# Política de Servicio Cualificado

# AUTORIDAD DE SELLADO CUALIFICADO DE TIEMPO DE FIRMAPROFESIONAL (TSA)

Versión: 201021

Clasificación: Público

BARCELONA
EDIF. ESADECREAPOLIS
AV. TORRE BLANCA, 57 - LOCAL 386
08173 SANT CUGAT DEL VALLÈS
+34 934 774 245

MADRID
VELÁZQUEZ 59, 1º CTRO.-IZDA.
28001 MADRID
+34 915 762 181

WWW.FIRMAPROFESIONAL.COM

**Restricciones de utilización y revelación de los datos contenidos en este documento.**

# Histórico de versiones

| Versión | Sección y cambios | Fecha de Publicación |
|---|---|---|
| 6.0 | Para consultar cambios entre versiones anteriores, por favor envíe un correo a info@firmaprofesional.com | 15/04/2014 |
| 170705 | Cambio de plantilla y numeración de versiones, pasando a seguir el formato AAMMDD (año, mes y día de la publicación)<br>Adaptación a servicio cualificado eIDAS. | 05/07/2017 |
| 200226 | Cambio de plantilla.<br>Correcciones de inconsistencia terminológica: timestamp, Time-Stamping, etc.<br>Realizadas aclaraciones sobre la custodia.<br>Incorporación apartado 7.8. Control por Pérdida de Calibración<br>Incorporación de los datos del nuevo sello de tiempo | 26/02/2020 |
| 201021 | Actualización del certificado de TSA | 21/10/2020 |

# Índice

# 1. Introducción

## 1.1. Descripción General

Firmaprofesional, como Prestador de Servicios de Confianza que emite certificados cualificados según el REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, también ofrece servicios de Sellado de Tiempo.

Este documento tiene como objetivo describir el funcionamiento de los **Servicios de Sellado de Tiempo** ofrecidos por Firmaprofesional y establecer las condiciones de uso, obligaciones y responsabilidades de las distintas entidades involucradas.

El citado Reglamento (UE 910/2014), recoge y regula la emisión de sellos de tiempos definiéndolos como "datos en formato electrónico que vinculan otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante".

Además , es intención de Firmaprofesional dotar a los sellos de tiempo emitidos la condición de "Sellos de Tiempo cualificados" cumpliendo los requisitos establecidos en el artículo 42 del Reglamento (UE) 910/2014.

Este documento se basa en la norma ETSI EN 319 421 "Policy and Security Requirements for Trust Service Providers issuing Time-Stamps" así como los perfiles son de acuerdo con la norma ETSI EN 319 422 "Time-stamping protocol and time-stamp token profiles".

Esta Política de Sellado de Tiempo 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:** | Política Servicio de Autoridad de Sellado de Tiempo (TSA) |
| **Versión:** | 201021 |
| **Descripción:** | Política de Servicio Cualificado de Sellado de Tiempo de la Autoridad de Sellado de Tiempo de Firmaprofesional (TSA) |
| **Fecha de Emisión:** | 21/10/2020 |
| **OIDs** | 0.4.0.2023.1.1 |
| **Localización** | http://www.firmaprofesional.com/cps |

# 2. Resumen

El sellado de tiempo (Time-stamping) es un mecanismo on-line que permite demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo.

Firmaprofesional es Autoridad de Sellado de Tiempo (TSA o Time-stamping Authority) que actúa como tercera parte de confianza testificando la existencia de dichos datos electrónicos en una fecha y hora concretos.

Los servicios de sellado de tiempo no son públicos, por lo que será necesario contratar el servicio previamente con Firmaprofesional. Los servicios de sellado de tiempo se comercializan en forma de paquetes anuales, limitando el número máximo de peticiones de sellado de tiempo que un cliente puede realizar anualmente.

Firmaprofesional ofrece dos servicios de Sellado de Tiempo diferentes:

- **Servicio de Sellado de Tiempo:** El cliente realiza una petición de sellado de tiempo según la norma RFC 3161 a una URL de Firmaprofesional, obteniendo como respuesta una evidencia digital firmada por la TSA de Firmaprofesional.

