Política de certificación

Certification policy

Certificados de Sello de Órgano

Versión 2.0

Fecha: 28/02/2018

Seguridad documental

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

Índice

1. **INTRODUCCIÓN**
1.1 Descripción General
1.2 Nombre del Documento e identificación
1.3 Definiciones y acrónimos

2. **ENTIDADES PARTICIPANTES**
2.1 Autoridades de Certificación (CA)
2.2 Autoridad de Registro (RA)
2.3 Solicitante
2.4 Suscriptor
2.5 Custodio de Claves
2.6 Tercero que confía en los certificados

3. **CARACTERÍSTICAS DE LOS CERTIFICADOS**
3.1 Periodo de validez de los certificados
3.2 Tipo de soporte
3.3 Uso particular de los certificados de sello de Administración, órgano o entidad de derecho público

4. **PROCEDIMIENTOS OPERATIVOS**
4.1 Proceso de emisión de certificados
4.2 Revocación de certificados
4.3 Renovación de certificados

5. **PERFIL DE LOS CERTIFICADOS**
5.1 Campos comunes a los dos niveles
5.2 Nivel alto
5.3 Nivel medio

1. Introducción

1.1 Descripción general

Los Certificados de sello de Administración, órgano o entidad de derecho públicoson certificados reconocidos expedido 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.
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 910/2014 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 **"CP Sello de Órgano"** (OID 1.3.6.1.4.1.13177.10.1.21.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 – Sello de Órgano
Versión:	2.0
Descripción:	Política de Certificación para Certificados de sello de Administración, órgano o entidad de derecho público
Fecha de Emisión:	28/02/2018
OIDs	1.3.6.1.4.1.36035.1.10.1 – Nivel Alto – *Dispositivo Cualificado de Creación de Firma (DCCF) Portable* 1.3.6.1.4.1.36035.1.10.2 – Nivel Medio –*Software* 1.3.6.1.4.1.36035.1.10.3 – Nivel Alto – *DCCF Centralizado*
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 Corporativos de sello de administración, órgano o entidad de derecho público deben ser emitidos por la CA Subordinada "SIGNE Autoridad de Certificación", que emite certificados digitales a Corporaciones Públicas.

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 cualquier persona autorizada por su propia organización para ello.

2.4 Suscriptor

El suscriptor del certificado será una Administración Pública, identificada por su CIF y denominación.

2.5 Custodio de claves

El custodio de claves será la persona física solicitante del certificado, debidamente autorizado por su Organización para ello.

2.6 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 del Ministerio de la Presidencia.

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 3 años.

3.2 Tipo de soporte

Los certificados de sello de Administración, órgano o entidad de derecho público se emitirán en los siguientes tipos de soporte en función de dónde se cree y resida el par de claves, dando lugar a dos niveles de aseguramiento:

DCCF Portable, DCCF Centralizado: Nivel ALTO
Soporte *software*: Nivel MEDIO

3.2.1 Soporte en hardware

Las claves privadas de los certificados emitidos en soporte hardware se generan y almacenan en un dispositivo cualificado de creación de firma (DCCF) como una tarjeta o un dispositivo criptográfico que ofrecen, al menos, las garantías indicadas en el artículo 23 de la ley 59/2003, y en el Anexo II del Reglamento UE 910/2014
Esta condición se indicará en el propio certificado mediante los siguientes campos:

- Extensión “Certificate Policies” con valor OID “**1.3.6.1.4.1.36035.1.10.1**”

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

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.

En los casos en que SIGNE pueda garantizar que las claves criptográficas del firmante han sido creadas en un Dispositivo Cualificado de Creación de Firma (DCCF) centralizado, en cumplimiento de los requisitos establecidos en el artículo 24 de la Ley 59/2003, de 19 diciembre, de Firma Electrónica, y en el Anexo II del Reglamento UE 910/2014, esta condición se indicará en el propio certificado mediante los siguientes campos:

- Extensión “Certificate Policies” con valor OID “**1.3.6.1.4.1.36035.1.10.3**”
- Extensión QcStatement con valor “id-etsi-qcs-QcSSCD” habilitado

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.

