Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

CONSEJO GENERAL
PROCURADORES
DE ESPAÑA

ADENDA AL CONTRATO ENTRE EL CONSEJO GENERAL DE PROCURADORES DE LOS TRIBUNALES Y LA FÁBRICA NACIONAL DE MONEDA Y TIMBRE PARA LA PRESTACIÓN DE SERVICIOS CERTIFICACIÓN DE FIRMA ELECTRÓNICA Y OTROS SERVICIOS RELATIVOS A LA ADMINISTRACIÓN ELECTRÓNICA Y DE LA SOCIEDAD DE LA INFORMACIÓN

En Madrid, a 3 de mayo de 2016

REUNIDOS

De una parte, el Excmo. Sr. D. Juan Carlos Estévez Fernández-Novoa con DNI 635219-M, Presidente del Consejo General de Procuradores de los Tribunales actuando en nombre y representación del mismo en virtud de las competencias atribuidas.

Y de otra, Don Jaime Sánchez Revenga, como Director General, cargo para el que fue nombrado por el Real Decreto 286/2012, de 27 de enero, BOE núm. 24 de 28 de enero de 2012, en nombre y representación de la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda (FNMT – RCM), según resulta del artículo 19 de su Estatuto, siendo esta entidad Organismo Público, Entidad Pública Empresarial, teniendo su domicilio institucional en Madrid, calle Jorge Juan número 106 y código de identificación Q28/26004 – J.

Reconociéndose ambas partes la capacidad legal necesaria para formalizar la presente Adenda,

EXPONEN

PRIMERO.- Que el CONSEJO GENERAL DE PROCURADORES DE LOS TRIBUNALES y la FNMT-RCM suscribieron, con fecha 1 de diciembre de 2004, un Contrato cuyo objeto consiste en la prestación de servicios de certificación de firma electrónica y otros servicios relativos a la administración electrónica y de la sociedad de la información, de conformidad con las condiciones que son detalladas en el Contrato.

SEGUNDO.- Las nuevas actividades de la sociedad de la información surgidas por el incremento del uso de las redes de comunicación y que, en parte, han sido reguladas, entre otras, por las leyes 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico y 56/2007, de 28 de diciembre, de medidas de impulso de la sociedad de la información, están mejorando la actividad de los servicios públicos y del sector privado y sus relaciones con los particulares gracias a la inmediatez en la obtención de la información y la posibilidad creciente de realizar transacciones y contrataciones por vía electrónica a través de la Red y a la necesidad de otorgar seguridad técnica y jurídica a los sistemas de interlocución telemática en las actividades de prestación de servicios. Una de las actividades que realiza la FNMT-RCM para otorgar seguridad y fiabilidad a las transacciones electrónicas es la de sellado de tiempo, que realiza como tercera parte de confianza.

TERCERO.- La FNMT-RCM, dispone de la infraestructura técnica necesaria para la realización de los servicios de sellado electrónico de tiempo (sellado de tiempo o *time stamping*) y cuenta con una larga experiencia en el sector. Las actividades de tercero de confianza en lo relativo a la prueba de los contratos celebrados por vía electrónica han de sujetarse a las reglas generales de las correspondientes leyes procesales y, en su caso, a lo establecido en la legislación sobre firma electrónica.

CUARTO.- Estando ambas partes interesadas en facilitar a los usuarios las relaciones de carácter mercantil a través de las técnicas y medios electrónicos, informáticos y telemáticos (EIT), se procede a la formalización de la presente adenda con arreglo a las siguientes

CLÁUSULAS

PRIMERA.- OBJETO

El objeto de la presente adenda es la prestación, por parte de la FNMT-RCM al Consejo General de Procuradores de los Tribunales, de los siguientes servicios:

- Sellado electrónico de tiempo para las actividades propias del CONSEJO GENERAL DE PROCURADORES DE LOS TRIBUNALES y uso dentro de su organización, a los efectos de dejar constancia de la fecha y hora de la existencia de un determinado documento o transacción electrónica, de conformidad con lo establecido en la presente adenda. Este sellado electrónico de tiempo no incluye la custodia y almacenamiento del documento electrónico sobre el que se aplica el referido sellado.

- Otros servicios auxiliares al anterior recogidos en el Anexo I.

