Signe - Autoridad de Certificación

Política de certificación

Certification policy

Certificados corporativos de Persona Física

Versión 1.4

Fecha: 06/06/2016

Seguridad documental

Versión	Cambios	Fecha
1.0	Creación del documento	02/11/2010
1.1		
1.2		
1.3	Cambios en el formato	24/03/2015
1.4	Modificación documento. Inclusión definiciones y acrónimos. Actualización userNotice	06/06/2016

Índice

1. Introducción

1.1 Descripción General

Los **Certificados Corporativos de Persona Física** son certificados reconocidos de persona física según la Ley 59/2003 de Firma Electrónica que identifican al Suscriptor como Corporación y al Firmante como vinculado a esa Corporación, ya sea como empleado, asociado, colaborador, cliente o proveedor.
Los Certificados Corporativos de Persona Física sólo pueden ser utilizados por el propio Firmante.
La solicitud y emisión de los Certificados Corporativos de Persona Física 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.
El presente documento es una adaptación de la Política de Certificación "***CP Certificados Corporativos de Persona Física"*** (OID 1.3.6.1.4.1.13177.10.1.2.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 Física
Versión:	1.3
Descripción:	Política de Certificación para Certificados Corporativos de Persona Física
Fecha de Emisión:	15/09/2011
OIDs	1.3.6.1.4.1.36035.1.2.1 – Nivel Alto – *Hardware* criptográfico 1.3.6.1.4.1.36035.1.2.2– Nivel Medio –*Software*
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/wp-content/uploads/2014/10/DPC_1.2.pdf

2. Entidades participantes

2.1 Autoridades de Certificación (CA)

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

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 (empresas, entidades privadas o públicas) 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, como empleados, colaboradores, clientes. 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 los certificados para los empleados o personas vinculadas con la indicada Corporación.
Los profesionales autónomos o empresarios individuales, al no disponer de una personalidad jurídica que los represente, podrán solicitar un Certificado Corporativo de Persona Física en el que la identidad de la persona física y de la persona jurídica seráigual.

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 NIF, que tenga una vinculación (de empleado, colaborador, etc) con el Suscriptor.

2.6 Custodio de Claves

El custodio de las claves es el propio Firmante.

2.7 Tercero que confía en los certificados

Los certificados Corporativos de Persona Física 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 Física tendrán un periodo de validez de 3 años.

3.2 Tipos de soporte

Los Certificados Corporativos de Persona Física 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 en hardware

Las claves privadas de los certificados emitidos en soporte hardware se generan y almacenan enun dispositivo de creación de firma como una tarjeta o un dispositivo criptográfico queofrecen, al menos, las garantías indicadas en el artículo 23 de laley 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 de Persona Física con DSCF permite realizar firmas electrónicas reconocidas.

Las claves de certificados generadas en tarjeta criptográfica no pueden ser copiadas de ninguna manera, por lo que si se pierde o se estropea el dispositivo del Suscriptor, será necesario realizar un nuevo proceso de emisión de certificado.

Los Certificados Corporativos de Persona Física en Hardware están identificados mediante el OID (1.3.6.1.4.1.36035.1.2.1) 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 Física 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 Física 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 Corporativos de Persona Física 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 Física en Software están identificados mediante el OID (1.3.6.1.4.1.36035.1.2.2) en la extensión "X509v3 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 Persona Física deben ser, en general, utilizados dentro del marco de la relación jurídica de servicio entre el empleado y la empresa. 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 entidad que actúa como RA de SIGNE.

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, organización, etc).

El uso del certificado de Persona Física emitido en servidor criptográfico queda restringido a la firma de las copias electrónicas de los títulos. Adicionalmente, no se podrá realizar una firma electrónica mediante el certificado en servidor criptográfico sin previa autenticación del firmante mediante certificado electrónico reconocido y sin autorización mediante firma reconocida e inserción del código secreto (PIN).

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 su uso 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 Física.

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.

En el caso de que el Solicitante actúe en representación de otra persona física se deberá obtener la aceptación del certificado por parte del Firmante antes de que el certificado pueda ser considerado válido.

