



Signe - Autoridad de Certificación

Política de certificación
Certification policy
**Certificados corporativos
de Persona Jurídica**

Versión 1.1

Fecha: 24/03/2015

| Versión | Cambios | Fecha |
|----------------|------------------------|--------------|
| 1.0 | Creación del documento | 02/11/2010 |
| 1.1 | Cambios en el formato | 24/03/2015 |

Índice

- 1 INTRODUCCIÓN
 - 1.1 Descripción general
 - 1.2 Nombre del documento e identificación

- 2 ENTIDADES PARTICIPANTES
 - 2.1 Autoridades de certificación (CA)
 - 2.2 Autoridad de Registro (RA)
 - 2.3 Solicitante
 - 2.4 Suscriptor
 - 2.5 Firmante
 - 2.6 Custodio de Claves
 - 2.7 Tercero que confía en los certificados

- 3 CARACTERÍSTICAS DE LOS CERTIFICADOS
 - 3.1 Periodo de validez de los certificados
 - 3.2 Tipo de soporte
 - 3.3 Uso particular de los certificados
 - 3.4 Tarifas

- 4 PROCEDIMIENTOS OPERATIVOS
 - 4.1 Proceso de emisión de certificados
 - 4.2 Revocación de certificados
 - 4.3 Renovación de certificados

- 5 PERFIL DEL CERTIFICADO
 - 5.1 Nombre distinguido (DN)
 - 5.2 Extensiones de los certificados

1 Introducción

1.1 Descripción general

Los **Certificados Corporativos de Persona Jurídica** son certificados reconocidos según el Art.7 de la Ley 59/2003 de Firma Electrónica que identifican al Suscriptor y Firmante como una Corporación con personalidad jurídica.

La solicitud y emisión de los Certificados Corporativos de Persona Jurídica se realiza a través de las Autoridades de Registro de Signe.

Los Certificados Corporativos de Persona Jurídica permiten también facturación electrónica.

En el presente documento se exponen las condiciones particulares referentes a este tipo de certificado. Esta Política de Certificación (PC) está subordinada al cumplimiento de la Declaración de Prácticas de Certificación (DPC) de Signe.

El presente documento es una adaptación de la Política de Certificación “**CP Corporativos de Persona Jurídica**” (OID 1.3.6.1.4.1.13177.10.1.5.D) de Firmaprofesional para SIGNE AC. Ambas políticas comparten aspectos como las características de los certificados, procedimientos y perfiles, y se diferencian en el alcance (siendo la presente más limitada) y en qué Autoridad de Certificación emite los certificados.

1.2 Nombre del documento e identificación

| | |
|--------------------------|---|
| Nombre: | PC – Certificados Corporativos de Persona Jurídica |
| Versión: | 1.1 |
| Descripción: | Política de Certificación para Certificados Corporativos de Persona Jurídica |
| Fecha de Emisión: | 02/11/2010 |
| OID | 1.3.6.1.4.1.36035.1.3.1 – Nivel Alto – <i>Hardware</i> criptográfico 1.3.6.1.4.1.36035.1.3.2 – Nivel Medio – <i>Software</i> |
| Localización | https://www.signe.es/signe-ac/dpc |

2 Entidades participantes

2.1 Autoridades de certificación (CA)

Los Certificados Corporativos de Persona Jurídica deben ser emitidos por la CA Subordinada “Signe Autoridad de Certificación”, que emite certificados digitales a Corporaciones Privadas.

2.2 Autoridad de registro (RA)

Signe actuará como Autoridad de Registro para la emisión de certificados corporativos de persona jurídica, estableciendo:

- Los mecanismos y procedimientos necesarios para realizar la identificación y autenticación del Suscriptor, cumpliendo con lo estipulado en la DPC.
- Los dispositivos de creación de firma a utilizar.

2.3 Solicitante

El Solicitante es la persona física que solicita el certificado corporativo de Persona Jurídica.