El CONSEJO GENERAL DE PROCURADORES DE LOS TRIBUNALES exonera a la FNMT-RCM de los servicios de conservación hasta el límite legal previsto en el art. 20.1.f) de la Ley 59/2003 de firma electrónica. FNMT-RCM facilitará a petición del Consejo la información técnica que obre en poder de la FNMT-RCM siempre que se encuentre en vigor y al corriente de pago la presente adenda, a los efectos que el Consejo pueda realizar la custodia la información y documentación relativa al certificado reconocido, si así lo considera por la naturaleza de las operaciones y transacciones.

SEGUNDA.- RÉGIMEN DE PRESTACIÓN DE LOS SERVICIOS

1.- La prestación del servicio a que se refiere la cláusula primera, se realizará atendiendo a lo establecido en:

- Anexo I: Sellado de Tiempo.

2.- La fuente de tiempo utilizada por la FNMT-RCM para el sellado de tiempo está sincronizada con el laboratorio del Real Instituto y Observatorio de la Armada de San Fernando (Cádiz), en adelante ROA, quién de conformidad con lo previsto sobre la hora legal en el Real Decreto 1308/1992, de 23 de octubre está declarado como patrón nacional de tiempo y del que, como prueba, se obtienen certificaciones del estado de sincronismo a petición de la FNMT-RCM y da un tiempo que, como mínimo, tendrá la precisión de entre uno y diez milisegundos sobre el tiempo de un receptor GPS al que la Autoridad de Fechado Digital de la FNMT-RCM se conecta a través de un protocolo NTP y que será el tiempo del momento en que se realiza una transacción electrónica susceptible de serle aplicado un sellado electrónico.

La acreditación de la realización de un sellado electrónico de tiempo por la FNMT-RCM, debidamente suscrito electrónicamente por las partes y por la propia FNMT-RCM, se someterá como prueba, en su caso, a la valoración de los tribunales competentes, de conformidad con las normas procesales de aplicación.

TERCERA.- OBLIGACIONES DE LAS PARTES.

1.- Para la prestación efectiva de los servicios objeto de la presente adenda, la FNMT-RCM se compromete a realizar las siguientes prestaciones adicionales:

- Emisión al CONSEJO GENERAL DE PROCURADORES DE LOS TRIBUNALES, de un certificado de firma electrónica y/o de servidor, necesarios para la suscripción de las peticiones de sellados. La FNMT-RCM no aceptará certificados de firma electrónica de Prestadores de Servicios de Certificación no reconocidos por la propia FNMT-RCM.

- Prestación al CONSEJO GENERAL DE PROCURADORES DE LOS TRIBUNALES los servicios de acreditación de los sellados electrónicos de tiempo efectuados durante el tiempo de vigencia de la presente adenda, siempre que las solicitudes de servicios hayan sido firmadas electrónicamente por CONSEJO GENERAL DE PROCURADORES DE LOS TRIBUNALES.

- Autorización del uso de los derechos de propiedad industrial y/o intelectual correspondientes a las aplicaciones necesarias para el cumplimiento de la adenda, referida exclusivamente a licencias instrumentales de usuario. Queda prohibida la sublicencia, uso y autorización a terceros de la tecnología cedida temporalmente por aplicación de la presente adenda.

2.- Por su parte, el CONSEJO GENERAL DE PROCURADORES DE LOS TRIBUNALES se obliga a:

- Aceptar que los registros de las operaciones (logs), efectuados y conservados por la FNMT-RCM, sobre los servicios prestados al CONSEJO GENERAL DE PROCURADORES DE LOS TRIBUNALES en virtud de las solicitudes realizadas, harán prueba para justificar el servicio efectuado.

- Tener disponibles las aplicaciones informáticas y los equipos necesarios para la petición de sellados de tiempo, a la FNMT-RCM.

- Conservar el soporte de las transacciones electrónicas que han servido de base para la realización de las solicitudes de servicio a la FNMT-RCM.

- Cifrar las comunicaciones emitidas y recibidas, mediante el protocolo SSL.

- Firmar electrónicamente, las peticiones de sellados electrónicos de tiempo, mediante el certificado de firma electrónica proporcionado por la FNMT-RCM.