- **Servicio de Sellado de Tiempo con Custodia de Evidencias:** Firmaprofesional almacena y custodia una copia de cada evidencia digital generada y la pone a disposición del cliente en caso necesario.

Firmaprofesional no almacenará copias de los sellos de tiempo emitidos a menos que se contrate previamente el servicio de custodia de sellos de tiempo.

# 3. Definiciones y abreviaturas

## 3.1. Definiciones

- **Prestador de Servicios de Confianza:** persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica
- **Sello de Tiempo:** es un tipo especial de firma electrónica emitida por un prestador de servicios de confianza que permite garantizar la integridad de un documento en una fecha y hora determinadas.
- **Autoridad de Sellado de Tiempo:** entidad de confianza que emite sellos de tiempo.
- **Módulo Criptográfico Hardware:** módulo hardware utilizado para realizar funciones criptográficas y almacenar claves en modo seguro.
- **Función Hash:** es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales.
- **Listas de Certificados Revocados:** lista donde figuran las relaciones de certificados revocados.

## 3.2. Abreviaturas

| | |
|---|---|
| **CRL** | Certificate Revocation List |
| **FIPS** | Federal Information Processing Standards |
| **HSM** | Hardware Security Module |
| **IETF** | Internet Engineering Task Force |
| **PSC** | Prestador de Servicios de Confianza |
| **RFC** | Request for comment |
| **TSA** | Autoridad de Sellado de Tiempo |
| **TSP** | Protocolo de Sellado de Tiempo |
| **TST** | Token de sello de tiempo |
| **UTC** | Universal Time Coordinated |

# 4. Conceptos Generales

## 4.1. Autoridad de Sellado de Tiempo (TSA)

Una Autoridad de sellado de tiempo (TSA) es un Prestador de Servicios de Confianza que proporciona certeza sobre la preexistencia de determinados documentos electrónicos en un momento dado.

## 4.2. Servicio de Sellado de Tiempo

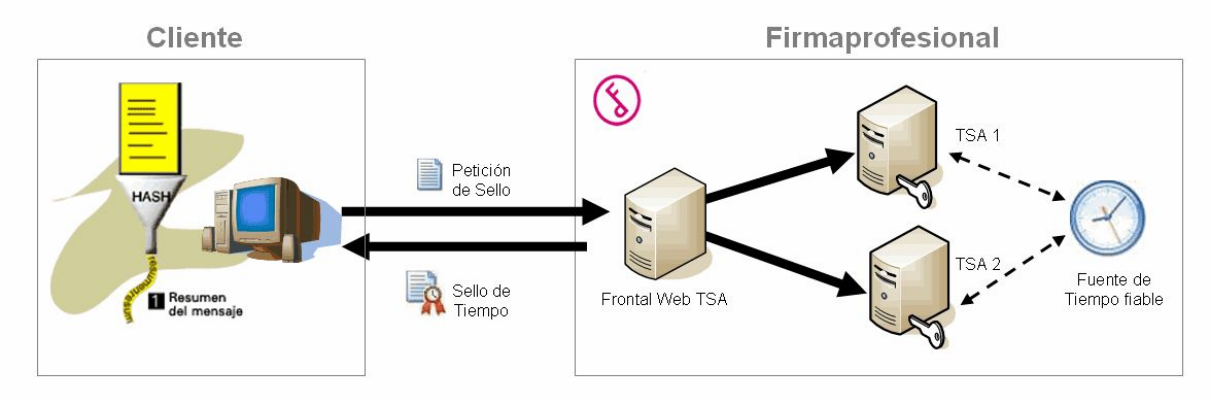
El sellado de tiempo (Time-stamping) es un mecanismo on-line que permite demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo.

