SIGNE Autoridad de Certificación

Política de Certificación de **Certificados Corporativos de Sello Electrónico**

Documento:	SIGNE-ES-AC-PC-COR-04
Versión:	3.1
Fecha:	21/06/2021
Tipo de documento:	PÚBLICO

Historial 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 sello electrónico 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

3.0	Añadido etiquetado del tipo de documento. Adaptación a la Ley 6/2020. Cambio del certificado de la Autoridad de Certificación Subordinada de SIGNE. Añadidos en el soporte Otros dispositivos los tipos dispositivo criptográfico portable, dispositivo criptográfico centralizado y dispositivo externo. Correcciones menores.	24/02/2021
3.1	Cambio del número de teléfono del servicio de revocación telefónico de SIGNE. Eliminación de que se podrá solicitar la revocación de un certificado telefónicamente o por correo electrónico a la RA en la que se tramitó la correspondiente solicitud de certificado. Eliminación de que se atenderá la solicitud de revocación por correo electrónico en horario de oficina. Correcciones menores.	21/06/2021

Índice

1. Introducción 5
1.1. Descripción general 5
1.2. Nombre del documento e identificación 6
1.3. Definiciones y siglas 6
2. Entidades participantes 7
2.1. Autoridades de Certificación (CA) 7
2.2. Autoridad de Registro (RA) 7
2.3. Solicitante 7
2.4. Suscriptor 7
2.5. Creador del sello 7
2.6. Custodio de claves 8
2.7. Tercero que confía en los certificados 8
3. Características de los certificados 9
3.1. Periodo de validez de los certificados 9
3.2. Tipos de soporte 9
3.2.1. Dispositivo Cualificado de Creación de Sello electrónico (DCCS) 9
3.2.2. Otros dispositivos 10
3.3. Uso particular de los certificados 10
3.3.1. Usos apropiados de los certificados 10
3.3.2. Usos no autorizados de los certificados 11
3.4. Tarifas 11
4. Procedimientos operativos 12
4.1. Proceso de emisión de certificados 12
4.2. Revocación de certificados 14
4.3. Renovación de certificados 14
5. Perfil de los certificados 15
5.1. Nombre distinguido (DN) 15
5.2. Extensiones comunes de los certificados 16
5.3. Extensiones de los certificados en Otros dispositivos 17
5.4. Extensiones de los certificados en DCCS 17

1. Introducción

1.1. Descripción general

Los certificados Corporativos de Sello Electrónico son certificados 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") y conforme a la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza (en adelante, "Ley 6/2020"), que identifican al Suscriptor y Creador del sello como una Corporación (empresa, entidad privada o pública) con personalidad jurídica.

La finalidad de estos certificados es poder firmar digitalmente en nombre de la Corporación documentos o datos electrónicos. Estos certificados tienen como objetivo cumplir las mismas funciones que realizan los "sellos de empresa o de entidad pública" 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.

La solicitud y emisión de los certificados Corporativos de Sello Electrónico se puede realizar a través de SIGNE o de las propias organizaciones a las que se vincula cada certificado, actuando éstas como Autoridades de Registro de SIGNE. No obstante, también se pueden utilizar otras entidades 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 (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 "Certificados de Sello Electrónico - Certificados Corporativos de Sello Empresarial" (OID 1.3.6.1.4.1.13177.10.1.10.D) 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 de Certificados Corporativos de Sello Electrónico
Código	SIGNE-ES-AC-PC-COR-04
Versión	3.1
Descripción	Política de Certificación de Certificados Corporativos de Sello Electrónico
Fecha de emisión	21/06/2021
Tipo de documento	PÚBLICO
OID	1.3.6.1.4.1.36035.1.5.1 – Dispositivo Cualificado de Creación de Sello electrónico portable (DCCS portable) - Nivel Alto 1.3.6.1.4.1.36035.1.5.3 – Dispositivo Cualificado de Creación de Sello electrónico 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 siglas

Las definiciones y siglas se pueden encontrar especificadas en el documento “Declaración de Prácticas de Certificación” 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 Certificacion - 2020**", CA Subordinada de la CA Raíz de Firmaprofesional.

2.2. Autoridad de Registro (RA)

La gestión de las solicitudes y la emisión 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 la emisión de los certificados Corporativos de Sello Electrónico a nombre de la propia Corporación, quien 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, del Solicitante y del Suscriptor, cumpliendo con lo estipulado en la DPC y la presente PC.
- Los dispositivos de creación de sello electrónico a utilizar, que previamente SIGNE haya homologado.

