 firma profesional	Política de Certificación - Certificados de Servidor Seguro (SSL)	
	Versión	4.0
	Fecha	01/07/2008


POLÍTICA DE CERTIFICACIÓN
CERTIFICATION POLICY (CP)

CERTIFICADOS DE SERVIDOR SEGURO (SSL)

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	Certificados multidominio	5
3.4	Uso particular de los certificados de servidor seguro	5
3.4.1	Usos apropiados de los certificados.....	5
3.4.2	Usos no autorizados de los certificados.....	5
3.5	Tarifas.....	6
4	PROCEDIMIENTOS OPERATIVOS.....	7
4.1	Proceso de emisión de certificados.....	7
4.2	REvocación de certificados	8
4.3	Renovación de certificados	8
5	PERFIL DE LOS CERTIFICADOS	9
5.1	Nombre distinguido (DN).....	9
5.2	Extensiones de los certificados	10

 firmaprofesional	Política de Certificación - Certificados de Servidor Seguro (SSL)	
	Versión	4.0
	Fecha	01/07/2008

1 INTRODUCCIÓN

1.1 DESCRIPCIÓN GENERAL

Los Certificados de Servidor Seguro son certificados expedidos a organizaciones para dispositivos informáticos, programas o aplicaciones, bajo la responsabilidad del suscriptor o titular del certificado. La finalidad del certificado SSL es poder autenticar de forma segura el servidor en la red y permitir a los usuarios crear una conexión segura mediante el protocolo SSL (o TLS).

La solicitud y emisión de los Certificados de Servidor Seguro se realiza a través de las Autoridades de Registro de Firmaprofesional.

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 Servidor Seguro (SSL)
Versión:	4.0
Descripción:	Política de Certificación para Certificados de Servidor Seguro (SSL)
Fecha de Emisión:	01/07/2008
OIDs	1.3.6.1.4.1.13177.10.1.3.1
Localización	http://www.firmaprofesional.com/cps

Anteriormente, esta Política de Certificación recibía el nombre de:

- Tipo II.C - CERTIFICADOS DE SERVIDOR SEGURO (1.3.6.1.4.1.13177.10.1.3.1)

 firmaprofesional	Política de Certificación - Certificados de Servidor Seguro (SSL)	
	Versión	4.0
	Fecha	01/07/2008

2 ENTIDADES PARTICIPANTES

2.1 AUTORIDADES DE CERTIFICACIÓN (CA)

Los Certificados de Servidor Seguro 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 Servidor Seguro. También podrá actuar como RA para la emisión de certificados de Servidor Seguro cualquier entidad que tenga un contrato de vinculación de RA con Firmaprofesional.

2.3 SOLICITANTE

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

2.4 SUSCRIPTOR

El suscriptor del certificado será una Persona Jurídica, identificada por medio de una URL.


2.5 CUSTODIO DE CLAVES

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 Servidor Seguro 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 Servidor Seguro (SSL)	
	Versión	4.0
	Fecha	01/07/2008

3 CARACTERISTICAS DE LOS CERTIFICADOS

3.1 PERIODO DE VALIDEZ DE LOS CERTIFICADOS

Los certificados de Servidor Seguro tendrán un periodo de validez de 1, 2 o 3 años.

3.2 TIPO DE SOPORTE

Los certificados de servidor seguro se emitirán en soporte software.

3.3 CERTIFICADOS MULTIDOMINIO

Los Certificados de Servidor Seguro Multidominio permiten validar diferentes URLs del mismo dominio con el mismo certificado.

Esta funcionalidad se consigue utilizando "Caracteres Wildcards" para las URLs tal como se definen en el estándar **RFC 2818 "HTTP Over TLS"**.

Según este estándar, se permite utilizar el carácter "asterisco" como comodín dentro de una URL. De este modo, un certificado con la URL "*.dominio.com" podrá ser utilizado para cualquier subdominio, como "subdominio1.dominio.com", "subdominio2.dominio.com", "www.dominio.com", etc...

El uso de "wildcards" en certificados de Servidor Seguro SSL está soportado por los principales navegadores de Internet y resulta muy útil cuando se disponen de muchos subdominios del mismo dominio de Internet y se desea utilizar un único certificado para todos ellos.