El Servicio de Sellado de Tiempo de Firmaprofesional se basa en el uso del protocolo TSP sobre HTTP, definido en la norma ***RFC 3161 "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".***

Los pasos para generar un sello de tiempo son los siguientes:

- El cliente calcula el hash del documento a sellar.
- El cliente envía una solicitud de sello de tiempo a una URL determinada de Firmaprofesional siguiendo el protocolo RFC 3161 over HTTP, incluyendo el hash del documento a sellar.
- Firmaprofesional recibe la petición, realiza un control de acceso del cliente y revisa si la petición está completa y correcta.
- Si el resultado es correcto, la TSA firma la petición generando un Sello de Tiempo (incluyendo el hash del documento, la fecha y hora obtenida de una fuente fiable y la firma electrónica de la TSA).
- El sello de tiempo se envía de vuelta al Cliente.
- El Cliente debe validar la firma del sello y custodiarlo debidamente.

- Si se ha contratado el servicio de custodia, la TSA mantendrá un registro de las respuestas generadas a disposición del cliente para su futura verificación.




## 4.3. Clientes

Los clientes deben adaptar sus sistemas para poder realizar peticiones de sellado de tiempo mediante el protocolo TSP. Firmaprofesional no proporciona ningún software ni librerías de integración al cliente para realizar estas funciones.

Existen librerías públicas que implantan el protocolo TSP en diversos lenguajes de programación:

- **BouncyCastle** (http://www.bouncycastle.org): Conjunto de librerías criptográficas que implementan el protocolo TSP en los lenguajes Java y C#
- **OpenSSL** (http://www.openssl.org): La librería criptográfica OpenSSL implementa el protocolo TSP en lenguaje C.
- **IAIK:** Incluye librerías criptográficas en Java que implementan el protocolo TSP. Estas librerías son gratuitas únicamente para propósitos no comerciales
- **Adobe Reader:** La aplicación Adobe Reader permite validar sellos de tiempo incluidos en documentos PDF.
- **Prosign:** La herramienta de firma de PDFs ofrecida gratuitamente por Firmaprofesional permite incorporar sellos de tiempo a los documentos firmados.

# 5. Entidades Participantes

## 5.1. Prestadores de Servicios de Confianza (PSC)

Según el Reglamento (UE) 910/2014, se denomina Prestador de Servicios de Certificación (PSC) la persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianza.

Se denomina Prestador cualificado de servicios de confianza a aquél prestador de servicios de confianza que presta uno o varios servicios de confianza cualificados y al que el organismo de supervisión ha concedido la cualificación.

Firmaprofesional está incluida en la TSL española como prestador cualificado desde la entrada en vigor del Reglamento europeo el 1 de julio de 2016.

## 5.2. Autoridad de Sellado de Tiempo (TSA)

Firmaprofesional es un PSC que actúa como Autoridad de Sellado de Tiempo (TSA). Firmaprofesional ofrecerá los servicios de confianza por sí misma y por sus propios medios, sin delegarlos en ninguna otra entidad.

Firmaprofesional puede utilizar diferentes sistemas para generar sellos de tiempo, proporcionando alta disponibilidad al servicio.

## 5.3. Cliente

Los clientes son los usuarios del servicio, los cuales envían peticiones de sellado y reciben sellos de tiempo siguiendo el protocolo "RFC 3161 Time Stamp Protocol (TSP)".

Los servicios de Sellado de Tiempo de Firmaprofesional no son públicos. Para poder acceder a los servicios de sellado de tiempo, el Cliente deberá contratar previamente el servicio con Firmaprofesional.

## 5.3. Tercero que confía en los sellos de tiempo

El Reglamento (UE) 910/2014, recoge y regula la emisión de sellos de tiempos definiéndolos como "datos en formato electrónico que vinculan otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante".

Por lo tanto, cualquier usuario podrá validar los sellos de tiempo libremente basando en la confianza en Firmaprofesional como Prestador de Servicios Cualificados de Certificación que emite certificados cualificados.

