CERTIFICADOS DE EMPLEADO PÚBLICO

Política de Certificado

Versión: 171121

Clasificación: Público

Firmado digitalmente por:
FIRMAPROFESIONAL, S.A.
Fecha y hora: 21.11.2017 11:25:26

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 **5**

1.1. DESCRIPCIÓN GENERAL 5

1.2. IDENTIFICACIÓN DEL DOCUMENTO 5

2. ENTIDADES PARTICIPANTES **6**

2.1. AUTORIDADES DE CERTIFICACIÓN (CA) 6

2.2. AUTORIDAD DE REGISTRO (RA) 6

2.3. SOLICITANTE 6

2.4. SUSCRIPTOR 6

2.5. FIRMANTE 6

2.6. TERCERO QUE CONFÍA EN LOS CERTIFICADOS 6

3. CARACTERÍSTICAS DE LOS CERTIFICADOS **7**

3.1. PERIODO DE VALIDEZ DE LOS CERTIFICADOS 7

3.2. DISPOSITIVOS DE CREACIÓN DE FIRMA 7

3.3. USO PARTICULAR DE LOS CERTIFICADOS 7

3.3.1. Usos apropiados de los certificados 7

3.3.2. Usos no autorizados de los certificados 8

3.4. TARIFAS 8

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. CAMPOS COMUNES A LOS DOS NIVELES 11

5.1.1. Certificado 11

5.1.2. Extensiones de los certificados 12

5.2. NIVEL ALTO 12
5.2.1. Extensiones de los certificados 12
5.3. NIVEL MEDIO 13
5.3.1. Extensiones de los certificados 13

1. INTRODUCCIÓN

1.1. DESCRIPCIÓN GENERAL

Los Certificados de Empleado Público son certificados reconocidos que permiten identificar telemáticamente a los suscriptores como Administraciones Públicas y a los firmantes como personas al servicio de la administración pública.

Los certificados de Empleado Público son certificados que siguen los requisitos establecidos en el artículo 43 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, para la firma electrónica del personal al servicio de las Administraciones Públicas.

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 10 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 Empleado Público son acordes al Anexo I del Reglamento UE 910/2014 que especifica los requisitos para los certificados cualificados de persona física.

La finalidad del certificado de Empleado Público es poder autenticarse frente a los sistemas y ciudadanos y realizar firmas electrónicas reconocidas en los términos establecidos en la Ley 59/2003, de 19 de diciembre de 2003, de Firma Electrónica.

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 Empleado Público
Versión:	171121
Descripción:	Política de Certificación para Certificados de Empleado Público
Fecha de Emisión:	21/11/2017
OIDs	1.3.6.1.4.1.13177.10.1.22.1 Nivel Alto con DCCF portable 1.3.6.1.4.1.13177.10.1.22.3 Nivel Alto con DCCF centralizado 1.3.6.1.4.1.13177.10.1.22.2 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 del certificado cualquier Corporación Pública para los empleados públicos vinculados a ella. Cuando la Corporación Pública se establezca como RA de Firmaprofesional, podrá gestionar las solicitudes de los Empleados Públicos que dependan de ella,

2.4. SUSCRIPTOR

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

2.5. FIRMANTE

El firmante será el empleado público como persona física, identificada por su nombre, apellidos y NIF.

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

2.6. TERCERO QUE CONFÍA EN LOS CERTIFICADOS

Los Certificados de Empleado Público 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

El periodo de validez será el que se indique en el propio certificado, con un máximo de 4 años.

3.2. DISPOSITIVOS DE CREACIÓN DE FIRMA

En los casos en que Firmaprofesional pueda garantizar que las claves criptográficas del firmante han sido creadas en un Dispositivo Cualificado de Creación de Firma (DCCF) portable, 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 "**1.3.6.1.4.1.13177.10.1.22.1**"*
- *Extensión QcStatement con valor "id-etsi-qcs-QcSSCD" habilitado*

En los casos en que Firmaprofesional 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 "**1.3.6.1.4.1.13177.10.1.22.3**"*
- *Extensión QcStatement con valor "id-etsi-qcs-QcSSCD" habilitado*

En cualquier otro caso, se indicará en el propio certificado mediante los siguientes campos:

- *Extensión "Certificate Policies" con valor OID "**1.3.6.1.4.1.13177.10.1.22.2**"*
- *Extensión QcStatement con valor "id-etsi-qcs-QcSSCD" deshabilitado*

3.3. USO PARTICULAR DE LOS CERTIFICADOS

3.3.1. 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:

- Identificar al firmante como Empleado Público.
- 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 estrictamente particulares.

