Signe - Autoridad de Certificación

Política de certificación

Certification policy

Certificados Corporativos de Sello Electrónico

Versión: 1.2
Fecha: 31/07/2018

Versión	Cambios	Fecha
1.0	Creación del documento.	28/02/2018
1.1	• Corrección en OID del apartado 1.2. • Correcciones de formato. • Corrección en la extensión Key Usage para quitar el bit de cifrado • Corrección en el procedimiento de emisión	11/04/2018
1.2	Homogeneización de la terminología sobre los distintos soportes de los certificados.	31/07/2018

Índice

1. Introducción

1.1. Descripción general

Los **Certificados Corporativos de Sello Electrónico** son certificados digitales reconocidos, en los términos de la Ley 59/2003, 19 de diciembre, de Firma Electrónica, (en adelante L59/2003) y cualificados de sello electrónico, 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 eIDAS), que identifican al suscriptor y firmante como una Corporación con personalidad jurídica.

La finalidad de estos certificados es poder firmar en nombre de la organización documentos electrónicos de manera automática. Estos certificados tienen como objetivo cumplir las mismas funciones que realizan los "Sellos de Empresa" en los documentos en papel.

Estos certificados se ajustan a los requisitos que impone la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público y han sido autorizados para su utilización en facturación electrónica y digitalización certificada por la Agencia Tributaria.

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 Sello Empresarial"** (OID 1.3.6.1.4.1.13177.10.1.10.2) 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 Sello Electrónico
Versión:	1.2
Descripción:	Política de Certificación para Certificados de sello electrónico
Fecha de Emisión:	31/07/2018
OIDs	1.3.6.1.4.1.36035.1.5.1 – Dispositivo Cualificado de Creación de Sello portable (DCCS portable) - Nivel Alto 1.3.6.1.4.1.36035.1.5.3 – Dispositivo Cualificado de Creación de Sello centralizado (DCCS centralizado) - Nivel Alto 1.3.6.1.4.1.36035.1.5.2 – Otros dispositivos - Nivel Medio
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)" en https://www.signe.es/signe-ac/dpc/

2. Entidades participantes

2.1. Autoridades de certificación (CA)

Los Certificados Sello Electrónico deben ser emitidos por la CA Subordinada "***SIGNE Autoridad de Certificación***", que emite certificados digitales a Corporaciones Públicas o 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

Podrán solicitar estos certificados de Sello Electrónico 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 corporativo de Sello Electrónico será responsabilidad de la persona física solicitante.

La identidad del custodio es verificada de forma indubitada por la Autoridad de Registro, que conserva la documentación acreditativa correspondiente, a disposición de los órganos judiciales, cuando actúen en el ejercicio de las funciones que tienen atribuidas y de las autoridades competentes en los demás supuestos previstos en el artículo 11.2 de la Ley Orgánica de Protección de Datos de Carácter Personal, cuando así se requiera.

2.7. Tercero que confía en los certificados

Estos certificados son certificados reconocidos/cualificados que cumplen los requisitos que establecen la L59/2003 y Reglamento UE 910/2014 (eIDAS).

Los terceros que confíen en estos certificados deben tener presente las limitaciones en su uso, tanto cuantitativas como cualitativas, que se contienen en la CPS y en la presente CP.

3. Características de los certificados

3.1. Periodo de validez de los certificados

El periodo de validez será el que se indique en el propio certificado, con un máximo de 5 años.

3.2. Uso particular de los certificados

3.2.1. Usos apropiados de los certificados

Los certificados emitidos por SIGNE podrán usarse en los términos establecidos por la normativa vigente aplicable a la firma electrónica, con las condiciones adicionales que se establecen en la CPS, y en esta CP.

Estos certificados pueden ser utilizados para autenticarse en sistemas de comunicaciones seguras, para la remisión de comunicaciones comerciales, para publicar informaciones en el web de la empresa, etc.

Estos certificados son válidos para su utilización para la firma automatizada de documentos, para la facturación electrónica y digitalización certificada y se ajustan a los requisitos que impone la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público.

3.2.2. 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 CP y en la CPS.

No se recomienda su uso para el cifrado de documentos.

3.2.3. Tarifas

El precio de los certificados de Sello Electrónico y las condiciones de pago de este tipo de certificados será necesario consultarlas telefónicamente o por mail con SIGNE.

4. Procedimientos operativos

4.1. Proceso de emisión de certificados

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

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.

La RA de SIGNE 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 se detallan a continuación:

a) Solicitud

En el momento de la solicitud, el Solicitante deberá presentar una autorización firmada (Hoja de solicitud) con los datos del Solicitante (las personas autorizadas a obtener un certificado de Sello Electrónico).

