MINISTERIO
DE INCLUSIÓN, SEGURIDAD SOCIAL
Y MIGRACIONES

SECRETARÍA DE ESTADO
DE LA SEGURIDAD SOCIAL
Y PENSIONES

Gerencia de Informática
de la Seguridad Social

Certificados de Sello Electrónico de ACGISS

Política de certificación

V 2.1.3
(Octubre 2020)

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
1.2.2	Modificación del perfil de los certificados	04-01-2011
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.	22-02-2017
2.0.2	Revisiones de redacción	28-04-2017
2.1	Corrección de erratas y modificación de perfil de sello	19-07-2017
2.1.1	Cambios derivados de la revisión anual: corrección de erratas y actualización de Ministerio.	03-08-2018
2.1.2	Revisión anual interna	31-07-2019
2.1.3	Revisión anual, actualización del Logo del Ministerio y cambios derivados de auditoría eIDAS 2020	30-10-2020

Índice

1. INTRODUCCIÓN 1
1.1. PRESENTACIÓN 1
1.2. NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN 1
1.3. PARTICIPANTES DE LA PKI 2
1.3.1. Autoridades de Registro 2
1.3.2. Suscriptores y usuarios finales 2
1.4. USO DE LOS CERTIFICADOS 2
1.4.1. Tipos y clases de certificados emitidos 2
1.4.2. Usos permitidos de los certificados de Sello 2
1.4.3. Aplicaciones prohibidas 2
1.5. ADMINISTRACIÓN DE LA POLÍTICA 3
1.6. DEFINICIONES Y ACRÓNIMOS 3
2. REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN 3
3. IDENTIFICACIÓN Y AUTENTICACIÓN 3
3.1. GESTIÓN DE NOMBRES 3
3.1.1. Tipos de nombres 3
3.2. VALIDACIÓN INICIAL DE LA IDENTIDAD 4
3.2.1. Prueba de posesión de clave privada 4
3.2.2. Autenticación de la identidad de una organización 4
3.3. IDENTIFICACIÓN Y AUTENTICACIÓN DE LA SOLICITUD DE RENOVACIÓN 4
3.4. IDENTIFICACIÓN Y AUTENTICACIÓN DE LA SOLICITUD DE REVOCACIÓN 4
4. REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS 5
4.1. SOLICITUD DE EMISIÓN DE CERTIFICADO 5
4.1.1. Quién puede efectuar una solicitud de certificado de sello 5
4.1.2. Proceso de registro y responsabilidades 5
4.2. TRAMITACIÓN DE LA SOLICITUD DE CERTIFICADO 5
4.2.1. Realización de las funciones de identificación y autenticación 5
4.2.2. Aprobación o denegación de las solicitudes 6
4.3. EMISIÓN DE CERTIFICADO 6
4.3.1. Acciones de la ACGISS durante el proceso de emisión 6

4.3.2. Notificación de la emisión al suscriptor/titular 6
4.4. ACEPTACIÓN DEL CERTIFICADO 6
4.4.1. Conducta que constituye aceptación del certificado 6
4.5. USO DEL PAR DE CLAVES Y DEL CERTIFICADO 7
4.5.1. Uso por los suscriptores 7
4.6. RENOVACIÓN DE CERTIFICADO SIN RENOVACIÓN DE CLAVES 7
4.7. RENOVACIÓN DE CERTIFICADO CON RENOVACIÓN DE CLAVES 7
4.7.1. Circunstancias para la renovación con cambio de claves de un certificado 7
4.8. MODIFICACIÓN DE CERTIFICADOS 7
4.9. REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS 8
4.9.1. Legitimación para solicitar la revocación 8
4.9.2. Procedimiento de solicitud de revocación 8
4.9.3. Plazo máximo de procesamiento de la solicitud de revocación 8
4.10. SERVICIOS DE COMPROBACIÓN DEL ESTADO DE LOS CERTIFICADOS 8
4.11. FINALIZACIÓN DE LA SUSCRIPCIÓN 8
4.12. CUSTODIA Y RECUPERACIÓN DE CLAVES 8
5. CONTROLES DE SEGURIDAD FÍSICA, GESTIÓN Y OPERACIONES 8
5.1. PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD 9
6. CONTROLES DE SEGURIDAD TÉCNICA 9
6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES 9
6.1.1. Generación del par de claves 9
6.1.2. Envío de la clave privada al suscriptor 9
6.1.3. Envío de la clave pública al emisor del certificado 10
6.1.4. Longitud de las claves 10
6.1.5. Usos admitidos de las claves 10
6.2. PROTECCIÓN DE LA CLAVE PRIVADA 10
6.2.1. Estándares de módulos criptográficos 10
6.2.2. Repositorio de la clave privada 10
6.2.3. Backup de la clave privada 11
6.2.4. Método de activación de la clave privada 11
6.3. OTROS ASPECTOS DE GESTIÓN DEL PAR DE CLAVES 11
6.4. DATOS DE ACTIVACIÓN 11

