave	*Automático*
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de la CA	*Automático*
2.2. Subject Key Identifier	Identificador de la clave pública del suscriptor	*Automático*
2.5. Qualified Certificate Statements		
2.5.1. QcCompliance	Indicación de certificado cualificado	OID 0.4.0.1862.1.1
2.5.2. QcEuRetentionPeriod	Período de conservación	OID 0.4.0.1862.1.3 =15
2.5.3. QcType-esign	Certificado de firma	OID 0.4.0.1862.1.6.1
2.5.4. QcPDS	Lugar donde se encuentra la declaración PDS	OID 0.4.0.1862.1.5 https://www.seg-social.es/ACGISS https://sede.seg-social.gob.es/descarga/ACGISS_PDSEmployee.pdf
2.6. Certificate Policies		
2.6.1. Policy Identifier	OID que indica certificado de empleado público nivel medio según política AGE	2.16.724.1.3.5.7.2
2.6.2. Policy Identifier	QCP-n	0.4.0.194112.1.0
2.6.4. Policy Qualifier ID		
2.6.4.1 CPS Pointer	URL de la Política de certificación	http://www.seg-social.es/ACGISS
2.6.4.2 User Notice	URL Condiciones de Uso	Certificado cualificado de empleado público, nivel medio. Consulte las condiciones de uso en http://www.seg-social.es/ACGISS
2.7. Subject Alternative Name		
2.7.2. Directory Name	Identidad Administrativa	
2.7.2.1. Tipo de certificado	Indica la naturaleza del certificado	2.16.724.1.3.5.7.2.1 = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO (de nivel medio)
2.7.2.2. Nombre de la entidad suscriptora	Nombre de la Entidad suscriptora de la que depende el empleado	2.16.724.1.3.5.7.2.2 = SECRETARIA DE ESTADO DE LA SEGURIDAD SOCIAL
2.7.2.3. CIF entidad suscriptora	CIF de la Entidad suscriptora	2.16.724.1.3.5.7.2.3 = S2819001E
2.7.2.4. DNI/NIE del responsable	NIF/NIE del empleado	2.16.724.1.3.5.7.2.4 = "NIF/NIE"
2.7.2.6. Nombre de pila	Nombre del empleado	2.16.724.1.3.5.7.2.6 = "NOMBRE"
2.7.2.7. Primer apellido	Primer apellido del empleado	2.16.724.1.3.5.7.2.7 = "PRIMER APELLIDO"
2.7.2.8. Segundo apellido	Segundo apellido del empleado	2.16.724.1.3.5.7.2.8 = "SEGUNDO APELLIDO"
2.8. Issuer Alternative Name	Nombre alternativo de contacto de la entidad emisora	
2.8.1. rfc822Name	Correo electrónico de contacto	acgiss.soporte.giss@seg-social.es

2.9. cRLDistributionPoint		
2.9.1. distributionPoint	Punto de distribución nº1	http://crl.seg-social.gob.es/ac_sub.crl
2.10. Authority Info Access		
2.10.1. Access Method	ID de On-line Certificate Status Protocol	Id-ad-ocsp
2.10.2. Access Location	dirección web del OCSP	http://ocsp.seg-social.gob.es/
2.10.3. Access Method	ID de localización del certificado de CA emisora del certificado	Id-ad-caIssuers
2.10.4. Access Location	URL acceso a certificado SUBCA	http://www.seg-social.es/ACGISS/Certs/SUBCA_GISS01 http://www.seg-social.es/ACGISS/SUBCA_GISS01
2.11. Basic Constraints		
2.11.2. Path Length Constraints	Puede especificarse un número máximo de niveles.	Ninguno

3. X.509v3 Extensions (FIRMA Y AUTENTICACIÓN)		
2.3. Key Usage		
2.3.1. Digital Signature		"1"
2.3.2. Content Commitment		"1"
2.3.3. Key Encipherment		"0"
2.3.4. Data Encipherment		"0"
2.3.5. Key Agreement		"0"
2.3.6. Key CertificateSignature		"0"
2.3.7. CRL Signature		"0"
2.4 Extended Key Usage		
2.4.1. Email Protection		"1"
2.4.2. Client Authentication		"1"
2.6. Certificate Policies		
2.6.3. Policy Identifier	OID asociado al certificado de firma y autenticación	2.16.724.1.4.2.2.1.2.11

4. X.509v3 Extensions (CIFRADO)		
2.3. Key Usage		
2.3.1. Digital Signature		"0"
2.3.2. Content Commitment		"0"
2.3.3. Key Encipherment		"1"
2.3.4. Data Encipherment		"1"
2.3.5. Key Agreement		"0"
2.3.6. Key CertificateSignature		"0"
2.3.7. CRL Signature		"0"
2.4 Extended Key Usage		
2.4.1. Email Protection		"1"
2.4.2. Client Authentication		"0"
2.6. Certificate Policies		
2.6.3. Policy Identifier	OID asociado al certificado de cifra	2.16.724.1.4.2.2.1.2.12

7.2. Perfil de la lista de certificados revocados (CRLs)

Según lo establecido en la DPC.

