PRESTADOR DEL SERVICIO DE CERTIFICACION DEL CORPME

SERVICIO DE SELLADO DE TIEMPO
DECLARACIÓN DIVULGACIÓN TSA

El presente documento constituye un extracto de los derechos y obligaciones contenidos en las Prácticas y Políticas de Sellado de Tiempo del Colegio de Registradores de la Propiedad y Mercantiles de España (en adelante CORPME) y aplica a los **Servicio de Sellado de Tiempo**. Esta Declaración de Divulgación resume lo dispuesto en las Prácticas y Políticas de Sellado de Tiempo publicada.

Los efectos legales del servicio, así como los derechos y obligaciones asociados al mismo, se interpretarán en todo caso atendiendo a la legislación vigente, Prácticas y Políticas de Sellado de Tiempo en la versión obrante en cada momento en la siguiente URL: http://pki.registradores.org/normativa/index.htm.

Antes de hacer uso del servicio, se recomienda leer la presente Declaración de Divulgación, al objeto de valorar adecuadamente la confianza que ofrece. No se podrá alegar la ignorancia de esta Declaración de Divulgación para eximirse de las responsabilidades propias ni para exigirlas a otra parte.

1. Información de contacto del Prestador de Servicios de Confianza

Colegio de Registradores de la Propiedad y Mercantiles de España.

Prestador del Servicio de Certificación del CORPME.

C/ DIEGO DE LEON, 21.

28006-MADRID

Teléfono: 902181442 / 912701699

Email: psc@registradores.org

Web: http://pki.registradores.org/normativa/index.htm

2. Descripción del 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 CORPME es una 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.

Actualmente, la TSA está compuesta de una única Unidad de Sellado de Tiempo (TSU o Time Stamping Unit) que emite los sellos de tiempo bajo la política con OID 1.3.6.1.4.1.17276.0.3.1.1 descrita en las Prácticas y Políticas de Sellado de Tiempo.

La TSA garantiza que la hora y fecha incluidas en los sellos se mantienen dentro de los márgenes de precisión de la referencia temporal proporcionada por la Sección de Hora del Real Instituto y Observatorio de la Armada en San Fernando, que en ningún caso podrán superar una desviación máxima de un segundo. Por lo tanto, la TSA del CORPME proporciona una precisión de un segundo.

El CORPME ofrece el servicio de Sellado de Tiempo de la siguiente forma:

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

3. Límites de uso

La TSA del CORPME permite generar sellos de tiempo sobre cualquier tipo de documento u objeto, con o sin firma electrónica de cualquier tipo.

Los algoritmos de HASH admitidos son: SHA-1 (no recomendado), SHA-224, SHA-256, SHA-384, SHA-512.

Los servicios de sellado de tiempo no son gratuitos, por lo que será necesario contratar el servicio previamente con CORPME. Los servicios de sellado de tiempo se podrán comercializar bajo la limitación temporal que se acuerde y/o de número de peticiones de sellado de tiempo. En todo caso, las condiciones de facturación de la TSA son revisadas, garantizando que no se aplican cargas adicionales a las establecidas en los contratos.

Para poder acceder a los servicios de sellado de tiempo, el Cliente deberá contratar previamente el servicio con el CORPME.

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

El cliente debe adaptar sus sistemas al protocolo TSP para poder realizar peticiones de sellado de tiempo. El servicio de sellado de tiempo ofrecido por el CORPME no proporciona ningún software ni librerías de integración al cliente. Para adaptar los sistemas, 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#
- **OpenTSA** (http://www.opentsa.org): Es una ampliación de la librería criptográfica OpenSSL que implementa el protocolo TSP en lenguaje C.
- **Digistamp** (http://digistamp.com/toolkitDoc/MSToolKit.htm): Toolkit basado en la librería criptográfica CryptoAPI de Microsoft que implementa el protocolo TSP en Visual Basic
- **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 8 permite validar sellos de tiempo incluidos en documentos PDF.

