GOBIERNO DE ESPAÑA

MINISTERIO
DE POLÍTICA TERRITORIAL
Y ADMINISTRACIÓN PÚBLICA

SECRETARÍA DE ESTADO
PARA LA FUNCIÓN PÚBLICA

DIRECCIÓN GENERAL PARA
EL IMPULSO DE LA
ADMINISTRACIÓN ELECTRÓNICA

# GUÍA DE USO DEL SELLO DE TIEMPO Y MARCA DE TIEMPO. USO DE LA TS@ (TIME STAMPING AUTHORITY)

**Madrid, septiembre 2011**

Esta publicación ha sido elaborada por la Dirección General para el Impulso de la Administración Electrónica

1ª edición electrónica



Catálogo general de publicaciones oficiales:
http://publicacionesoficiales.boe.es

Catálogo de publicaciones de la Secretaría General Técnica del Ministerio de Política Territorial y Administración Pública:
http://www.mpt.gob.es/publicaciones.html

Edita: Ministerio de Política Territorial y Administración Pública
Secretaría General Técnica

NIPO: 850-11-041-7

@dministración electrónica

Proteja el medio ambiente.
No imprima si no es imprescindible

# 1 INTRODUCCIÓN

En este documento se realizará una descripción general de la Autoridad de Sellado de Tiempo, en adelante TS@, del Ministerio de Política Territorial y Administración Pública (en adelante, MPTAP), explicando su funcionamiento básico, funcionalidades así como las principales consideraciones legales referentes al sellado de tiempo.

En el documento se centrará especialmente en la definición de "sello de tiempo" así como las diferencias legales con una "marca de tiempo", con el objetivo de aclarar a las administraciones públicas que utilicen el servicio de sellado ofrecido por el MPTAP cuando han de utilizar un mecanismo u otro, exponiendo ejemplos de de trámites en los que es necesaria la obtención de un sello de tiempo.

Adicionalmente, se especificaran algunas características generales y definiciones relativas al sellado de tiempo, detallando los procesos ofrecidos por la Autoridad de Sellado del MPTAP y las entidades que intervienen en estos.

# 2 OBJETIVOS

Los objetivos de este documento son principalmente dos:

- Esclarecer cuándo es obligatorio el sellado de tiempo en trámites administrativos y cuando es suficiente con incluir una marca de tiempo asociada al documento. Esta aclaración legal es importante por motivos de eficiencia, ya que de esta forma se pueden evitar la generación innecesaria de timestamp, reduciendo los costes de integración de las aplicaciones así como aumentando la eficiencia del servicio de sellado.
- Definir técnicamente los conceptos de sello de tiempo y marca de tiempo.

# 3 DIFERENCIAS ENTRE SELLO DE TIEMPO Y MARCA DE TIEMPO

En la **Ley 11/2007** del 22 de Junio referente al acceso electrónico de los ciudadanos a los Servicios Públicos se especifica, en el **artículo 29.2:**

> *"Los documentos administrativos incluirán referencia temporal, que se garantizará a través de medios electrónicos cuando la naturaleza del documento así lo requiera."*

En esta ley se habla de "referencia temporal", sin especificar el tipo. Las posibles referencias temporales que se pueden asociar a un documento electrónico se establecen en el

**Real Decreto 1671/2009**, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, concretamente en el **Capítulo II, artículo 147**.

> *"Artículo 47. Referencia temporal de los documentos administrativos electrónicos.*
>
> *La Administración General del Estado y sus organismos públicos dependientes o vinculados asociarán a los documentos administrativos electrónicos, en los términos del artículo 29.2 de la Ley 11/2007, de 22 de junio, una de las siguientes modalidades de referencia temporal, de acuerdo con lo que determinen las normas reguladoras de los respectivos procedimientos:*
>
> *a) «Marca de tiempo» entendiendo por tal la asignación por medios electrónicos de la fecha y, en su caso, la hora a un documento electrónico. La marca de tiempo será utilizada en todos aquellos casos en los que las normas reguladoras no establezcan la utilización de un sello de tiempo.*
>
> *b) «Sello de tiempo», entendiendo por tal la asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento."*

Por tanto, los dos tipos de referencias posibles son Marca de Tiempo y Sello de Tiempo, siendo la norma que regula el procedimiento donde residirán los documentos electrónicos la que dicta la conveniencia de la utilización de uno u otro tipo.

En este sentido, se dan dos escenarios utilizando la misma técnica de sellado:

- El servicio es propio del Organismo que lo presta, tanto en la gestión de la fuente de tiempo como en la generación de la referencia temporal. En este caso, estamos ante una marca de tiempo.
- El servicio lo debe prestar un Organismo "third party authority". El MPTAP se constituye como prestador y, por lo tanto, se le deben solicitar las referencias temporales de este tipo para los trámites administrativos que exijan una validez realizada por alguien externo a las partes implicadas.

