POLÍTICA DE CERTIFICACIÓN

CERTIFICATION POLICY (CP)

CERTIFICADOS DE SERVICIO SEGURO (VA/TSA)

Versión 6.0

Firmado digitalmente por:
FIRMAPROFESIONAL, S.A.

firmaprofesional

Oficina Barcelona ESADECREAPOLIS - 1B13. Avenida Torre Blanca, 57. Sant Cugat del Valles. - 08173 Barcelona. Telf: 93.477.42.45
Oficina Madrid Velázquez 59, 1º Ctro-Izqda – 28001 Madrid – Tel: 91.576.21.81

INDICE

1 INTRODUCCIÓN 3

1.1 Descripción General 3
1.2 Identificación del Documento 3

2 ENTIDADES PARTICIPANTES 4

2.1 Autoridades de Certificación (CA) 4
2.2 Solicitante 4
2.3 Suscriptor 4
2.4 Tercero que confía en los certificados 4

3 CARACTERISTICAS DE LOS CERTIFICADOS 5

3.1 Periodo de validez de los certificados 5
3.2 Uso particular de los certificados 5
3.3 Tarifas 5

4 PROCEDIMIENTOS OPERATIVOS 6

4.1 Proceso de emision de certificados 6
4.2 Revocacion de certificados 6
4.3 Renovacion de certificados 6

5 PERFIL DE LOS CERTIFICADOS 7

5.1 Nombre distinguido (DN) 7
5.2 Extensiones de los certificados 7

1 INTRODUCCIÓN

1.1 DESCRIPCIÓN GENERAL

Los Certificados de Servicio Seguro son certificados que permiten firmar evidencias digitales como **Autoridad de Sellado de Tiempo (TSA)** o **Autoridad de Validación (VA**). Su emisión y utilización requerirá las máximas garantías de seguridad.

Los Certificados de Servicio Seguro se emitirán únicamente a entidades de reconocido prestigio que establezcan un acuerdo de colaboración previo con Firmaprofesional. Estas entidades deberán disponer de un dispositivo HSM certificado FIPS 140-1 Nivel 2 para la custodia de las claves privadas del certificado.

Los Certificados de Servicio 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 IDENTIFICACIÓN DEL DOCUMENTO

Nombre:	CP Servicio Seguro
Versión:	6.0
Descripción:	Política de Certificación para Certificados de Servicio Seguro (TSA/VA)
Fecha de Emisión:	15/04/2014
OIDs	1.3.6.1.4.1.13177.10.1.4.1
Localización	http://www.firmaprofesional.com/cps

Anteriormente, esta Política de Certificación recibía el nombre de:

- Tipo II.C - CERTIFICADO DE SERVICIO SEGURO (1.3.6.1.4.1.13177.10.1.4.1)

2 ENTIDADES PARTICIPANTES

2.1 AUTORIDADES DE CERTIFICACIÓN (CA)

Estos certificados pueden ser emitidos por una CA Subordinada de Firmaprofesional o directamente por la CA Root de Firmaprofesional según las necesidades.

La gestión de las solicitudes y emisiones de los certificados será realizada directamente por Firmaprofesional.

Firmaprofesional establecerá:

- Qué criterios se deben cumplir para solicitar un certificado.
- Los mecanismos y procedimientos necesarios para realizar la identificación y autenticación del suscriptor, cumpliendo con lo estipulado en la CPS.

2.2 SOLICITANTE

Estos certificados se emitirán únicamente a entidades de reconocido prestigio que establezcan un acuerdo de colaboración previo con Firmaprofesional.

2.3 SUSCRIPTOR

El suscriptor estos certificados será la entidad que aparezca identificada en el certificado

2.4 TERCERO QUE CONFÍA EN LOS CERTIFICADOS

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

Estos certificados tendrán un periodo de validez a definir por Firmaprofesional en función de cada caso particular. Si el certificado incluye la extensión “OCSP no check”, el periodo de validez máximo estará limitado a 1 año.

En el caso de que la clave de firma esté bajo el exclusivo control de Firmaprofesional, la duración del certificado podrá ser la máxima posible. En caso contrario la validez del certificado no excederá los cuatro años.

3.2 USO PARTICULAR DE LOS CERTIFICADOS

3.2.1 Usos apropiados de los certificados

Estos certificados podrán usarse en los términos establecidos por la CPS, y lo establecido en la legislación vigente al respecto.

- Los certificados de **Autoridad de Sellado de Tiempo** deberán utilizarse únicamente para la firma de sellos de tiempo. Como referencia se deberá seguir el estándar RFC 3161 “*Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*” y sus sucesivas actualizaciones.

- Los certificados de **Autoridad de Validación** deberán utilizarse únicamente para la firma de evidencias respecto a la validez de un certificado en un periodo de tiempo concreto. Como referencia se deberá seguir el estándar RFC 2560 *“OCSP - Online Certificate Status Protocol*” y sus sucesivas actualizaciones.

3.2.2 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 certificados para cualquier otro diferente a los establecidos en esta Política de Certificación, como por ejemplo Cifrado, Autenticación o Firma Electrónica de documentos.

3.3 TARIFAS

Las tarifas de estos certificados se establecerán por Firmaprofesional y al suscriptor mediante un contrato privado de prestación de servicios.

4 PROCEDIMIENTOS OPERATIVOS

4.1 PROCESO DE EMISION DE CERTIFICADOS

El proceso de emisión de estos certificados se realizará de manera manual siguiendo las máximas garantías de seguridad en el proceso.

El procedimiento de emisión de estos certificados requerirá la supervisión directa del Departamento Técnico de Firmaprofesional.

Estos certificados se emitirán únicamente a entidades de reconocido prestigio que establezcan un acuerdo de colaboración previo con Firmaprofesional. Estas entidades deberán disponer de un dispositivo HSM certificado FIPS 140-1 Nivel 2 para la custodia de las claves privadas del certificado

4.2 REVOCACION DE CERTIFICADOS

Debido a las especiales características de este tipo de certificados, la revocación de este tipo de certificados requerirá la autorización del Director Técnico de Firmaprofesional.

4.3 RENOVACION DE CERTIFICADOS

La renovación de este tipo de certificados implicará necesariamente realizar el proceso de generación de un nuevo certificado.

5 PERFIL DE LOS CERTIFICADOS

5.1 NOMBRE DISTINGUIDO (DN)

Campo del DN	Nombre	Descripción
CN, Common Name	Nombre	*URL del servicio.*
O, Organization	Organización	*Nombre de la Organización que ofrece el servicio seguro*
C, Country	País	*C*= ES

5.2 EXTENSIONES DE LOS CERTIFICADOS

Extensión	Crítica	Valores
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Digital Signature Non Repudiation
X509v3 Extended Key Usage	Sí	*Uno de los siguientes valores:* OCSP_RESPONDER TIME_STAMP
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	-	policyIdentifier: 1.3.6.1.4.1.13177.10.1.4.1 CPSuri: http://www.firmaprofesional.com/cps User Notice: (Según el caso): • Certificado de Servicio Seguro TSA • Certificado de Servicio Seguro OCSP
1.3.6.1.5.5.7.48.1.5 id-pkix-ocsp-nocheck (Opcional)	-	*OCSP No Check*
X509v3 Subject Alternative Name (Opcional)	-	*<email del suscriptor>*
X509v3 Issuer Alternative Name (Opcional)	-	URI:http://www.firmaprofesional.com
X509v3 Authority Information Access (Opcional)	-	*<URI dónde se encuentra el certificado de la CA>*