Signe - Autoridad de Certificación

Política de certificación

Certification policy

Certificados Corporativos de Sello Electrónico

Documento:	SIGNE-ES-AC-PC-COR-04
Versión:	1.4
Fecha:	19/03/2020

Registro de Versiones

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
1.3	Cambios en el formato. Homogeneización de la terminología de entidades participantes (Solicitante, Suscriptor, Creador de sello, Custodio de claves). Añadida la posibilidad de que el Solicitante autorice a otra persona como Custodio de claves. Se cambia el período de validez de los certificados de 5 años a 1, 2 ó 3 años. Homogeneización con el resto de Políticas de Certificación en la generación de claves y entrega del certificado en soporte Otros dispositivos utilizando un dispositivo software. Aclaraciones en la activación de los datos de creación de firma en DCCS centralizado. Añadida la revocación por correo electrónico. Eliminación de campo E-mail del DN. Aclaraciones en campos del DN. Correcciones menores.	22/03/2019
1.4	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 Custodio de Claves, conforme a lo establecido en la Ley 59/2003. Correcciones menores.	19/03/2020

Índice

1. Introducción

1.1. Descripción general

Los Certificados Corporativos de Sello Electrónico son certificados reconocidos, en los términos de la Ley 59/2003, 19 de diciembre, de firma electrónica (en adelante, "Ley 59/2003") 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, "Reglamento eIDAS"), que identifican al Suscriptor y Creador del sello 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 **"PC Sello Empresarial"** (OID 1.3.6.1.4.1.13177.10.1.10.2) de Firmaprofesional para SIGNE Autoridad de Certificación. 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
Código	SIGNE-ES-AC-PC-COR-04
Versión	1.4
Descripción	Política de Certificación de Certificados Corporativos de Sello Electrónico
Fecha de emisión	19/03/2020
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 Corporativos de Sello Electrónico son emitidos por "***SIGNE Autoridad de Certificación***", CA Subordinada de la CA Raíz de Firmaprofesional.

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 públicas) podrá actuar como Autoridad de Registro de SIGNE para la gestión de las solicitudes y emisiones de los certificados. 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 Custodio de claves, cumpliendo con lo estipulado en la DPC.
- Los dispositivos de creación de sello 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.

2.4. Suscriptor

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

2.5. Creador del sello

El Creador del sello es la persona jurídica que consta en el certificado.

De acuerdo con el Reglamento eIDAS, el Creador del sello es la persona jurídica que crea el sello electrónico.

2.6. Custodio de claves

La custodia de los datos de creación de sello asociados a cada certificado corporativo de Sello Electrónico será responsabilidad de la persona física Solicitante o de otra persona física autorizada por el Solicitante.

La identidad del custodio de claves 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 Ley 59/2003 y el Reglamento 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 DPC y en la presente PC.

3. Características de los certificados

3.1. Periodo de validez de los certificados

Los certificados Corporativos de Sello Electrónico tendrán un periodo de validez de 1, 2 ó 3 años.

3.2. Tipos de soporte

Los Certificados Corporativos de Sello Electrónico 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:

- Dispositivo Cualificado de Creación de Sello (DCCS): Nivel Alto
- Otros dispositivos: Nivel Medio

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

3.2.1. Dispositivo cualificado de creación de sello (DCCS)

Las claves privadas de los certificados emitidos en DCCS se generan y almacenan en un dispositivo cualificado de creación de sello (DCCS) como una tarjeta o un dispositivo criptográfico que ofrece, al menos, las garantías indicadas en el artículo 24 de la Ley 59/2003, y en el Anexo II del Reglamento eIDAS *mutatis mutandis* a los requisitos de los dispositivos cualificados de creación de sello electrónico.

Esta condición se indicará en el propio certificado mediante los siguientes campos:

Para DCCS portable:

- Extensión “Certificate Policies” con valor OID “1.3.6.1.4.1.36035.1.5.1”

Para DCCS centralizado:

- Extensión “Certificate Policies” con valor OID “1.3.6.1.4.1.36035.1.5.3”

En todo caso:

- Extensión QcStatements con valor “id-etsi-qcs-QcSSCD” habilitado

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

3.2.2. Otros dispositivos

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

Por lo anterior, SIGNE no puede garantizar que las claves criptográficas han sido creadas en un Dispositivo Cualificado de Creación de Sello (DCCS), en cumplimiento de los requisitos establecidos en el artículo 24 de la Ley 59/2003 y en el Anexo II del Reglamento eIDAS *mutatis mutandis* a los requisitos de los dispositivos cualificados de creación de sello electrónico. Esta condición se indicará en el propio certificado mediante los siguientes campos:

- Extensión "Certificate Policies" con valor OID "1.3.6.1.4.1.36035.1.5.2"
- Extensión QcStatements con valor "id-etsi-qcs-QcSSCD" deshabilitado

Las claves de certificados generadas en Otros dispositivos generalmente pueden ser copiadas a otros soportes, por lo tanto, es posible realizar copias de seguridad de los mismos.