- En las aplicaciones informáticas en las que los usuarios se relacionen con el CONSEJO GENERAL DE PROCURADORES DE LOS TRIBUNALES, ésta asume la obligación de incorporar una cláusula o mención en los contratos respecto a que las actividades realizadas por la FNMT-RCM (sellados electrónicos de tiempo, tercera parte de confianza), harán prueba inter-partes en las relaciones que el CONSEJO GENERAL DE PROCURADORES DE LOS TRIBUNALES mantenga con los citados usuarios.

- El CONSEJO GENERAL DE PROCURADORES DE LOS TRIBUNALES deberá cumplir las obligaciones dimanantes de las normas sobre consumidores y usuarios, ventas a distancia y comercio electrónico. La FNMT-RCM no es parte en las relaciones de los consumidores y usuarios con el CONSEJO GENERAL DE PROCURADORES DE LOS TRIBUNALES.

CUARTA.- CESIÓN Y SUBCONTRATACIÓN.

El CONSEJO GENERAL DE PROCURADORES DE LOS TRIBUNALES no podrá actuar, por cuenta de terceros, como prestador de estos servicios revendiendo directamente los recibidos de la FNMT-RCM, por aplicación de la presente adenda.

Queda prohibido al CONSEJO GENERAL DE PROCURADORES DE LOS TRIBUNALES la cesión de la presente adenda a terceros sin autorización previa de la FNMT-RCM. Las subcontrataciones que el CONSEJO GENERAL DE PROCURADORES DE LOS TRIBUNALES pudiera realizar en aplicación de la presente adenda y que afectaran a la seguridad y fiabilidad de la prestación del servicio, deberán ser aprobadas, previamente a su realización, por la FNMT-RCM.

QUINTA.- RESPONSABILIDAD

La FNMT-RCM como prestador de los servicios citados en la cláusula primera y el CONSEJO GENERAL DE PROCURADORES DE LOS TRIBUNALES, como usuario del sistema de sellado electrónico de tiempo y partícipe en el procedimiento de encriptación y remisión de solicitudes de sellados a la FNMT-RCM, responderán cada una en el ámbito de sus respectivas funciones de los daños y perjuicios que causara el funcionamiento del sistema de acuerdo con las reglas generales del ordenamiento jurídico que sean de aplicación y de conformidad con las obligaciones asumidas a través de la presente adenda.

En todo caso, se presumirá la veracidad de los documentos o transacciones remitidos y firmados electrónicamente por el CONSEJO GENERAL DE PROCURADORES DE LOS TRIBUNALES sobre los que la FNMT-RCM aplicará un sellado electrónico de tiempo, y que tales datos no se han producido en fraude de terceros, ni infringen la legalidad vigente. El CONSEJO GENERAL DE PROCURADORES DE LOS TRIBUNALES asumirá y responderá de cualquier reclamación o reivindicación sobre la veracidad y legalidad de los documentos electrónicos remitidos por el CONSEJO GENERAL DE PROCURADORES DE LOS TRIBUNALES, exonerando a la FNMT-RCM de cualquier responsabilidad sobre los contenidos que no son conocidos por esta Entidad Pública.

Específicamente, la FNMT-RCM solo responderá de su actuación en relación con el servicio prestado en aplicación de la presente adenda, no siendo responsable de las transacciones y/o negocio jurídico de fondo que el usuario realizara en el ámbito de actuación del CONSEJO GENERAL DE PROCURADORES DE LOS TRIBUNALES cualquiera que sea su cuantía, siempre que los posibles daños y perjuicios no provengan de una actuación dolosa o con culpa grave de la FNMT-RCM en el servicio prestado.

El CONSEJO GENERAL DE PROCURADORES DE LOS TRIBUNALES mantendrá indemne a la FNMT-RCM de cualquier derecho o acción ejercida por el usuario o por el CONSEJO GENERAL DE PROCURADORES DE LOS TRIBUNALES en sus relaciones recíprocas y que se basen en el negocio jurídico de fondo sobre el que la FNMT-RCM haya prestado los servicios descritos en esta adenda.

Se establece como límite máximo de responsabilidad de la FNMT-RCM por los servicios derivados de esta adenda, y con efectos de cláusula penal de conformidad con el artículo 1152 y siguientes del Código Civil, la cantidad que se corresponda con el 50% del importe fijo de la contraprestación económica anual. Esta cantidad sustituirá, en caso de incumplimiento, la posible indemnización por daños y perjuicios que procediera.

SEXTA.- ENTRADA EN VIGOR Y DURACIÓN.