6.4.1. Generación e instalación de los datos de activación 11
6.4.2. Protección de los datos de activación 11
6.5. CONTROLES DE SEGURIDAD INFORMÁTICA 11
6.6. CONTROLES TÉCNICOS DEL CICLO DE VIDA 11
6.7. CONTROLES DE SEGURIDAD DE RED 12
6.8. SELLADO DE TIEMPO 12
7. PERFILES DE CERTIFICADOS 12
7.1. PERFIL DE CERTIFICADO 12
7.1.1. Certificado de sello electrónico de nivel alto 12
7.1.2. Certificado de sello electrónico de nivel medio 14
7.2. PERFIL DE LA LISTA DE CERTIFICADOS REVOCADOS (CRLS) 16
7.3. PERFIL OCSP 16
8. AUDITORÍA DE CONFORMIDAD 17
8.1. FRECUENCIA DE LA AUDITORÍA DE CONFORMIDAD 17
8.2. IDENTIFICACIÓN Y CALIFICACIÓN DEL AUDITOR 17
8.3. RELACIÓN DEL AUDITOR CON LA ENTIDAD AUDITADA 17
8.4. RELACIÓN DE ELEMENTOS OBJETO DE AUDITORÍA 17
8.5. ACCIONES A EMPRENDER COMO RESULTADO DE UNA FALTA DE CONFORMIDAD 17
8.6. TRATAMIENTO DE LOS RESULTADOS DE LAS AUDITORÍAS 17
9. REQUISITOS COMERCIALES Y LEGALES 17
9.1. TARIFAS 17
9.2. CAPACIDAD FINANCIERA 18
9.3. CONFIDENCIALIDAD 18
9.4. PROTECCIÓN DE DATOS PERSONALES 18
9.5. DERECHOS DE PROPIEDAD INTELECTUAL 18
9.6. OBLIGACIONES Y RESPONSABILIDAD CIVIL 18
9.6.1. Suscriptores 18
9.7. RENUNCIAS DE GARANTÍAS 18
9.8. LIMITACIONES DE RESPONSABILIDAD ..... 19~~18~~
9.9. INDEMNIZACIONES 19
9.10. PLAZO Y FINALIZACIÓN 19
9.11. NOTIFICACIONES 19

9.12. MODIFICACIONES DE LA POLÍTICA 19
9.12.1. Procedimiento para las modificaciones 19
9.12.2. Periodo y mecanismos para notificaciones 19
9.12.3. Circunstancias en las que un OID tiene que ser cambiado 19
9.13. RESOLUCIÓN DE CONFLICTOS 2019
9.14. LEGISLACIÓN APLICABLE 20
9.15. CONFORMIDAD CON LA LEGISLACIÓN VIGENTE 20
9.16. CLÁUSULAS DIVERSAS 20
9.17. OTRAS CLÁUSULAS 20

1. INTRODUCCIÓN

1.1. Presentación

La Seguridad Social, a través de su Autoridad de Certificación ACGISS emitirá certificados de sello electrónico para los Órganos o Entidades de la Seguridad Social que lo soliciten.

Se trata de certificados cualificados a sello electrónico emitidos teniendo en cuenta los requisitos establecidos en el Reglamento UE nº 910/2014.

Estos certificados se emiten como certificados de sello electrónico de Órgano o Administración, conforme al art. 19 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 sello electrónico. 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. Nombre del documento e identificación

Nombre del documento	Certificados Sello. Políticas de Certificación
Versión	2.1.3
Estado del documento	Aprobado
Fecha de emisión	30 de octubre de 2020
OID (Interno GISS)	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)
Localización	http://www.seg-social.es/ACGISS

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)

1.3. Participantes de la PKI

1.3.1. Autoridades de Registro

El registro de los certificados de sello se debe realizar en las oficinas centrales de la Gerencia de Informática de la Seguridad Social. La Autoridad de Registro responsable de la emisión será el Centro de Seguridad de la Información (CSI) de la GISS.

