CERTIFICADOS DE SELLO DE ADMINISTRACIÓN, ÓRGANO O ENTIDAD DE DERECHO PÚBLICO

Política de Certificado

Versión: 171121

Clasificación: Público

Firmado digitalmente por: FIRMAPROFESIONAL, S.A.
Fecha y hora: 21.11.2017 11:26:08

ATENCIÓN: El original vigente de este documento se encuentra en formato electrónico en la web de Firmaprofesional: https://www.firmaprofesional.com/cps

Histórico de versiones

Versión	Sección y cambios	Fecha publicación
6.0	Para consultar cambios entre versiones anteriores, por favor envíe un correo a info@firmaprofesional.com	15/04/2014
171121	Cambio de plantilla y numeración de versiones, pasando a seguir el formato AAMMDD (año, mes y día de la publicación) Inclusión del presente apartado. Adaptación a eIDAS. Añadido Dispositivo Cualificado de Creación de Firma (DCCF) centralizado.	21/11/2017

Índice

1. INTRODUCCIÓN

1.1. Descripción general

Los **Certificados de Sello de Administración, órgano o entidad de derecho público** son certificados reconocidos 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.

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.

En el presente documento se exponen las condiciones particulares referentes a este tipo de certificado. Esta Política de Certificación (en adelante, la "CP") está sujeta al cumplimiento de la Declaración de Prácticas de Certificación (en adelante, la "CPS") de Firmaprofesional, a la que incorpora por referencia.

1.2. Identificación del Documento

Nombre:	CP Sello de Órgano
Versión:	171121
Descripción:	Política de Certificación para Certificados de Sello de Administración, órgano o entidad de derecho público
Fecha de Emisión:	21/11/2017
OIDs	1.3.6.1.4.1.13177.10.1.21.1 Nivel Alto, Dispositivo Cualificado de Creación de Firma (DCCF) portable 1.3.6.1.4.1.13177.10.1.21.3 Nivel Alto, Dispositivo Cualificado de Creación de Firma (DCCF) centralizado 1.3.6.1.4.1.13177.10.1.21.2 Nivel Medio
Localización	http://www.firmaprofesional.com/cps

2. ENTIDADES PARTICIPANTES

2.1. Autoridades de Certificación (CA)

Estos certificados deben ser emitidos por la CA Subordinada "***AC Firmaprofesional - AAPP***", que emite certificados digitales a Corporaciones Públicas.

2.2. Autoridad de Registro (RA)

La gestión de las solicitudes y emisiones de los certificados será realizada por las entidades que actúen como Autoridades de Registro de Firmaprofesional.

Cada entidad que actúe como RA de Firmaprofesional establecerá:

- Los criterios que se deben cumplir para solicitar un certificado, sin entrar en contradicción con lo estipulado en la CPS y la presente CP.
- Los mecanismos y procedimientos necesarios para realizar la identificación y autenticación del firmante, cumpliendo con lo estipulado en la CPS y la presente CP.
- Los dispositivos de creación de firma a utilizar, de entre los que previamente Firmaprofesional haya homologado.

2.3. Solicitante

Podrá realizar la solicitud de estos certificados cualquier persona autorizada por la Administración, Órgano o Entidad de derecho público.

2.4. Suscriptor

El suscriptor del certificado será la Administración, Órgano o Entidad de derecho público que aparece identificada en el Certificado.

2.5. Tercero que confía en los certificados

Estos certificados están reconocidos por **@firma**, la Plataforma de validación y firma electrónica del Ministerio de la Presidencia.

3. CARACTERISTICAS 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 3 años.

3.2. Uso particular de los certificados

3.2.1. 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.

3.2.2. 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. Tarifas

Firmaprofesional cobrará al Suscriptor lo acordado en el contrato de prestación de servicios firmado por las partes.

Firmaprofesional podrá establecer las tarifas que considere oportunas a los suscriptores, así como establecer los medios de pago que considere más adecuado 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 Firmaprofesional.