Podrán solicitar certificados corporativos de personas jurídicas sus administradores, representantes legales y voluntarios con poder bastante a estos efectos.

2.4 Suscriptor

El Suscriptor de este tipo de certificados es la persona jurídica que consta en el certificado

2.5 Firmante

El Firmante de este tipo de certificados es la persona jurídica que consta en el certificado.

2.6 Custodio de Claves

La custodia de los datos de creación de firma asociados a cada certificado electrónico de persona jurídica será responsabilidad de la persona física (Solicitante), cuya identificación se incluirá en el certificado electrónico.

2.7 Tercero que confía en los certificados

Los Certificados Corporativos de Persona Jurídica son certificados reconocidos según la Ley de Firma Electrónica. Los terceros que confíen en estos certificados deben tener presente las limitaciones en su uso.

3 Características de los certificados

3.1 Periodo de validez de los certificados

Los Certificados Corporativos de Persona Jurídica tendrán un periodo de validez de 3 años.

3.2 Tipo de soporte

Los Certificados Corporativos de Persona Jurídica se emitirán en dos tipos de soporte en función de dónde se cree y resida el par de claves, dando lugar a dos niveles de aseguramiento:

- Soporte *hardware* criptográfico: Nivel ALTO
- Soporte *software*: Nivel MEDIO

La Corporación decidirá el tipo de soporte en el que emite sus certificados.

3.2.1 Soporte hardware

Las claves privadas de los certificados emitidos en soporte hardware se generan y almacenan en un dispositivo de creación de firma como una tarjeta o un dispositivo criptográfico que ofrecen, al menos, las garantías indicadas en el artículo 23 de la ley 59/2003.

Según la Ley 59/2003 *“Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma”*. Por lo tanto, la utilización de Certificados Corporativos de Persona Jurídica con DSCF permite realizar firmas electrónicas reconocidas.

Los Certificados Corporativos de Persona Jurídica en Hardware están identificados mediante el OID (1.3.6.1.4.1.36035.1.3.1) en la extensión “X509v3 Certificate Policies”.

3.2.2 Soporte en software

Las claves privadas de los certificados emitidos en soporte software se generan y almacenan en un navegador de Internet, como por ejemplo Microsoft Explorer.

Según la Ley 59/2003 *“Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma”*. Por lo tanto, la utilización de Certificados Corporativos de Persona Jurídica en software no cumple con todos los requisitos que marca la ley para la firma reconocida. Sin embargo de acuerdo con el artículo 21 de la ley 11/2007 los Certificados Corporativos de Persona Jurídica emitidos en software siendo certificados reconocidos, aunque no produzcan firmas reconocidas, serán admitidos por las Administraciones Públicas siempre y cuando SIGNE ponga a disposición de las Administraciones Públicas la información precisa en condiciones que resulten tecnológicamente viables y sin que suponga coste alguno para aquellas.

Los Certificados de Persona Jurídica en software pueden ser copiados a otros soportes, por lo tanto es posible realizar copias de seguridad de los mismos.

Los Certificados Corporativos de Persona Jurídica en Software están identificados mediante el OID (1.3.6.1.4.1.36035.1.3.2) en la extensión “X509v3 Certificate Policies”.

3.3 Uso particular de los certificados

3.3.1 Usos apropiados de los certificados

Los Certificados Corporativos de Persona Jurídica emitidos por SIGNE podrán usarse en los términos establecidos por la DPC, y en lo establecido en la legislación vigente al respecto, concretamente de acuerdo con el artículo 7 de la ley 59/2003.

Los certificados emitidos bajo esta PC pueden ser utilizados por el custodio de claves con los siguientes propósitos:

- Garantizar la integridad del documento firmado.
- No repudio de origen (firma electrónica).
- Identificación de la persona jurídica ante terceros que confíen en los certificados.

3.3.2 Usos no autorizados de los certificados

No se autoriza su uso para la realización de transacciones comerciales o financieras por medio digital.