1.3.2. Suscriptores y usuarios finales

Los certificados de sello están dirigidos a los diferentes Órganos o Entidades de la Seguridad Social con rango al menos de Subdirección General.

A los efectos de esta Política, se considerará suscriptor y titular del certificado al Órgano o Entidad de la Seguridad Social a cuyo nombre se emite el certificado.

Por otra parte, se considerará solicitante del certificado a la persona física debidamente habilitada y acreditada para realizar la solicitud del certificado en representación de dicho Órgano o Entidad.

1.4. Uso de los certificados

1.4.1. Tipos y clases de certificados emitidos

Los certificados de sello electrónico se emiten como certificados de actuación automatizada dentro de la jerarquía de la PKI 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.

1.4.2. Usos permitidos de los certificados de Sello

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.

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

1.4.3. Aplicaciones prohibidas

No se utilizarán los certificados de sello para fines distintos de los especificados en la presente Política.

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 sello electrónico 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.

Además de las condiciones generales establecidas en la DPC respecto a la gestión de nombres, en los certificados de sello se utilizan los siguientes campos de identidad administrativa en el "Nombre Alternativo del Sujeto" (SubjectAlternativeName):

Tipo de certificado **OID 2.16.724.1.3.5.6.1.1 (nivel alto)** **OID 2.16.724.1.3.5.6.2.1 (nivel medio)**	TIPO DE CERTIFICADO (SELLO ELECTRÓNICO DE NIVEL ALTO O MEDIO)
Nombre de la entidad suscriptora **OID 2.16.724.1.3.5.6.1.2 (nivel alto)** **OID 2.16.724.1.3.5.6.2.2 (nivel medio)**	NOMBRE OFICIAL DE LA ENTIDAD SUSCRIPTORA
NIF entidad suscriptora **OID 2.16.724.1.3.5.6.1.3 (nivel alto)** **OID 2.16.724.1.3.5.6.2.3 (nivel medio)**	NIF DE LA ENTIDAD SUSCRIPTORA

3.2. Validación inicial de la identidad

La pertenencia de los diferentes Órganos o Entidades solicitantes de los certificados de sello al ámbito de la Seguridad Social, garantiza la capacidad de ésta de autenticar y acreditar la identidad de los suscriptores.

3.2.1. Prueba de posesión de clave privada

La prueba de posesión de clave privada 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 organización

Los Órganos o Entidades solicitantes del certificado de sello pertenecen al ámbito de la Secretaría de Estado de la Seguridad Social. Son entidades cuya organización y dirección aparecen en documentos oficiales publicados en BOE. Antes de que una entidad solicite un certificado de sello electrónico de nivel alto deberá aprobar la correspondiente Resolución, según lo establecido en el art. 19 del RD 1671/2009.

La autenticación del solicitante se lleva a cabo mediante los instrumentos presentes en la Administración Pública al efecto.

3.3. Identificación y autenticación de la solicitud de renovación

Se realiza de la misma forma que para la validación inicial de la identidad.

3.4. Identificación y autenticación de la solicitud de revocación

El inicio de una solicitud de revocación se produce:

- De oficio por la GISS por las causas estipuladas en la Declaración de Prácticas de Certificación.
- Por una persona habilitada para ello por el Órgano o la Entidad titular del certificado a través del correspondiente formulario. La solicitud deberá enviarse a la Autoridad de Registro con la documentación necesaria para autenticar dicha habilitación.

4. REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS

4.1. Solicitud de emisión de certificado

4.1.1. Quién puede efectuar una solicitud de certificado de sello

La solicitud de un certificado de sello se realiza bajo petición de los Órganos o Entidades pertenecientes a la Secretaría de Estado de la Seguridad Social, con rango de Subdirección General o superior.

De acuerdo con el art. 19 del RD 1671/2009, la creación de sellos electrónicos se realizará mediante resolución del titular de la Entidad competente, que se publicará en la sede electrónica y contendrá al menos lo siguiente:

a) Órgano titular del sello que será el responsable de su utilización.

b) Características técnicas generales del sistema de firma y certificado aplicable.

c) Servicio de validación para la verificación del certificado.

d) Actuaciones y procedimientos en los que podrá ser utilizado.