7.3. Perfil OCSP

Según lo establecido en la DPC.

8. AUDITORÍA DE CONFORMIDAD

8.1. Frecuencia de la auditoría de conformidad

Por tratarse de certificados cualificados será necesario realizar al menos una evaluación de conformidad con el Reglamento UE nº 910/2014 con periodicidad bienal. El prestador o el organismo supervisor puede estimar la necesidad de realizar auditorías adicionales para mantener la confianza en los servicios prestados.

8.2. Identificación y calificación del auditor

Según lo establecido en la DPC.

8.3. Relación del auditor con la entidad auditada

Según lo establecido en la DPC

8.4. Relación de elementos objeto de auditoría

Según lo establecido en la DPC.

8.5. Acciones a emprender como resultado de una falta de conformidad

Según lo establecido en la DPC.

8.6. Tratamiento de los resultados de las auditorías

Por tratarse de certificados cualificados, los resultados de las auditorías serán remitidos al organismo supervisor.

9. REQUISITOS COMERCIALES Y LEGALES

9.1. Tarifas

Según lo establecido en la DPC.

9.2. Capacidad financiera

Según lo establecido en la DPC.

9.3. Confidencialidad

Según lo establecido en la DPC.

9.4. Protección de datos personales

Según lo establecido en la DPC.

9.5. Derechos de propiedad intelectual

Según lo establecido en la DPC.

9.6. Obligaciones y responsabilidad civil

Según lo establecido en la DPC.

9.6.1. Titulares de los certificados

Además de las obligaciones generales establecidas en la DPC, los titulares de los certificados de empleado emitidos por ACGISS están obligados 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.
- 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.
- 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.

9.7. Renuncias de garantías

Según lo establecido en la DPC.

9.8. Limitaciones de responsabilidad

Según lo establecido en la DPC.

9.9. Indemnizaciones

Según lo establecido en la DPC.

9.10. Plazo y finalización

Según lo establecido en la DPC.

9.11. Notificaciones

Según lo establecido en la DPC.

9.12. Modificaciones de la política

9.12.1. Procedimiento para las modificaciones

La ACGISS puede modificar, de forma unilateral, este documento, siempre que proceda según el procedimiento establecido al efecto, teniendo en cuenta lo siguiente:

- La modificación tiene que estar justificada desde el punto de vista técnico, legal o comercial.
- La modificación propuesta por la ACGISS no puede ir en contra de la normativa interna de la GISS.
- Se establece un control de modificaciones, para garantizar, en todo caso, que las especificaciones resultantes cumplan los requisitos que se intentan cumplir y que dieron pie al cambio.
- Se establecen las implicaciones que el cambio de especificaciones tiene sobre el usuario, y se prevé la necesidad de notificarle dichas modificaciones.
- La nueva normativa tiene que ser aprobada por la GISS siguiendo los procedimientos establecidos.

9.12.2. Periodo y mecanismos para notificaciones

En caso de que las modificaciones realizadas puedan afectar a las condiciones de prestación de los certificados, la ACGISS las notificará a los usuarios individualmente, a través de su página web o a través de la Intranet de la Seguridad Social.

9.12.3. Circunstancias en las que un OID tiene que ser cambiado

Según lo establecido en la DPC.

9.13. Resolución de conflictos

Según lo establecido en la DPC.

9.14. Legislación aplicable

Según lo establecido en la DPC.

9.15. Conformidad con la legislación vigente

Según lo establecido en la DPC.

Particularmente aplicarán las siguientes secciones de los estándares a los certificados de empleado:

- ETSI EN 319 411-1: requisitos aplicables a cualquier PC y condiciones específicas para NCP. Además, los términos y condiciones (PDS) para certificados de empleado se estructura de acuerdo con el Anexo A de este estándar.
- ETSI EN 319 411-2: requisitos aplicables a cualquier política de certificación y condiciones específicas definidas para QCP-n.
- ETSI EN 319 412-1, EN 319 412-2 y EN 319 412-5: perfiles de certificados cualificados para personas físicas.

9.16. Cláusulas diversas

Según lo establecido en la DPC.

9.17. Otras cláusulas

Según lo establecido en la DPC.