4. PROCEDIMIENTOS OPERATIVOS

4.1. Proceso de emisión de certificados

Los pasos a seguir para la obtención del certificado se detallan a continuación:

a) Solicitud

Se deberá presentar la referencia al Diario Oficial en el que aparece la disposición de creación de la Sede Electrónica.

La creación de sellos electrónicos se realizará mediante resolución de la Subsecretaría del Ministerio o titular del organismo público competente, que se publicará en la sede electrónica correspondiente.

Las solicitudes de estos certificados deberán realizarse directamente a Firmaprofesional dirigiéndose a algún colaborador que actúe como RA de Firmaprofesional.

En los casos en que Firmaprofesional ya haya verificado previamente la identidad de la Persona Jurídica y del solicitante, no será necesario realizar verificaciones adicionales. En concreto:

- Si el solicitante dispone de un Certificado Corporativo de Representante Legal vigente emitido por Firmaprofesional.
- Si la Corporación actúa como RA de Firmaprofesional para la emisión de sus propios certificados.

a) Aceptación de la solicitud

Firmaprofesional verificará que:

- Existe la Sede Electrónica y se corresponde con los datos publicados en la Resolución de creación de la misma
- Existe una resolución de la Subsecretaría del Ministerio o titular del organismo público competente por la que se crea el Sello Electrónico y está publicada en la Sede Electrónica correspondiente.
- Los datos de la solicitud del certificado de Sello Electrónico coinciden con los datos publicados en la resolución
- La solitud la realiza un representante del Titular del Sello Electrónico debidamente acreditado y autorizado para ello.

En caso de solicitar nivel ALTO, se deberá aportar evidencia de que la generación y custodia de claves se realiza en un dispositivo hardware criptográfico

b) Tramitación

Cada Autoridad de Registro de Firmaprofesional tendrá acreditadas a una serie de personas para actuar como **Operador de RA** frente a Firmaprofesional. Los Operadores de RA habrán sido

autorizados para realizar esta función y habrán sido previamente instruidos en la operativa de emisión de certificados. Cada Operador de RA dispondrá de un Certificado Digital en DCCF (Dispositivo Cualificado de Creación de Firma) propio, que le permitirá gestionar las solicitudes de certificados de usuarios.

Las fases de la tramitación son las siguientes:

1. **Generación de claves**

   El Operador de RA validará la veracidad y exactitud de los datos del firmante y del solicitante

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

   El Operador de RA validará que el solicitante 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.

2. **Emisión del certificado**

   El Operador de RA generará la petición de certificado en un formato estándar y la enviará a Firmaprofesional.

   Firmaprofesional validará la integridad de la petición y que ha sido generada por un Operador de RA debidamente autorizado. Tras esta validación se procederá a la emisión del certificado.

   En los casos en que Firmaprofesional tenga garantía de que el dispositivo en el que se han generado el par de claves es un DCCF, el certificado se emitirá con el OID correspondiente.

3. **Entrega**

   Una vez se ha generado el certificado, y antes de que la RA pueda entregarlo al solicitante, éste último deberá:

   - Personarse ante la RA en cumplimiento del artículo 13 de la Ley 59/2003, salvo en los casos en que esta personación no sea necesaria tal como recoge el propio artículo.

   - Aceptar formalmente la entrega del certificado dejando evidencia documental en poder de la RA.

   Finalmente, la RA hará entrega del certificado al solicitante, ya sea entregándole el DCCF portable, los mecanismos de autenticación y operación remota de firma electrónica o habilitándole los mecanismos para su descarga y posterior uso.

4.2. Revocación de certificados

Según se especifica en la Declaración de Prácticas de Certificación (CPS)

4.3. Renovación de certificados

El suscriptor deberá dirigirse a su RA, y proceder a la generación de un certificado nuevo.