La presente adenda entrará en vigor el día de su firma y su duración se extenderá a lo estipulado en el Contrato de referencia.

Y, en prueba de conformidad, ambas partes suscriben el presente documento, por duplicado, en el lugar y fecha indicado en el encabezamiento.

FÁBRICA NACIONAL DE MONEDA Y TIMBRE – REAL CASA DE LA MONEDA	*CONSEJO GENERAL DE PROCURADORES DE LOS TRIBUNALES*
Fdo: Jaime Sánchez Revenga	*Fdo:* Juan Carlos Estévez Fernández-Novoa

ANEXO I

SERVICIOS A PRESTAR

SELLADO DE TIEMPO

INTRODUCCIÓN

El sellado de tiempo es un método para probar que un conjunto de datos (*datum*) existió antes de un momento dado y además que ningún bit de estos datos ha sido modificado desde entonces.
Además, el sellado de tiempo proporciona un valor añadido a la utilización de firma digital ya que ésta por si sola no proporciona ninguna información acerca del momento de creación de la firma. Los certificados digitales utilizados por el algoritmo de la firma digital tienen un periodo de validez y por lo tanto, la firma sin el fechado digital, pasada la validez del certificado, siempre puede ser repudiada.

Para asociar los datos con un específico momento de tiempo es necesario utilizar una Autoridad de Sellado (TSA - *Time Stamp Authority*) como tercera parte de confianza.

PROTOCOLO

La TSA centraliza la emisión de certificados temporales. El papel que jugará esta entidad será producir, almacenar, verificar y renovar los certificados temporales. La TSA será una tercera parte de confianza (TTP), siendo su firma sobre el certificado temporal suficiente para probar la validez de éste.

Este protocolo permite el sellado de tiempo de cualquier tipo de información digital, y protege la confidencialidad de los datos fechados.

El usuario del servicio de sellado de tiempo debe ser poseedor de un certificado emitido por la Autoridad de Certificación de esta FNMT y que deberá ser solicitado por el usuario o parte autorizada.

La TSA hace uso de un certificado exclusivamente emitido para labores de sellado de tiempo, es decir, en su certificado está presente críticamente la extensión "extendedKeyUsage", cuyo valor es id-kp-timestamping.

Solicitud de sellado de tiempo

Una vez que el usuario dispone de un certificado X.509 y su correspondiente clave privada podrá realizar peticiones de sellado de tiempo. El proceso para realizar una petición de sellado es el siguiente:

1. El usuario selecciona el fichero electrónico del cual se solicitará el sellado a la TSA.

2. La aplicación cliente compone un resumen (hash) del contenido de ese fichero.
3. El usuario selecciona la política de servicio que desea, el número de referencia, la versión,...
4. La aplicación cliente compone una petición de fechado digital y la envía vía HTTPS.

Respuesta de sellado de tiempo

Una vez que la TSA haya recibido la solicitud de sellado y la haya aceptado, procederá a devolver a la aplicación cliente la respuesta de sellado o Response vía HTTPS. Este Response es un objeto que contiene un campo obligatorio que es el estado de la operación y en caso de que se haya realizado satisfactoriamente contiene además un objeto CMS SignedData, que es la firma del objeto que contiene toda la información del certificado de tiempo. El cliente podrá optar por almacenar directamente ese Response, validándolo previamente o también podrá optar por realizar la verificación del mismo, en caso de que no haya habido errores. Para ello:

1. La aplicación cliente recompone el objeto Response, extrayendo el estado de la operación, y si éste es GRANTED se puede extraer también el objeto CMS SignedData.
2. La aplicación cliente recompone el objeto CMS SignedData, extrayendo los datos firmados y verificando que la firma es correcta, haciendo uso del certificado de la TSA incluido en el objeto CMS.
3. Se obtienen los certificados incluidos en el objeto CMS y se hace "path validation".
4. La aplicación cliente obtendrá los datos de sellado del token.

ESTÁNDARES APLICABLES

La definición del servicio de Sellado de Tiempo está basada en las especificaciones del estándar IETF-PKIX RFC-3161 – "*Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*" y la correspondiente norma ISO 18014-2, en la cual la FNMT-RCM ha participado como elaboradores de la misma.
A continuación se describen brevemente algunos de los puntos del mencionado estándar que tienen mayor impacto en la definición de la solución final del servicio.