# 6. Obligaciones y responsabilidades

## 6.1. Firmaprofesional

### 6.1.1. Obligaciones

Firmaprofesional, actuando como Autoridad de Sellado de Tiempo (TSA) se obliga a:

- Respetar lo dispuesto en esta Política de Sellado de Tiempo.
- Proteger sus claves privadas de forma segura.
- Emitir sellos de tiempo conforme a esta Política y a los estándares de aplicación.
- Garantizar que la hora y fecha incluidas en los sellos se mantienen dentro de los márgenes precisión establecida en el contrato entre el cliente y Firmaprofesional, que en ningún caso pueden ser superiores a un segundo[1].
- Emitir sellos de tiempo según la información enviada por el cliente y libres de errores de entrada de datos.
- Emitir sellos de tiempos cuyo contenido mínimo sea el definido por la normativa vigente, cuando sea aplicable.
- Publicar esta Política de Sellado de Tiempo
- Informar sobre las modificaciones de la Política a clientes y terceros que confían
- Establecer los mecanismos de generación de la información relevante en las actividades descritas, protegiéndolas ante pérdida, destrucción o falsificación.
- Custodiar los sellos de tiempo emitidos para los clientes que contraten el servicio de custodia

Firmaprofesional, en su actividad de prestación de servicios de confianza, responderá por el incumplimiento de lo establecido en esta Política de Sellado de Tiempo y, allí donde sea

[1] ETSI EN 319 421 V1.1.1 Ap 7.7.2.b; ETSI 102 023 v010201 5.1; ETSI 101 861 v010201 5.2.1

aplicable, por lo que dispone la Ley 59/2003, de 19 de diciembre, de firma electrónica o su normativa de desarrollo.

Sin perjuicio de lo anterior Firmaprofesional no garantizará los algoritmos y estándares criptográficos utilizados ni responderá de los daños causados por ataques externos a los mismos, siempre que hubiere aplicado la diligencia debida según el estado de la técnica en cada momento, y hubiere actuado conforme a lo dispuesto en las presentes Políticas de TSA y en la legislación vigente, donde sea aplicable.

### 6.1.2. Obligaciones para la emisión de sellos de tiempo cualificados

Cuando Firmaprofesional declara un sello de tiempo como cualificado siguiendo el Reglamento UE Nº 910/2014 (eIDAS), el certificado de clave pública de verificación de la firma es expedido bajo la política de certificados declarada en ETSI EN 319 411-2, que incorpora además los requerimientos de la ETSI EN 319 411-1.

Para indicar que los sellos de tiempo son cualificados, Firmaprofesional incorpora el campo "Time-stamp policy" el OID recogido en la norma 0.4.0.2023.1.1

Firmaprofesional emite los sellos electrónicos cualificados por medio de una TSU exclusivamente para éstos, y no emite sellos electrónicos no cualificados desde la misma TSU. Para ello dispondrá de otra TSU.[2]

### 6.1.3. Responsabilidad Financiera

Firmaprofesional será responsable de los perjuicios causados de forma deliberada o por negligencia a cualquier persona física o jurídica en razón del incumplimiento de las obligaciones establecidas en el Reglamento[3] (UE) nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014.

### 6.1.4. Exoneración de responsabilidad

Firmaprofesional no será responsable en ningún caso cuando se encuentre ante cualquiera de estas circunstancias:

[2] De acuerdo con ETSI EN 319 421 v1.1.1 Ap 8.2

[3] De acuerdo con el artículo 13 del Reglamento ReIDAS.

- Estado de guerra, desastres naturales, funcionamiento defectuoso de los servicios eléctricos, las redes telemáticas y/o telefónicas o de los equipos informáticos utilizados por el Cliente o por los Terceros, o cualquier otro caso de fuerza mayor.
- Por el uso indebido o fraudulento de los sellos de tiempo.
- Por el uso indebido de la información contenida en el Certificado o en la CRL.
- Por el contenido de los mensajes o documentos sellados.
- En relación a acciones u omisiones del Cliente:
    - Negligencia en la conservación de sus datos de acceso al servicio de sellado de tiempo, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación.
    - Extralimitación en el uso del sello de tiempo, según lo dispuesto en la normativa vigente y en la presente Política de TSA.
- En relación a acciones u omisiones del Usuario, tercero que confía en el certificado:
    - Falta de comprobación de la suspensión o pérdida de vigencia del certificado electrónico de la TSA publicada en el servicio de consulta sobre la vigencia de los certificados o falta de verificación de la firma electrónica.
- Por actuaciones de personas, entidades u organismos que, sin suscribir un contrato con Firmaprofesional procedan a realizar estos servicios para terceros. Todo ello sin perjuicio de las acciones legales que pudieran corresponder.

