

POLÍTICA DE CERTIFICACIÓN
CERTIFICATION POLICY (CP)

CERTIFICADOS CORPORATIVOS
DE FACTURA ELECTRÓNICA

Versión 5.0

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 | Firmante..... | 4 |
| 2.6 | Custodio de Claves | 5 |
| 2.7 | Tercero que confía en los certificados | 5 |
| 3 | CARACTERISTICAS DE LOS CERTIFICADOS | 6 |
| 3.1 | Periodo de validez de los certificados | 6 |
| 3.2 | Tipos de soporte | 6 |
| 3.2.1 | Dispositivo Seguro de Creación de Firma (DSCF)..... | 6 |
| 3.2.2 | Soporte en Software | 6 |
| 3.3 | Uso particular de los certificados..... | 7 |
| 3.3.1 | Limitación en la cuantía de las transacciones | 7 |
| 3.3.2 | Usos apropiados de los certificados..... | 7 |
| 3.3.3 | Usos no autorizados de los certificados | 7 |
| 3.4 | Tarifas | 7 |
| 4 | PROCEDIMIENTOS OPERATIVOS..... | 8 |
| 4.1 | Proceso de emisión de certificados | 8 |
| 4.2 | Revocación de certificados..... | 9 |
| 4.3 | Renovación de certificados | 9 |
| 5 | PERFIL DE LOS CERTIFICADOS | 10 |
| 5.1 | Nombre distinguido (DN)..... | 10 |
| 5.2 | Extensiones de los certificados | 11 |

1 INTRODUCCIÓN

1.1 DESCRIPCIÓN GENERAL

Los **Certificados Corporativos de Factura Electrónica** son certificados reconocidos de persona física según la Ley 59/2003 de Firma Electrónica que identifican al suscriptor como Corporación y al firmante como persona con poderes de representación de una organización para firmar Facturas Electrónicas en nombre de dicha entidad.

Los Certificados Corporativos de Factura Electrónica de Firmaprofesional son básicamente idénticos a los Certificados Corporativos de Persona Física, salvo por el hecho de que el firmante del certificado está explícitamente autorizado para firmar facturas en nombre de la entidad.

Estos certificados pueden ser emitidos en dos tipos de soporte: hardware y software.

La solicitud y emisión de los Certificados Corporativos de Persona Física se puede realizar a través de las propias organizaciones a las que se vincula cada certificado, actuando como Autoridades de Registro de Firmaprofesional. No obstante también se pueden utilizar otras entidades no vinculadas con el firmante que sean Autoridades de Registro de Firmaprofesional.

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

1.2 NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

| | |
|--------------------------|---|
| Nombre: | CP Factura Electrónica |
| Versión: | 4.0 |
| Descripción: | Política de Certificación para Certificados Corporativos de Factura Electrónica |
| Fecha de Emisión: | 26/07/2010 |
| OIDs | 1.3.6.1.4.1.13177.10.1.6.1 (en DSCF) 1.3.6.1.4.1.13177.10.1.6.2 (en software) |
| Localización | http://www.firmaprofesional.com/cps |

Anteriormente, estas Políticas de Certificación recibían los nombres de:

- Tipo II.A - CERTIFICADOS CORPORATIVOS RECONOCIDOS PARA LA EMISION DE FACTURA ELECTRONICA CON DSCF (1.3.6.1.4.1.13177.10.1.6.1)
- Tipo II.B - CERTIFICADOS CORPORATIVOS RECONOCIDOS PARA LA EMISION DE FACTURA ELECTRONICA (1.3.6.1.4.1.13177.10.1.6.2)
- CERTIFICADOS DE FACTURA ELECTRONICA CON DSCF (1.3.6.1.4.1.13177.10.1.6.1)
- CERTIFICADOS DE FACTURA ELECTRONICA SOFTWARE (1.3.6.1.4.1.13177.10.1.6.2)

2 ENTIDADES PARTICIPANTES

2.1 AUTORIDADES DE CERTIFICACIÓN (CA)

Los Certificados Corporativos de Persona Física deben ser emitidos por la CA Subordinada “**AC Firmaprofesional - CA1**”, que emite certificados digitales a Corporaciones Privadas.

