

POLÍTICA DE CERTIFICACIÓN ***CERTIFICATION POLICY (CP)***

CERTIFICADOS CORPORATIVOS **DE FIRMA MOVIL**

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	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
3.3	Uso particular de los certificados de Firma Móvil.....	7
3.3.1	Usos apropiados de los certificados.....	7
3.3.2	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	Revocacion de certificados.....	9
4.3	Renovacion 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 Firma Móvil** son certificados digitales de persona física emitidos para ser utilizados desde dispositivos móviles.

Los Certificados de Firma Móvil emitidos por Firmaprofesional son certificados digitales reconocidos según la Ley 59/2003 de 19 de diciembre de firma electrónica, y pueden ser utilizados para realizar firmas electrónicas reconocidas.

La gestión y el uso de estos certificados se basa en el estándar propuesto por ETSI bajo el nombre de M-COMM MSS (*Mobile Commerce - Mobile Signature Service*), formado por los informes técnicos TR 102 203 y TR 102 206, y por las especificaciones técnicas TS 102 204 y TS 102 207.

Siguiendo las recomendaciones que aparecen en el estándar propuesto, las claves serán emitidas en un dispositivo seguro de creación de firma (DSCF), y serán accesibles únicamente desde el propio terminal móvil.

La solicitud y emisión de los Certificados de Firma Móvil se realiza a través del operador de telecomunicaciones al que pertenezca el suscriptor, actuando como Autoridad 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 las Condiciones Generales expuestas en la Declaración de Prácticas de Certificación (CPS) de Firmaprofesional.

1.2 NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

Nombre:	CP Corporativo Firma Móvil
Versión:	5.0
Descripción:	Política de Certificación para Certificados Corporativos de Firma Móvil
Fecha de Emisión:	26/07/2010
OIDs	1.3.6.1.4.1.13177.10.1.9.1
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 - CA1**”, que emite certificados digitales a Corporaciones Privadas o por una CA Subordinada específica creada a nombre del operador de telecomunicaciones que actúe como RA.

2.2 AUTORIDAD DE REGISTRO (RA)

Tal y como viene estipulado en la CPS, la gestión de las solicitudes y emisiones de los certificados será realizada por las entidades que actúen como Autoridades de Registro de Firmaprofesional.

En el caso de los certificados de firma móvil, la función de RA podrá estar desempeñada por la propia compañía de telecomunicaciones. Cada operadora será responsable de la emisión de los certificados a sus propios usuarios, y en ningún caso podrá emitir certificados a usuarios de otra compañía.

Será responsabilidad de cada RA establecer:

- Los grupos de usuarios que podrán solicitar este tipo de certificado.
- Las posibles tarifas a pagar por el suscriptor.
- El tipo y modelo de dispositivo seguro de creación de firma.
- Los mecanismos y procedimientos necesarios para realizar la identificación y autenticación del suscriptor, cumpliendo con lo estipulado en la CPS.

2.3 SOLICITANTE

Podrán solicitar este tipo de certificados aquellos usuarios que sean clientes del operador de telecomunicaciones que actúe como RA de Firmaprofesional y que entren dentro del grupo de usuarios autorizados para ello.

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 TERCERO QUE CONFÍA EN LOS CERTIFICADOS

Las entidades que confíen en estos certificados y deseen hacer uso de ellos para autenticar a los usuarios y validar firmas electrónicas, deberán integrarse en la red del Operador de telecomunicaciones, siguiendo el estándar propuesto por ETSI bajo el nombre de M-COMM MSS (*Mobile Commerce - Mobile Signature Service*), formado por los informes técnicos TR 102 203 y TR 102 206, y por las especificaciones técnicas TS 102 204 y TS 102 207.

Cada operador establecerá su propio modelo de negocio para la comercialización de este tipo de servicios.

3 CARACTERÍSTICAS DE LOS CERTIFICADOS

3.1 PERIODO DE VALIDEZ DE LOS CERTIFICADOS

El plazo de validez de los certificados de Firma móvil será determinado por el Operador de Telecomunicaciones según su criterio, con un máximo de 3 años.

3.2 TIPOS DE SOPORTE

Las claves de los Certificados de Firma Móvil deberán generarse en un dispositivo seguro de creación de firma integrado en un teléfono móvil. Cada RA decidirá el modelo de soporte en el que emite sus certificados.

3.2.1 Dispositivo Seguro de Creación de Firma (DSCF)

Las claves privadas de estos certificados se generan y almacenan en la tarjeta SIM del teléfono móvil, que actuará como “Dispositivo Seguro de Creación de Firma (DSCF)”.

Las tarjetas SIM utilizadas por el operador de telecomunicaciones para alojar las claves de los certificados deberán estar homologadas 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 operador de telecomunicaciones establecerá los procedimientos necesarios para la gestión y comunicaciones del PIN y el PUK a los usuarios.

En todo, Firmaprofesional no conocerá ni tendrá acceso a los PIN y PUK de ningún usuario.