### 6.1.5. Cese de la actividad de la TSA

Antes del cese de su actividad la TSA realizará las siguientes actuaciones:

- Informará a todos los suscriptores, usuarios o entidades con los cuales tenga acuerdos u otro tipo de relación del cese con la anticipación mínima de 2 meses, o el periodo que establezca la legislación vigente.
- Revocará toda autorización a entidades subcontratadas para actuar en nombre de la TSA en el procedimiento de emisión de sellos de tiempo.

- Informará a la administración competente, con la antelación indicada, el cese de su actividad y el destino que se vaya a dar a los sellos de tiempo emitidos hasta la fecha, especificando, en su caso, si se va a transferir la gestión y a quien.
- Revocará los certificados de las TSU.[4]

## 6.2. Cliente

El Cliente estará obligado a cumplir con lo dispuesto por la normativa y además a:

- Respetar lo dispuesto en los documentos contractuales firmados con la TSA.
- Verificar la corrección de la firma digital del sello de tiempo y la validez del certificado de la TSA en el momento de firmarlo.
- Verificar que el hash contenido en el sello de tiempo coincide con el que envió.
- Almacenamiento y conservación de los sellos de tiempo entregados por la TSA. Es responsabilidad del Cliente almacenar los sellos de tiempo, si prevé que le serán necesarios en el futuro.

## 6.3. Tercero que confía en los sellos de tiempo

Será obligación de los Usuarios cumplir con lo dispuesto por la normativa vigente y además:

- Verificar la corrección de la firma del sello de tiempo y la validez del certificado de la TSA en el momento de firmarlo.

[4] De acuerdo con ETSI EN 319 421 v1.1.1 AP 7.14

# 7. Requerimientos operacionales

## 7.1. Control de acceso

Firmaprofesional realizará un control de acceso al servicio basado en direcciones IP, por lo tanto el Cliente deberá informar a Firmaprofesional de las direcciones IP desde donde se realizarán las peticiones.

Alternativamente se ofrece un control de acceso basado en usuario y contraseña para entornos con IPs dinámicas.

## 7.2. Obtención del tiempo fiable

Como fuente fiable de tiempo, Firmaprofesional dispone de un Reloj Atómico de Rubidio modelo **SyncServer 600** con una precisión garantizada por el fabricante de un desfase inferior a 1 microsegundo al día. El reloj atómico se sincroniza por GPS, permitiendo un nivel de confianza de STRATUM 1. Adicionalmente se realiza una sincronización de tiempos con el ROA mediante el Protocolo NTP a través de Internet (RFC 1305 Network Time Protocol)

La Sección de Hora del **Real Instituto y Observatorio de la Armada en San Fernando (ROA)** tiene como misión principal el mantenimiento de la unidad básica de Tiempo, declarado a efectos legales como Patrón Nacional de dicha unidad, así como el mantenimiento y difusión oficial de la escala "Tiempo Universal Coordinado" (UTC), considerada a todos los efectos como la base de la hora legal en todo el territorio nacional (Real Decreto 1308/1992, de 23 de octubre, por el que se declara al Laboratorio del Real Instituto y Observatorio de la Armada como laboratorio depositario del Patrón Nacional de Tiempo y laboratorio asociado al Centro Español de Metrología.). Para ello se colabora con el Consejo Superior de Investigaciones Científicas (CSIC), controlando y monitorizando la sincronización de las máquinas principales de distribución de tiempo en España, tres de las cuales (dos localizadas en el INSOB y una tercera en Madrid) pertenecen a la Sección.

## 7.3. Tiempo de Custodia

Para el caso del **Servicio de Sellado de Tiempo** sin custodia no se garantiza la custodia de las respuestas enviadas. Será responsabilidad del cliente custodiarlas de manera adecuada.

## 7.4. Solicitud de Sellos de Tiempo

Las solicitudes de sellos se adherirán a la sintaxis de la especificación **"RFC 3161 Time Stamp Protocol (TSP)"** descrito en el Apartado 3.4. "Time-Stamp Protocol via http" de la especificación, con las restricciones de la norma ETSI TS 101 861.