2.2 AUTORIDAD DE REGISTRO (RA)

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

Adicionalmente, la propia Corporación (empresas, entidades privadas o públicas) podrá actuar como Autoridad de Registro de Firmaprofesional para la gestión de las solicitudes y emisiones de los certificados a aquellas personas físicas con las que tenga una vinculación directa, como empleados, colaboradores, clientes. La propia Corporación será el suscriptor de todos estos certificados emitidos.

Cada Corporación que actúe como RA establecerá:

- Qué criterios 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.
- Los dispositivos de creación de firma a utilizar, que previamente Firmaprofesional haya homologado.

2.3 SOLICITANTE

El solicitante es el representante legal o voluntario (apoderado general) de la Corporación (empresa, entidad privada o pública) que adquiere los certificados a nombre de los firmantes.

2.4 SUSCRIPTOR

La Corporación es el Suscriptor de los certificados y por lo tanto el propietario de los certificados emitidos.

2.5 FIRMANTE

El firmante será la persona física identificada en el certificado por su nombre, apellidos y NIF, que tenga una vinculación (de empleado, colaborador, etc) con el suscriptor.

2.6 CUSTODIO DE CLAVES

El custodio de las claves es el propio firmante. El custodio de las claves también puede ser la propia Corporación siempre que garantice la custodia en un Dispositivo Seguro de Creación de Firma (Hardware Criptográfico Seguro certificado FIPS 140-2, CC EAL 4+ o similar) y que se mantenga el uso de las claves bajo el control exclusivo del firmante.

2.7 TERCERO QUE CONFÍA EN LOS CERTIFICADOS

Dado que el único objetivo de este tipo de certificados es la firma de facturas electrónicas, estos certificados únicamente están acreditados en la [Agencia Española de Administración Tributaria \(AEAT\)](#).

Los terceros que confían en estos certificados únicamente deben hacerlo en referencia a la validación y verificación de facturas electrónicas.

3 CARACTERÍSTICAS DE LOS CERTIFICADOS

3.1 PERIODO DE VALIDEZ DE LOS CERTIFICADOS

Los Certificados de Factura Electrónica tendrán un periodo de validez de 1, 2, 3 o 4 años.

3.2 TIPOS DE SOPORTE

Los Certificados de Factura Electrónica pueden generarse en dos tipos de soporte: Hardware o Software. Cada RA decidirá el tipo de soporte en el que emite sus certificados.

3.2.1 *Dispositivo Seguro de Creación de Firma (DSCF)*

Las claves privadas de los certificados emitidos en soporte hardware se generan y almacenan en un “Dispositivo Seguro de Creación de Firma (DSCF)”, como una Tarjeta Inteligente o un Token criptográfico. Los DSCF proporcionados por Firmaprofesional están homologados según la norma europea CEN CWA 14169.

Según la Ley 59/2003 “*Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma*”. Por lo tanto, la utilización de Certificados de Colegiado con DSCF permite realizar firmas electrónicas reconocidas cumpliendo con todos los requisitos que marca la ley.

Las claves de certificados generadas en DSCF no pueden ser copiadas de ninguna manera, por lo que si se pierde o se estropea el dispositivo, será necesario realizar un nuevo proceso de emisión de certificado.

Para activar el DSCF será necesario introducir el código de activación (PIN). Si se introduce el PIN tres veces seguidas de manera incorrecta, el dispositivo quedará bloqueado, y por lo tanto inservible. Para desbloquear la tarjeta será necesario introducir el código de desbloqueo (PUK).

El PIN y el PUK son secretos y personales para usuario y son entregados al suscriptor por la RA en el proceso de emisión del certificado. Tanto el PIN como el PUK pueden ser modificados posteriormente por el usuario utilizando las aplicaciones correspondientes.


