Signe - Autoridad de Certificación

Política de certificación

Certification policy

Certificados Corporativos de Firma Empresarial

Documento:	SIGNE-ES-AC-PC-COR-02
Versión:	1.1
Fecha:	19/03/2020

Registro de Versiones

Versión	Cambios	Fecha
1.0	Creación del documento	22/03/2019
1.1	Ajuste de la codificación del documento. En el proceso de emisión de certificados, se añade una excepción a la identificación presencial del Solicitante y del Firmante. En el proceso de emisión de certificados, se explica el caso de que el soporte utilizado sea un dispositivo criptográfico del tipo tarjeta o token. Correcciones menores.	19/03/2020

Índice

1. Introducción

1.1. Descripción General

Los Certificados Corporativos de Firma Empresarial son certificados electrónicos de persona física según la Ley 59/2003, de 19 de diciembre, de firma electrónica (en adelante, "Ley 59/2003") que identifican al Suscriptor como Corporación y al Firmante como vinculado a esa Corporación, como su representante legal o voluntario (apoderado general).

Los Certificados Corporativos de Firma Empresarial son certificados de firma electrónica según el Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (en adelante, "Reglamento eIDAS").

Los Certificados Corporativos de Firma Empresarial sólo pueden ser utilizados por el propio Firmante.

La solicitud y emisión de los Certificados Corporativos de Firma Empresarial se puede realizar a través de las propias organizaciones a las que se vincula cada certificado, actuando como Autoridades de Registro de SIGNE. No obstante, también se pueden utilizar otras entidades no vinculadas con el Firmante que sean Autoridades de Registro de SIGNE.

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

1.2. Nombre del documento e identificación

Nombre	PC Certificados Corporativos de Firma Empresarial
Código	SIGNE-ES-AC-PC-COR-02
Versión	1.1
Descripción	Política de Certificación de Certificados Corporativos de Firma Empresarial
Fecha de emisión	19/03/2020
OIDs	1.3.6.1.4.1.36035.1.20.2 – Otros dispositivos - Nivel Medio[1]
Localización	https://www.signe.es/signe-ac/dpc

1.3. Definiciones y acrónimos

Las definiciones y acrónimos se pueden encontrar especificadas en el documento "Declaración de Prácticas de Certificación (DPC)" URL https://www.signe.es/signe-ac/dpc

[1] Otros dispositivos diferentes de Dispositivo Cualificado de Creación de Firma (DCCF)

2. Entidades participantes

2.1. Autoridades de Certificación (CA)

Los Certificados Corporativos de Firma Empresarial deben ser emitidos por la CA Subordinada "***SIGNE Autoridad de Certificación***", que emite certificados digitales a Corporaciones (empresas, entidades privadas o públicas).

2.2. Autoridad de Registro (RA)

La gestión de las solicitudes y emisiones de los certificados será realizada por SIGNE o por entidades que actúen como Intermediarios de SIGNE.

Adicionalmente, la propia Corporación (empresa, entidad privada o pública) podrá actuar como Autoridad de Registro de SIGNE para la gestión de las solicitudes y emisiones de los certificados a aquellas personas físicas con las que tenga una vinculación directa. La propia Corporación será el Suscriptor de todos estos certificados emitidos.

Cada Corporación que actúe como RA establecerá:

- Qué criterios se deben cumplir para solicitar un certificado, sin entrar en contradicción con lo estipulado en la DPC y la presente PC.
- Los mecanismos y procedimientos necesarios para realizar la identificación y autenticación del Firmante, cumpliendo con lo estipulado en la DPC.
- Los dispositivos de creación de firma a utilizar, que previamente SIGNE haya homologado.

2.3. Solicitante

El Solicitante es el representante legal o voluntario (apoderado general) de la Corporación (empresa, entidad privada o pública) que adquiere el certificado para dicho representante.

2.4. Suscriptor

La Corporación es el Suscriptor de los certificados y por lo tanto el propietario de los certificados emitidos.

2.5. Firmante

El Firmante será la persona física identificada en el certificado por su nombre, apellidos y número de documento de identificación presentado (NIF o NIE para España, CUI o Nº Carné de Extranjería para Perú), que tenga una vinculación de representante legal o voluntario con el

Suscriptor.

El Firmante y el Solicitante serán la misma persona física.

De acuerdo con el Reglamento eIDAS, el Firmante es la persona física que crea la firma electrónica.

2.6. Custodio de claves

El Custodio de claves es el propio Firmante.

2.7. Tercero que confía en los certificados

Los certificados Corporativos de Firma Empresarial son certificados electrónicos según la Ley 59/2003 y de firma electrónica según el Reglamento eIDAS.