La URL del servicio de Sellado de Tiempo de Firmaprofesional sin custodia de sellos es:

http://servicios.firmaprofesional.com/tsa

La URL del servicio de Sellado de Tiempo de Firmaprofesional con custodia de sellos es:

http://servicios.firmaprofesional.com/tsadb

## 7.5. Funciones HASH

El servicio soporta los siguientes algoritmos de Hash en las peticiones. GOST3411, SHA1, SHA224, SHA256, SHA384, SHA512, RIPEMD128, RIPEMD160, RIPEMD256.

Se recomienda no utilizar el algoritmo SHA1 ya que se considera poco seguro. La guía CCN-CERT 807, para enero de 2017, recomienda el uso de los algoritmos SHA-256, SHA-384 y SHA-512.

En las respuestas de los sellos de tiempo se utiliza el algoritmo SHA256.

## 7.6. Formato de las solicitudes

El formato de envío de las solicitudes sigue el siguiente esquema:

***Content type: application/timestamp-query***

***Method: POST***

***Content-length:*** ***required***

<<Contiene la solicitud de sello de tiempo en ASN.1, codificado en DER>>

Los campos opcionales según la especificación RFC 3161 se tratan de la siguiente manera:

| Campo | Tratamiento |
|---|---|
| nonce | Opcional. Si está presente, la respuesta contiene el mismo valor. |
| reqPolicy | Sin uso |
| certReq | Sin uso |
| extensions | Sin uso |

## 7.7. Formato de las respuestas

Si la solicitud no se puede procesar, se devuelve una respuesta http indicando un código de error cuando no puede responder con un time-stamp. Los posibles errores son:

| Causa | Error | Descripción |
|---|---|---|
| Falta el campo content-length | 411 | CONTENT_LENGTH REQUIRED |
| Content-length demasiado grande | 413 | REQUEST ENTITY TOO LARGE |
| Content-type incorrecto | 415 | UNSUPPORTED MEDIA TYPE |
| Los datos no son un time-stamp request | 400 | BAD REQUEST |
| Servidor no responde | 500 | SERVER INTERNAL ERROR |

Si accede a la URL del servicio con un navegador o utilizando el método GET, el servidor mostrará una página web informando del error (y devolverá un Código 200).

Las respuestas se envían en el siguiente formato:

***Content type:*** ***application/timestamp-reply***

***Method:*** ***POST***

***Content-length:*** ***required***

<<Contiene la respuesta de sello de tiempo en ASN.1, codificado en DER >>

Los campos opcionales según la especificación RFC 3161 se tratan de la siguiente manera:

| Campo | Tratamiento |
|---|---|
| Time-stamp policy | 0.4.0.2023.1.1 |
| ordering | Falso |
| nonce | Si la petición lo contiene se devuelve el mismo valor<br>Si no, se crea uno nuevo |

| | |
|---|---|
| Certificados adjuntos | <Certificado de TSA><br><Certificado de CA Subordinada> |
| accuracy | No presente |
| tsa | No presente |
| extensions | No presente |

## 7.8. Control por Pérdida de Calibración

Firmaprofesional monitoriza la correcta calibración del reloj de su TSU. En caso de detectar una desviación superior a la establecida en la presente política el servicio de TSA se detendrá automáticamente.

## 7.9. Certificado de TSA

### 7.9.1. Generación del Certificado

Para la generación del certificado de Autoridad de Sellado de Tiempo, se sigue la ***Política de Certificación de Servicio Seguro*** de Firmaprofesional (OID 1.3.6.1.4.1.13177.10.1.4.1), disponible en la dirección http://www.firmaprofesional.com/cps.

Las claves privadas[5] de la TSA se generan y custodian en un dispositivo criptográfico seguro (HSM) que cumple los requerimientos que se detallan en FIPS 140-2 nivel 2 o superior, o con un nivel EAL 4+ o superior de acuerdo con ISO/IEC 15408.

Firmaprofesional puede disponer de diversas TSA para garantizar la alta disponibilidad del servicio de sellado de tiempo.

Los certificados TSA utilizados tendrán una longitud mínima de 2048 bits, una duración de 6 años y, establecido en esta política, una duración de las claves de 3 años desde el momento de inicio de validez del certificado asociado.

