Signe - Autoridad de Certificación

Política de certificación

Certification policy

Certificados de Sello de Órgano

Documento:	SIGNE-POL-ADM-AC-01
Versión:	2.3
Fecha:	22/03/2019

Registro de Versiones

Versión	Cambios	Fecha
1.0	Creación del documento	02/11/2010
1.1	Cambios en el formato	24/03/2015
1.2	Modificación documento. Inclusión definiciones y acrónimos	06/06/2016
2.0	Adaptación eIDAS	28/02/2018
2.1	Correcciones en los OIDs Corrección en la extensión *Key Usage* para quitar el bit de cifrado Corrección en el procedimiento de emisión	11/04/2018
2.2	Homogeneización de la terminología sobre los distintos soportes de los certificados.	31/07/2018
2.3	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 3 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. Aclaraciones en campos del DN. Inclusión de campo *rfc822Name* en SAN. Correcciones menores.	22/03/2019

Índice

1. Introducción

1.1. Descripción general

Los Certificados de sello de Administración, órgano o entidad de derecho público son certificados cualificados expedidos a Administraciones Públicas, órganos o entidades de derecho público para dispositivos informáticos, programas o aplicaciones, bajo la responsabilidad del suscriptor o titular del certificado, de acuerdo con las indicaciones del artículo 40 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y son certificados reconocidos, en los términos de la Ley 59/2003, 19 de diciembre, de firma electrónica (en adelante, Ley 59/2003).

La presente política se adhiere a las definiciones de los niveles de aseguramiento alto y medio y a los perfiles de certificados establecidos en el punto 9 del documento "Perfiles de Certificados electrónicos" de la Subdirección General de Información, Documentación y Publicaciones del Ministerio de Hacienda y Administraciones Públicas.

Los Certificados de Sello de Administración, órgano o entidad de derecho público son acordes al Anexo III del Reglamento (UE) Nº 910/2014 el 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 especifica los requisitos para los certificados cualificados de sello electrónico.

La finalidad del certificado de sello de Administración, órgano o entidad de derecho público es poder firmar en nombre del órgano en sistemas de firma electrónica para la actuación administrativa automatizada.

Los Certificados de sello de Administración, órgano o entidad de derecho público permiten también facturación electrónica.

La solicitud y emisión de los Certificados de sello de Administración, órgano o entidad de derecho público se realiza a través de las 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.

El presente documento es una adaptación de la Política de Certificación **"PC Sello de Órgano"** (OID 1.3.6.1.4.1.13177.10.1.21.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 Certificados de Sello de Órgano
Versión	2.3
Descripción	Política de Certificación de Certificados de sello de Administración, órgano o entidad de derecho público
Fecha de emisión	22/03/2019
OIDs	1.3.6.1.4.1.36035.1.10.1 – Dispositivo Cualificado de Creación de Sello portable (DCCS portable) - Nivel Alto 1.3.6.1.4.1.36035.1.10.3 – Dispositivo Cualificado de Creación de Sello centralizado (DCCS centralizado) - Nivel Alto 1.3.6.1.4.1.36035.1.10.2 – 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)" URL https://www.signe.es/signe-ac/dpc

2. Entidades participantes

2.1. Autoridades de Certificación (CA)

Los Certificados de sello de Administración, órgano o entidad de derecho público son emitidos por ***"SIGNE Autoridad de Certificación"***, CA Subordinada de la CA Raíz de Firmaprofesional.

2.2. Autoridad de Registro (RA)

SIGNE actuará directamente como Autoridad de Registro para la emisión de certificados de sello de Administración, órgano o entidad de derecho público.

2.3. Solicitante

Podrá realizar la solicitud de un certificado de sello de Administración, órgano o entidad de derecho público el representante legal o voluntario de la organización.

2.4. Suscriptor

El Suscriptor del certificado será la Administración Pública, identificada por su NIF y denominación, que consta en el certificado.

2.5. Creador del sello

El Creador del sello será la Administración Pública, identificada por su NIF y denominación, 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 de sello de Administración, órgano o entidad de derecho público será responsabilidad de la persona física Solicitante o de otra persona física autorizada por el Solicitante.

2.7. Tercero que confía en los certificados

Los certificados de sello de Administración, órgano o entidad de derecho público de SIGNE cumplen los requisitos para ser reconocidos por @firma, la Plataforma de validación y firma electrónica ofrecida por el Gobierno de España.

3. Características de los certificados

3.1. Periodo de validez de los certificados

Los certificados de sello de Administración, órgano o entidad de derecho público tendrán un periodo de validez de 1, 2 ó 3 años.

3.2. Tipo de soporte

Los certificados de sello de Administración, órgano o entidad de derecho público 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 organización 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 “1.3.6.1.4.1.36035.1.10.1”

Para DCCS centralizado:

- Extensión “Certificate Policies” con valor OID “1.3.6.1.4.1.36035.1.10.3”

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 "1.3.6.1.4.1.36035.1.10.2"
- 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 usados como mecanismo de identificación y autenticación en sistemas de firma electrónica para la actuación administrativa automatizada tal como establece el artículo 42 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

3.3.2. Usos no autorizados de los certificados

No se permite la utilización distinta de lo establecido en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público para este tipo de certificados.

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 de Administración, órgano o entidad de derecho público 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 Corporación Pública no tuviera firmado el contrato de prestación de servicios de certificación con SIGNE, éste deberá ser firmado por el representante legal (el Órgano superior unipersonal de representación o el Órgano en quien se delegue o el Responsable de Recursos Humanos) 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

El Solicitante se personará ante SIGNE o un agente comercial de ésta para identificarse como representante de la organización a la que pertenece.