2.3. Solicitante

El Solicitante es el representante legal o voluntario (apoderado) de la Corporación que adquiere los certificados.

2.4. Suscriptor

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

El Suscriptor es la persona jurídica cuyos datos constan en el certificado.

2.5. Creador del sello

El Creador del sello es la persona jurídica identificada en el certificado por su denominación o razón social y código identificativo (por ejemplo, NIF en España, Nº RUC en Perú).

El Suscriptor y el Creador del sello serán la misma persona jurídica.

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 electrónico, o de los datos de acceso a los mismos, 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 por la Autoridad de Registro, que registrará los datos y conservará la documentación acreditativa correspondiente, con el objetivo de permitir determinar la identidad de la persona física a la que se haya entregado el certificado, para su identificación en procedimientos judiciales o administrativos.

2.7. Tercero que confía en los certificados

Los terceros que confíen en estos certificados deben tener presentes las limitaciones en su uso.

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 hasta 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 electrónico (DCCS): Nivel Alto
- Otros dispositivos: Nivel Medio

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

3.2.1. Dispositivo Cualificado de Creación de Sello electrónico (DCCS)

Las claves privadas de los certificados emitidos en DCCS se generan y almacenan en un dispositivo cualificado de creación de sello electrónico que ofrece, al menos, las garantías indicadas 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 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.

Las claves de certificados generadas en DCCS centralizado pueden ser copiadas protegidas por un dispositivo criptográfico hardware (HSM) y por los datos de activación de las mismas bajo custodia del Custodio de claves, por lo tanto, es posible realizar copias de seguridad de las mismas.

3.2.2. Otros dispositivos

Las claves privadas de los certificados emitidos en Otros dispositivos no se generan en un dispositivo cualificado de creación de sello electrónico, en cumplimiento de los requisitos establecidos 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 privadas de los certificados emitidos en Otros dispositivos se pueden generar en los siguientes tipos de dispositivos:

- Dispositivo criptográfico portable
- Dispositivo criptográfico centralizado
- Dispositivo software
- Dispositivo externo

Las claves de certificados generadas en dispositivo criptográfico portable 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.

Las claves de certificados generadas en dispositivo criptográfico centralizado pueden ser copiadas protegidas por un dispositivo criptográfico hardware (HSM) y por los datos de activación de las mismas bajo custodia del Custodio de claves, por lo tanto, es posible realizar copias de seguridad de las mismas.

Las claves de certificados generadas en dispositivo software pueden ser copiadas a otros soportes, por lo tanto, es posible realizar copias de seguridad de las mismas.

La posibilidad de realizar copias de seguridad de las claves de certificados generadas en dispositivo externo, así como la protección de dichas copias estará determinada por el tipo de dispositivo criptográfico donde se haya generado la clave privada.

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 en la DPC y en la legislación vigente al respecto.

Los certificados Corporativos de Sello Electrónico pueden ser utilizados para autenticarse en sistemas de comunicaciones seguras, y para firmar digitalmente documentos o datos

electrónicos.

Estos certificados son válidos para su utilización para la firma digital automatizada de documentos o datos electrónicos, y para la facturación electrónica y la digitalización certificada, ajustándose 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.

Se permite el uso de estos certificados en las relaciones del Suscriptor con las Administraciones Públicas.

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

SIGNE o la RA podrán establecer las tarifas que considere oportunas a los Suscriptores, así como establecer los medios de pago que consideren más adecuados 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 o de la RA.

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 o voluntario de la Corporación en el momento de solicitar un certificado.

El Solicitante deberá incluir en la solicitud una autorización firmada 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 comercial de la Corporación o nombre del sistema o aplicación de firma que constará en el certificado; Departamento o unidad que gestiona el sistema o aplicación de firma en la Corporación (opcional); Ámbito geográfico de la Corporación o de vinculación del sistema o aplicación de firma con la Corporación; Nombre y apellidos, Código identificativo (por ejemplo, DNI, NIE u otro tipo de NIF en España; DNI o Nº Carné de Extranjería en Perú; Nº Pasaporte), Cargo en la organización y Dirección de correo electrónico de la persona autorizada.

Además, el Solicitante y el Custodio de claves deberán confirmar que han sido informados del Régimen obligatorio de uso del certificado, documento habrá sido entregado al Solicitante y habrá sido firmado por éste, quedando bajo custodia de la RA y del que el Custodio de claves podrá obtener una copia.

b) Aceptación de la solicitud

La RA realizará la identificación y autenticación del Suscriptor, del Solicitante y del Custodio de claves según lo especificado en la DPC en los apartados de validación inicial de la identidad relativos a la autenticación de la identidad de una persona jurídica y de una persona física.

