

POLÍTICA DE CERTIFICACIÓN

CERTIFICATION POLICY (CP)

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

Versión 1.0

INDICE

1	INTRODUCCIÓN	3
1.1	Descripción general	3
1.2	Nombre del Documento e identificación.....	3
2	ENTIDADES PARTICIPANTES	4
2.1	Autoridades de Certificación (CA).....	4
2.2	Autoridad de Registro (RA).....	4
2.3	Solicitante	4
2.4	Suscriptor	4
2.5	Custodio de Claves.....	4
2.6	Tercero que confía en los certificados	4
3	CARACTERISTICAS DE LOS CERTIFICADOS	5
3.1	Periodo de validez de los certificados	5
3.2	Tipo de soporte.....	5
3.3	Uso particular de los certificados de sello de Administración, órgano o entidad de derecho público	5
3.3.1	Usos apropiados de los certificados	5
3.3.2	Usos no autorizados de los certificados	5
3.4	Tarifas	5
4	PROCEDIMIENTOS OPERATIVOS.....	6
4.1	Proceso de emisión de certificados	6
4.2	Revocación de certificados	8
4.3	Renovación de certificados.....	8
5	PERFIL DE LOS CERTIFICADOS	9
5.1	Campos comunes a los dos niveles.....	9
5.1.1	Certificado	9
5.1.2	Extensiones de los certificados	10
5.2	Nivel ALTO	10
5.2.1	Certificado	10
5.2.2	Extensiones de los certificados	10
5.3	Nivel MEDIO.....	11
5.3.1	Certificado	11
5.3.2	Extensiones de los certificados	11

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, según los requisitos establecidos en la Ley 11/2007, de 23 de junio, de Accesos Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP).

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.

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 Firmaprofesional.

Estos certificados pueden emitirse según dos niveles de aseguramiento, dependiendo del soporte en el que se cree y resida el par de claves:

- MEDIO: soporte *software*
- ALTO: soporte *hardware* criptográfico

La presente política sigue las definiciones de los niveles de aseguramiento 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

En el presente documento se exponen las Condiciones Particulares referentes a este tipo de certificado. Esta Política de Certificación está subordinada al cumplimiento de las Condiciones Generales expuestas en la Declaración de Prácticas de Certificación (CPS) de Firmaprofesional.

1.2 NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

Nombre:	CP Sello de Órgano
Versión:	1.0
Descripción:	Política de Certificación para Certificados de sello de Administración, órgano o entidad de derecho público
Fecha de Emisión:	26/07/2010
OIDs	1.3.6.1.4.1.13177.10.1.21.1 Nivel Alto – <i>Hardware</i> criptográfico 1.3.6.1.4.1.13177.10.1.21.2 Nivel Medio - <i>Software</i>
Localización	http://www.firmaprofesional.com/cps

2 ENTIDADES PARTICIPANTES

2.1 AUTORIDADES DE CERTIFICACIÓN (CA)

Los Certificados Corporativos de Colegiado deben ser emitidos por la CA Subordinada “**AC Firmaprofesional - AAPP**”, que emite certificados digitales a Corporaciones Públicas.

2.2 AUTORIDAD DE REGISTRO (RA)

Firmaprofesional actuará directamente como Autoridades de Registro para la emisión de certificados de sello de Administración, órgano o entidad de derecho público. También podrá actuar como RA para la emisión de certificados de sello de Administración, órgano o entidad de derecho público cualquier entidad que tenga un contrato de vinculación de RA con Firmaprofesional.

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 Firmaprofesional están 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 soporte *software* (nivel MEDIO) o *hardware* (nivel ALTO)¹.

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

Los Certificados de sello de Administración, órgano o entidad de derecho público pueden ser usados como mecanismo de identificación y autenticación en sistemas de firma electrónica para la actuación administrativa automatizada².

3.3.2 Usos no autorizados de los certificados

No se permite la utilización distinta de lo establecido en esta Política y en la Declaración de Practicas de Certificación.

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 Firmaprofesional.

El pago por estos certificados podrá realizarse en efectivo o por transferencia bancaria.

¹ Los niveles vienen definidos en 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

² LAECSP. Art. 18

4 PROCEDIMIENTOS OPERATIVOS

4.1 PROCESO DE EMISIÓN DE CERTIFICADOS

Si la Corporación Pública ya ha firmado el contrato de prestación de servicios de certificación y su representante legal (el Órgano superior unipersonal de representación o el Órgano en quien se delegue o el Responsable de Recursos Humanos) dispone del certificado corporativo de persona física representante, este representante legal estará autorizado a emitir los certificados directamente accediendo a los servicios de Firmaprofesional, tramitando las correspondientes hojas de entrega.

Si la Corporación Pública no tuviera firmado el contrato de prestación de servicios de certificación con Firmaprofesional, deberá ser firmado por el representante legal en el momento de solicitar un certificado.

La Corporación o una RA de Firmaprofesional se encargará de tramitar las solicitudes y proceder a la emisión de los certificados cumpliendo siempre con los términos generales descritos en la CPS.