Posteriormente, la solicitud de emisión del certificado la realizará la persona habilitada para ello en la Resolución por dicho Órgano o Entidad a través de los formularios disponibles para ello.

4.1.2. Proceso de registro y responsabilidades

La ACGISS asegura que las solicitudes de certificados son completas, precisas y están debidamente autorizadas.

La solicitud se realiza mediante un formulario en el que deberán constar los datos del Órgano titular del certificado de Sede y los de la persona física autorizada para llevar a cabo dicha solicitud. La solicitud será firmada por este representante y remitida a la Autoridad de Registro de la GISS. La firma de la solicitud comporta el conocimiento y aceptación de las condiciones de uso del certificado de sello por todas las partes.

La Autoridad de Registro será la encargada de comprobar que todos los datos son correctos antes de proceder a la petición del certificado a la ACGISS.

4.2. Tramitación de la solicitud de certificado

4.2.1. Realización de las funciones de identificación y autenticación

La Autoridad de Registro identificará al solicitante y comprobará la validez de su habilitación. La autenticación de la solicitud proviene de la validación de la firma del formulario por parte del solicitante.

La Autoridad de Registro comprobará la corrección de los datos incluidos en el formulario mediante la consulta de los documentos oficiales y bases de datos correspondientes.

4.2.2. Aprobación o denegación de las solicitudes

Será denegada toda solicitud que no cumpla los requisitos establecidos en la presente política y en el procedimiento establecido al efecto. También serán denegados los formularios incorrectamente rellenados o firmados por personal no habilitado para realizar la petición.

4.3. Emisión de certificado

4.3.1. Acciones de la ACGISS durante el proceso de emisión

Después que la Autoridad de Registro compruebe la identidad del solicitante y verifique la documentación aportada, enviará la solicitud a la ACGISS como Autoridad de Certificación para la emisión del certificado correspondiente.

La generación de las claves y la emisión del certificado tendrán lugar una vez que la Autoridad de Registro haya introducido los datos en la aplicación de registro.

En el caso de certificados de nivel alto, las claves se generan en el interior de un módulo criptográfico HSM certificados como dispositivos cualificados de creación de firmas y no se extraen en ningún momento del mismo. Existirán mecanismos para garantizar este extremo de acuerdo con lo especificado en el correspondiente procedimiento de gestión de claves.

En el caso de certificados de nivel medio, las claves puede generarlas el usuario o la CA. Si las claves se generan en la CA, se remiten protegidas, junto con los correspondientes certificados, al solicitante por correo electrónico con acuse de recibo. Por otra parte, telefónicamente o por otro canal, envía al solicitante el PIN necesario para la instalación del certificado. La Autoridad de Registro garantiza que no guarda copias de las claves privadas de los certificados de sello que emita.

Una vez generadas las claves, se envían las claves públicas a la Autoridad de Certificación para su firma.

La ACGISS genera los certificados vinculándolos de forma segura con la información del Órgano o Entidad, garantizando la utilización de productos y sistemas fiables protegidos de toda alteración y el registro de los datos relativos a la emisión.

4.3.2. Notificación de la emisión al suscriptor/titular

La Autoridad de Registro notifica la emisión al suscriptor/titular por medio de un correo electrónico al solicitante.

4.4. Aceptación del certificado

4.4.1. Conducta que constituye aceptación del certificado

Se acepta el certificado de sello en el momento en que se 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.

4.5. Uso del par de claves y del certificado

4.5.1. Uso por los suscriptores

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.

4.6. Renovación de certificado sin renovación de claves

Según lo establecido en la DPC.

4.7. Renovación de certificado con renovación de claves

La renovación de certificados seguirá de forma general el mismo procedimiento que el especificado para la emisión inicial de los mismos, mediante el envío del formulario correspondiente.

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

La renovación de los certificados puede producirse por:

- Fin del período de vigencia de los certificados.
- Re-emisión de oficio por parte de la Seguridad Social derivada de una actualización de la infraestructura o de los perfiles de los certificados.

En ambos casos se realizará una comunicación al titular con antelación suficiente para que pueda realizar la solicitud de renovación dentro del plazo previsto.

4.8. Modificación de certificados

Según lo establecido en la DPC.

4.9. Revocación y suspensión de certificados

4.9.1. Legitimación para solicitar la revocación

La solicitud de revocación del certificado por parte del titular se realizará mediante un procedimiento análogo al utilizado para la solicitud de su emisión, mediante el envío del formulario correspondiente.