No se permite el uso que sea contrario a la normativa española y comunitaria, a los convenios internacionales ratificados por el estado español, a las costumbres, a la moral y al orden público. Tampoco se permite la utilización distinta de lo establecido en esta Política y en la Declaración de Prácticas de Certificación.

No se recomienda el uso de estos certificados para el cifrado de documentos.

3.4 Tarifas

SIGNE cobrará al Suscriptor (Corporación), lo acordado en el contrato de prestación de servicios firmado por las partes.

SIGNE podrá establecer las tarifas que considere oportunas a los Suscriptores, así como establecer los medios de pago que considere más adecuado en cada caso. Para más detalles sobre el precio y condiciones de pago de este tipo de certificados será necesario consultar con el Departamento Comercial de SIGNE.

4 Procedimientos Operativos

4.1 Proceso de emisión de certificados

Si la Corporación no tuviera firmado el contrato de prestación de servicios de certificación con SIGNE, deberá ser firmado por el representante legal en el momento de solicitar un certificado corporativo de persona jurídica.

El Solicitante deberá haberse personado ante SIGNE o un agente comercial de ésta para identificarse como representante de la organización a la que pertenece. En caso de disponer de un certificado electrónico que le identifique como tal, podrá utilizarlo para probar su identidad ante SIGNE.

Los pasos a seguir para la obtención del certificado son los siguientes:

a) Solicitud

En el momento de la solicitud, el Solicitante deberá presentar una autorización firmada (Hoja de solicitud) con los datos relativos a la Persona Jurídica.

b) Aceptación de la solicitud

La RA verificará la identidad del Solicitante, su vinculación con la entidad (su condición de representante o apoderado), la existencia de ésta, y los datos a incluir en el certificado.

La RA podrá verificar los datos anteriores según uno de los siguientes procedimientos:

- Al Solicitante con su NIF o pasaporte.
- A la relación que vincula el Solicitante como representante legal o voluntario de la organización.
- Mediante conexión telemática con los correspondientes registros públicos o especiales (por ejemplo con un acceso en línea al Registro de Universidades o al Registro Mercantil).
- Mediante la solicitud de las escrituras públicas, contratos, estatutos, pactos o cualesquiera otros documentos que puedan acreditar la constitución de la entidad, su vigencia e identificación de los miembros que las integran.

c) Tramitación

Una vez aceptada, la RA tramitará la solicitud del certificado.

d) Generación de claves

El primer paso de la tramitación será la generación de claves según el soporte que se utilice:

En software

El Solicitante recibirá por correo electrónico la confirmación de la solicitud, y deberá proceder a la generación de claves en su ordenador siguiendo las instrucciones de la RA.

Una vez el par de claves generadas, el Solicitante obtendrá un código que deberá presentar ante la RA para finalizar el proceso de emisión.

En hardware

Se procederá a la activación del dispositivo y seguidamente se entregará a la RA para que genere el par de claves.

Las claves serán generadas por el Solicitante, o por la RA en los sistemas indicados por el Solicitante, utilizando aplicaciones compatibles con los estándares de PKI, haciendo entrega a la RA de una petición de certificado en **formato PKCS#10**.

e) Emisión del certificado

Una vez las claves generadas, la RA procederá a la emisión del certificado, firmando la petición de generación de certificado y enviándola a la CA.

Una vez el certificado generado, y antes que la RA pueda entregarlo al Solicitante (o un representante del Solicitante), éste último deberá:

- Recibir y leer el “Régimen obligatorio de uso del certificado”.
- Aceptar las condiciones de emisión mediante la firma del “Acto de entrega”.

f) Entrega

Finalmente, la RA hará entrega del certificado al Solicitante.

En software

El Solicitante podrá descargarse de forma segura el certificado en su ordenador.

En hardware

La RA cargará el certificado en el dispositivo del Solicitante.

