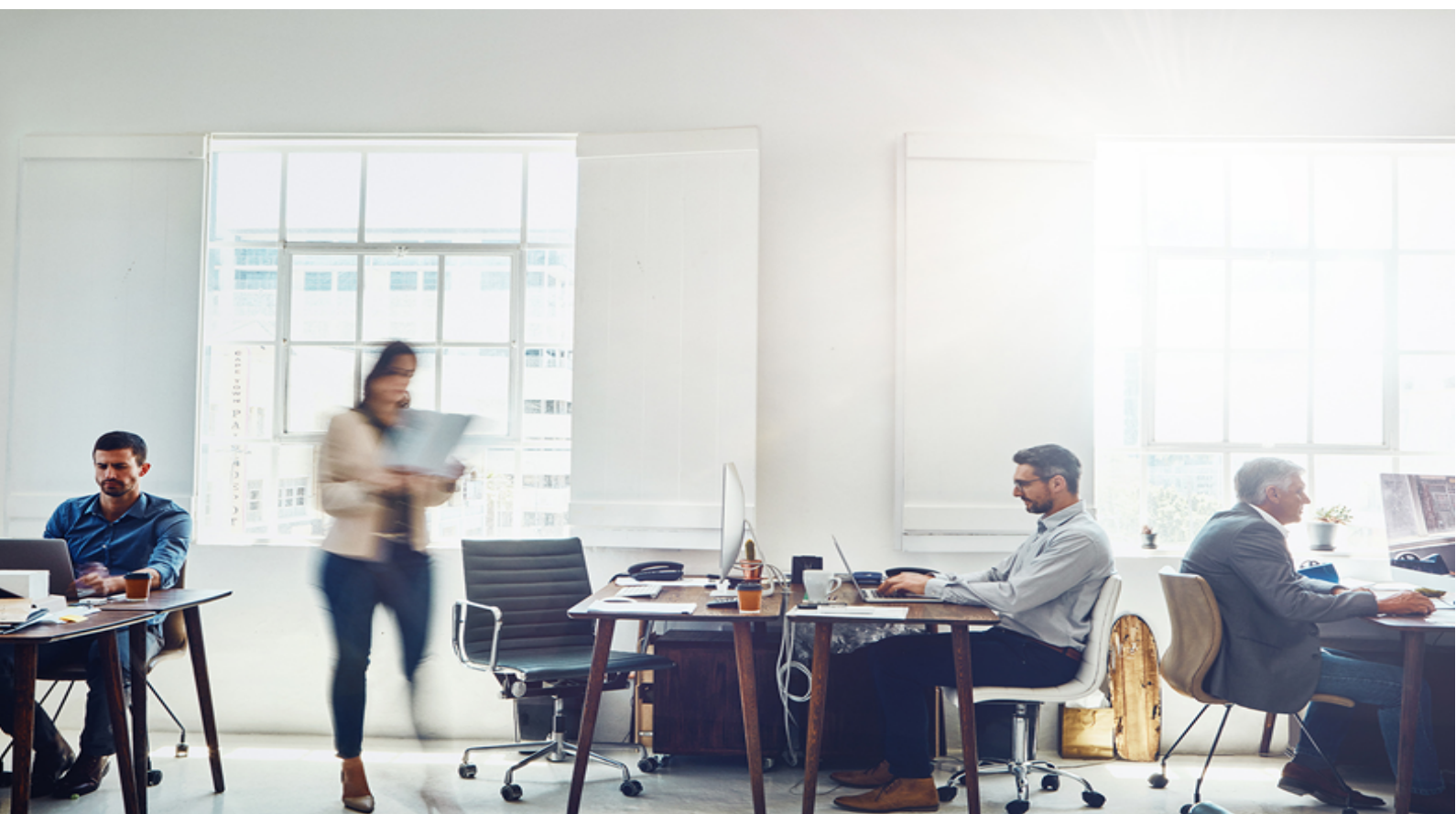


Política de Certificación

Certificados de un solo uso OTC (One-Time Certificate)

Versión: 210407

Clasificación: Público



Histórico de versiones

Versión	Sección y cambios	Fecha de Publicación
200612	Versión Inicial	12/06/2020
200728	<p>Sección 3.2. Dispositivo de creación de firma: se aclara el mecanismo de activación de la clave privada (datos de creación de firma).</p> <p>Sección 4.1.1. Solicitud: se aclaran los pasos y mecanismos para la solicitud.</p> <p>Sección 4.2 Revocación de los certificados: se añade la necesidad de emitir CRLs.</p>	28/07/2020
210407	<ul style="list-style-type: none">• Adaptación a la nueva Ley 6/2020, reguladora de determinados aspectos de los servicios electrónicos de confianza.• Modificación de OID	07/04/2021