Asimismo la revocación podrá realizarse de oficio por la ACGISS.

4.9.2. Procedimiento de solicitud de revocación

Para solicitar la revocación el titular deberá remitir el correspondiente formulario a la Autoridad de Registro, firmado por una persona autorizada para ello.

La Autoridad de Registro comprobará la información indicada en el formulario según lo establecido anteriormente en esta política.

4.9.3. Plazo máximo de procesamiento de la solicitud de revocación

La solicitud de revocación se atenderá lo antes posible una vez recibido el correspondiente formulario en la Autoridad de Registro. Se aplicará un procedimiento especial cuando la revocación derive de la puesta en peligro de la seguridad de las claves fuera del horario laboral.

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

Las claves privadas de los certificados de sello de nivel alto se almacenan en varios HSM organizados en clúster, lo que garantiza la correcta protección y recuperación de las claves en caso necesario.

Para los certificados de sello de nivel medio no se realiza almacenamiento ni custodia de las claves privadas.

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 sello electrónico, serán registrados específicamente los siguientes eventos:

- Solicitudes de certificados de sello.
- Datos relacionados con la emisión, renovación y revocación de los certificados de sello.
- Cambios en las políticas de certificados de sello.
- Firma de los certificados de sello.
- En certificados de sello de nivel medio, logs relacionados con el acceso y preparación del HSM y la generación de las claves privadas de los sellos.
- En certificados de nivel medio, comunicaciones relevantes con la persona responsable de los certificados.
- Otros relacionados con la operación de los sistemas de la infraestructura en la emisión de certificados de sello.

6. CONTROLES DE SEGURIDAD TÉCNICA

6.1. Generación e instalación del par de claves

6.1.1. Generación del par de claves

En el caso de certificados de nivel alto, las claves se generan de forma segura en el interior de un módulo criptográfico HSM certificado como dispositivo cualificado de creación de firmas. Existirán mecanismos definidos en el correspondiente procedimiento de gestión de claves que garanticen que la emisión se realiza correctamente.

En el caso de los certificados de nivel medio, el par de claves de los certificados de sello se genera por los usuarios o en la Autoridad de Registro. En este último caso, una vez creado el certificado, se envían tanto las claves como el certificado al solicitante correspondiente y se borra cualquier copia de las mismas.

6.1.2. Envío de la clave privada al suscriptor

La clave privada de los certificados de sello de nivel alto no se envía al suscriptor sino que queda almacenada en el interior del HSM.

Para los certificados de sello de nivel medio, si la ha generado la AR la clave privada se envía cifrada al solicitante, junto con la clave pública y el certificado, mediante un correo electrónico. La contraseña del mismo se facilitará por el medio alternativo que se estime más conveniente según las circunstancias, ya sea telefónicamente, presencialmente o por correo postal.

6.1.3. Envío de la clave pública al emisor del certificado

En los certificados de nivel alto, la clave pública se exporta del HSM y es enviada a través de la aplicación de registro a la Autoridad de Certificación para su firma.

En los certificados de nivel medio, se envía la clave pública a la Autoridad de Certificación para la firma del certificado y posteriormente se le facilita al solicitante.

6.1.4. Longitud de las claves

Las claves de los certificados de sello serán 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, tanto para los certificados de sello de nivel alto como para los de nivel medio, es el siguiente:

KeyUsage	Digital Signature Content Commitment KeyEncipherment
ExtendedKeyUsage	Email Protection Client Authentication

6.2. Protección de la clave privada

6.2.1. Estándares de módulos criptográficos

En los certificados de nivel alto, la clave privada se encuentra almacenada en el interior del HSM que cuenta con las medidas de seguridad adecuadas para su protección. Los HSM están certificados FIPS 140-2 nivel 3 o superior y CC EAL 4+, y como dispositivos cualificados de creación de firma de acuerdo con la normativa de aplicación.

6.2.2. Repositorio de la clave privada

Los certificados de sello de nivel alto se almacenan en el interior de los HSM en los que se han generado.

Para los certificados de nivel medio, si la generación de las claves se realiza en la Autoridad de Registro, las claves privadas no se almacenen en ella. Una vez remitida al solicitante, la protección de la clave privada del certificado será responsabilidad de éste. Los certificados de sello de nivel medio se instalarán en servidores adecuadamente protegidos con control de acceso.