Esta autorización debe incluir: Nombre, DNI y Cargo en la organización de cada 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 los datos de la Corporación que se incluirán en el certificado de Sello Electrónico.

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 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 Otros dispositivos

Como norma general, el Suscriptor recibirá por correo electrónico la confirmación de la solicitud, y deberá proceder a la descarga de claves y certificado 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 Dispositivos Cualificados de Creación de Sello (DCCS)

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.

f) Entrega

Finalmente, la RA hará entrega del certificado al Suscriptor.

En Otros dispositivos

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

En Dispositivos Cualificados de Creación de Sello (DCCS)

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

Centralizado: 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 cualificado emitido en un DCCF.

4.2. Revocación de certificados

El Suscriptor deberá solicitar la revocación de su certificado en caso de pérdida, compromiso de claves 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**

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 de los certificados

Los certificados de sello electrónico de SIGNE siguen las recomendaciones del Esquema de identificación y firma electrónica de las Administraciones públicas, Bloque I: Perfiles de certificados electrónicos, en su versión V1.7.3 del 18/11/2009.

5.1. Nombre distinguido (DN)

Campo del DN	Nombre	Descripción
CN, Common Name	Nombre	*Contendrá el nombre comercial de la persona jurídica*
SN, Serial Number	CIF	*<CIF de la persona jurídica>*
O, Organization	Organización	*Contendrá la denominación exacta de la persona jurídica según aparezca en el Registro mercantil*
OI, organizationIdentifier	Identificador de la organización	VATES-*<CIF de la persona jurídica>(*)*
OU, Organization Unit (Opcional)	Unidad en la organización	*Contendrá el Departamento o Unidad*
E, Email Address (Opcional)	Correo electrónico	*Contendrá una dirección de correo electrónico de contacto con la empresa*
ST, State	Ubicación Geográfica	*Ámbito geográfico de vinculación del suscriptor.*
C, Country	País	*Código de país de dos dígitos según ISO 3166-1. Por defecto "ES".*

(*) Según lo estipulado en la norma ETSI EN 319 412-1

5.2. Extensiones comunes de los certificados

Extensión	Crítica	Valores
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Digital Signature Non Repudiation
X509v3 Extended Key Usage	-	TLS Web Client Authentication Email 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-caIssuers* *Access Location: <URI de acceso al certificado de la CA emisora>*
X509v3 CRL Distribution Points	-	*<URI de la CRL>*
X509v3 Subject Alternative Name (Opcional)	-	*<Email de contacto>*
QcStatements	-	*Id-etsi-qcs-QcCompliance 0.4.0.1862.1.1 (Indicando que el certificado es cualificado)* *Id-etsi-qcs-QcRetentionPeriod 0.4.0.1862.1.3 (Custodia de documentación durante 15 años)* *Id-etsi-qcs-QcPDS 0.4.0.1862.1.5 (URL con el documento que contiene los PKI Disclosure Statements):* https://www.signe.es/signe-ac/dpc/pds_en.pdf *Id-etsi-qcs-QcType-eseal 0.4.0.1862.1.6.2 (Certificado de sellos electrónicos)*

5.3. Extensiones de los certificados en Otros dispositivos

Extensión	Crítica	Valores
X509v3 Certificate Policies	-	*<OID de la política de certificación de Signe correspondiente al certificado>* *1.3.6.1.4.1.36035.1.5.2 (Otros dipositivos - Nivel Medio)* *<URI de la CPS>* *User Notice: Este es un Certificado de Sello Electrónico cualificado* *<OID "for EU qualified certificates issued to legal persons" según ETSI EN 319 411-2>* *QCP-l:0.4.0.194112.1.1*

5.4. Extensiones de los certificados con DCCS

Extensión	Crítica	Valores
X509v3 Certificate Policies	-	*<OID de la política de certificación de Signe correspondiente al certificado>* *1.3.6.1.4.1.36035.1.5.1 (DCCS portable - Nivel Alto)* *ó* *1.3.6.1.4.1.36035.1.5.3 (DCCS centralizado - Nivel Alto)* *<URI de la CPS>* *User Notice: Este es un Certificado de Sello Electrónico cualificado en DCCS* *<OID "for EU qualified certificates issued to legal persons" según ETSI EN 319 411-2>* *QCP-l-qscd: 0.4.0.194112.1.3*
QcStatements	-	*Id-etsi-qcs-QcSSCD 0.4.0.1862.1.4* *(indica que la clave privada se custodia en un DCCS)*