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.

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 recomienda su uso para el cifrado de documentos.

3.4. 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 son los siguientes:

a) **Solicitud**

Las Administraciones Públicas que actúen como RA de Firmaprofesional podrán tramitar directamente las solicitudes y proceder a la emisión de los certificados para sus Empleados Públicos accediendo a los sistemas de gestión y emisión de certificados de Firmaprofesional. El usuario que desee solicitar un certificado deberá ponerse en contacto con su Organización y realizar la solicitud en la forma que cada Corporación establezca.

b) **Aceptación de la solicitud**

La Organización validará la identidad del solicitante y su condición del empleado público.

c) **Tramitación**

Cada Organismo Público que actúe como 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 por la RA 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 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 valida la veracidad y exactitud de los datos del firmante.

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

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.

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 firmante, 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.

Mediante estos procedimientos, Firmaprofesional garantiza que ningún firmante dispone del certificado antes de que se haya realizado el proceso de personación requerido en el artículo 13 de la Ley 59/2003.

4.2. REVOCACIÓN DE CERTIFICADOS

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

4.3. RENOVACIÓN DE CERTIFICADOS

Existen dos procedimientos:

a) **Proceso de renovación presencial:** El firmante 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 firmante ha solicitado la renovación, éste recibirá una notificación de la RA para iniciar la renovación a través de la página web de Firmaprofesional.

El período de validez de los certificados renovados online estará condicionado por los requisitos que establece la Ley 59/2003 en su artículo 13.4.

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	*Denominación (nombre "oficial") de la Administración, organismo o entidad de derecho público suscriptora del certificado, a la que se encuentra vinculada el empleado.*
OU, Organization Unit	Descripción del tipo de certificado	*"CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO"*[1]
OU, Organization Unit (Opcional)	Unidad en la organización	*Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado*
OU, Organization Unit (Opcional)	*Número de identificación del suscriptor del certificado (supuestamente unívoco).*	*Se corresponde con el NRP o NIP*
Title (opcional)	Puesto o cargo	*Debe incluir el puesto o cargo de la persona física, que le vincula con la Administración, organismo o entidad de derecho público suscriptora del certificado.*
serialNumber[2]	NIF	*NIF o NIE del empleado público. Se utilizará la semántica propuesta por la norma ETSI EN 319 412-1*
SN, Surname	Apellidos (persona física)	*Primer y segundo apellidos (de acuerdo con documento de identidad -DNI, pasaporte, ...-)* + " - DNI " + *NIF del empleado público*
GN, Given name	Nombre	*Nombre de pila del firmante tal y como aparece en el documento de identidad utilizado*
CN, Common Name	Nombre, apellidos y NIF	*Nombre y dos apellidos de acuerdo con documento de identidad (DNI/Pasaporte)* + " - DNI " + *NIF del empleado público*
C, Country	País	*Código de país de dos dígitos según ISO 3166-1.* *Por defecto "ES".*

[1] "Todos los literales se introducen en mayúsculas" excepto el dominio/subdominio y el correo electrónico, según documento "Perfiles de certificados Electrónicos" de abril de 2016 del Ministerio de Hacienda y Administraciones Públicas.

[2] SerialNumber = p. ej: IDCES-00000000G. 3 caracteres para indicar el número de documento (IDC= documento nacional de identidad) + 2 caracteres para identificar el país (ES) + Número de identidad (Printable String)) Size [RFC 5280] 64

5.1.2. Extensiones de los certificados

Extensión	Crítica	Valores
Subject Alternative Name (opcional)	-	*rfc822Name:* mail de contacto
Basic Constraints	*Sí*	*CA:FALSE*
Subject Key Identifier	-	*<id de la clave pública del certificado, obtenido a partir del hash de la misma>*
Authority Key Identifier	-	*<id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma>*
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>*
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*[3]*:* 0.4.0.1862.1.5 *(URI: https://www.firmaprofesional.com/cps/pds_en.pdf)* *Id-etsi-qcs-QcType:* 0.4.0.1862.1.6.1 *(**qct-esign**, indica que es un certificado para crear firmas electrónicas).*