La Seguridad Social garantiza que las claves privadas se utilizan bajo el control de sus Entidades.

6.2.3. Backup de la clave privada

En el caso de certificados de sello de nivel alto, se dispone de backup de las claves proporcionado por un clúster de HSMs que replican las claves en diversas localizaciones.

No se realiza backup de la clave privada de los certificados de nivel medio.

6.2.4. Método de activación de la clave privada

La clave privada de los certificados de sello de nivel alto se activa a través de la Plataforma de Servicios de Seguridad de la GISS, con controles de acceso específicos.

La clave privada de los certificados de sello de nivel medio se activa mediante la introducción de la correspondiente contraseña de operación a través de las aplicaciones de la Seguridad Social que lo usen por parte del responsable del certificado.

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 sello consiste en una contraseña proporcionada por la Autoridad de Registro a las personas autorizadas para su uso.

6.4.2. Protección de los datos de activación

Sólo las personas autorizadas conocen la contraseña asociada al certificado, que se remite por un canal independiente. Estas personas serán las responsables de la protección de los datos de activación a partir de ese momento.

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

7.1.1. Certificado de sello electrónico de nivel alto

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 del certificado.	GISS01
1.4.6. Serial Number	Número único de identificación de la entidad de certificación	Q2827003A
1.4.8. 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		
1.5.1. Country (C)	ES	ES
1.5.2. Organization (O)	Denominación del suscriptor	SECRETARIA DE ESTADO DE LA SEGURIDAD SOCIAL
1.5.4. Organizational Unit (OU)	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado.	ACTUACION AUTOMATIZADA
1.5.5. Organizational Unit (OU)	Tipo certificado= "sello electrónico"	SELLO ELECTRONICO

1.5.3 Organizational Unit (OU)	Identificación del suscriptor según DIR3	"Número DIR3 de la Entidad" Ej: SE = E04926001
1.5.6. Descripción	Descripción uso certificado	NIVEL ALTO
1.5.7. Serial Number	Número único de identificación de la entidad	"NIF de la Entidad" Ej: SE = S2819001E
1.5.9. Common Name (CN)	Denominación del certificado	"Nombre del sello electrónico" Ej: "SELLO ELECTRONICO DE LA SEGURIDAD SOCIAL"
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. Key Identifier	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*
2.3. Key Usage		
2.3.1. Digital Signature		"1"
2.3.2. Content Commitment		"1"
2.3.3. Key Encipherment		"1"
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"
2.5. 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: 15 años	OID 0.4.0.1862.1.3 =15
2.5.3. QcSSCD	Uso de dispositivo seguro de firma	OID 0.4.0.1862.1.4
2.5.4. QcType-eseal	Certificado de Sello	OID 0.4.0.1862.1.6.2
2.5.5. QcPDS	Lugar donde se encuentra la PDS	OID 0.4.0.1862.1.5 http://www.seg-social.es/ACGISS https://sede.seg-social.gob.es/descarga/ACGISS_PDSSeal.pdf
2.6. Certificate Policies		
2.6.1. Policy Identifier	Certificado de sello de nivel alto según política AGE	2.16.724.1.3.5.6.1
2.6.2. Policy Identifier	QCP-l-qscd	0.4.0.194112.1.3
2.6.3. Policy Identifier	OID asociado a la PC de ACGISS	2.16.724.1.4.2.2.1.1.2
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 sello electrónico, nivel alto. Consulte las condiciones de uso en http://www.seg-social.es/ACGISS Nuevo CIF de la GISS desde jun 2017: Q2802407C

2.7. Subject Alternative Name		
2.7.2. Directory Name	Identidad Administrativa	
2.7.2.1. Tipo de certificado	Indica la naturaleza del certificado	2.16.724.1.3.5.6.1.1 = SELLO ELECTRONICO DE NIVEL ALTO
2.7.2.2. Nombre de la entidad suscriptora	Entidad suscriptora del certificado	2.16.724.1.3.5.6.1.2 = "Nombre de la Entidad suscriptora" Ej: SECRETARIA DE ESTADO DE LA SEGURIDAD SOCIAL
2.7.2.3. NIF entidad suscriptora	NIF de le Entidad suscriptora	2.16.724.1.3.5.6.1.3 = "NIF Entidad" Ej: SE = S2819001E
2.8. Issuer Alternative Name	Nombre alternativo de la persona 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