5. PERFIL DE LOS CERTIFICADOS

5.1. Campos comunes a los dos niveles

5.1.1. Certificado

Campo del DN	Nombre	Descripción
O, Organization	Organización	Contendrá la denominación de la Administración a la que pertenece el órgano (p.e. "Ministerio de Igualdad ")
Organization Identifier		Identificador de la organización distinto del nombre. Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)
OU, Organization Unit	Unidad en la organización	"SELLO ELECTRONICO"
Serial Number	CIF	CIF de la Administración Pública, órgano o entidad de derecho público
SN, Surname (opcional)	Apellidos (persona física)	Primer y segundo apellidos (de acuerdo con documento de identidad -DNI, pasaporte, ...-) + " - DNI " + NIF del custodio de la clave privada
GN, Given name (opcional)	Nombre (persona física)	Nombre de pila, de acuerdo con documento de identidad (DNI, pasaporte, ...) del custodio de la clave privada
CN, Common Name	Denominación del sistema o aplicación	p.e. "PLATAFORMA DE VALIDACIÓN DEL AYUNTAMIENTO DE xxx"
C, Country	País	C= 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 Client Authentication*
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-calssuers* *Access Location: <URI de acceso al certificado de la CA emisora>*
X509v3 CRL Distribution Points	-	*<URI de la CRL>*

Qualified Certificate Statements	*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-QcPDS[1]:*** 0.4.0.1862.1.5 ***(URI:*** *https://www.firmaprofesional.com/cps/pds_en.pdf****)*** ***Id-etsi-qcs-QcType:*** 0.4.0.1862.1.6.2 ***(qct-eseal, indica que es un certificado para crear sellos electrónics).***

5.2. Nivel ALTO

5.2.1. Extensiones de los certificados

Extensión	Crítica	Valores
X509v3 Certificate Policies	-	*<OID de la política de certificación correspondiente al certificado>* 1.3.6.1.4.1.13177.10.1.21.1: DCCF portable 1.3.6.1.4.1.13177.10.1.21.3: DCCF centralizado *<URI de la CPS>* *User Notice: "Certificado cualificado de sello de Administración, órgano o entidad de derecho público, nivel alto. Dirección del prestador de servicios de confianza: Paseo de la Bonanova, 47. 08017 Barcelona"* *<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>*
Qualified Certificate Statements	*Sí*	*Id-etsi-qcs-QcSSCD:* 0.4.0.1862.1.4 *(indica que la clave privada se custodia en un DCCF)*
X509v3 Subject Alternative Name	-	*rfc822Name:* mail de contacto (Opcional) *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/NIE del custodio> (opcional)* *OID: 2.16.724.1.3.5.6.1 .5 = <CN del DN>* *OID: 2.16.724.1.3.5.6.1 .6 = <Given name> (opcional)* *OID: 2.16.724.1.3.5.6.1 .7 = <Primer apellido del custodio>[2] (opcional)* *OID: 2.16.724.1.3.5.6.1 .8 = <Segundo apellido del custodio>[3](opcional)* *OID: 2.16.724.1.3.5.6.1 .9 = <correo electrónico del custodio> (opcional)*

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

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

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

5.3. Nivel MEDIO

5.3.1. Extensiones de los certificados

Extensión	Crítica	Valores
X509v3 Certificate Policies	-	*<OID de la política de certificación correspondiente al certificado>* 1.3.6.1.4.1.13177.10.1.21.2 *<URI de la CPS>* *User Notice: "Certificado cualificado de sello de Administración, órgano o entidad de derecho público, nivel medio. Dirección del prestador de servicios de confianza: Paseo de la Bonanova, 47. 08017 Barcelona"* *<OID de la política de certificación del MHAP: 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 Subject Alternative Name	-	*rfc822Name:* mail de contacto (Opcional) *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/NIE del custodio> (opcional)* *OID: 2.16.724.1.3.5.6.2.5 = <CN del DN>* *OID: 2.16.724.1.3.5.6.2.6 = <Given name> (opcional)* *OID: 2.16.724.1.3.5.6.2.7 = <Primer apellido del custodio>*[4] *(opcional)* *OID: 2.16.724.1.3.5.6.2.8 = <Segundo apellido del custodio>*[5] *(opcional)* *OID: 2.16.724.1.3.5.6.2.9 = <correo electrónico del custodio> (opcional)*

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

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