4.2 Revocación de certificados

El Suscriptor deberá solicitar la revocación de su certificado en caso de pérdida, robo, compromiso de claves u otras causas descritas en la CPS.

Para solicitar la revocación del certificado el Suscriptor puede:

- Revocar online su certificado en la página web de SIGNE.
- Llamar al servicio de revocación en horario de oficina: **902 30 17 01**

Para toda información complementaria referente a la revocación de los certificados, referirse al apartado correspondiente de la DPC.

4.3 Renovación de certificados

El Solicitante deberá ponerse en contacto con la RA y solicitar la generación de un certificado nuevo.

5 Perfil del certificado

5.1 Nombre distinguido (DN)

El DN estos certificados contendrá como mínimo los elementos que se citan con el formato siguiente, siguiendo la “Alternativa 2” propuesta en las especificaciones técnicas relacionadas con la Orden Ministerial HAC/1181/2003 de la Agencia Tributaria (AEAT)¹.

| Campo del DN | Nombre | Descripción |
|------------------------------------|--------------------------|---|
| CN, Common Name | Nombre | <i>Razón Social</i> |
| serialNumber | Número de identificación | <i>NIF del titular del certificado (persona jurídica o entidad sin personalidad jurídica)</i> |
| E, E-mail | E-mail | <i>Correo electrónico del solicitante.</i> |
| ST, State | Ubicación Geográfica | <i>Ámbito geográfico de la entidad.</i> |
| C, Country | País | <i>Código de país de dos dígitos según ISO 3166-1. Por defecto “ES”.</i> |
| 1.3.6.1.4.1.18838.1.1 ² | Número de identificación | <i>NIF del responsable</i> |
| SN, surName | Apellidos | <i>Apellidos del responsable (como constan en el DNI)</i> |
| GN, givenName | Nombre de Pila | <i>Nombre propio del responsable (como consta en el DNI)</i> |

¹ Los Certificados Corporativos de Persona Jurídica emitidos por Signe están de acuerdo a la Orden HAC/1181/2003, de 12 de mayo, por la que se establecen normas específicas sobre el uso de la firma electrónica en las relaciones tributarias por medios electrónicos, informáticos y telemáticos con la Agencia Estatal de Administración Tributaria. (B.O.E. 15-05-2003)

² OID definido por la Agencia Tributaria (AEAT) destinado a este propósito específico

5.2 Extensiones de los certificados

| Extensión | Crítica | Valores |
|-------------------------------------|---------|--|
| X509v3 Subject Alternative Name | - | <email del Suscriptor> |
| X509v3 Basic Constraints | Sí | CA:FALSE |
| X509v3 Key Usage | Sí | Digital Signature Non Repudiation Key Encipherment, Data Encipherment, Key Agreement |
| X509v3 Extended Key Usage | - | TLS Web Client Authentication E-mail Protection |
| X509v3 Subject Key Identifier | - | <id de la clave pública del certificado, obtenido a partir del hash de la misma> |
| X509v3 Authority Key Identifier | - | <id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma> |
| X509v3 Authority Information Access | - | <URI dónde se encuentra el certificado de la CA> |
| X509v3 CRL Distribution Points | - | <URI de la CRL> |
| X509v3 Certificate Policies | - | <OID de la política de certificación correspondiente al certificado> <URI de la DPC> User Notice : Este es un certificado reconocido corporativo de persona jurídica |
| QcStatements | - | Id-etsi-qcs-QcCompliance (indicando que el certificado reconocido) Id-etsi-qcs-QcSSCD (indica que la clave privada se custodia en un DSCF) |
| 1.3.6.1.4.1.13177.10.1.5.1.2 | - | <i>Datos Registrales</i> : Especifica los Datos Registrales de la empresa tal como aparecen en el Registro Mercantil |

La extensión “1.3.6.1.4.1.13177.10.1.5.1.2” es propietaria de Firmaprofesional. Su uso es opcional.