3.4 USO PARTICULAR DE LOS CERTIFICADOS DE SERVIDOR SEGURO

3.4.1 Usos apropiados de los certificados


Los Certificados de Servidor Seguro pueden ser utilizados para autenticar la identidad de un servidor, y establecer luego un canal de transmisión seguro entre el servidor y el usuario del servicio.

En general estos certificados se utilizarán para autenticar un Servidor Web mediante el protocolo SSL (o TLS), aunque también pueden ser utilizados en otro tipo de servidores como Servidores de Correo o Servidores de Ficheros, o con otro tipo de protocolos como IPSEC o SAML.

3.4.2 Usos no autorizados de los certificados

No se permite la utilización distinta de lo establecido en esta Política y en la Declaración de Practicas de Certificación.


No se permite el uso de este tipo de certificado para la firma electrónica de documentos.

 firmaprofesional	Política de Certificación - Certificados de Servidor Seguro (SSL)	
	Versión	4.0
	Fecha	01/07/2008

3.5 TARIFAS

El precio de los certificados de Servidor Seguro (SSL) 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.

 firma profesional	Política de Certificación - Certificados de Servidor Seguro (SSL)	
	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 siempre con los términos generales descritos en la CPS.

Los pasos a seguir para la obtención del certificado se detallan a continuación:

a) Solicitud

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

- La autorización de la Organización solicitante a la persona física que presenta la solicitud para la emisión del certificado.
- La identidad de la persona física.
- La titularidad del nombre de dominio, certificada por un representante legal de la organización.
- La acreditación por un medio fehaciente de la existencia de la entidad conforme a Derecho.

b) Aceptación de la solicitud

La RA verificará la identidad del solicitante, su vinculación con la entidad, la existencia de ésta, y los datos a incluir en el certificado.

c) Tramitación

Una vez aceptada la solicitud, 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 aplicaciones de servidores que pueden configurarse con el protocolo SSL, como IIS de Microsoft, incluyen herramientas para generar claves y peticiones de certificados.

e) Emisión del certificado

La RA procederá a la emisión del certificado, firmando la petición de certificado en formato PKCS#10 y enviándola a la CA.

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

 firmaprofesional	Política de Certificación - Certificados de Servidor Seguro (SSL)	
	Versión	4.0
	Fecha	01/07/2008

- 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

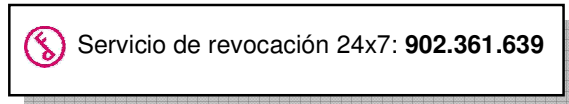
- Finalmente, la RA hará entrega del certificado al suscriptor permitiendo su descarga de forma segura desde Internet.

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:

- En horario de oficina:
 - Ponerse en contacto telefónicamente o presencialmente con su RA.
- 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:

- 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 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.


 firma profesional	Política de Certificación - Certificados de Servidor Seguro (SSL)	
	Versión	4.0
	Fecha	01/07/2008

5 PERFIL DE LOS CERTIFICADOS

5.1 NOMBRE DISTINGUIDO (DN)

El DN de los certificados de Servidor Seguro 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	<p>Contendrá la URL, nombre de dominio o identificación del dispositivo o servicio poseedor de las claves o de la aplicación.</p> <p>Para certificados multidominio, la URL seguirá el formato <i>*.dominio.com</i></p>
O, Organization	Organización	Contendrá el nombre de la entidad responsable del dispositivo.
OU, Organization Unit	Unidad en la organización	Contendrá el Departamento o Unidad al que está adscrito el dispositivo servidor
ST, State	Ubicación Geográfica	Ámbito geográfico de vinculación del suscriptor.
C, Country	País	Código de país de dos dígitos según ISO 3166-1. Por defecto "ES".

 firmaprofesional	Política de Certificación - Certificados de Servidor Seguro (SSL)	
	Versión	4.0
	Fecha	01/07/2008

5.2 EXTENSIONES DE LOS CERTIFICADOS

Extensión	Crítica	Valores
X509v3 Issuer Alternative Name	-	URI:http://www.firmaprofesional.com
X509v3 Subject Alternative Name	-	Email de contacto
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Digital Signature Non Repudiation Key Encipherment
X509v3 Extended Key Usage	-	Server Authentication (1.3.6.1.5.5.7.3.1)
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 de Servidor Seguro.