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 sede electrónica

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 del certificado	07-04-2010

Índice

1. INTRODUCCIÓN

1.1. Presentación

Las sedes electrónicas en el ámbito de actuación de las Administraciones Públicas, son direcciones electrónicas disponibles para los ciudadanos.

La ACGISS emitirá certificados de Sede Electrónica para los órganos o entidades de la Seguridad Social que lo soliciten, de acuerdo con lo establecido en la Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos y su normativa de desarrollo. Según el Art. 17 de la Ley 11/2007, los certificados de Sede se utilizarán para la identificación de las sedes electrónicas y para el establecimiento de comunicaciones seguras con las mismas.

El objetivo de este documento es establecer la Política de Certificación específica de dichos certificados de Sede Electrónica.

Para elaborar su contenido se ha seguido la estructura de la RFC 3647, incluyendo aquellos apartados que resultan específicos para este tipo de certificado. 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 Sede. Políticas de Certificación
Versión	1.2.1
Estado del documento	Aprobado
Fecha de emisión	07 de abril de 2010
OID	2.16.724.1.4.2.1.2
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 sede electronica (2)

1.3. Participantes de la PKI

1.3.1. Entidades de Registro

El registro de los certificados de Sede Electrónica se debe realizar en las oficinas centrales de la Gerencia de Informática de la Seguridad Social.

1.3.2. Usuarios finales

Los certificados de Sede Electrónica están dirigidos a los diferentes órganos de la Seguridad Social con rango al menos de Dirección General.

A los efectos de esta Política, se considerará Titular del certificado al órgano o entidad de la Seguridad Social que tenga la titularidad, gestión y administración de la dirección electrónica a través de la que se accede a la sede electrónica.

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. Usos de los certificados

1.4.1. Usos permitidos de los Certificados de Sede

Los certificados de sede, se utilizan para la identificación de las sedes electrónicas y para el establecimiento de comunicaciones seguras con ellas.

1.4.2. Aplicaciones prohibidas

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

2. IDENTIFICACIÓN Y AUTENTICACIÓN

2.1. Validación inicial de la identidad

La pertenencia de los diferentes órganos o entidades solicitantes de los certificados de Sede al ámbito de la Seguridad Social, garantiza la capacidad de ésta de autenticar y acreditar la identidad de los suscriptores.

2.1.1. Prueba de posesión de clave privada

La clave privada se genera en el interior del servidor en el que se instalará la sede electrónica, quedando probada la posesión de la misma por el envío de la correspondiente clave pública a la ACGISS mediante PKCS#10.

2.2. Identificación y autenticación de la solicitud de renovación

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

2.3. Identificación y autenticación de la solicitud de revocación

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

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

3.1. Solicitud de emisión de certificado

3.1.1. Quién puede efectuar una solicitud de certificado de Sede

La solicitud de un certificado de Sede Electrónica se realiza bajo petición de los órganos o entidades pertenecientes a la Secretaría de Estado de la Seguridad Social, con rango de Dirección General o superior.

La solicitud la realiza la persona física habilitada para ello en cada órgano o entidad de que se trate.

3.1.2. 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 de forma manuscrita por este representante y remitida a la Entidad de Registro.

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

3.2. Tramitación de la solicitud de certificación

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

Junto con esta información también enviará la clave pública remitida por el suscriptor del certificado para su firma.

3.3. Emisión de certificado

3.3.1. Acciones de la ACGISS durante el proceso de emisión

La emisión del certificado tendrá lugar una vez que la Entidad de Registro haya introducido los datos en la aplicación de registro, junto con la clave pública remitida por el solicitante.

La ACGISS será la encargada de generar los certificados solicitados y de firmar tanto estos como las claves públicas, para su envío al solicitante por correo electrónico cifrado y con acuse de recibo.

3.4. Aceptación del certificado

3.4.1. Conducta que constituye aceptación del certificado

La considerará que se acepta el certificado de Sede una vez que quede constancia de la recepción por el suscriptor, sin que exista comunicación en contra de rechazo o modificación de los datos contenidos en el mismo en un plazo de 10 días hábiles.

3.5. Uso del par de claves y del certificado

3.5.1. Uso por los suscriptores

La utilización de los certificados de Sede atenderá a los usos previstos en la Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos y en su normativa de desarrollo.

3.6. Renovación de certificado con renovación de claves

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

3.7. Revocación y suspensión de certificados

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.

4. CONTROLES DE SEGURIDAD TÉCNICA

4.1. Generación e instalación del par de claves

4.1.1. Generación del par de claves

Los pares de claves de los certificados se generan en el servidor en el que está ubicada la Sede Electrónica.

4.1.2. Envío de la clave privada al suscriptor

La clave privada se genera en el servidor del suscriptor, por lo que no se realiza ningún tipo de envío.

4.1.3. Envío de la clave pública al emisor del certificado

La clave pública se envía a la Entidad de Registro mediante PKCS#10.

4.1.4. Longitud de las claves

Las claves de los certificados de Sede serán 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 de cada tipo de certificado es el siguiente:

Certificado de sede electrónica	
KeyUsage	digitalSignature (80): Certificados de firma keyEncipherment (20): Certificados de cifra
ExtKeyUsage	Authentication TSL Web Server

4.2. Protección de la clave privada

La generación de las claves se realiza en el servidor del suscriptor, lo que garantiza que permanece bajo su exclusivo control. No se realiza ningún tipo de envío de la clave privada a la ACGISS.

La protección de las claves privadas del certificado será responsabilidad del titular del mismo.

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.

5. PERFILES DE CERTIFICADOS

5.1. Perfil de certificado

Campos Certificados Sede Electrónica Administrativa	
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: **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="Denominación de Nombre o Dominio", OU="Sede Electrónica Administrativa,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	Authentication TSL Web Server
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 OID2.16.724.1.4.2.1.2 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:1.3.6.1.4.1.14862.1.4.2.2.1=”**Sede Electronica Administrativa**” OID:1.3.6.1.4.1.14862.1.4.2.2.2=”**Nombre Entidad Subscriptora**” OID: 1.3.6.1.4.1.14862.1.4.2.2.3=”**NIF Entidad Subscriptora”** OID:1.3.6.1.4.1.14862.1.4.2.2.4 “**Nombre de la Sede Electrónica**” OID:1.3.6.1.4.1.14862.1.4.2.2.5 “**Dominio al que pertenece la Sede**”

6. REQUISITOS COMERCIALES Y LEGALES

6.1. Obligaciones y responsabilidad civil

6.1.1. Suscriptores

Los suscriptores de los certificados de Sede 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 Sede de acuerdo con lo especificado en la presente Política de Certificación.