El estándar RFC3161 define entre otros, el formato de la solicitud de un sellado de tiempo y de la respuesta generada por la TSA. También establece los diferentes requerimientos de seguridad que debería cumplir una TSA.
Uno de estos requerimientos, es que todos los sellados de tiempo generados por la TSA deben estar firmados digitalmente por ella con la clave privada de un certificado digital válido emitido especialmente para este propósito.
Por otro lado el mencionado estándar especifica que los sellados de tiempo (*tokens*) generados por la TSA no pueden incluir ninguna identificación del cliente que ha solicitado la operación. Como consecuencia, no es necesario que los mensajes de solicitud

de sellado de tiempo que recibe la TSA contengan algún tipo de autenticación del cliente.

El estándar enumera diferentes mecanismos de transporte para mensajes de TSA. Ninguno de estos métodos es obligatorio; todos ellos son opcionales e incluso se contempla la posibilidad de soportar en un futuro nuevos mecanismos. Los mecanismos que especifican el documento RFC3161 son:

- Protocolo utilizando correo electrónico
- Protocolo basado en la utilización de *FTP*
- Protocolo basado en sockets utilizando el puerto IP 318
- Protocolo vía http/ssl.

También hay que recalcar que el estándar solamente define la operación de solicitud de sellado de tiempo y de la respuesta correspondiente, dejando otros tipos de operaciones, como por ejemplo la validación del sellado, sin ninguna especificación, aunque se deba realizar la implementación de este tipo de operaciones.

El estándar RFC 2630 define el formato usado para la encapsulación de datos firmados, cifrados, resumidos o para la autenticación de mensajes arbitrarios. La RFC 2630 deriva del PKCS#7 versión 1.5 (RFC 2315).

Dentro de la iniciativa EESSI se ha recogido la anterior normativa a través de la ETSI TS 101 861, según se ha extraído en el presente texto.

ESTRUCTURAS DE DATOS

Las estructuras de datos utilizadas en el protocolo son las siguientes:

```
TimeStampRequest ::= SEQUENCE {
        version Integer { v1(1) },
        messageImprint MessageImprint,
        reqPolicy PolicyInformation  OPTIONAL,
        nonce Integer  OPTIONAL,
        certReq BOOLEAN DEFAULT FALSE,
        extensions [0] IMPLICIT Extensions OPTIONAL
}

TimeStampResp ::= SEQUENCE {
        status PKIStatusInfo,
        timeStampToken TimeStampToken OPTIONAL
}

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
}
```

FUENTE DE TIEMPO

La fuente de tiempo segura es un servicio que proporciona el instante exacto en el momento en el que se realiza la petición.

Las fuentes de tiempo utilizadas por la Autoridad de Fechado Digital es el ROA.
Una vez recibida la fuente de tiempo distribuye la referencia temporal a la Autoridad de Fechado Digital haciendo uso del protocolo NTP (Network Time Protocol) con una precisión de entre uno (1) y diez (10) milisegundos.

ACTUALIZACIÓN TECNOLÓGICA.

La FNMT someterá el servicio a la actualización tecnológica constante que permita que la disponibilidad del servicio y el acceso al mismo cumpla en todo momento los criterios técnicos iniciales así como aquellos que fruto de los avances tecnológicos o del desarrollo normativo, le sean de aplicación.

Dicha actualización se realizará, tratando de evitar en la medida de lo posible, el cambio en los procedimientos seguidos hasta la fecha de la actualización por los titulares.

La FNMT notificará a los titulares con 2 meses de antelación las actualizaciones que pudieran causar modificaciones en los procedimientos de acceso a la dirección o de consulta del contenido depositado.

PRÁCTICAS DEL SERVICIO

La declaración detallada de prácticas del servicio se publicará en la dirección electrónica de la FNMT y podrá ser variada sin previo aviso. La variación no limitará el servicio.

https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion

Nota sobre prestación de los servicios:

Los servicios contemplados en el presente Anexo I, que preste la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, se realizarán de conformidad con lo establecido en la legislación aplicable a los mismos y los acuerdos, convenios o contratos que suscriba la FNMT-RCM con las diferentes administraciones públicas o con personas o entidades privadas.

ANEXO II

CONDICIONES ECONÓMICAS

Fechado Digital

El precio anual de este servicio es 2.900€.

Las cantidad expuesta anteriormente no incluye el IVA legalmente establecido.