Índice

1. Introducción	5
1.1. Descripción general	5
1.2. Identificación del documento	5
2. Entidades Participantes	6
2.1. Prestador de Servicios de Certificación (PSC)	6
2.2. Autoridad de Registro (RA)	6
2.3. Solicitante	6
2.4. Suscriptor	6
2.5. Punto de Verificación Presencial	6
2.6. Firmante	7
2.7. Tercero que confía en los certificados	7
2.8. Custodio de claves	7
2.9. Otras entidades	7
2.9.1. Sistema de firma electrónica mediante certificados OTC	7
3. Características de los Certificados	8
3.1. Periodo de validez de los certificados	8
3.2. Dispositivo de creación de firma	8
3.3. Uso particular de los certificados	8
3.3.1. Usos apropiados de los certificados	8
3.3.2. Usos no autorizados de los certificados	8
3.4. Tarifas	8
3.5 Responsabilidades	8
4. Procedimientos operativos	9
4.1. Proceso de emisión de los certificados	9
4.1.1 Solicitud	9
4.1.2 Aceptación de la solicitud	9
4.1.3 Tramitación	9

4.2. Revocación de los certificados	10
4.3. Renovación de los certificados	10
5. Controles de Seguridad física, instalaciones, gestión y operacionales	11
6. Controles de seguridad técnica	11

1. Introducción

1.1. Descripción general

Los certificados de un solo uso (en adelante certificados OTC) son certificados no cualificados expedidos a personas físicas en software (programas o aplicaciones).

La **finalidad de los certificados emitidos bajo esta política es** poder firmar documentos electrónicos de manera asistida, para la producción de firmas electrónicas mediante programas o sistemas informáticos, que permitan **garantizar la integridad de los documentos electrónicos firmados** con las máximas garantías de protección de datos de carácter personal de la persona física cuyos datos aparecen en el certificado.

La solicitud y emisión de los certificados OTC se realiza a través de un proceso automático.

La vigencia de los mismos es de 24 horas y, aunque están pensados para realizar una única firma en procesos de firma esporádicos, durante su vigencia podrían realizar más firmas.

En el presente documento se exponen las Condiciones Particulares referentes a este tipo de certificado. Esta Política de Certificación (en adelante "CP") está subordinada al cumplimiento de las Condiciones Generales expuestas en la Declaración de Prácticas de Certificación (en adelante "CPS") de Firmaprofesional.

1.2. Identificación del documento

Nombre:	CP Certificados de un solo uso (OTC - One Time Certificates)
Versión:	210407
Descripción:	Política de Certificación para Certificados de un solo uso (OTC)
Fecha de Emisión:	07/04/2021
OIDs:	1.3.6.1.4.1.13177.101.2 (en otros dispositivos)
Localización:	http://www.firmaprofesional.com/cps

2. Entidades Participantes

2.1. Prestador de Servicios de Certificación (PSC)

Estos certificados deben ser emitidos por Firmaprofesional como [Prestador de Servicios de Certificación](#) mediante su Autoridad de Certificación Subordinada "AC Firmaprofesional – OTC" (*One-Time Certificates*) o "AC Firmaprofesional – OTC 2020".

2.2. Autoridad de Registro (RA)

Actuará como RA la entidad encargada de la gestión del programa o sistema informático que realiza la solicitud de generación de certificados OTC a la CA.

Los datos requeridos para la creación del certificado serán enviados a la RA por el Solicitante y seguidamente la RA los transmitirá a la CA.

La RA no verificará la veracidad de la información proporcionada por el Solicitante para la emisión de los certificados OTC.

2.3. Solicitante

Podrán solicitar certificados OTC las entidades que hayan suscrito un acuerdo de prestación de servicios con la RA.

2.4. Suscriptor

Es Suscriptor de los certificados la propia RA, esto es, la entidad que gestiona el sistema o programa informático encargado de solicitar la emisión de los certificados a la CA.

Los certificados deberán ser generados, almacenados y utilizados únicamente en y desde el programa o sistema informático del Suscriptor.

2.5. Punto de Verificación Presencial

Es recomendable que el Solicitante implemente un paso de verificación de identidad previo a la solicitud y emisión del certificado y a la generación de la firma electrónica, aunque no es requerido por la presente política.

No obstante, se deberá permitir al Firmante, en cualquier caso, verificar y aceptar los datos personales que van a ser utilizados para generar el certificado antes de proceder a la emisión del mismo.