En este caso, el certificado se emitirá con un periodo de carencia durante el cual el certificado no será válido. Finalizado el periodo de carencia, si el Solicitante dispone de los medios para acceder a la clave privada y no ha conseguido la aceptación formal del certificado por parte del Firmante, el Solicitante deberá revocar el certificado de inmediato. En caso contrario se le considerará responsable de todos los perjuicios que puedan ocasionarse por el uso del certificado, especialmente los referentes a la protección de datos de carácter personal del Firmante.

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 de los Firmantes (las personas autorizadas a obtener un certificado de persona física).

Los datos de esta autorización debe incluir: Nombre, DNI y Cargo en la organización de cada persona autorizada.

La RA verificará presencialmente la identidad de los Firmantes.

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 o certificados.

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 conexióntelemáticacon 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 delos 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 software

El Suscriptor 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 Suscriptor 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 Firmante, 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”, documento que quedará bajo custodia de la RA y de la que el Firmante podrá obtener una copia.

f) Entrega

Finalmente, la RA hará entrega del certificado al Suscriptor.

En software

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

En hardware:

Tarjeta criptográfica: La RA cargará el certificado en el dispositivo delSuscriptor. El código de activación del dispositivo de creación de firma será entregado únicamente al Firmante.

Módulo de Seguridad Hardware: La RA cargará el certificado en el dispositivo en el que se hayan generado previamente el par de claves. Para la activación de los datos de creación de firma en el módulo de seguridad, el Firmante deberá utilizar un certificado reconocido emitido en un DSCF.

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:

- 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

Existen dos procedimientos:

a) **Proceso de renovación presencial:** El Suscriptor deberá ponerse en contacto conSIGNE, y proceder a la generación de un certificado nuevo.

b) **Proceso de renovación online:** Si el Suscriptor ha autorizado la renovación, éste recibirá una notificación de la RA por correo electrónico para iniciar la renovación a través de la página web de SIGNE.

5. Perfil de los certificados

5.1 Nombre distinguido (DN)

El DN de los Certificados Corporativos de Persona Física contendrá como mínimo los elementos que se citan con el formato anterior. 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
E, E-mail	E-mail	Correo electrónico del Firmante
O, Organization	Organización	Nombre del Suscriptor (empresa o entidad privada o pública) con la que existe una vinculación con el Firmante En caso que el Suscriptor sea un autónomo, se puede incluir el nombre comercial de su establecimiento, su CNAE o IAE
1.3.6.1.4.1.4710.1.3.2[1]	CIF de la Organización	CIF correspondiente a la persona o entidad a la que está vinculado el Firmante.
OU, Organization Unit	Unidad en la organización	Contendrá uno de los siguientes valores: El Departamento al que pertenezca el Firmante Tipo de vinculación con la organización.
T, Title	Título	Cargo, titulo o rol del Firmante en la organización.
ST, State	Ubicación Geográfica	Ámbito geográfico de vinculación del Firmante.
C, Country	País	Código de país de dos dígitos según ISO 3166-1. Por defecto “ES”.
serialNumber	Número de Serie	NIF o NIE del Firmante.
SN, surName	Apellidos	Apellidos del Firmante
GN, givenName	Nombre de Pila	Nombre del Firmante

[1] OID propiedad de la empresa Safelayer Secure Communications SA, dedicado a contener un Número de Identificación Fiscal (NIF) o un Código de Identificación Fiscal (CIF).

5.2 Extensiones de los certificados

Extensión	Crítica	Valores
X509v3 Subject Alternative Name	-	<email del Firmante>
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	-	Access Method: Id-ad-ocsp Access Location: <URI de acceso al servicio OCSP>
X509v3 CRL Distribution Points	-	<URI de la CRL>
X509v3 Certificate Policies	-	<OID de la política de certificación correspondiente al certificado> <URI de la DPC> UserNotice : Certificado de Persona Fisica reconocido
QcStatements	-	Id-etsi-qcs-QcCompliance (indicando que el certificado reconocido) Id-etsi-qcs-QcSSCD (indica que la clave privada se custodia en un DSCF)

Una compañía de GRUPO signe

signe