COLEGIO DE REGISTRADORES DE LA PROPIEDAD Y MERCANTILES DE ESPAÑA

SCR Servicio de Certificación de los Registradores

Renovación de la Solución PKI del Colegio de Registradores

Política de Sellado de Tiempo del Colegio de Registradores

CONTROL DOCUMENTAL

DOCUMENTO/ARCHIVO	
Título: **Políticas de Sellado de Tiempo**	Nombre Archivo/s:
Código:	Soporte lógico:
Fecha: **27/10/2010**	Ubicación física:
Versión: **Versión 1.0**	

REGISTRO DE CAMBIOS		
Versión	Fecha	Motivo del cambio
1.0		Versión inicial

DISTRIBUCIÓN DEL DOCUMENTO	
Nombre	Área

CONTROL DEL DOCUMENTO			
PREPARADO	**REVISADO**	**APROBADO**	**ACEPTADO**

ÍNDICE

1. INTRODUCCIÓN

El Servicio de Certificación del Colegio de Registradores (en adelante SCR), órgano del Colegio de Registradores de la Propiedad, Mercantiles y de Bienes Muebles de España (en adelante CORPME) como Prestador de Servicios de Certificación que emite certificados reconocidos según la Ley 59/2003 de 19 de diciembre de firma electrónica, también ofrece servicios de Sellado de Tiempo.

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

La Ley 59/2003 de Firma Electrónica no recoge ni regula la emisión de sellos de tiempos. Sin embargo, es intención del CORPME dotar a los sellos de tiempo emitidos la condición de “Sellos de Tiempo reconocidos” equivalente a la condición de “Firmas electrónicas reconocidas”, en la medida que esto sea posible y comprometiéndose a cumplir con la legislación aplicable en cada caso.

Esta Política de Sellado de Tiempo está subordinada al cumplimiento de las Condiciones Generales expuestas en la **Declaración de Prácticas de Certificación (DPC)** del CORPME.

1.1. RESUMEN

El sellado de tiempo (Timestamping) 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 Timestamp 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 gratuitos, por lo que será necesario contratar el servicio previamente con el 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.
.

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 del CORPME.

- **Servicio de Custodia de Sellos de Tiempo**: El CORPME almacena y custodia una copia de cada evidencia digital generada y la pone a disposición del cliente en caso necesario.

1.2. DEFINICIONES Y ABREVIATURAS

1.2.1. Definiciones

- **Prestador de Servicios de Certificación**: 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 tercero 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 o suspendidos.

1.2.2. Abreviaturas

PSC Prestador de Servicios de Certificación

TSA Autoridad de Sellado de Tiempo

TSP Protocolo de Sellado de Tiempo

TST Token de sello de tiempo

IETF Internet Engineering Task Force

CEN Comité Europeo de Normalización

FIPS Federal Information Processing Standards

CWA CEN Workshop Agreement

RFC Request for comment

UTC Universal Time Coordinated

CRL Certificate Revocation List

HSM Hardware Security Module

2. CONCEPTOS GENERALES

2.1. SERVICIO DE SELLADO DE TIEMPO

El sellado de tiempo (Timestamping) 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.

La implementación de la política de sellado de tiempo se debe cumplir con el protocolo 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 del CORPME siguiendo el protocolo RFC 3161, incluyendo el hash del documento a sellar
- El CORPME recibe la petición, revisa si la si la petición está completa y correcta y realiza un control de acceso en función de la IP del cliente.
- 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.
- La TSA mantendrá un registro de los sellos emitidos para su futura verificación durante al menos 5 años.

2.2. AUTORIDAD DE SELLADO DE TIEMPO (TSA)

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

2.3. CLIENTES

Los clientes son los usuarios del servicio, los cuales envían peticiones de sellado y reciben sellos de tiempo siguiendo el protocolo RFC3161 Time Stamp Protocol (TSP).

Los clientes deben adaptar sus sistemas para poder realizar peticiones de sellado de tiempo. 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.

3. POLITICA DE SELLADO DE TIEMPO

3.1. VISTA INICIAL

Los servicios de sellado de tiempo no son gratuitos, por lo que será necesario contratar el servicio previamente con el CORPME. Los servicios de sellado de tiempo se podrán comercializar bajo la limitación temporal y/o de número de peticiones de sellado de tiempo que se acuerde.

El CORPME 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 del CORPME (**http://tsa.registradores.org o https://tsa.registradores.org**), obteniendo como respuesta una evidencia digital firmada por la TSA del CORPME.

- **Servicio de Custodia de Sellos de Tiempo**: El CORPME almacena y custodia una copia de cada evidencia digital generada y la pone a disposición del cliente en caso necesario.

La política de sellado de tiempo del CORPME de basa en los estándares:

- RFC 3161 “Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)”.

- ETSI TS 101 862, Qualified Certificate Profile

- CWA 14167 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements.