Cualquier documento firmado de los que se deriven derechos y obligaciones para los intervinientes en el PSC del CORPME, así como los registros de auditoría asociados, se almacenarán durante un periodo mínimo de quince (15) años.

El CORPME utilizará diferentes sistemas para generar sellos de tiempo, proporcionando alta disponibilidad al servicio. Además, el servicio de información del estado de certificados, en sus dos variantes (CRL's y OCSP), está disponible 24 horas todos los días del año, tanto para los terceros que confían como para los titulares de los certificados u otras partes que los requieran.

4. Obligaciones del 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.

5. Obligaciones de las terceras partes

Será obligación de los terceros que confían en los sellos de tiempo es 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.

6. Limitaciones de responsabilidad

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

- 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.
- Falta de veracidad de la información suministrada para emitir el sello.
- 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 las Prácticas y Políticas de la 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.

7. Acuerdos aplicables y Prácticas y Políticas de Sellado de Tiempo

Las Prácticas y Políticas de Sellado de Tiempo, publicada en la dirección http://pki.registradores.org/normativa/index.htm, recogen la información pública y características del Servicio de Sellado de Tiempo del CORPME como PSC, recogiendo las obligaciones y procedimientos que se compromete a cumplir en relación con dicho servicio.

Las actividades que el CORPME pueda subcontratar para llevar a cabo su actividad como PSC se desarrollan según lo establecido en sus Prácticas y Políticas de Sellado de Tiempo y en los contratos y acuerdos formalizados con las entidades que realizan tales actividades. En estos casos, el acceso a la información propiedad del CORPME por parte de terceros sigue el protocolo definido en la Declaración de Prácticas de Certificación de esta entidad, publicada en la dirección http://pki.registradores.org/normativa/index.htm, en cuanto a la identificación de riesgos, establecimiento de controles de seguridad para proteger el acceso a la información y la formalización de los correspondientes acuerdos de confidencialidad y, si procede, el contrato para el tratamiento de datos de carácter personal en cumplimiento de la normativa vigente.

8. Política de reembolso

Los servicios de sellado de tiempo se reembolsarán bajo las condiciones establecidas en cada tipo de contrato.

9. Ley aplicable, quejas y resolución de disputa

Las operaciones y funcionamiento del PSC del CORPME, así como las Prácticas y Políticas de Sellado de Tiempo, estarán sujetas a la normativa que les sea aplicable y en especial a:

- Directiva 1999/93/CE, del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la Firma Electrónica.
- Reglamento UE 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.
- Ley 59/2003, de 20 de diciembre, de Firma Electrónica.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

Todas las reclamaciones entre usuarios y CORPME deberán ser comunicadas por la parte en disputa al CORPME, con el fin de intentar resolverlo entre las mismas partes.

Para la resolución de cualquier conflicto que pudiera surgir con relación a la prestación de servicios de certificación, las partes, con renuncia a cualquier otro fuero que pudiera corresponderles, se someten a los Juzgados y Tribunales españoles, con independencia del lugar dónde se hubieran utilizado los certificados emitidos.

10. Licencias y repositorio, marcas confiables y auditoría

El CORPME, como PSC, mantiene varias acreditaciones y certificaciones de sus servicios de confianza, de las cuales aplican específicamente al Servicio de Sellado de Tiempo:

- ETSI EN 319 421 “Policy and Security Requirements for Trust Service Providers issuing Time-Stamps” y ETSI EN 319 422 “Time-stamping protocol and time-stamp token profiles”.

Puede comprobarse la inclusión de los certificados cualificados expedidos por el CORPME en la lista de prestadores de servicios de confianza (TSL) de España, a través del siguiente enlace:

https://sede.minetur.gob.es/es-ES/datosabiertos/catalogo/lista-prestadores-tsl.

Asimismo, el CORPME está registrado como prestador cualificado en el Ministerio de Energía, Turismo y Agenda Digital:

http://www.minetad.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/Prestadores.aspx

Conforme a lo establecido en el Reglamento UE nº 910/2014, el CORPME realizará auditorías bienales de conformidad con dicho Reglamento.

Madrid, Junio de 2017.