En la utilización de sellos de tiempo para procedimientos de nivel alto del Esquema Nacional de Seguridad se seguirán las indicaciones de la norma de seguridad CCN-STIC-807.

[5] De acuerdo con ETSI EN 319 421 v1.1.1 Ap 7.6.2

### 7.9.2. Publicación del certificado

El certificado de la TSA se adjunta en la respuesta de cada Sellado de Tiempo que se emite. El certificado del servicio TSA Cualificado está publicado en: http://crl.firmaprofesional.com/tsa/tsa.crt

### 7.9.3. Cambio de certificado de TSA

Se establecen los controles para garantizar la renovación de las claves antes de la extinción de su vigencia.

El certificado de la TSA puede ser cambiado en cualquier momento por otro certificado de TSA igualmente válido según la ***Política de Certificación de Servicio Seguro*** de Firmaprofesional.

Este cambio no se comunicará a los usuarios del servicio, los cuales deberían confiar en todos los sellos emitidos por Firmaprofesional y firmados con certificados válidos de TSA dentro de la jerarquía de certificación.

Las claves asociadas serán destruidas de forma que no puedan ser recuperadas, conforme a las instrucciones del fabricante del HSM que las genera y alberga.

### 7.9.4. Certificado de TSA en Producción

El certificado de la TSA utilizado en producción tiene los siguientes valores:

| Campo | Valor |
|---|---|
| Subject | CN = FIRMAPROFESIONAL CLOUD QUALIFIED TSU - 2020<br>organizationIdentifier = VATES-A62634068<br>O = Firmaprofesional S.A.<br>C = ES |
| Issuer | CN = AC Firmaprofesional - CUALIFICADOS<br>SERIALNUMBER = A62634068<br>OU = Certificados Cualificados<br>O = Firmaprofesional S.A.<br>C = ES |
| S/N | 487cc77aacc40a8c693f98d4f217071d |
| Validity | notBefore: 06 agosto 2020 12:39:33<br>notAfter: 05 agosto 2026 12:39:33 |
| Private Key Usage Period | 3 años |
| Hash SHA1 | 0DE5286CD35DF67528E6E6FFAC3A380996C8F419 |

El certificado de la TSA utilizado anteriormente en producción tiene los siguientes valores:

| Campo | Valor |
|---|---|
| Subject | CN = FIRMAPROFESIONAL CLOUD QUALIFIED TSU<br>organizationIdentifier = VATES-A62634068<br>O = Firmaprofesional S.A.<br>C = ES |
| Issuer | CN = AC Firmaprofesional - INFRAESTRUCTURA<br>SERIALNUMBER = A62634068<br>OU = Security Services<br>O = Firmaprofesional S.A.<br>C = ES |
| S/N | 71 8d 3d 05 8e 49 40 29 5d 5a a0 22 df 53 08 55 |
| Validity | notBefore: 06 febrero 2020 10:39:13<br>notAfter: 04 febrero 2026 10:39:13 |
| Private Key Usage Period | 3 años |
| Hash SHA1 | 4a f1 30 53 81 ea 97 04 59 c7 b9 16 c0 e2 35 1b 88 30 52 1e |

| Campo | Valor |
|---|---|
| Subject | CN = FIRMAPROFESIONAL CLOUD QUALIFIED TSU<br>organizationIdentifier = VATES-A62634068<br>O = Firmaprofesional S.A.<br>C = ES |
| Issuer | CN = AC Firmaprofesional - INFRAESTRUCTURA<br>SERIALNUMBER = A62634068<br>OU = Security Services<br>O = Firmaprofesional S.A.<br>C = ES |
| S/N | 55 81 05 6f d6 3c f7 b7 |
| Validity | notBefore: lunes, 27 de febrero de 2017 14:19:33<br>notAfter: domingo, 26 de febrero de 2023 14:19:33 |
| Private Key Usage Period | 3 años |
| Hash SHA1 | cb 2c 8d 8c df f2 aa 58 00 6f b1 ea c5 71 a4 86 96 5c fe b2 |

firmaprofesional

Firmaprofesional, S.A.

Octubre de 2020