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 tras la tramitación será la generación de claves según el soporte que se utilice:

DCCS portable o centralizado, Otros dispositivos de los tipos dispositivo criptográfico portable o centralizado

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

Portable: las claves serán generadas por un Operador de RA en el dispositivo, haciendo entrega a la RA de una petición de certificado en formato PKCS #10.

Centralizado: las claves serán generadas por el Custodio de claves en el dispositivo, haciendo entrega a la RA de una petición de certificado en formato PKCS #10.

Otros dispositivos del tipo 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 generación de certificados.
- Para poder acceder a la aplicación online de generación 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 generación del certificado (incluye la generación de las claves, la emisión del certificado y la descarga de ambos en formato PKCS #12 protegido con una contraseña que él mismo habrá establecido).

Otros dispositivos del tipo dispositivo externo

- Las claves habrán sido generadas previamente en un dispositivo externo gestionado por el Suscriptor y/o el Custodio de claves.
- El Custodio de claves entregará a la RA la clave pública en 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:

DCCS portable o centralizado, Otros dispositivos de los tipos dispositivo criptográfico portable o centralizado

Portable: la RA cargará el certificado en el dispositivo en el que se hayan generado previamente las claves. El código de activación del dispositivo 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 las claves. Para la activación de los datos de creación de sello electrónico en el

dispositivo, el sistema informático configurado por el Custodio de claves deberá utilizar:

- **DCCS centralizado:** una contraseña definida por el Custodio de claves.
- **Dispositivo criptográfico centralizado:** una contraseña definida por el Custodio de claves y unos códigos proporcionados a éste por SIGNE.

Otros dispositivos del tipo dispositivo software

- La generación del certificado por el Custodio de claves incluye la descarga conjunta de la clave privada y del certificado en formato PKCS #12 protegido con una contraseña que él mismo habrá establecido.
- El Custodio de claves 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 generación del certificado.

Otros dispositivos del tipo dispositivo externo

- El Custodio de claves recibirá por correo electrónico un enlace para descargar el certificado.
- El Custodio de claves descargará el certificado y lo cargará en el dispositivo en el que se hayan generado previamente las claves.

4.2. Revocación de certificados

El Suscriptor o el Custodio de claves 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 o el Custodio de claves pueden:

- Llamar al servicio de revocación telefónico de SIGNE (horario de oficina[1]): **+34 918 06 10 08**
- Enviar un correo electrónico a SIGNE: signe-ac@signe.com

En el apartado correspondiente de la DPC se encuentra toda la información complementaria referente a la revocación de certificados.

4.3. Renovación de certificados

SIGNE Autoridad de Certificación enviará una notificación de recordatorio de caducidad del certificado por correo electrónico al Suscriptor 45 días, 30 días y 15 días antes de la fecha de caducidad del certificado.

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

[1] Días laborables en Madrid de lunes a viernes, de 8:30 a 18:30

5. Perfil de los certificados

5.1. Nombre distinguido (DN)

El DN de los certificados Corporativos de Sello Electrónico contendrá los atributos que se indican a continuación. Todos los valores serán verificados por la Autoridad de Registro.

Atributo del DN	Nombre	Descripción
CN, Common Name	Nombre	*Contendrá uno de los siguientes valores:* *- Nombre comercial de la persona jurídica* *- Denominación del sistema o aplicación de firma*
Serial Number	Número de serie	*Código identificativo de la persona jurídica (por ejemplo, NIF en España, Nº RUC en Perú)*
O, Organization Name	Organización	*Denominación o razón social de la persona jurídica*
OI, Organization Identifier	Identificador de la organización	*Código identificativo de la persona jurídica, codificado según ETSI EN 319 412-1 con el tipo VAT (national value added tax identification number, por ejemplo, NIF en España, RUC en Perú)* *Ejemplo:* VATES-B0085974Z
OU, Organizational Unit Name (Opcional)	Unidad en la organización	*Departamento o Unidad que gestiona el sistema o aplicación de firma en la persona jurídica*
S, State or Province Name	Estado/Provincia	*Ámbito geográfico (por ejemplo, provincia en España y Perú) de la persona jurídica o de vinculación del sistema o aplicación de firma con la persona jurídica*
C, Country Name	País	*Código de dos letras según ISO 3166-1 donde está registrada la persona jurídica*

5.2. Extensiones comunes de los certificados

Extensión	Crítica	Valores
X509v3 Subject Alternative Name	-	rfc822Name: *email de contacto de la persona jurídica*
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 en 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