5.2. NIVEL ALTO

5.2.1. Extensiones de los certificados

Extensión	Crítica	Valores
Key Usage	*Sí*	*Content Commitment*
X509v3 Certificate Policies	-	*<OID de la política de certificación correspondiente al certificado>* 1.3.6.1.4.*1.13177.10.1.22.1: DCCF portable* *1.3.6.1.4.1.13177.10.1.22.3: DCCF centralizado* *<URI de la CPS>* *User Notice: "Éste es un Certificado Cualificado de personal, nivel alto. Dirección del prestador de servicios de confianza: Paseo de la Bonanova, 47. 08017 Barcelona"* *<OID de la política de certificación europea: 0.4.0.194112.1.2>* *(Corresponde a la política para certificados EU cualificados emitidos a personas físicas "QCP-n-qscd", con uso de un DCCF)* *<OID de la política de certificación empleado público: 2.16.724.1.3.5.**7.1**>*

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

Qualified Certificate Statements	*Sí*	*Id-etsi-qcs-QcSSCD:* 0.4.0.1862.1.4 *(indica que la clave privada se custodia en un DCCF)*
Subject Alternative Name	-	*directoryName:* *OID: 2.16.724.1.3.5.7.1.1 = "certificado electrónico de empleado público"* *OID: 2.16.724.1.3.5.7.1.2 = <O del DN>* *OID: 2.16.724.1.3.5.7.1.3 = <CIF de la entidad suscriptora>* *OID: 2.16.724.1.3.5.7.1.4 = <serialNumber del DN>* *OID: 2.16.724.1.3.5.7.1.5 = Número de identificación del suscriptor del certificado (supuestamente unívoco). Se corresponde con el NRP o NIP. (tercera entrada <OU del DN>)* *OID: 2.16.724.1.3.5.7.1.6 = <Given name>* *OID: 2.16.724.1.3.5.7.1.7 = <Primer apellido del empleado público>* *OID: 2.16.724.1.3.5.7.1.8 = <Segundo apellido del empleado público>* *OID: 2.16.724.1.3.5.7.1.9 = <correo electrónico del empleado público>* *OID: 2.16.724.1.3.5.7.1.10 = Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado (segunda entrada <OU del DN>)* *OID: 2.16.724.1.3.5.7.1.11 = <Cargo, T del DN>*

5.3. NIVEL MEDIO

5.3.1. Extensiones de los certificados

Extensión	Crítica	Valores
Key Usage	*Sí*	*Digital Signature* *Content Commitment* *Key Encipherment*
Extended Key Usage	-	*Email protection* *TLS Web Client Authentication*
Certificate Policies	-	*<OID de la política de certificación correspondiente al certificado>* 1.3.6.1.4.1.13177.10.1.22.2 *<URI de la CPS>* *User Notice: "Éste es un Certificado Cualificado de personal, nivel medio. Dirección del prestador de servicios de confianza: Paseo de la Bonanova, 47. 08017 Barcelona"* *<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)* *<OID de la política de certificación empleado público: 2.16.724.1.3.5.**7.2**>*

Subject Alternative Name	-	(opcional) otherName-userPrincipalName (UPN): Usuario en el dominio Windows del empleado público *directoryName:* *OID: 2.16.724.1.3.5.7.2.1 = "certificado electrónico de empleado público"* *OID: 2.16.724.1.3.5.7.2.2 = <O del DN>* *OID: 2.16.724.1.3.5.7.2.3 = <CIF de la entidad suscriptora>* *OID: 2.16.724.1.3.5.7.2.4 = <serialNumber del DN>* *OID: 2.16.724.1.3.5.7.2.5 = Número de identificación del suscriptor del certificado (supuestamente unívoco). Se corresponde con el NRP o NIP. (tercera entrada <OU del DN>)* *OID: 2.16.724.1.3.5.7.2.6 = <Given name>* *OID: 2.16.724.1.3.5.7.2.7 = <Primer apellido del empleado público>* *OID: 2.16.724.1.3.5.7.2.8 = <Segundo apellido del empleado público>* *OID: 2.16.724.1.3.5.7.2.9 = <correo electrónico del empleado público>* *OID: 2.16.724.1.3.5.7.2.10 = Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado (segunda entrada <OU del DN>)* *OID: 2.16.724.1.3.5.7.2.11 = <Cargo, T del DN>*