2.6. Firmante

El firmante en este tipo de certificados es la persona física que consta en el certificado. La identidad del firmante no es verificada de forma indubitada por la Autoridad de Registro.

2.7. Tercero que confía en los certificados

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

2.8. Custodio de claves

La custodia de los datos de creación de firma asociados a cada certificado OTC se realizará en los sistemas de la RA bajo su responsabilidad.

2.9. Otras entidades

2.9.1. Sistema de firma electrónica mediante certificados OTC

El Suscriptor de los certificados es el encargado de la gestión del programa o sistema informático de firma electrónica que realiza además la solicitud de emisión y la custodia del certificado del Firmante.

Dicho sistema podrá ser auditado por Firmaprofesional antes de la puesta en funcionamiento del servicio de emisión de certificados OTC.

3. Características de los Certificados

3.1. Periodo de validez de los certificados

Los certificados OTC tendrán un periodo de validez de 24 horas.

3.2. Dispositivo de creación de firma

Los certificados OTC podrán generarse en soporte software o en Módulos *Hardware* de Seguridad (HSM). La activación del uso de la clave privada se realiza mediante la interacción del firmante con el Sistema de firma del suscriptor, generalmente una acción de firma biométrica sobre un dispositivo con pantalla (tablet o móvil) que muestra los datos que se van a firmar.

3.3. Uso particular de los certificados

3.3.1. Usos apropiados de los certificados

Los certificados OTC pueden ser utilizados para la producción de firmas electrónicas a través del *Sistema de firma electrónica mediante certificados OTC* del Suscriptor, **que permite garantizar la integridad de los documentos electrónicos firmados.**

3.3.2. Usos no autorizados de los certificados

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.

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

No se recomienda su uso para el cifrado de documentos si no se dispone de una copia de seguridad del certificado.

3.4. Tarifas

Será responsabilidad de la RA establecer el precio de los certificados OTC.

3.5 Responsabilidades

Según se especifica en la Declaración de Prácticas de Certificación (CPS).

4. Procedimientos operativos

4.1. Proceso de emisión de los certificados

Los pasos a seguir para la obtención del certificado son los siguientes:

4.1.1 Solicitud

El acceso a dicho servicio de solicitud será puesto a disposición del SOLICITANTE por FIRMAPROFESIONAL, pudiendo acceder al mismo sólo las personas y sistemas informáticos que, bajo su responsabilidad, hayan sido autorizadas por el SOLICITANTE.

La solicitud y emisión de los certificados OTC se realiza a través de un proceso automático, mediante una petición autenticada en el momento previo a la realización de una operación de firma electrónica.

La petición deberá incluir datos identificativos del firmante (nombre, apellidos y DNI, NIE o número de pasaporte del firmante o cualquier otro identificador único del usuario), que habrán sido introducidos por el propio Firmante o comunicados a la RA con anterioridad, y que opcionalmente pueden provenir de una fuente autenticada de datos (como una base de datos, un CRM o ERP corporativo). La petición podrá incorporar además información relativa al documento que se va a firmar en la plataforma e información del dispositivo que va a realizar la firma.

La petición contendrá una petición de firma de certificado en formato PKCS#10.

4.1.2 Aceptación de la solicitud

Se aceptarán por defecto todas las solicitudes provenientes de un Solicitante, esto es, una fuente autorizada por la RA.

4.1.3 Tramitación

Firmaprofesional recibirá la solicitud de emisión de certificado, emitirá el certificado y proveerá el certificado generado al sistema de la RA que lo solicitó.

4.2. Revocación de los certificados

Dada la limitada vigencia de los certificados no se prevé la necesidad de realizar revocaciones de certificados, si bien Firmaprofesional quedará facultada para revocar el certificado del cliente en caso de que se den circunstancias que así lo recomienden.

No obstante, FIRMAPROFESIONAL deberá emitir las correspondientes listas de certificados revocados (CRLs) por razones técnicas, en los términos y condiciones recogidos en la Política de Certificación.

Para el resto de cuestiones relacionadas con las revocación y consulta del estado de los certificados, según se especifique en la Declaración de Prácticas de Certificación (CPS).

4.3. Renovación de los certificados

Dada la limitada vigencia de los certificados no se realizarán renovaciones de certificados.

5. Controles de Seguridad física, instalaciones, gestión y operacionales

Se encuentra especificado en la Declaración de Prácticas de Certificación

6. Controles de seguridad técnica

Se encuentra especificado en la Declaración de Prácticas de Certificación



Firmaprofesional, S.A.

Marzo de 2021