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

a) Solicitud

Deberá ser realizada por el solicitante, cumpliendo con lo descrito en la CPS y presentando, como mínimo, la documentación siguiente:

- Cuando la tramitación la realiza directamente la Corporación Pública convertida en RA:
 - Una hoja de pedido firmada por el solicitante de la corporación. Indicando para qué órgano de la Administración se desea el certificado.
- Cuando la tramitación la realiza una RA que no sea la misma Corporación Pública:
 - Una hoja de pedido firmada por el solicitante y autorizada por el representante legal de la Corporación Pública, indicando para qué órgano de la Administración se desea el certificado.
 - La acreditación por un medio fehaciente de la existencia de la entidad conforme a Derecho.
 - La resolución de la Subsecretaría del Ministerio o titular del organismo público competente.
- 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) Aceptación de la solicitud

Quando la Corporación Pública es RA

La aceptación es automática ya que la RA es la misma Corporación

Cuando se utiliza a Firmaprofesional o un agente comercial como RA

La RA verificará la identidad del solicitante, su vinculación con la entidad, 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 competente³.

c) Tramitación

Una vez aceptada la solicitud, la Organización Pública o la RA tramitará la solicitud del certificado

d) Generación de claves

Las claves de firma serán generadas en los sistemas del solicitante utilizando sus propias aplicaciones compatibles con los estándares de PKI.

En caso de solicitar nivel ALTO, la generación y custodia de claves se realizará en un dispositivo *hardware* criptográfico.

El solicitante entregará a la RA una petición de certificado en formato PKCS#10.

Generalmente, las aplicaciones de servidores que pueden configurarse con el protocolo SSL, como IIS de Microsoft, incluyen herramientas para generar claves y peticiones de certificados.

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 suscriptor, éste último deberá:

- Identificarse presencialmente ante la RA, según el procedimiento que ésta le comunique.
- Recibir la Hoja de Entrega y Aceptación.

f) Entrega

Finalmente, la RA hará entrega del certificado al suscriptor permitiendo su descarga de forma segura desde Internet.

³ RD091671. Art. 19.1

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 CPS.

Para solicitar la revocación del certificado el suscriptor puede:

1. En horario de oficina:
 - Ponerse en contacto telefónicamente o presencialmente con su RA.
2. Fuera de horario de oficina:
 - Revocar online su certificado en la página web de Firmaprofesional.
 - Llamar al servicio de revocación 24x7: 902.361.639

Para toda información complementaria referente a la revocación de los certificados, referirse al apartado correspondiente de la CPS.

4.3 RENOVACIÓN DE CERTIFICADOS

Existen dos procedimientos:

- a) **Proceso de renovación presencial:** El suscriptor deberá dirigirse a su RA, y proceder a la generación de un certificado nuevo.
- b) **Proceso de renovación online:** Si la RA dispone del servicio y el suscriptor ha contratado la renovación, éste recibirá una notificación de la RA por correo electrónico para iniciar la renovación a través de la página web de Firmaprofesional.

5 PERFIL DE LOS CERTIFICADOS

Los certificados de sello de Administración, órgano o entidad de derecho público de Firmaprofesional 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 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 del DN	Nombre	Descripción
O, Organization	Organización	<i>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. "Ministerio de Igualdad ")</i>
OU, Organization Unit	Unidad en la organización	<i>"SELLO ELECTRONICO"</i>
SN, Serial Number	CIF	<i>CIF de la Administración Pública, órgano o entidad de derecho público (p.e., para el caso del "Instituto de la Juventud", Q2828002B)</i>
Surname	Apellidos (persona física)	<i>Primer y segundo apellidos (de acuerdo con documento de identidad - DNI, pasaporte, ...) + " - DNI " + NIF del custodio de la clave privada</i>
Given name	Nombre	<i>Nombre de pila, de acuerdo con documento de identidad (DNI, pasaporte, ...)</i>
CN, Common Name	Denominación del sistema o aplicación	<i>p.e. "PLATAFORMA DE VALIDACIÓN DEL AYUNTAMIENTO DE xxx"</i>
C, Country	País	<i>Código de país de dos dígitos según ISO 3166-1. Por defecto "ES".</i>

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 Data 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>
X509v3 CRL Distribution Points	-	<URI de la CRL>
X509v3 Certificate Policies	-	<OID de la política de certificación correspondiente al certificado> <URI de la CPS>
Qualified Certificate Statements	Sí	qcCompliance qcEuRetentionPeriod: 15 años

5.2 NIVEL ALTO

5.2.1 Certificado

Campo	Nombre	Descripción
Signature Algorithm	Algoritmo de firma	RsaWithSHA1, con longitud de claves de 2048 o superior

5.2.2 Extensiones de los certificados

Extensión	Crítica	Valores
X509v3 Certificate Policies	-	User Notice: "Certificado reconocido de sello de Administración, órgano o entidad de derecho público de Administración, órgano o entidad de derecho público, nivel alto. Consulte las condiciones de uso en " + URL de la DPC
Qualified Certificate Statements	Sí	qcSSCD
X509v3 Subject Alternative Name	-	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 = <Given name> OID: 2.16.724.1.3.5.2.1.7 = <Primer apellido del custodio> ⁴

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

Extensión	Crítica	Valores
		OID: 2.16.724.1.3.5.2.1.8 = <Segundo apellido del custodio> ⁵ OID: 2.16.724.1.3.5.2.1.9 = <correo electrónico del custodio>

5.3 NIVEL MEDIO

5.3.1 Certificado

Campo	Nombre	Descripción
Signature Algorithm	Algoritmo de firma	RsaWithSHA1, con longitud de claves de 1024 o superior

5.3.2 Extensiones de los certificados

Extensión	Crítica	Valores
X509v3 Certificate Policies	-	User Notice: "Certificado reconocido de sello de Administración, órgano o entidad de derecho público de Administración, órgano o entidad de derecho público, nivel medio. Consulte las condiciones de uso en " + URL de la DPC
X509v3 Subject Alternative Name	-	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 = <Given name> OID: 2.16.724.1.3.5.2.2.7 = <Primer apellido del custodio> ⁶ OID: 2.16.724.1.3.5.2.2.8 = <Segundo apellido del custodio> ⁷ 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, ...)

⁷ de acuerdo con documento de identidad (DNI, pasaporte, ...)