



CERTIFICADOS PERSONALES

Política de Certificado

Versión: 171121

Clasificación: Público

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
150429	Versión inicial	29/04/2015
171121	Cambios en el perfil (adecuación Reglamento eIDAS)	21/11/2017

Índice

1. INTRODUCCIÓN	4
1.1. Descripción General	4
1.2. Identificación del Documento	4
2. ENTIDADES PARTICIPANTES	5
2.1. Prestador de Servicios de Confianza (PSC)	5
2.2. Autoridad de Registro (RA)	5
2.3. Solicitante	5
2.4. Suscriptor	5
2.5. Firmante	5
2.6. Tercero que confía en los certificados	5
3. CARACTERÍSTICAS DE LOS CERTIFICADOS	7
3.1. Periodo de validez de los certificados	7
3.2. Uso particular de los certificados	7
3.2.1. Usos apropiados de los certificados	7
3.2.2. Usos no autorizados de los certificados	7
3.2.3. Tarifas	7
4. PROCEDIMIENTOS OPERATIVOS	9
4.1. Proceso de emisión de certificados	9
4.2. Revocación de certificados	10
4.3. Renovación de certificados	10
5. PERFIL DE LOS CERTIFICADOS	11
5.1. Nombre distinguido (DN)	11
5.2. Extensiones de los certificados	11

1. INTRODUCCIÓN

1.1. Descripción General

Los Certificados Personales son Certificados Reconocidos de Persona Física para firma electrónica según la Ley 59/2003, 19 de diciembre, de Firma Electrónica, emitido a los ciudadanos españoles y otras personas físicas que necesitan relacionarse con las Administraciones públicas y otras instituciones.

Los Certificados Personales son certificados cualificados porque cumplen los requisitos establecidos en el anexo I del Reglamento UE 910/2014.

La solicitud y emisión de estos certificados se puede realizar a través de las Autoridades de Registro de Firmaprofesional habilitadas para tal fin.

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 Certificados Personales
Versión:	171121
Descripción:	Política de Certificación para Certificados Personales
Fecha de Emisión:	21/11/2017
OIDs:	1.3.6.1.4.1.13177.10.1.40.2 (en otros dispositivos)
Localización:	http://www.firmaprofesional.com/cps

2. ENTIDADES PARTICIPANTES

2.1. Prestador de Servicios de Confianza (PSC)

Estos certificados deben ser emitidos por Firmaprofesional como Prestador de Servicios de Confianza que emite certificados reconocidos según la Ley 59/2003 de Firma Electrónica y cualificados según el Reglamento UE 910/2014.

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.

2.3. Solicitante

Solicitante es la persona física mayor de edad que en nombre propio solicita la emisión de un certificado a Firmaprofesional.

2.4. Suscriptor

El Suscriptor es la persona física o jurídica que ha contratado los servicios de confianza de Firmaprofesional, por lo tanto, será el propietario del certificado y en consecuencia, tendrá los derechos de revocación y suspensión sobre el certificado.

2.5. Firmante

El firmante será la persona física identificada en el certificado por su nombre, apellidos y NIF, NIE o número de pasaporte. En la presente política, el Solicitante y el Firmante son la misma persona física.

El firmante es la persona física que crea la firma electrónica.

2.6. Tercero que confía en los certificados

Estos certificados son certificados reconocidos que cumplen los requisitos que establece la Ley de Firma Electrónica.

Los terceros que confíen en estos certificados deben tener presente las limitaciones en su

uso, tanto cuantitativas como cualitativas, que se contienen en la CPS, en la presente CP y en el propio certificado.

3. CARACTERÍSTICAS 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 5 años.

3.2. Uso particular de los certificados

3.2.1. Usos apropiados de los certificados

Los certificados emitidos por Firmaprofesional podrán usarse en los términos establecidos por la normativa vigente aplicable a la firma electrónica, con las condiciones adicionales que se establecen en la CPS, y en esta CP.

Los certificados emitidos bajo esta CP pueden ser utilizados con los siguientes propósitos:

- Garantizar la identidad del firmante.
- Garantizar la integridad del documento firmado.
- Identificar al firmante del documento.

Se permite el uso de estos certificados en las relaciones del firmante con las Administraciones Públicas y en los usos particulares.

3.2.2. 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 CP y en la CPS.

No se autoriza el uso de los certificados emitidos bajo esta CP para cifrar ni recibir documentos cifrados.

3.2.3. Tarifas

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 son los siguientes:

1. Solicitud

Las solicitudes de estos certificados se podrán realizar de dos maneras:

1. dirigiéndose personalmente a alguna de las RA de Firmaprofesional habilitadas para tal fin, o
2. mediante el uso de un certificado electrónico reconocido vigente, siempre que Firmaprofesional pueda comprobar de forma automatizada la fecha de la última personación del Solicitante ante el Prestador de Servicios de Confianza con cuyo certificado se realiza la solicitud.

2. Aceptación de la solicitud

La RA deberá comprobar la veracidad de los datos suministrados por el solicitante que, de ser correctos, pasará a la fase de tramitación.