El **Real Decreto 4/2010,** de 8 de enero, por el que se regula el **Esquema Nacional de Interoperabilidad** en el ámbito de la Administración Electrónica establece las siguientes dos definiciones en su anexo 'Glosario de términos':

– ***M arca de tiempo:*** *La asignación por medios electrónicos de la fecha y, en su caso, la hora a un documento electrónico.*

– ***Sello de tiempo:*** *La asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento.*

Fundamentalmente son dos conceptos administrativos parecidos pero técnicamente son iguales ya que ambos son una estructura de datos que indica una fecha y hora asociada a un documento electrónico. La principal diferencia reside en que la marca de tiempo puede ser generada por cualquier aplicación, sin cumplir ningún requisito específico y un sello de tiempo solo puede ser emitido por una tercera parte de confianza llamada Autoridad de Sellado de Tiempo. Esta tercera parte de confianza debe ser un prestador de servicios reconocido por el Ministerio de Industria y Comercio.

Hay que tener en cuenta que la marca de tiempo puede ser igual de precisa que un sello de tiempo, ya que esta referencia temporal puede obtenerse a través de la hora de un servidor que este sincronizado mediante el protocolo NTP con una fuente de tiempo fiable y precisa. Si no hay mención explícita en la norma, o no se determina su necesidad en base a un análisis de riesgos, no sería necesario incluir un sello de tiempo.

El sello de tiempo garantiza fehacientemente que una serie de datos (preparados por el solicitante de sello) han existido y no han sido modificados desde un momento determinado (gracias al sello de tiempo emitido por el tercero de confianza). Es un tipo de firma electrónica que es verificable y solo puede generarse por prestadores de servicio reconocidos, con unas políticas definidas y asegurando una precisión determinada y fiabilidad en los datos generados. Además, el hecho de que la hora sea proporcionada por sistema certificado, independiente y ajeno al procedimiento ofrece garantías de imparcialidad ante un posible litigio.

## 3.1 ¿CUÁNDO UTILIZAR UN SELLO DE TIEMPO?

Si la norma que regula el procedimiento no establece la necesidad de determinar fehacientemente el momento del trámite, el **Real Decreto 3/2010,** de 8 de enero, por el que se regula el **Esquema Nacional de Seguridad** en el ámbito de la Administración Electrónica establece una serie de principios y requisitos con el fin de garantizar la seguridad en los sistemas de información y una adecuada protección de la misma.

En su artículo 1 (Objeto) determina:

> *… El Esquema Nacional de Seguridad está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Será aplicado por las Administraciones públicas para asegurar el acceso,* ***integridad****, dis-*

*ponibilidad, **autenticidad**, confidencialidad, **trazabilidad** y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.*

De acuerdo al Anexo I del esquema, se distinguen entre tres tipos de sistemas de información en función de su criticidad y nivel de seguridad exigible: ALTO, MEDIO y BAJO y se define un sistema de nivel alto como:

*Nivel ALTO. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.*

*Se entenderá por perjuicio muy grave:*

1. *La anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose.*
2. *El sufrimiento de un daño muy grave, e incluso irreparable, por los activos de la organización.*
3. *El incumplimiento grave de alguna ley o regulación.*
4. *Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.*
5. *Otros de naturaleza análoga.*

Y de nivel medio como:

*Nivel MEDIO. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.*

*Se entenderá por perjuicio grave:*

1. *La reducción significativa la capacidad de la organización para atender eficazmente a sus obligaciones fundamentales, aunque estas sigan desempeñándose.*
2. *El sufrimiento de un daño significativo por los activos de la organización.*
3. *El incumplimiento material de alguna ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.*

4. *Causar un perjuicio significativo a algún individuo, de difícil reparación.*

5. *Otros de naturaleza análoga*

Las dimensiones de seguridad a la que hacen referencia los niveles de seguridad, también se definen en el Esquema Nacional de Seguridad:

*2. Dimensiones de la seguridad.*

*A fin de poder determinar el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas, y de poder establecer la categoría del sistema, se tendrán en cuenta las siguientes dimensiones de la seguridad, que serán identificadas por sus correspondientes iniciales en mayúsculas:*

*a) Disponibilidad [D].*

*b) Autenticidad [A].*

*c) Integridad [I].*

*d) Confidencialidad [C].*

*e) Trazabilidad [T].*

*3. Determinación del nivel requerido en una dimensión de seguridad.*

*Una información o un servicio pueden verse afectados en una o más de sus dimensiones de seguridad. Cada dimensión de seguridad afectada se adscribirá a uno de los siguientes niveles: BAJO, MEDIO o ALTO*

El Real Decreto anteriormente mencionado sólo obliga de forma explícita a las aplicaciones con un nivel de seguridad alto a utilizar el sellado de tiempo con el objetivo de cumplir la dimensión de seguridad exigida en el ámbito de la trazabilidad. Sin embargo, otras aplicaciones con nivel de seguridad bajo o medio también pueden requerirlo, por ejemplo la notificación de una denuncia.