7.1.2. Certificado de sello electrónico de nivel medio

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 del certificado.	GISS01
1.4.6. Serial Number	Número único de identificación de la entidad de certificación	Q2827003A
1.4.8. 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		

1.5.1. Country (C)	ES	ES
1.5.2. Organization (O)	Denominación del suscriptor	SECRETARIA DE ESTADO DE LA SEGURIDAD SOCIAL
1.5.4. Organizational Unit (OU)	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado.	ACTUACION AUTOMATIZADA
1.5.5. Organizational Unit (OU)	Tipo certificado= "sello electrónico"	SELLO ELECTRONICO
1.5.3 Organizational Unit (OU)	Identificación del suscriptor según DIR3	"Número DIR3 de la Entidad" Ej: SE = E04926001
1.5.6. Descripción	Descripción uso certificado	NIVEL MEDIO
1.5.7. Serial Number	Número único de identificación de la entidad	"NIF de la Entidad" Ej: SE = S2819001E
1.5.9. Common Name (CN)	Denominación del certificado	"Nombre del sello electrónico" Ej: "SELLO ELECTRONICO DE LA SEGURIDAD SOCIAL"
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. Key Identifier	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*
2.3. Key Usage		
2.3.1. Digital Signature		"1"
2.3.2. Content Commitment		"1"
2.3.3. Key Encipherment		"1"
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"
2.5. 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: 15 años	OID 0.4.0.1862.1.3 =15
2.5.3. QcType-eseal	Certificado de Sello	OID 0.4.0.1862.1.6.2
2.5.4. QcPDS	Lugar donde se encuentra la declaración PDS	OID 0.4.0.1862.1.5 http://www.seg-social.es/ACGISS https://sede.seg-social.gob.es/descarga/ACGISS_PDSSeal.pdf
2.6. Certificate Policies		
2.6.1. Policy Identifier	Certificado de sello de nivel medio según política AGE	2.16.724.1.3.5.6.2
2.6.2. Policy Identifier	QCP-l	0.4.0.194112.1.1
2.6.3. Policy Identifier	OID asociado a la PC de ACGISS	2.16.724.1.4.2.2.1.1.1
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 sello electrónico, nivel medio/sustancial. Consulte las condiciones de uso en http://www.seg-social.es/ACGISS Nuevo CIF de la GISS desde jun 2017: Q2802407C
2.7. Subject Alternative Name		
2.7.2. Directory Name	Identidad Administrativa	
2.7.2.1. Tipo de certificado	Indica la naturaleza del certificado	2.16.724.1.3.5.6.2.1 = SELLO ELECTRONICO DE NIVEL MEDIO
2.7.2.2. Nombre de la entidad suscriptora	Entidad suscriptora del certificado	2.16.724.1.3.5.6.2.2 = "Nombre de la Entidad suscriptoras" Ej: SECRETARIA DE ESTADO DE LA SEGURIDAD SOCIAL
2.7.2.3. NIF entidad suscriptora	NIF de le Entidad suscriptora	2.16.724.1.3.5.6.2.3 = "NIF Entidad" Ej: SE = S2819001E
2.8. Issuer Alternative Name	Nombre alternativo de la persona 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

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. Suscriptores

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

a. Suministrar a la ACGISS la información necesaria para realizar su correcta identificación.

b. Notificar cualquier cambio en los datos aportados para la emisión del certificado durante su periodo de validez.

c. Custodiar las claves privadas de manera diligente.

d. Realizar un uso adecuado del certificado de sello de acuerdo con lo especificado en la presente Política de Certificación.

e. En el caso de certificados de sello de nivel alto, generar las claves en el interior de un módulo criptográfico HSM certificado como dispositivo cualificado de creación de firmas.

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 titulares y usuarios directamente, 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 sello:

- ETSI EN 319 411-1: requisitos aplicables a cualquier PC y condiciones específicas para NCP. Además, en el caso de certificados de sello de nivel alto, aplicarán también las condiciones NCP+.

  Los términos y condiciones (PDS) para certificados de sello se estructuran 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-l-qscd (certificados de sello de nivel alto) o condiciones QCP-l (certificados de sello de nivel medio).

- ETSI EN 319 412-1, EN 319 412-3 y EN 319 412-5: perfiles de certificados cualificados para personas jurídicas.

9.16. Cláusulas diversas

Según lo establecido en la DPC.

9.17. Otras cláusulas

Según lo establecido en la DPC.