POLÍTICA DE CERTIFICACIÓN
CERTIFICATION POLICY (CP)

CERTIFICADOS DE SERVIDOR SEGURO (SSL)

Versión 5.1

INDICE

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 es poder autenticar de forma segura el servidor en la red y permitir a los usuarios crear una conexión segura mediante protocolos criptográficos estándar, como SSL, TLS, IPSEC o SAML.

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

Los Certificados de Servidor Seguro 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
Versión:	5.1
Descripción:	Política de Certificación para Certificados de Servidor Seguro (SSL)
Fecha de Emisión:	23/09/2010
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)

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.

2.3 SOLICITANTE

Podrá realizar la solicitud de un Certificado de Servidor Seguro cualquier persona autorizada por su propia organización para ello o directamente el representante legal de la Corporación.

2.4 SUSCRIPTOR

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

2.5 TERCERO QUE CONFÍA EN LOS CERTIFICADOS

Los Certificados de Servidor Seguro de Firmaprofesional están reconocidos por **Microsoft** en todas sus aplicaciones, incluyendo Internet Explorer, y por la Fundacion Mozilla, incluyendo el navegador **Firefox.**

Los terceros que confíen en estos certificados deben tener presente las limitaciones en su uso.

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, 3, 4 o 5 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.domino.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

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.

3.5 TARIFAS

El precio de los Certificados s 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.

4 PROCEDIMIENTOS OPERATIVOS

4.1 PROCESO DE EMISION DE CERTIFICADOS

Si la Corporación ya ha firmado el contrato de prestación de servicios de certificación y su representante legal dispone del certificado de persona física representante, este representante legal estará autorizado a emitir los certificados directamente accediendo a los servicios de Firmaprofesional, tramitando las correspondientes hojas de entrega.

Si la Corporación no tuviera firmado el contrato de prestación de servicios de certificación con Firmaprofesional, deberá ser firmado por el representante legal en el momento de solicitar un certificado de Servidor seguro.

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

a) Solicitud

Las solicitudes sólo pueden cursarse mediante la RA propia de Firmaprofesional.

Sin perjuicio de lo establecido en la correspondiente Declaración de Prácticas de Certificación (CPS) de Firmaprofesional, para garantizar que una entidad solicitante tiene control sobre el dominio (URL) que solicita incluir en un certificado se realizan dos tipos de comprobaciones:

- Organizacionales: se solicita la titularidad del nombre de dominio, certificada por un representante legal de la organización.
- Técnicas: se consultan los siguientes servicios whois autenticados:
    - Para dominios "*.es", consultar el siguiente servicio WHOIS autenticado: https://www.nic.es/sgnd/dominio/publicInformacionDominios.action
    - Para el resto de dominios:
        - consultar en http://www.iana.org/domains/root/db/ cuál es el servidor WHOIS autorizado para buscar información sobre el dominio, dependiendo del dominio de alto nivel (TLD), es decir, dependiendo de si el dominio acaba en .com, .org, .co, .net, ...
        - consultar el servicio WHOIS pertinente.
-

b) Aceptación de la solicitud

La aceptación es automática cuando la RA es la misma Corporación

La RA (cuando no sea la Corporación) 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 Corporación (o la RA cuando no sea Corporación) 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

- Identificarse presencialmente ante la RA, según el procedimiento que ésta le comunique.
- Recibir la Hoja de Entrega y Aceptación.

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:

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 s 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 subject:commonName (OID: 2.5.4.3)	Nombre	*Contendrá la URL, nombre de dominio o identificación del dispositivo o servicio poseedor de las claves o de la aplicación.* *Para certificados multidominio, la URL seguirá el formato "*.dominio.com"*[1]
O, Organization subject:organizationName (OID 2.5.4.10)	Organización	*Contendrá el nombre de la entidad responsable del dispositivo exactamente como está inscrita en el Registro.*
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*".*
Business Category subject:businessCategory (OID: 2.5.4.15)	Categoría entidad	"V1.0, Clause 5.(b)", "V1.0, Clause 5.(c)", "V1.0, Clause 5.(d)", or "V1.0, Clause 5.(e)"[2]
subject:jurisdictionOfIncorporationLocalityName (OID: 1.3.6.1.4.1.311.60.2.1.1)	Localidad del Registro	*Localidad*
subject:jurisdictionOfIncorporationStateOrProvinceName (OID: 1.3.6.1.4.1.311.60.2.1.2)	Provincia del Registro	*provincia*
subject:jurisdictionOfIncorporationCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3)	País del Registro	*país*
Registration Number Subject:serialNumber (OID: 2.5.4.5)	Número del registro	*Número*
subject:streetAddress (OID: 2.5.4.9)	Dirección empresa	*Dirección [opcional]*

[1] No podrá ser multidominio identificando multitud de dominios mediante "*.empresa.com", pero si se permite validar diversos dominios.

[2] De acuerdo con las secciones 7.2.2, 7.2.3, 7.2.4 or 7.2.5 del documento http://www.cabforum.org/Guidelines_v1_2.pdf

subject:localityName (OID: 2.5.4.7)	Localidad empresa	*Localidad*
subject:stateOrProvinceName (OID: 2.5.4.8)	Provincia empresa	*provincia*
subject:countryName (OID: 2.5.4.6)	País empresa	*País*
subject:postalCode (OID: 2.5.4.17)	Código Postal empresa	*Cp [opcional]*

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.*