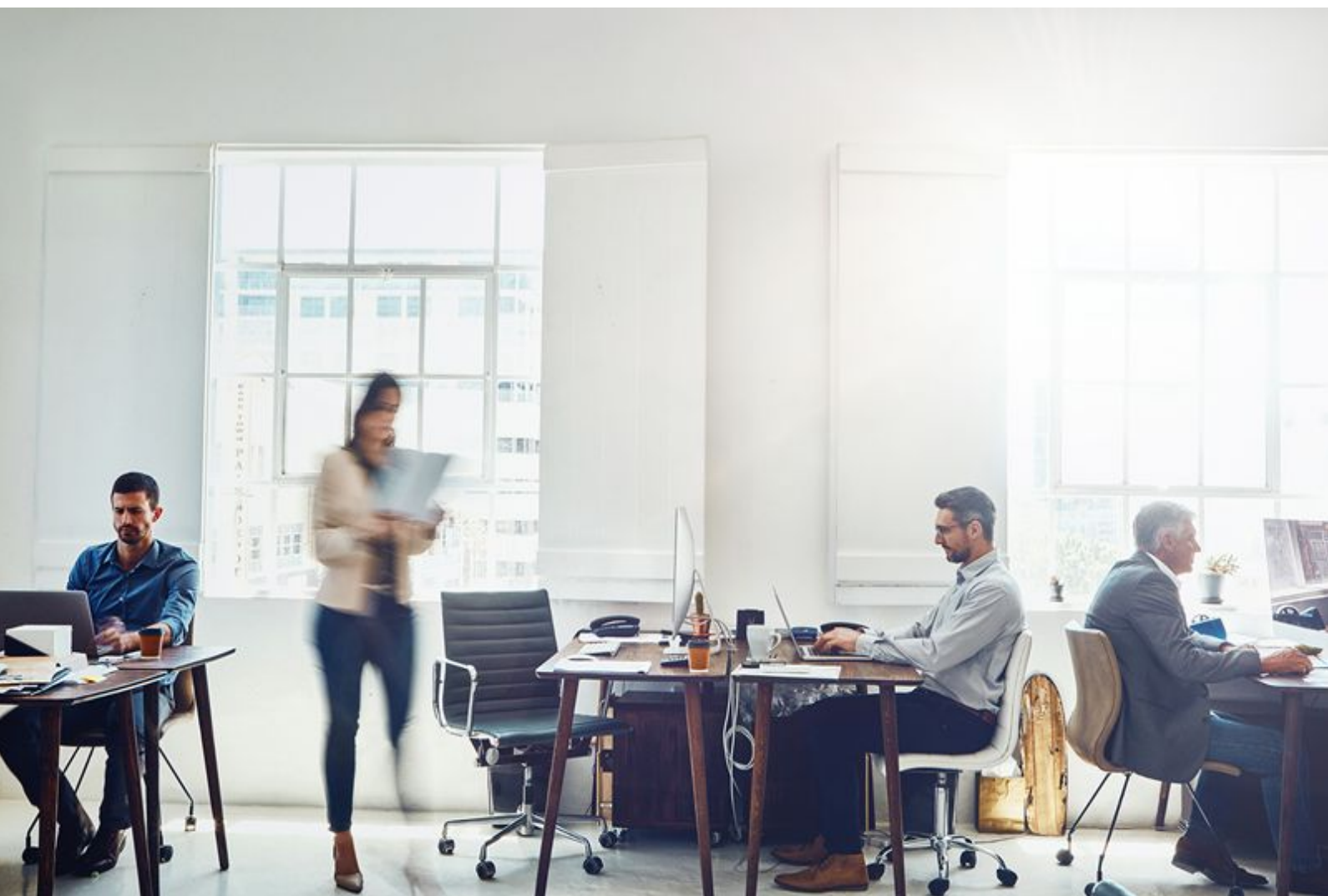


Textos Divulgativos PKI (PDS)

Declaración de Divulgación de Firmaprofesional sobre Certificados OTC

Versión: 200612

Clasificación: Público



Restricciones de uso y divulgación de la información contenida en este documento

© Junio 2020 Firmaprofesional, S.A.

Este documento contiene la información esencial a conocer sobre el servicio de emisión de certificados OTC de la Entidad de Certificación Firmaprofesional.