Lo dispuesto en el párrafo anterior podrá no ser exigible en los siguientes casos:

1. Cuando la identidad u otras circunstancias permanentes de los solicitantes de los certificados constaran ya a la RA en virtud de una relación preexistente, en la que, para la identificación del interesado, se hubieran empleado los medios señalados en esta sección y el período de tiempo transcurrido desde la identificación es menor de cinco años.
2. Cuando para solicitar un certificado se utilice otro vigente para cuya expedición se hubiera identificado al firmante en la forma prescrita en apartado y le conste a la RA que el período de tiempo transcurrido desde la identificación es menor de cinco años.

3. Tramitación

Una vez aceptada la solicitud, se enviará al solicitante la información necesaria para que pueda generar el par de claves en sus sistemas, previa autenticación del mismo.

Firmaprofesional recibirá la solicitud de certificado automáticamente tras la generación de claves, emitirá el certificado y proveerá los medios para que el solicitante lo instale en sus sistemas.

4.2. Revocación de certificados

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

4.3. Renovación de certificados

La renovación de los certificados siempre se realiza con generación de un nuevo par de claves.

Existen los siguientes procedimientos:

1. **Presencial:** el firmante deberá dirigirse personalmente a una RA y proceder a la solicitud de un certificado nuevo.
2. **Online:** el firmante deberá conectarse al servicio online que ofrece Firmaprofesional con su certificado actual aún vigente y firmar electrónicamente la solicitud de renovación o disponer de algún otro mecanismo que permita autenticar su identidad y voluntad de renovar el certificado. La posibilidad de realizar la renovación online estará condicionada por los requisitos que establezca la legislación vigente en materia de firma electrónica.
3. **Automático:** si el firmante acepta esta posibilidad en el momento de emisión del certificado, antes de que caduque el certificado vigente se generará automáticamente un nuevo certificado con las mismas claves. La posibilidad de realizar la renovación automática estará condicionada por establezca la legislación vigente en materia de firma electrónica

5. PERFIL DE LOS CERTIFICADOS

5.1. Nombre distinguido (DN)

Campo del DN	Nombre	Descripción
CN, Common Name	Nombre	<i>Nombre y apellidos del firmante</i>
serialNumber	Número de serie	<i>NIF, NIE o número de pasaporte del firmante¹. Ej: "IDCES-123456789Z"</i>
SN, surName	Apellidos	<i>Apellidos del firmante tal y como aparecen en el documento de identidad utilizado</i>
GN, givenName	Nombre de pila	<i>Nombre de pila del firmante tal y como aparece en el documento de identidad utilizado</i>
C, Country	País	<i>Código de país de dos dígitos según ISO 3166-1. Por defecto "ES".</i>

5.2. Extensiones de los certificados

Extensión	Crítica	Valor
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Digital Signature Content Commitment Key Encipherment
X509v3 Extended Key Usage	-	TLS Web Client Authentication
X509v3 Subject Key Identifier	-	<i><id de la clave pública del certificado, obtenido a partir del hash de la misma></i>

¹ En caso de que el firmante no disponga de NIF o NIE, se indicará el Número de Pasaporte en el formato indicado en el apartado correspondiente de la CPS. Se seguirá la codificación acorde a ETSI EN 319 412-1

X509v3 Authority Key Identifier	-	<id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma>
X509v3 CRL Distribution Points	-	<URI de la CRL>
X509v3 Certificate Policies	-	<p><OID de la política de certificación correspondiente al certificado> 1.3.6.1.4.1.13177.10.1.40.2</p> <p><URI de la CPS></p> <p>User Notice: “Éste es un Certificado Personal de Persona Física cualificado. Dirección del prestador de servicios de confianza: Paseo de la Bonanova, 47. 08017 Barcelona”</p> <p><OID de la política de certificación europea: 0.4.0.194112.1.0> (Corresponde a la política para certificados EU cualificados emitidos a personas físicas “QCP-n”, sin uso de un DCCF)</p>
qcStatements	-	<p>Id-etsi-qcs-QcCompliance: 0.4.0.1862.1.1 (indicando que el certificado cualificado)</p> <p>Id-etsi-qcs-QcRetentionPeriod: 0.4.0.1862.1.3 (con un valor de 15 años)</p> <p>Id-etsi-qcs-QcPDS²: 0.4.0.1862.1.5 (URI: https://www.firmaprofesional.com/cps/pds_en.pdf)</p> <p>Id-etsi-qcs-QcType: 0.4.0.1862.1.6.1 (qct-esign, indica que es un certificado para crear firmas electrónicas).</p>

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

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 Subject Alternative Name	-	(opcional) RFC822:<email del firmante> directoryName: 1.3.6.1.4.1.13177.0.1: Nombre de pila de la persona física tal y como aparece en su documento de identidad. 1.3.6.1.4.1.13177.0.2: Primer apellido de la persona física tal y como aparece en su documento de identidad 1.3.6.1.4.1.13177.0.3: Segundo apellido de la persona física tal y como aparece en su documento de identidad (este campo puede estar vacío)