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 normativa vigente aplicable a la firma electrónica, con las condiciones adicionales que se establecen en la DPC, y en esta PC.

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.

3.3.2. 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 PC y en la DPC.

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

3.4. 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

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, 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. Esta identificación presencial deberá ser realizada en el momento la solicitud, excepto, conforme a lo establecido en la Ley 59/2003, 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 los datos del Custodio de claves (la persona autorizada a obtener un certificado corporativo de Sello Electrónico).

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 Custodio de claves podrá obtener una copia.

La RA verificará presencialmente la identidad del Custodio de claves 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, conforme a lo establecido en la Ley 59/2003, cuando la identidad del Custodio de Claves 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.

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 software:

- El Custodio de claves 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 Custodio de claves proporcione el código de autenticación recibido. Una vez autenticado, el Custodio de claves 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).

En Dispositivos Cualificados de Creación de Sello (DCCS)

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

Las claves serán generadas por el Custodio de claves 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 Custodio de claves según el soporte que se utilice:

En Otros dispositivos

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

- El Custodio de claves 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 Custodio de claves podrá instalar las claves y el certificado en su sistema informático introduciendo la contraseña que él mismo estableció en el momento de la descarga.

En Dispositivos Cualificados de Creación de Sello (DCCS)

Portable: 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 sello será entregado únicamente al Custodio de claves (en el caso de que éste no aporte su propio dispositivo).

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 sello en el módulo de seguridad, el sistema informático configurado por el Custodio de claves deberá utilizar una contraseña definida por él mismo.

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**
- 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 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 o la denominación del sistema o aplicación de firma automática*
SN, Serial Number	Identificación de la organización	*Identificador de la persona jurídica, tal como figura en los registros oficiales (por ejemplo, NIF para España, RUC para Perú)*
O, Organization	Organización	*Contendrá la denominación exacta de la persona jurídica según aparezca en el Registro mercantil*
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.
OU, Organizational Unit (Opcional)	Unidad en la organización	*Contendrá el Departamento o Unidad*
ST, State	Ubicación Geográfica	*Ámbito geográfico de vinculación del suscriptor*
C, Country	País	*Código de país de dos dígitos según ISO 3166-1 donde está registrada la organización*

5.2. Extensiones comunes de los certificados

Extensión	Crítica	Valores
X509v3 Subject Alternative Name	-	rfc822Name: *email de contacto*
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Digital Signature Content Commitment
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>
QcStatements	-	id-etsi-qcs-QcCompliance (indica que el certificado es cualificado) id-etsi-qcs-QcRetentionPeriod: 15 (años de retención de la documentación del certificado) id-etsi-qcs-QcPDS: https://www.signe.es/signe-ac/dpc/pds_en.pdf (URI de la PDS en lengua inglesa) id-etsi-qcs-QcType: id-qct-eseal (indica que es un certificado para crear sellos electrónicos)

5.3. Extensiones de los certificados en Otros dispositivos

Extensión	Crítica	Valores
X509v3 Certificate Policies	-	OID de la política de certificación correspondiente al certificado: 1.3.6.1.4.1.36035.1.5.2 (Otros dispositivos - Nivel Medio) URI de la DPC: http://www.signe.es/signe-ac/dpc User Notice: Este es un Certificado de Sello Electrónico cualificado OID de la política de certificación europea: 0.4.0.194112.1.1 (corresponde a la política para certificados EU cualificados emitidos a personas jurídicas sin uso de un DCCS "QCP-l")

5.4. Extensiones de los certificados con DCCS

Extensión	Crítica	Valores
X509v3 Certificate Policies	-	OID de la política de certificación correspondiente al certificado: 1.3.6.1.4.1.36035.1.5.1 (DCCS portable - Nivel Alto) o 1.3.6.1.4.1.36035.1.5.3 (DCCS centralizado - Nivel Alto) URI de la DPC: http://www.signe.es/signe-ac/dpc User Notice: Este es un Certificado de Sello Electrónico cualificado en DCCS OID de la política de certificación europea: 0.4.0.194112.1.3 (corresponde a la política para certificados EU cualificados emitidos a personas jurídicas con uso de un DCCS "QCP-l-qscd")
QcStatements	-	id-etsi-qcs-QcSSCD (indica que la clave privada se custodia en un DCCS)

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