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 Firma Empresarial tendrán un periodo de validez de 1, 2 ó 3 años.

3.2. Tipos de soporte

Los Certificados Corporativos de Firma Empresarial se emitirán Otros dispositivos[2].

3.2.1. Otros dispositivos[2]

Las claves privadas de los certificados emitidos en Otros dispositivos no se generan obligatoriamente en un dispositivo cualificado.

Los Certificados Corporativos de Persona Física en Otros dispositivos están identificados mediante el OID 1.3.6.1.4.1.36035.1.20.2 en la extensión "Certificate Policies".

3.3. Uso particular de los certificados

3.3.1. Usos apropiados de los certificados

Los certificados emitidos por SIGNE podrán usarse en los términos establecidos por la DPC, y lo establecido en la legislación vigente al respecto.

Los Certificados Corporativos de Firma Empresarial deben ser, en general, utilizados dentro del marco de la relación jurídica de servicio entre el Firmante y la Corporación (empresa, entidad privada o pública). En concreto, pueden ser utilizados con los siguientes propósitos:

a) Integridad del documento firmado.
b) No repudio de origen.
c) Identificación del Firmante y su vinculación con la Corporación, y/o identificación de la Corporación.

Se permite el uso de estos certificados en las relaciones personales del Firmante con las Administraciones Públicas y en otros usos estrictamente personales siempre y cuando no exista una prohibición del Suscriptor (empresa, entidad privada o pública).

[2] Otros dispositivos diferentes de Dispositivo Cualificado de Creación de Firma (DCCF)

3.3.2. Usos no autorizados de los certificados

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.

Dado que los certificados no se han diseñado para el cifrado de información, SIGNE no recomienda su uso para tal cometido.

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

La RA se encargará de tramitar las solicitudes y proceder a la emisión de los certificados cumpliendo siempre con los términos generales descritos en la DPC.Los pasos a seguir para la obtención del certificado son los siguientes:

a) Solicitud

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 Firma Empresarial.

El Solicitante deberá haberse personado ante SIGNE o un agente comercial de ésta para identificarse como representante de la organización a la que pertenece. Esta identificación presencial deberá ser realizada en el momento la solicitud, excepto cuando la identidad del Solicitante constara ya a SIGNE en virtud de una relación preexistente, en la que se hubiera identificado presencialmente al interesado y el período de tiempo transcurrido desde dicha identificación es menor de cinco años.

En el momento de la solicitud, el Solicitante deberá presentar una autorización firmada (Hoja de solicitud) con sus propios datos como Firmante (la persona autorizada a obtener un certificado corporativo de Firma Empresarial).

Los datos de esta autorización deben incluir: Nombre, Número de documento de identificación que será presentado (por ejemplo, NIF o NIE para España, CUI o Nº Carné de Extranjería para Perú), Cargo en la organización y Dirección de correo electrónico de la persona autorizada y la confirmación de lectura del Régimen obligatorio del uso del certificado, documento que quedará bajo custodia de la RA y de la que el Firmante podrá obtener una copia.

La RA verificará presencialmente la identidad del Firmante con su documento de identificación presentado (por ejemplo, DNI o NIE en España, DNI o Carné de Extranjería en Perú). Esta identificación presencial deberá ser realizada en el momento la solicitud, excepto cuando la identidad del Firmante constara ya a SIGNE en virtud de una relación preexistente, en la que se hubiera identificado presencialmente al interesado y el período de tiempo transcurrido desde dicha identificación es menor de cinco años.

b) Aceptación de la solicitud

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

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

- Al Solicitante con su documento de identificación presentado (por ejemplo, DNI o NIE en España, DNI o Carné de Extranjería en Perú).
- A la relación que vincula el Solicitante como representante legal o voluntario de la Corporación:
    - 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, en función del soporte que se utilice.

d) Generación de claves

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

En Otros dispositivos

En el caso de que el soporte utilizado sea un dispositivo criptográfico del tipo tarjeta o token:

- Se procederá a la activación del dispositivo y seguidamente se generará el par de claves en el mismo.

En el caso de que el soporte utilizado sea un dispositivo software:

- El Firmante recibirá por correo electrónico la confirmación de la solicitud, juntamente con un código de autenticación a la aplicación online de emisión de certificados.
- Para poder acceder a la aplicación online de emisión de certificados será necesario que el Firmante proporcione el código de autenticación recibido. Una vez autenticado, el Firmante procederá a la descarga del certificado electrónico (incluye la generación de las claves, la emisión del certificado y la descarga de ambos protegidos con una contraseña que él mismo establecerá).