Ni Firmaprofesional ni la RA conocen el PIN ni el PUK de las tarjetas, por lo que los dispositivos bloqueados no podrán ser utilizados, siendo necesario realizar un nuevo proceso de emisión de certificado.

Los Certificados de Factura Electrónica en DSCF están identificados mediante el OID (1.3.6.1.4.1.13177.10.1.6.1) en la extensión “X509v3 Certificate Policies”

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.

Según la Ley 59/2003 “*Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma*”. Por lo tanto, la utilización de Certificados de Colegiado en software no cumple con todos los

| | | |
|---|---|------------|
|  firmaprofesional | Política de Certificación Certificados Corporativos de Factura Electrónica | |
| | Versión | 5.0 |
| | Fecha | 27/07/2010 |

requisitos que marca la ley que marca la ley para la firma reconocida. Sin embargo, actualmente la mayor parte de las organizaciones públicas o privadas españolas reconocen la firma electrónica realizada con certificados en software como firma reconocida.

Los Certificados de Factura Electrónica en software pueden ser copiados a otros soportes, por lo tanto es posible realizar copias de seguridad de los mismos.

Los Certificados de Factura Electrónica en Software están identificados mediante el OID (1.3.6.1.4.1.13177.10.1.6.2) en la extensión "X509v3 Certificate Policies"

3.3 USO PARTICULAR DE LOS CERTIFICADOS

3.3.1 Limitación en la cuantía de las transacciones

No existe límite en la cuantía de las facturas firmadas con este tipo de certificado. Salvo que se indique de manera explícita en el propio certificado en la extensión "qcStatements" (OID 1.3.6.1.5.5.7.1.3.).

3.3.2 Usos apropiados de los certificados

Los certificados de Factura Electrónica están expresamente restringidos a la firma de facturas electrónicas.

Según lo recomendado en el CWA 15579 "*e-Invoices and digital signatures*", la firma de la factura electrónica por el suscriptor deberá utilizarse para garantizar la autenticidad y la integridad de ésta y no como un acto de compromiso con su contenido.

3.3.3 Usos no autorizados de los certificados

No está autorizado cualquier otro uso diferente a la firma de facturas electrónicas.

3.4 TARIFAS

El precio de estos certificados dependerá de la duración de los mismos. El pago por estos certificados podrá realizarse en efectivo o por transferencia bancaria.

Para más detalles sobre el precio y condiciones de pago de este tipo de certificados será necesario consultar telefónicamente o por mail con Firmaprofesional o con la RA que actúe en nombre de Firmaprofesional.

4 PROCEDIMIENTOS OPERATIVOS

4.1 PROCESO DE EMISION DE CERTIFICADOS

La RA se encargará de tramitar las solicitudes y proceder a la emisión de los certificados cumpliendo con los procedimientos descritos en la CPS.

Los pasos a seguir para la obtención del certificado son los siguientes:

a) Solicitud

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

- El solicitante deberá estar autorizado a solicitar el certificado.
- El solicitante deberá entregar la documentación requerida por la RA para tramitar la solicitud.

b) Aceptación de la solicitud

La RA verificará la identidad del solicitante y la vinculación del suscriptor con la entidad así como los datos a incluir en el certificado.

c) Tramitación

Una vez aceptada, la RA tramitará la solicitud del certificado, en función del soporte que se utilice.

d) Generación de claves

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

• En software

El suscriptor recibirá por correo electrónico la confirmación de la solicitud, y deberá proceder a la generación de claves en su ordenador siguiendo las instrucciones de la RA.

Una vez el par de claves generadas, el suscriptor obtendrá un código que deberá presentar ante la RA para finalizar el proceso de emisión.

• En hardware

Se procederá a la activación del dispositivo y seguidamente se entregará a la RA para que genere el par de claves.

e) Emisión del certificado

Una vez las claves generadas, la RA procederá a la emisión del certificado, firmando la petición de generación de certificado y enviándola a la CA.