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 de sello de Administración, órgano o entidad de derecho público).

Los datos de esta autorización deben incluir: Datos de la AAPP, indicando para qué órgano de la Administración se desea el certificado, Nombre, Número de documento de identificación que será presentado (DNI), 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 (DNI).

La RA verificará los datos de la organización que se incluirán en el certificado de sello de Administración, órgano o entidad de derecho público.

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, los datos a incluir en el certificado y la publicación de la resolución de la Subsecretaría del Ministerio o titular del organismo público competente[1].

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

- Al solicitante con su documento de identificación presentado (DNI).
- 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, 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.

[1] RD1671/2009. Art. 19.1

e) Emisión del certificado

Una vez las claves generadas, la RA procederá a la emisión del certificado, firmando la petición de certificado en formato PKCS#10 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 firma 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

5.1. Nombre distinguido (DN)

El DN de los certificados de sello de Administración, órgano o entidad de derecho público contendrá como mínimo los elementos que se citan con el formato siguiente. Todos los valores de los componentes serán autenticados por la Autoridad de Registro:

Campo del DN	Nombre	Descripción
O, Organization	Organización	*Contendrá la denominación de la Administración a la que pertenece el órgano (p.e.* Universidad de Zoronda*)*
OI, Organization Identifier	Identificador de la organización	*Identificador de la persona legal, 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: "VATES" + "-" + <NIF de la persona legal>.* *Ejemplo:* VATES-B0085974Z
OU, Organizational Unit	Unidad en la organización	SELLO ELECTRONICO
SN, Serial Number	NIF	*NIF de la Administración Pública, órgano o entidad de derecho público (p.e., para el caso de* Universidad de Zoronda*,* Q5555555)
Surname	Apellidos (persona física)	*Primer y segundo apellidos del Custodio de claves (de acuerdo con el documento de identidad -DNI-) + " - DNI " + <NIF del Custodios>*
Givenname	Nombre	*Nombre de pila del Custodio de claves, de acuerdo con documento de identidad (DNI)*
CN, CommonName	Denominación del sistema o aplicación	*p.e.* PLATAFORMA eTITULO
C, Country	País	ES

5.2. Extensiones comunes de los certificados

Extensión	Crítica	Valores
X509v3 Subject Alternative Name	-	rfc822Name: *email de contacto de la Administración Pública, órgano o entidad de derecho público*
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 DistributionPoints	-	<URI de la CRL>
QcStatements	Sí	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 Subject Alternative Name	-	directoryName: OID: 2.16.724.1.3.5.6.2.1 = SELLO ELECTRONICO DE NIVEL MEDIO OID: 2.16.724.1.3.5.6.2.2 = *<O del DN>* OID: 2.16.724.1.3.5.6.2.3 = *<serialNumber del DN>* OID: 2.16.724.1.3.5.6.2.4 = *NIF del Custodio* OID: 2.16.724.1.3.5.6.2.5 = *<CN del DN>* OID: 2.16.724.1.3.5.6.2.6 = *Nombre del Custodio*[2] OID: 2.16.724.1.3.5.6.2.7 = *Primer apellido del Custodio*[2] OID: 2.16.724.1.3.5.6.2.8 = *Segundo apellido del Custodio*[2] OID: 2.16.724.1.3.5.6.2.9 = *email del Custodio*
X509v3 CertificatePolicies	-	OID de la política de certificación correspondiente al certificado: 1.3.6.1.4.1.36035.1.10.2 (Otros dispositivos - Nivel Medio) URI de la DPC: http://www.signe.es/signe-ac/dpc User Notice: Certificado cualificado de sello de Administración, órgano o entidad de derecho público, nivel medio OID de la política de certificación según Secretaría SGIADSC del MHAFP: 2.16.724.1.3.5.6.2 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")

[2] de acuerdo con documento de identidad (DNI)

5.4. Extensiones de los certificados con DCCS

Extensión	Crítica	Valores
X509v3 Subject Alternative Name	-	directoryName: OID: 2.16.724.1.3.5.6.1.1 = SELLO ELECTRONICO DE NIVEL ALTO OID: 2.16.724.1.3.5.6.1.2 = *<O del DN>* OID: 2.16.724.1.3.5.6.1.3 = *<serialNumber del DN>* OID: 2.16.724.1.3.5.6.1.4 = *NIF del Custodio* OID: 2.16.724.1.3.5.6.1.5 = *<CN del DN>* OID: 2.16.724.1.3.5.6.1.6 = *Nombre del Custodio*[3] OID: 2.16.724.1.3.5.6.1.7 = *Primer apellido del Custodio*[3] OID: 2.16.724.1.3.5.6.1.8 = *Segundo apellido del Custodio*[3] OID: 2.16.724.1.3.5.6.1 .9 = *email del Custodio*
X509v3 CertificatePolicies	-	OID de la política de certificación correspondiente al certificado: 1.3.6.1.4.1.36035.1.10.1 (DCCS portable - Nivel Alto) o 1.3.6.1.4.1.36035.1.10.3 (DCCS centralizado - Nivel Alto) URI de la DPC: http://www.signe.es/signe-ac/dpc User Notice: Certificado cualificado de sello de Administración, órgano o entidad de derecho público, nivel alto OID de la política de certificación según Secretaría SGIADSC del MINHAFP: 2.16.724.1.3.5.6.1 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	Sí	id-etsi-qcs-QcSSCD (indica que la clave privada se custodia en un DCCS)

[3] de acuerdo con documento de identidad (DNI)

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