Al tratarse de certificados en software, SIGNE no puede garantizar que las claves criptográficas del firmante han sido creadas en un Dispositivo Cualificado de Creación de Firma (DCCF), en cumplimiento de los requisitos establecidos en el artículo 24 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, y en el Anexo II del Reglamento UE 910/2014. 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 QcStatement con valor “id-etsi-qcs-QcSSCD” deshabilitado

Estos certificados pueden ser copiados a otros soportes, por lo tanto es posible realizar copias de seguridad de los mismos.

3.3 Uso particular de los certificados de sello de Administración, órgano o entidad de derecho público

3.3.1 Usos apropiados de los certificados

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.

3.3.3 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)por él mismo con los datos de la AAPP, indicando para qué órgano de la Administración se desea el certificado.

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 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.

d) Generación de claves

El primer paso de la tramitación será la generación de claves según el soporte que se utilice:

1. El Operador de RA valida la veracidad y exactitud de los datos del firmante.

2. En caso necesario, el Operador de RA gestionará la generación de claves para el firmante en un dispositivo de creación firma.

[1] RD1671/2009. Art. 19.1

3. El Operador de RA validará que el firmante está en posesión de la clave privada (datos de creación de firma) asociada a la clave pública (datos de verificación de firma) incluida en la petición de certificación

e) Emisión del certificado

La RA procederá a la emisión del certificado, firmando la petición de certificado en formato PKCS#10 y enviándola a la CA.
Una vez que se haya generado el certificado, y antes que la RA pueda entregarlo al Solicitante, 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".

f) Entrega

Finalmente, la RA hará entrega del certificado al Suscriptor permitiendo su descarga de forma segura desde Internet.
Para certificados en hardware criptográfico, el certificado deberá ser importado al dispositivo donde se generaron el par de claves.

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:

- 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

El Solicitante deberá ponerse en contacto con la RA y solicitar la generación de un certificado nuevo.

5. Perfil de los certificados

5.1 Campos comunes a los dos niveles

5.1.1 Certificado

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	Nombre	Descripción
SignatureAlgorithm	Algoritmo de firma	*RsaWithSHA2, con longitud de claves de 1024 o superior*

Campo del DN	Nombre	Descripción
O, Organization	Organización	*Contendrá la denominación exacta de la empresa según aparezca en el Registro mercantil, para el caso de organizaciones privadas.* *Contendrá la denominación de la Administración a la que pertenece el órgano (p.e. "*Universidad de Zoronda*")*
Organization Identifier	CIF	Identificador de la organización distinto del nombre. Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)
OU, OrganizationUnit	Unidad en la organización	"SELLO ELECTRONICO"
SN, Serial Number	CIF	*CIF de la Administración Pública, órgano o entidad de derecho público (p.e., para el caso del "*Universidad de Zoronda*", Q5555555)*
Surname (opcional)	Apellidos (persona física)	*Primer y segundo apellidos del titular del órgano administrativo (de acuerdo con el documento de identidad - DNI, pasaporte, ...-) +* " - DNI " *+ NIF del custodio de la clave privada*
Givenname (opcional)	Nombre	*Nombre de pila del titular del órgano administrativo, de acuerdo con documento de identidad (DNI, pasaporte, ...)*
CN, CommonName	Denominación del sistema o aplicación	*p.e.* "PLATAFORMA eTITULO"
C, Country	País	*Código de país de dos dígitos según ISO 3166-1.* *Por defecto "*ES*".*

5.1.2 Extensiones de los certificados

Extensión	Crítica	Valores
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Digital Signature Content Commitment Key Encipherment
X509v3 Extended Key Usage	-	Email protection TLS Web ClientAuthentication
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 AuthorityInformation 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>
QualifiedCertificateStatements	Sí	Id-etsi-qcs-QcCompliance: 0.4.0.1862.1.1 (indicando que el certificado cualificado) Id-etsi-qcs-QcRetentionPeriod: 0.4.0.1862.1.3 (con un valor de 15 años) Id-etsi-qcs-QcPDS2: 0.4.0.1862.1.5 (URI: https://www.firmaprofesional.com/cps) Id-etsi-qcs-QcType: 0.4.0.1862.1.6.2 (qct-**eseal**, indica que es un certificado para crear sellos electrónicos).

