


| | | |
|--|---|------------|
|  firma profesional | Política de Certificación - Certificados de Firma de Código | |
| | Versión | 4.0 |
| | Fecha | 01/07/2008 |


POLÍTICA DE CERTIFICACIÓN
CERTIFICATION POLICY (CP)

CERTIFICADOS DE FIRMA DE CODIGO

Versión 4.0

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 Firma de Código..... | 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 emision de certificados..... | 6 |
| 4.2 | Revocacion de certificados | 7 |
| 4.3 | Renovacion de certificados | 7 |
| 5 | PERFIL DE LOS CERTIFICADOS | 8 |
| 5.1 | Nombre distinguido (DN)..... | 8 |
| 5.2 | Extensiones de los certificados | 8 |

| | | |
|---|---|------------|
|  | Política de Certificación - Certificados de Firma de Código | |
| | Versión | 4.0 |
| | Fecha | 01/07/2008 |

1 INTRODUCCIÓN

1.1 DESCRIPCIÓN GENERAL

Los Certificados de Firma de Código son certificados emitidos a personas físicas o jurídicas para la firma de código ejecutable como por ejemplo applets de JAVA.

El Certificado de Firma de Código Corporativo identifica a una organización como autora y responsable de un determinado código ejecutable. El Certificado de Firma de Código Personal identifica a un programador concreto dentro de una organización como autor de un determinado código ejecutable.

El Certificado de Firma de Código Corporativo se suele utilizar en entornos abiertos para identificar a la organización responsable del código, mientras que el Certificado de Firma de Código Personal se suele utilizar en entornos cerrados para identificar al programador responsable del código.

Los Certificados de Firma de Código emitidos por Firmaprofesional no son certificados digitales reconocidos según la Ley 59/2003 de 19 de diciembre de firma electrónica.


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 Firma de Código |
| Versión: | 4.0 |
| Descripción: | Política de Certificación para Certificados de Firma de Código |
| Fecha de Emisión: | 01/07/2008 |
| OIDs | 1.3.6.1.4.1.13177.10.1.7.1 (Personal) 1.3.6.1.4.1.13177.10.1.8.1 (Corporativo) |
| Localización | http://www.firmaprofesional.com/cps |

Anteriormente, estas Políticas de Certificación recibían los nombres de:

- Tipo II.E - CERTIFICADO PERSONAL DE FIRMA DE CÓDIGO (1.3.6.1.4.1.13177.10.1.7.1)
- Tipo II.E - CERTIFICADO CORPORATIVO DE FIRMA DE CÓDIGO (1.3.6.1.4.1.13177.10.1.8.1)

| | | |
|---|---|------------|
|  firmaprofesional | Política de Certificación - Certificados de Firma de Código | |
| | Versión | 4.0 |
| | Fecha | 01/07/2008 |

2 ENTIDADES PARTICIPANTES

2.1 AUTORIDADES DE CERTIFICACIÓN (CA)

Los Certificados de Firma de Código deben ser emitidos por la CA Subordinada de Firmaprofesional

2.2 AUTORIDAD DE REGISTRO (RA)

Firmaprofesional actuará directamente como Autoridades de Registro para la emisión de certificados de Firma de Código. También podrá actuar como RA para la emisión de certificados de Firma de Código cualquier entidad que tenga un contrato de vinculación de RA con Firmaprofesional.

2.3 SOLICITANTE

Podrá realizar la solicitud de un certificado de Firma de Código cualquier persona autorizada por su propia organización para ello.

2.4 SUSCRIPTOR

El suscriptor de un certificado de Firma de Código Corporativo será una organización, mientras que el suscriptor de un certificado de Firma de Código Personal será la persona a la que se ha generado el certificado.

2.5 CUSTODIO DE CLAVES


En los certificados de Firma de Código Personal, el custodio de claves será el propio suscriptor.

En los certificados de Firma de Código Corporativo, el custodio de claves será el solicitante del certificado, debidamente autorizado por su Organización para ello.