3.2. IDENTIFICACIÓN DE LA POLÍTICA DE SELLADO DE TIEMPO

Nombre del documento	Política de Sellado de Tiempo del Colegio de Registradores
Versión del documento	1.0
Estado del documento	Versión
Fecha de emisión	20/12/2010
Fecha de expiración	No aplicable
OID (Object Identifier)	1.3.6.1.4.1.17276.0.3
Ubicación de la PC	http://pki.registradores.org/normativa/index.htm
DPC Relacionada	Declaración de Prácticas de Certificación del Servicio de Certificación del CORPME

3.3. ENTIDADES PARTICIPANTES

3.3.1. Prestador de servicios de certificación (PSC)

Según la Ley de Firma Electrónica, se denomina Prestador de Servicios de Certificación (PSC) la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.

3.3.2. Autoridad de Sellado de Tiempo (TSA)

El Servicio de Certificación del Colegio de Registradores (SCR), órgano del El CORPME, es un PSC que actúa como Autoridad de Sellado de Tiempo (TSA). El CORPME ofrecerá los servicios de certificación por a través del SCR, sin delegarlos en ninguna otra entidad.

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

3.3.3. Cliente

Los servicios de Sellado de Tiempo del CORPME no son públicos ni gratuitos. 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 deberá adaptar sus sistemas al protocolo TSP. El servicio de sellado de tiempo ofrecido por el CORPME no proporciona ningún software ni librerías de integración al cliente.

3.3.4. Tercero que confía en los sellos de tiempo

La Ley 59/2003 de Firma Electrónica no recoge ni regula la emisión de sellos de tiempos. Sin embargo, es intención del CORPME dotar a los sellos de tiempo emitidos la condición de “Sellos de Tiempo reconocidos” equivalente a la condición de “Firmas electrónicas reconocidas”, en la medida que esto sea posible y comprometiéndose a cumplir con la legislación aplicable en cada caso.

Por lo tanto, cualquier usuario podrá validar los sellos de tiempo libremente basándose en la confianza en el CORPME como Prestador de Servicios de Certificación que emite certificados reconocidos.

4. OBLIGACIONES Y RESPONSABILIDADES

4.1. SERVICIO DE CERTIFICACION DE LOS REGISTRADORES

4.1.1. Obligaciones

El CORPME, 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 el CORPME, que en ningún caso pueden ser superiores a un segundo.
- 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 de Sellado de Tiempo a clientes y terceros que confían en los sellos de tiempo.
- Establecer los mecanismos de generación y custodia 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 sellado de tiempo durante 5 años.

El CORPME, en su actividad de prestación de servicios de certificación, responderá por el incumplimiento de lo establecido en esta Política de Sellado de Tiempo y, allí donde sea 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 el CORPME 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.

4.1.2. Responsabilidad financiera

No aplicable por no tratarse de un servicio de emisión de certificados reconocidos según lo estipulado en la Ley de 59/2003 de Firma electrónica. La TSA no se hace responsable en caso de pérdidas por transacciones.

4.1.3. Exoneración 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 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.

4.1.4. Cese de 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.

4.2. 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.

4.3. TERCERO QUE CONFIA 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 firma.

5. REQUERIMIENTOS OPERACIONALES

5.1. OBTENCION DEL TIEMPO FIABLE

El CORPME 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(ROA)), considerada a todos los efectos como la base de la hora legal en todo el territorio nacional (R. D. 23 octubre 1992, núm. 1308/1992). Para ello se establece un proyecto de investigación por medio de la constitución de un Laboratorio de Tiempo en la sede del Real Observatorio desde el que se obtenga, trate y controle por medios informáticos la calidad del tiempo, que se enviará, a través de un canal de comunicación exclusivo y dedicado al Servicio de Sistemas de Información del Colegio de Registradores en Madrid, y desde el cual es distribuido.

5.2. CERTIFICADO DE TSA

5.2.1. Generación del certificado de TSA

El proceso de emisión de Certificado de Sellado de Tiempo (TSA) se realizarán de manera manual siguiendo las máximas garantías de seguridad en el proceso.

El certificado de Sellado de Tiempo (TSA) se emite y revoca por la Unidad de Tramitación Central, a petición de la Comisión Directora.

Siguiendo la política de certificación, el certificado de TSA ha de ser emitido por las CA´s Subordinadas del CORPME bajo el OID 1.3.6.1.4.1.17276.0.3

La estructura del certificado, referente a la extensión *subject* del certificado, es la que se describe en la siguiente tabla:

Campo	Valor	Descripción
C	ES	País
O	Colegio de Registradores de la Propiedad y Mercantiles de España	Organización
OU	Certificado Propio	
CN	Registradores de España - TSA	Nombre del Registro

Los campos más relevantes del certificado de TSA de del CORPME son:

Campo	Contenido Propuesto	Crítica	Observaciones
1. Certificate Policies	Se utilizará	NO	
Policy Identifier	2.5.29.32.0		
Notice Referente	Certificado sujeto a la DPC del CORPME, dirección prestador http://pki.registradores.org/normativa/direccion.html		
2. Subject Alternative Names	**Rfc822Name** = dirección correo electrónico	NO	[RFC3280]: Conforming implementations generating new certificates with electronic mail addresses MUST use the rfc822Name in the subject alternative name field (section 4.2.1.7) to describe such identities. Simultaneous inclusion of the EmailAddress attribute in the subject distinguished name to support legacy implementations is deprecated but permitted.
3. CRLDistributionPoints	**(1) HTTP:** http://pki.registradores.org/ /crls/crl_int_scr.crl **(2) LDAP:** ldap://ldap.registradores.org/ CN=CA%20INTERNA, OU=CERTIFICADO%20PROPIO, O=COLEGIO%20DE%20REGISTRADORES, C=ES ?certificateRevocationList?base ?objectclass=cRLDistributionPoint	NO	
4. Auth. Information	**OCSP:** https://ocsp.registradores.org/ **CA Raíz:** http://pki.registradores.org/ /certificados/ca_raiz_scr.crt	NO	

5. KeyUsage	Firma digital, Acuerdo de claves, Asegura la identidad.	SI	
6. Extented KeyUsage OID	1.3.6.1.5.5.7.3.8 (Firma de Sellos de Tiempo).	SI	

Las claves privadas de la TSA se generan y custodian en un dispositivo criptográfico seguro que cumple los requerimientos que se detallan en FIPS 140-3 nivel 3 y FIPS 140-2 nivel 3 en su caso.

El CORPME puede disponer de diversas TSA's para garantizar la alta disponibilidad del servicio de sellado de tiempo.

5.2.2. Publicación del certificado de TSA

El certificado de la TSA se adjunta en la respuesta de cada Sellado de Tiempo que se emite.

5.2.3. Cambio de certificado de TSA

El certificado de la TSA puede ser cambiado en cualquier momento por otro certificado de TSA igualmente válido según las ***Políticas de Certificación de Certificados*** del CORPME.

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

Por lo tanto, un usuario únicamente necesita confiar en el certificado de CA Root y las CA´s del CORPME para validar las firmas.

5.3. SOLICITUD DE SELLOS DE TIEMPO

Las solicitudes de sellos se adherirán a la sintaxis de la especificación "***RFC3161 Time Stamp Protocol (TSP)***" descrito en el Apartado 2.3. "Time-Stamp Protocol " de la especificación, con las restricciones de la norma ETSI TS 101 862.

Según disponga el CORPME las URLs del servicio de Sellado de Tiempo podrán ser:

http://tsa.registradores.org

O bien

https://tsa.registradores.org

Los algoritmos admitidos son SHA-1 y MD5.

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

```
TimeStampReq ::= SEQUENCE {
        Version INTEGER { v1(1) },
        messageImprint      MessageImprint,
        reqPolicy           TSAPolicyId             OPTIONAL,
        nonce               INTEGER                 OPTIONAL,
        certReq             BOOLEAN                 DEFAULT FALSE,
        extensions          [0]IMPLICIT Extensions  OPTIONAL }


MessageImprint ::= SEQUENCE {
        hashAlgorithm       AlgorithmIdentifier,
        hashedMessage       OCTET STRING }
```

5.4. RESPUESTA A LA SOLICITUD DE SELLOS DE TIEMPO

El formato de respuesta es el siguiente:

```
TimeStampResp ::= SEQUENCE {
        Status              PKIStatusInfo,
        timeStampToken      TimeStampToken      OPTIONAL }


PKIStatusInfo ::= SEQUENCE {
        status PKIStatus,
        statusString PKIFreeText OPTIONAL,
        failInfo PKIFailureInfo OPTIONAL
}
PKIStatus ::= INTEGER {
        granted (0),
        grantedWithMods (1)
        rejection (2),
        waiting (3),
        revocationWarning (4),
        revocationNotification (5)

}
PKIFailureInfo ::= BIT STRING {
        badAlg (0),
        badRequest (2),
        badDataFormat (5),
         timeNotAvailable (14),
        unacceptedPolicy (15),
```

```
        unacceptedExtension (16),
        ddInfoNotAvailable (17)
        ystemFailure (25)
}

TimeStampToken ::= ContentInfo
        -- contentType is id-signedData as defined in [CMS]
        -- content is SignedData as defined in([CMS])
        -- eContentType within SignedData is id-ct-TSTInfo
        -- eContent within SignedData is TSTInfo


id-ct-TSTInfo OBJECT IDENTIFIER ::= { iso(1) member-body(2)
us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) ct(1) 4}


TSTInfo ::= SEQUENCE {
        Version         INTEGER { v1(1) },
        policy          TSAPolicyId,
        messageImprint   MessageImprint,
        serialNumber    INTEGER,
        genTime         GeneralizedTime,
        accuracy        Accuracy                OPTIONAL,
        ordering        BOOLEAN                 DEFAULT FALSE,
        nonce           INTEGER                 OPTIONAL,
        tsa             0]GeneralName           OPTIONAL,
        extensions      [1]IMPLICIT Extensions  OPTIONAL }
```