[2] Obligatoria en lengua inglesa. Pueden incluirse otros QcPDS en otras lenguas.

5.2 Extensiones nivel alto

Extensión	Crítica	Valores
X509v3 CertificatePolicies	-	<OID de la política de certificación correspondiente al certificado> 1.3.6.1.4.1.36035.1.10.1: DCCFF portable 1.3.6.1.4.1.36035.1.10.3: DCCF centralizado <URI de la DPC> https://www.signe.es/signe-ac/dpc UserNotice: "Certificado cualificado de sello de Administración, órgano o entidad de derecho público de Administración, órgano o entidad de derecho público, nivel alto" <OID de la política de certificación según Secretaría SGIADSC: 2.16.724.1.3.5.6.1> < OID "for EU qualified certificates issued to legal persons" según ETSI EN 319 411-2: QCP-l-qscd: 0.4.0.194112.1.3>
QualifiedCertificateStatements	Sí	Id-etsi-qcs-QcSSCD: 0.4.0.1862.1.4 (indica que la clave privada se custodia en un DCCF)
X509v3 SubjectAlternativeName	-	directoryName: OID: 2.16.724.1.3.5.2.1.1 = "sello de Administración, órgano o entidad de derecho público" OID: 2.16.724.1.3.5.2.1.2 = <O del DN> OID: 2.16.724.1.3.5.2.1 .3 = <serialNumber del DN> OID: 2.16.724.1.3.5.2.1 .4 = <NIF/NIE del custodio> OID: 2.16.724.1.3.5.2.1 .5 = <CN del DN> OID: 2.16.724.1.3.5.2.1 .6 = <Givenname> OID: 2.16.724.1.3.5.2.1 .7 = <Primer apellido del custodio>3 OID: 2.16.724.1.3.5.2.1 .8 = <Segundo apellido del custodio>4 OID: 2.16.724.1.3.5.2.1 .9 = <correo electrónico del custodio>

[3] de acuerdo con documento de identidad (DNI, pasaporte, ...)

[4] de acuerdo con documento de identidad (DNI, pasaporte, ...)

5.3 Extensiones nivel medio

Extensión	Crítica	Valores
X509v3 CertificatePolicies	-	<OID de la política de certificación correspondiente al certificado> 1.3.6.1.4.1.36035.1.10.2 <URI de la DPC> UserNotice: "Certificado reconocido de sello de Administración, órgano o entidad de derecho público de Administración, órgano o entidad de derecho público, nivel medio" < OID de la política de certificación según Secretaría SGIADSC: 2.16.724.1.3.5.6.2> < OID "for EU qualified certificates issued to legal persons" según ETSI EN 319 411-2: QCP-l: 0.4.0.194112.1.1>
X509v3 SubjectAlternativeName	-	directoryName: OID: 2.16.724.1.3.5.2.2.1 = "sello de Administración, órgano o entidad de derecho público" OID: 2.16.724.1.3.5.2.2.2 = <O del DN> OID: 2.16.724.1.3.5.2.2.3 = <serialNumber del DN> OID: 2.16.724.1.3.5.2.2.4 = <NIF/NIE del custodio> OID: 2.16.724.1.3.5.2.2.5 = <CN del DN> OID: 2.16.724.1.3.5.2.2.6 = <Givenname> OID: 2.16.724.1.3.5.2.2.7 = <Primer apellido del custodio>[5] OID: 2.16.724.1.3.5.2.2.8 = <Segundo apellido del custodio>[6] OID: 2.16.724.1.3.5.2.2.9 = <correo electrónico del custodio>

[5] de acuerdo con documento de identidad (DNI, pasaporte, ...)

[6] de acuerdo con documento de identidad (DNI, pasaporte, ...)

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