Histórico de versiones

Versión	Sección y cambios	Fecha
200612	Versión inicial	12/06/2020

Índice

1. Información de contacto	6
1.1. Organización Responsable	6
1.2. Contacto	6
1.3. Contacto para procesos de renovación	6
2. Tipo y finalidad del certificado OTC	7
3. Límites en el Uso de Certificados	8
3.1. Límites de Uso del Firmante	8
3.2. Límites de uso del Verificador	8
4. Obligaciones del Suscriptor	10
4.1. Solicitud de Certificados	10
4.2. Obligaciones sobre la información	10
5. Obligaciones del Firmante	11
5.1. Obligaciones de Protección	11
5.2. Obligaciones de Uso Correcto	11
6. Obligaciones del Verificador	12
6.1. Decisión informada	12
6.2. Requisitos para la Verificación de Firma Electrónica	12
6.3. Fiabilidad de un Certificado no Verificado	13
6.4. Uso correcto y acciones prohibidas	13
6.5. Cláusula de indemnización	13
7. Obligaciones de FIRMAPROFESIONAL	15
7.1. Obligaciones relativas a la prestación del servicio de certificación digital	15
7.2. Obligaciones relativas a las Verificaciones de Registro	15
7.3. Periodos de Conservación	15
8. Política de Privacidad y protección de datos de carácter personal	17

9. Reclamaciones y resolución de conflictos

17

1. Información de contacto

1.1. Organización Responsable

La Entidad de Certificación Firmaprofesional, en adelante "FIRMAPROFESIONAL" es una iniciativa de:

FIRMAPROFESIONAL, S.A.
Calle Paseo Bonanova 47,
08017 Barcelona.
Tel: (+34) 902 361 639

1.2. Contacto

Para cualquier consulta, contactar con:

FIRMAPROFESIONAL, S.A.
Calle Paseo Bonanova 47,
08017 Barcelona.
Tel: (+34) 902 361 639

1.3. Contacto para procesos de renovación

No existe la posibilidad de renovación de este tipo de certificados

2. Tipo y finalidad del certificado OTC

Es un certificado no cualificado para persona física en software o en Módulos *Hardware* de Seguridad (HSM).

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 vigencia de estos certificados es de 24 horas.

Se identifica con el número OID: 1.3.6.1.4.1.13177.100.2

Se incluye en la Política de Certificación de Certificados de un solo uso (OTC- One Time Certificate)

3. Límites en el Uso de Certificados

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medioambientales severos.

3.1. Límites de Uso del Firmante

El certificado OTC emitido por Firmaprofesional se utilizará para la firma electrónica de documentos electrónicos.

El firmante debe utilizar los certificados suministrados por FIRMAPROFESIONAL exclusivamente para los usos autorizados que quedan posteriormente descritos en la sección Obligaciones del Firmante.

Asimismo, el firmante se compromete a usar el servicio de certificación digital de acuerdo con las instrucciones, manuales y procedimientos proporcionados por FIRMAPROFESIONAL.

Debe cumplir con toda ley o reglamento que pueda afectar a su derecho de uso de las herramientas criptográficas.

No puede adoptar medidas de inspección, alteración o ingeniería inversa del servicio de certificación digital de FIRMAPROFESIONAL sin previa autorización expresa.

3.2. Límites de uso del Verificador

Los certificados deben ser utilizados exclusivamente para sus funciones y propósitos establecidos, sin que se permita ningún otro uso.

Asimismo, deben ser utilizados de acuerdo con la ley de aplicación en vigor.

Los certificados de Entidad final, es decir, aquéllos que no son de Autoridad de Certificación, no pueden ser usados para firmar solicitudes de emisión, renovación, cancelación o

revocación de certificados, para firmar certificados de clave pública de ningún tipo ni para firmar listas de revocaciones de certificados (CRL).

El uso de firmas digitales en operaciones que contradiga este texto divulgativo se considerará como uso indebido a los efectos legales apropiados, liberando así a FIRMAPROFESIONAL de cualquier responsabilidad derivada de dicho uso que el firmante o cualquier tercero realice.

FIRMAPROFESIONAL no tendrá acceso a los datos contenidos en las transacciones con los certificados. Como consecuencia de la imposibilidad técnica de acceder a los contenidos de un mensaje, FIRMAPROFESIONAL no puede emitir ninguna validación de contenido, por lo que el suscriptor, firmante o persona responsable de estas operaciones asumirá cualquier responsabilidad derivada de los contenidos vinculados a la utilización de un certificado.