2.6 TERCERO QUE CONFÍA EN LOS CERTIFICADOS

Los certificados de Firma de Código de Firmaprofesional están reconocidos por Microsoft <http://support.microsoft.com/kb/931125> en todas sus aplicaciones, incluyendo Internet Explorer, y por la Fundación Mozilla <http://hecker.org/mozilla/ca-certificate-list>, incluyendo el navegador Firefox.

Los certificados de servidor seguro pueden ser utilizados libremente ante cualquier tercero que confíe en los certificados.

| | | |
|---|---|------------|
|  | Política de Certificación - Certificados de Firma de Código | |
| | Versión | 4.0 |
| | Fecha | 01/07/2008 |

3 CARACTERISTICAS DE LOS CERTIFICADOS

3.1 PERIODO DE VALIDEZ DE LOS CERTIFICADOS

Los Certificados de Firma de Código tendrán un periodo de validez de 1, 2 o 3 años.

3.2 TIPO DE SOPORTE

Los certificados de firma de código tanto personales como corporativos se emiten en soporte software.

3.3 USO PARTICULAR DE LOS CERTIFICADOS DE FIRMA DE CÓDIGO

3.3.1 *Usos apropiados de los certificados*

Los certificados de Firma de Código únicamente pueden ser utilizados para firmar código ejecutable, como por ejemplo *applets* Java.

El código firmado con un certificado de firma de código garantiza

- La integridad del código firmado.
- La autoría del código firmado


3.3.2 *Usos no autorizados de los certificados*

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

3.4 TARIFAS

El precio de los certificados de Firma de Código 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.

| | | |
|---|---|------------|
|  | Política de Certificación - Certificados de Firma de Código | |
| | Versión | 4.0 |
| | Fecha | 01/07/2008 |

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.

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.

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

Generalmente, las herramientas de desarrollo que permiten el uso de firma de código incluyen herramientas para generar claves y peticiones de certificados. Por ejemplo, la JDK de Java incluye las herramientas "keytool" y "jarsigner".

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.

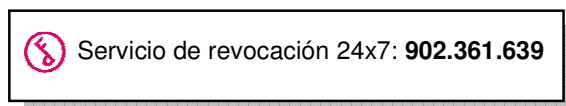
| | | |
|---|---|------------|
|  | Política de Certificación - Certificados de Firma de Código | |
| | Versión | 4.0 |
| | Fecha | 01/07/2008 |

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:




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.

| | | |
|---|---|------------|
|  | Política de Certificación - Certificados de Firma de Código | |
| | Versión | 4.0 |
| | Fecha | 01/07/2008 |

5 PERFIL DE LOS CERTIFICADOS

5.1 NOMBRE DISTINGUIDO (DN)

El DN de los certificados de Firma de Código 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 de la Organización (Certificados Corporativos) o Nombre del Programador (Certificados Personales)</i> |
| O, Organization | Organización | <i>Nombre de la Organización (Certificados Personales)</i> |

5.2 EXTENSIONES DE LOS CERTIFICADOS

| Extensión | Crítica | Valores |
|-------------------------------------|---------|--|
| X509v3 Issuer Alternative Name | - | <i>URI: http://www.firmaprofesional.com</i> |
| X509v3 Basic Constraints | Sí | <i>CA:FALSE</i> |
| X509v3 Key Usage | Sí | <i>Digital Signature Non Repudiation</i> |
| X509v3 Extended Key Usage | - | <i>CodeSigning (1.3.6.1.5.5.7.3.3)</i> |
| X509v3 Subject Key Identifier | - | <i><id de la clave pública del certificado, obtenido a partir del hash de la misma></i> |
| X509v3 Authority Key Identifier | - | <i><id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma></i> |
| X509v3 Authority Information Access | - | <i><URI dónde se encuentra el certificado de la CA></i> |
| X509v3 CRL Distribution Points | - | <i><URI de la CRL></i> |
| X509v3 Certificate Policies | - | <i><OID de la política de certificación correspondiente al certificado> <URI de la CPS> User Notice : Este es un certificado de firma de código.</i> |