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.

f) Entrega

Finalmente, la RA hará entrega del certificado al Firmante según el soporte que se utilice:

En Otros dispositivos

En el caso de que el soporte utilizado sea un dispositivo criptográfico del tipo tarjeta o token:

- La RA cargará el certificado en el dispositivo en el que se hayan generado previamente el par de claves. El código de activación del dispositivo de creación de firma será entregado únicamente al Firmante (en el caso de que éste no aporte su propio dispositivo).

En el caso de que el soporte utilizado sea un dispositivo software:

- El Firmante procederá a la descarga del certificado electrónico (incluye la generación de las claves, la emisión del certificado y la descarga de ambos protegidos con una contraseña que él mismo establecerá).
- El Firmante podrá instalar las claves y el certificado en su ordenador o sistema informático introduciendo la contraseña que él mismo estableció en el momento de la descarga.

4.2. Revocación de certificados

El Suscriptor deberá solicitar la revocación de su certificado en caso de pérdida, compromiso de claves, finalización de su vinculación con la corporación u otras causas descritas en la DPC.

Para solicitar la revocación del certificado el Suscriptor puede:

- Llamar al servicio de revocación en horario de oficina: **902 30 17 01**
- Enviar un correo electrónico (la revocación del certificado se realizará en horario de oficina): **signe-ac@signe.com**

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

4.3. Renovación de certificados

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

5. Perfil de los certificados

5.1. Nombre distinguido (DN)

El DN de los Certificados Corporativos de Firma Empresarial contendrá los elementos que se citan a continuación. Todos los valores de los componentes serán autenticados por la Autoridad de Registro:

Campo del DN	Nombre	Descripción
CN, Common Name	Nombre	*Nombre y Apellidos del Firmante*
OI, Organization Identifier	Identificador de la organización	*Identificador de la persona jurídica, tal como figura en los registros oficiales. Codificado según la Norma Europea ETSI EN 319 412-1, con único posible tipo VAT.* *El formato sería: "VAT" + "2 caracteres del código de país según ISO 3166-1" + "-" + "identificador de la persona jurídica (por ejemplo, NIF para España, RUC para Perú)".* *Ejemplo:* VATES-B0085974Z
O, Organization	Organización	*Nombre del Suscriptor (empresa o entidad privada o pública) con el que existe una vinculación con el Firmante*
OU, Organizational Unit	Unidad en la organización	*Departamento al que pertenezca el Firmante*
T, Title	Título	*Cargo, título o rol del Firmante en la organización.* *Por defecto:* Representante Legal
ST, State	Ubicación Geográfica	*Ámbito geográfico de vinculación del Firmante.*
C, Country	País	*Código de país de dos dígitos según ISO 3166-1, indicando el país emisor del documento de identificación presentado*
Serial Number	Número de Serie	*Identificador de la persona física, codificado según la Norma Europea ETSI EN 319 412-1, con los posibles tipos siguientes: IDC (por ejemplo, DNI en España o Perú) o PNO (por ejemplo, NIE en España, Carnet de Extranjería en Perú).* *El formato sería: "3 caracteres del tipo de identificador (IDC o PNO)" + "2 caracteres del código de país según ISO 3166-1" + "-" + "identificador de la persona física (por ejemplo, NIF o NIE para España, CUI o Nº Carné de Extranjería para Perú)".* *Ejemplo:* IDCES-00000000G
SN, Surname	Apellidos	*Apellidos del Firmante*
GN, Given Name	Nombre de Pila	*Nombre del Firmante*

5.2. Extensiones de los certificados

Extensión	Crítica	Valores
X509v3 Subject Alternative Name	-	rfc822Name: *email del Firmante* directoryName: 1.3.6.1.4.1.13177.0.1: *Nombre de pila de la persona física tal y como aparece en su documento de identidad* 1.3.6.1.4.1.13177.0.2: *Primer apellido de la persona física tal y como aparece en su documento de identidad* 1.3.6.1.4.1.13177.0.3: *Segundo apellido de la persona física tal y como aparece en su documento de identidad (este campo puede estar vacío)*
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Digital Signature Content Commitment
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	-	Access Method: id-ad-ocsp Access Location: <URI de acceso al servicio OCSP> Access Method: id-ad-calssuers Access Location: <URI de acceso al certificado de la CA emisora>
X509v3 CRL Distribution Points	-	<URI de la CRL>
X509v3 Certificate Policies	-	OID de la política de certificación correspondiente al certificado: 1.3.6.1.4.1.36035.1.20.2 (Otros dispositivos - Nivel Medio) URI de la DPC: http://www.signe.es/signe-ac/dpc

Una compañía de GRUPO signe

www.signe.es

Avda. de la Industria, 18
28760 Tres Cantos (Madrid)
España

Tel.: + 34 918 06 00 99
comercial@signe.es