Asimismo, cualquier responsabilidad que pudiera derivarse de la utilización más allá de los límites y condiciones de uso establecidos en este texto, así como cualquier otro uso indebido descrito en esta sección o que pudiera interpretarse como indebido en función de la legislación vigente, será imputable al suscriptor, al firmante o a la persona responsable de la custodia.

4. Obligaciones del Suscriptor

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

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

4.1. Solicitud de Certificados

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

4.2. Obligaciones sobre la información

Es responsabilidad del suscriptor que toda la información contenida en la solicitud del certificado sea exacta, completa a los efectos del certificado.

El suscriptor deberá informar inmediatamente a FIRMAPROFESIONAL:

- De cualquier inexactitud detectada en el certificado una vez ha sido emitido.
- De los cambios ocurridos en la información suministrada y/o registrada para la emisión del certificado.
- De la pérdida, robo, hurto o cualquier otro tipo de pérdida de control de la clave privada del firmante.

5. Obligaciones del 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.

5.1. Obligaciones de Protección

El firmante se compromete a usar el certificado únicamente en y desde el programa o sistema informático del Suscriptor, que activa el uso del certificado en el acto de firma tal y como esté establecido en el citado sistema informático.

5.2. Obligaciones de Uso Correcto

El firmante debe hacer uso del servicio de certificación suministrado por FIRMAPROFESIONAL, exclusivamente para los usos autorizados en la CPS y en cualquier otra instrucción, manual o procedimiento proporcionado al suscriptor.

El firmante debe cumplir con toda ley y reglamento que afecte a su derecho de uso de las herramientas criptográficas.

No puede adoptar medidas de inspección, alteración o ingeniería inversa de los servicios de certificación digital proporcionados.

El firmante reconocerá:

- a. Que al utilizar cualquier certificado y mientras el certificado no haya expirado ni haya sido cancelado o revocado, deberá aceptar dicha certificación y ésta será operativa.
- b. Que no actúan como entidades de certificación y que, por lo tanto, se comprometen a no utilizar las claves privadas correspondientes a las claves públicas contenidas en los certificados, a fin de la firma de los mismos.

6. Obligaciones del Verificador

6.1. Decisión informada

FIRMAPROFESIONAL informa al verificador que tiene acceso a información suficiente para tomar una decisión informada cuando verifica un certificado y basarse en la información contenida en el mismo.

Asimismo, el verificador reconoce que el uso del Registro y de las Listas de Revocación de Certificados (en adelante "CRLs") de FIRMAPROFESIONAL está regulado por la CPS de FIRMAPROFESIONAL y se compromete a cumplir los requisitos técnicos, operacionales y de seguridad descritos en dicha CPS.

6.2. Requisitos para la Verificación de Firma Electrónica

La verificación normalmente se ejecutará automáticamente por un software de verificación y siempre de acuerdo con los siguientes requisitos de la DPC:

- Es necesario utilizar el software adecuado para la verificación de una firma digital con los algoritmos y las longitudes de claves autorizadas en el certificado y/o ejecutar cualquier otra operación criptográfica, y establecer la cadena de certificados en la que se basa la firma electrónica a verificar, ya que la firma electrónica se verifica mediante esta cadena de certificados.
- Es necesario asegurar que la cadena de certificados identificados es la más adecuada para verificar la firma electrónica, ya que la firma puede estar basada en más de una cadena y es decisión del verificador asegurar el uso de la más apropiada.
- Es necesario verificar el estado de revocación de los certificados de la cadena con la información proporcionada por el Registro de FIRMAPROFESIONAL (con las CRLs por ejemplo), a fin de determinar la validez de todos los certificados de la cadena, ya que la firma electrónica sólo podrá ser considerada correctamente validada si todos y cada uno de los certificados de la cadena son correctos y operativos.

- Es necesario asegurar que todos los certificados de la cadena autorizan el uso de la clave privada por parte del suscriptor y el firmante. Cada certificado de la cadena tiene un indicador que hace referencia a las condiciones de uso aplicables para su revisión por parte de los verificadores.
- Es necesario verificar técnicamente la firma de todos los certificados de la cadena antes de confiar en el certificado usado por el firmante.