Una vez el certificado generado, y antes que la RA pueda entregarlo al suscriptor, éste último deberá:

- Identificarse presencialmente ante la RA, según el procedimiento que ésta le comunique.
- Leer, aceptar y firmar el instrumento jurídico vinculante con la RA.

f) Entrega

Finalmente, la RA hará entrega del certificado al suscriptor.

- **En software:** El suscriptor podrá descargarse de forma segura el certificado en su ordenador.
- **En hardware:** La RA entregará el dispositivo al suscriptor.

4.2 REVOCACION 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:

a) En horario de oficina:

- Ponerse en contacto telefónicamente o presencialmente con su RA.

b) 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 RENOVACION 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

5.1 NOMBRE DISTINGUIDO (DN)

El DN de los certificados de Factura Electrónica 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 |
|-------------------------------------|---------------------------|--|
| CN, Common Name | Nombre | <i>Nombre y Apellidos del firmante</i> |
| E, E-mail | E-mail | <i>Correo electrónico del firmante</i> |
| O, Organization | Organización | <i>Nombre de la Entidad que emite las facturas</i> |
| 1.3.6.1.4.1.4710.1.3.2 ¹ | CIF de la Organización | <i>CIF correspondiente a la Entidad que emite las facturas.</i> |
| OU, Organization Unit | Unidad en la organización | Contendrá uno de los siguientes valores: <ul style="list-style-type: none"> ▪ <i>El Departamento al que pertenezca el suscriptor</i> ▪ <i>Tipo de vinculación con la organización.</i> |
| T, Title | Título | <i>Cargo, título o rol en la organización del firmante</i> |
| ST, State | Ubicación Geográfica | <i>Ámbito geográfico de vinculación del firmante</i> |
| C, Country | País | <i>Código de país de dos dígitos según ISO 3166-1. Por defecto "ES".</i> |
| serialNumber | Número de Serie | <i>NIF o NIE del firmante</i> |
| SN, surName | Apellidos | <i>Apellidos del firmante</i> |
| GN, givenName | Nombre de Pila | <i>Nombre del firmante</i> |

En caso de que el firmante no disponga de NIF o NIE, contendrá un código de documento con el siguiente formato <P>-<T>-<XXXXXX>, donde:

- <P> Código del país (según ISO 3166-1)
- <T> es el tipo de documento (P para pasaporte)
- <XXXXXXXX> es el código del documento (el identificador utilizado en el país en el que está dada de alta la entidad a la que está vinculada el sujeto)

¹ OID propiedad de la empresa Safelayer Secure Communications SA, dedicado a contener un Número de Identificación Fiscal (NIF) o un Código de Identificación Fiscal (CIF).

5.2 EXTENSIONES DE LOS CERTIFICADOS

| Extensión | Crítica | Valores |
|-------------------------------------|---------|---|
| X509v3 Subject Alternative Name | - | <email del firmante> |
| X509v3 Issuer Alternative Name | - | URI:http://www.firmaprofesional.com |
| X509v3 Basic Constraints | Sí | CA:FALSE |
| X509v3 Key Usage | Sí | Digital Signature Non Repudiation Key Encipherment, Data Encipherment, Key Agreement |
| X509v3 Extended Key Usage | - | TLS Web Client Authentication E-mail Protection |
| 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 | - | <URI dónde se encuentra el certificado de la CA> |
| X509v3 CRL Distribution Points | - | <URI de la CRL> |
| X509v3 Certificate Policies | - | <OID de la política de certificación correspondiente al certificado> <URI de la CPS> User Notice : Este es un certificado personal reconocido para la emisión de factura electrónica. |
| QcStatements | - | Id-etsi-qcs-QcCompliance (indica certificado reconocido) Id-etsi-qcs-QcSSCD (cuando la clave privada se custodie en un DSCF) id-etsi-qcs-QcLimitValue = 60.000 |