Los Certificados de Firma Móvil en DSCF están identificados mediante el OID (1.3.6.1.4.1.13177.10.1.9.1) en la extensión “X509v3 Certificate Policies”

3.3 USO PARTICULAR DE LOS CERTIFICADOS DE FIRMA MÓVIL

3.3.1 Usos apropiados de los certificados

Los certificados de Firma Móvil podrán utilizarse únicamente en entornos compatibles con los estándares del ETSI relativos al M-COMM MSS (*Mobile Commerce - Mobile Signature Service*), formado por los informes técnicos TR 102 203 y TR 102 206, y por las especificaciones técnicas TS 102 204 y TS 102 207.

Los servicios incluidos en el modelo de *Mobile Signature Service* son:

- Autenticación de los usuarios
- Firma Electrónica

3.3.2 Usos no autorizados de los certificados

No se autoriza el uso de estos certificados para usos diferentes a los descritos por los estándares del ETSI relativos al M-COMM MSS (*Mobile Commerce - Mobile Signature Service*),

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 Política y en la Declaración de Prácticas de Certificación.

3.4 TARIFAS

El Operador de Telecomunicaciones que actúe como RA de Firmaprofesional podrá establecer el modelo de negocio que considere oportuno para la emisión, renovación y uso de este tipo de certificados.

La RA será la encargada de comunicar el modelo de negocio y las tarifas aplicables tanto a los usuarios como a los terceros que confíen los certificados.

4 PROCEDIMIENTOS OPERATIVOS

4.1 PROCESO DE EMISIÓN 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:

- **Solicitud**

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

- El solicitante deberá estar autorizado a realizar la solicitud del certificado.
- El solicitante deberá entregar la documentación requerida a la RA para tramitar la solicitud.

- **Aceptación de la solicitud**

La RA verificará la identidad del solicitante y la vigencia del contrato de telefonía, así como los datos a incluir en el certificado.

- **Tramitación**

Una vez aceptada, la RA tramitará la solicitud del certificado, registrando al suscriptor con los datos proporcionados.

Antes que la RA autorice la generación de claves y del certificado, el suscriptor deberá leer, aceptar y firmar el instrumento jurídico vinculante con la RA.

- **Generación de claves**

El usuario recibirá una notificación en su terminal móvil para proceder a la activación del dispositivo y generar el par de claves criptográficas.

- **Emisión del certificado**

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

- **Entrega**

El certificado generado podrá ser enviado al operador de telecomunicaciones, donde será almacenado. En todo caso, Firmaprofesional guardará una copia del certificado.

El usuario será notificado entonces que el certificado ha sido emitido satisfactoriamente.

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:

- Ponerse en contacto telefónicamente o presencialmente con la RA.
- Revocar online su certificado en la página web de Firmaprofesional.

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:

- **Proceso de renovación presencial:** El suscriptor deberá dirigirse a su RA, y proceder a la generación de un certificado nuevo.
- **Proceso de renovación online:** Si el operador de telecomunicaciones dispone del servicio y el suscriptor ha contratado la renovación, éste recibirá una notificación en su dispositivo móvil para firmar la renovación.

En todo caso, la renovación online del certificado deberá realizarse antes de la expiración del mismo.

5 PERFIL DE LOS CERTIFICADOS

5.1 NOMBRE DISTINGUIDO (DN)

Campo del DN	Nombre	Descripción
CN, Common Name	Nombre	Nombre y Apellidos del suscriptor.
E, E-mail	E-mail	Correo electrónico del suscriptor
O, Organization	Organización	Nombre de la Entidad con la cual el suscriptor mantiene la vinculación Adicionalmente se puede incluir el código y el número de la RA que gestionó la emisión del certificado, separados por el carácter "/".
C, Country	País	Código de país de dos dígitos según ISO 3166-1. Por defecto "ES".
serialNumber	Número de Serie	NIF o NIE del suscriptor (1)
SN, surName	Apellidos	Apellidos del Suscriptor
GN, givenName	Nombre de Pila	Nombre del Suscriptor
TelephoneNumber OID.2.5.4.20	ICCID	Código ICCID de la tarjeta del suscriptor (2)

(1) En caso de que el suscriptor 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)
- <XXXXXXX> 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)

(2) El código ICCID de 19 o 20 dígitos basado en el estándar internacional ISO/IEC 7812. El número está compuesto de 2 subpartes:

- Número de identificador del emisor (max. 7 dígitos):
 - MII (Major Industry Identifier), 2 dígitos. Su valor es 89 (telecomunicaciones).
 - Código de país, según la recomendación de la ITU E.164, 2 dígitos. Su valor es 34 (España).
 - Identificador del emisor, 2 dígitos (podrían ser 3) siendo los valores más comunes los siguientes:
 - Telefónica: 07
 - Vodafone: 56
 - Orange: 01
- Identificador de cuenta (12 + dígito de control).

El DN de los certificados de Firma Móvil contendrá como mínimo los elementos que se citan con el formato anterior. Todos los valores de los componentes serán autenticados por la RA.

5.2 EXTENSIONES DE LOS CERTIFICADOS

Extensión	Crítica	Valores
X509v3 Subject Alternative Name	-	<email del suscriptor>
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 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
QcStatements	-	Id-etsi-qcs-QcCompliance (indica certificado reconocido) Id-etsi-qcs-QcSSCD (indica que la clave privada se guarda en un DSCF)