6.3. Fiabilidad de un Certificado no Verificado

Si un verificador confía en un certificado no verificado, asumirá todo el riesgo derivado de esta acción.

6.4. Uso correcto y acciones prohibidas

El verificador se compromete a no usar información alguna sobre el estado de los certificados, ni de cualquier otro tipo que haya sido facilitada por FIRMAPROFESIONAL, en la realización de cualquier operación prohibida por la legislación vigente.

El verificador se compromete a no inspeccionar, interferir o realizar ingeniería inversa sobre la implementación técnica de los servicios de certificación públicos de FIRMAPROFESIONAL sin previo consentimiento escrito.

El verificador está obligado, además, a no poner en peligro intencionadamente la seguridad de los servicios públicos de certificación de FIRMAPROFESIONAL.

6.5. Cláusula de indemnización

Un tercero que confía en el certificado se compromete a eximir a FIRMAPROFESIONAL de toda responsabilidad por los daños y perjuicios derivados de cualquier acto u omisión que conduzcan a la responsabilidad, daño o pérdida, gastos de cualquier tipo (incluidos los gastos judiciales y los de representación legal en los que pudiera incurrir) por la publicación y el uso del certificado, cuando concurren alguna de las siguientes causas:

- Incumplimiento de las obligaciones del tercero que confía en el certificado.

- Falta de verificación del estado de un certificado para determinar que no está cancelado o revocado.
- Falta de verificación de la totalidad de las medidas de garantía previstas en la CPS o en las demás normativas de aplicación.

Los certificados de OTC no se deben utilizar para el cifrado de documentos, contenidos y mensajes de datos.

7. Obligaciones de FIRMAPROFESIONAL

7.1. Obligaciones relativas a la prestación del servicio de certificación digital

FIRMAPROFESIONAL se compromete a:

- a. Emitir, entregar, administrar, cancelar y revocar los certificados de acuerdo a las instrucciones del suscriptor en los casos y por los motivos descritas en la CPS de FIRMAPROFESIONAL.
- b. Ejecutar los servicios con los medios técnicos y materiales adecuados y con personal que cumpla las condiciones de cualificación y experiencia establecidas en la CPS.
- c. Cumplir los niveles de calidad en los servicios de acuerdo con los establecido en la CPS en cuanto a los aspectos técnicos, operativos y de seguridad.
- d. Comunicar a los terceros que lo soliciten, el estado de los certificados OTC de acuerdo con lo establecido en la CPS para los distintos servicios de verificación de los certificados.

7.2. Obligaciones relativas a las Verificaciones de Registro

FIRMAPROFESIONAL se compromete a emitir certificados en base a la información proporcionada por el suscriptor.

Es recomendable que el Solicitante del certificado 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.

7.3. Periodos de Conservación

FIRMAPROFESIONAL conservará los registros correspondientes a las solicitudes de emisión y renovación de certificados un mínimo de 15 años.

FIRMAPROFESIONAL almacenará la información de los registros durante un periodo de entre 1 y 15 años en función del tipo de información registrada.

8. Política de Privacidad y protección de datos de carácter personal

La información personal recabada de los usuarios registrados es almacenada en la base de datos propiedad de Firmaprofesional que asume las medidas de índole técnica, organizativa y de seguridad que garanticen la confidencialidad e integridad de la información de acuerdo con lo establecido en el Reglamento General de Protección de Datos (RGPD), y demás legislación aplicable.

Cualquier usuario registrado puede en cualquier momento ejercer el derecho de acceso, rectificación, oposición, supresión, limitación al tratamiento y portabilidad de sus datos de carácter personal suministrados a Firmaprofesional mediante comunicación escrita con referencia "tratamiento de datos". No obstante, si el usuario considera que su derecho a la protección de datos personales ha podido ser vulnerado, puede reclamar ante la Agencia Española de Protección de Datos.

Firmaprofesional tiene publicada su política de privacidad en <https://www.firmaprofesional.com/aviso-legal/#politica-de-privacidad>

9. Reclamaciones y resolución de conflictos

Para la resolución de cualquier conflicto que pudiera surgir en relación con este documento, la CP o el instrumento jurídico vinculante, las partes, con renuncia a cualquier otro fuero que pudiera corresponderles, se someten a la Corte Española de Arbitraje.



Firmaprofesional, S.A.

Junio 2020