En este sentido, en su punto 5.7.5 del ANEXO 2 (Medidas de seguridad) se indica lo siguiente:

*5.7.5. Sellos de tiempo [mp.info.5].*

| dimensiones | T | | |
|---|---|---|---|
| nivel | bajo | medio | alto |
| | no aplica | no aplica | aplica |

*Nivel ALTO*

*Los sellos de tiempo prevendrán la posibilidad del repudio posterior:*

1. *Los sellos de tiempo se aplicarán a aquella información que sea susceptible de ser utilizada como evidencia electrónica en el futuro.*
2. *Los datos pertinentes para la verificación posterior de la fecha serán tratados con la misma seguridad que la información fechada a efectos de disponibilidad, integridad y confidencialidad.*
3. *Se renovarán regularmente los sellos de tiempo hasta que la información protegida ya no sea requerida por el proceso administrativo al que da soporte.*

También obliga de forma explícita a utilizar el sellado de tiempo en las firmas electrónicas a las aplicaciones que se considere que deban garantizar la autenticidad del signatario y la integridad del contenido con un nivel de seguridad medio. Y en el caso de nivel medio, se precisa en el punto 5.7.4 del ANEXO 2 (Firma electrónica)

*5.7.4. Firma Electrónica [mp.info.4].*

| dimensiones | I A | | |
|---|---|---|---|
| nivel | bajo | medio | alto |
| | aplica | + | ++ |

…

*Nivel MEDIO*

…

2. *Se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa que aquélla soporte, sin perjuicio de que se pueda ampliar este período de acuerdo con lo que establezca la política de firma electrónica y de certificados que sea de aplicación. Para tal fin:*
   a. *Se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación:*
      1. *Certificados.*
      2. *Datos de verificación y validación.*

b. *Se protegerán la firma y la información mencionada en el apartado anterior con un sello de tiempo.*

Por lo tanto, se deberá utilizar el sello de tiempo en un procedimiento cuando la norma reguladora lo especifique claramente, instando a incorporar referencia temporal como tal, es decir, a la necesidad de disponer de una fuente fehaciente de tiempo o cuando la naturaleza del documento así lo requiera. Además, el uso del sellado de tiempo siempre será obligatorio en aquellos sistemas en los que, bajo la categorización del Esquema Nacional de Seguridad, tengan un nivel de seguridad alto.

## 3.2 EJEMPLOS

Como se ha mencionado en el punto anterior, existen dos casos en los que es obligatoria la inclusión de un sello de tiempo en vez de una marca de tiempo, si se necesita una referencia temporal para un documento en electrónico:

- Cuando la ley especifique explícitamente que requiere una fuente fehaciente de tiempo emitida por un tercero de confianza reconocido.
- Cuando se trate de una aplicación de nivel alto bajo el criterio del Esquema Nacional de Seguridad.

A continuación se exponen una serie de ejemplos de leyes donde se hace alusión a la necesidad de inclusión de referencias temporales asociadas a documentos y/o firmas electrónicas:

Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

En su Artículo 30, Recepción de solicitudes, escritos y comunicaciones, se determina que

*"El registro electrónico emitirá automáticamente por el mismo medio un recibo firmado electrónicamente, mediante alguno de los sistemas de firma del* ***artículo 18 de la Ley 11/2007, de 22 de junio,*** *con el siguiente contenido:*

- *Copia del escrito, comunicación o solicitud presentada, siendo admisible a estos efectos la reproducción literal de los datos introducidos en el formulario de presentación.*
- *Fecha y hora de presentación y número de entrada de registro.*
- *En su caso, enumeración y denominación de los documentos adjuntos al for-*

*mulario de presentación o documento presentado, seguida de la huella electrónica de cada uno de ellos.*

- *Información del plazo máximo establecido normativamente para la resolución y notificación del procedimiento, así como de los efectos que pueda producir el silencio administrativo, cuando sea automáticamente determinable.*

En este caso, el recibo firmado electrónicamente:

- Necesita el dato de la hora, sólo como dato firmado electrónicamente con la "firma para la actuación administrativa automatizada"
- El Organismo pudiera querer mejorar dicha firma incorporando una marca de tiempo, no obligatoria en la redacción del decreto. Mucho menos recurrir a una fuente externa de tiempo, en petición de sello.

Ley 30/2007 de Contratos del Sector Público

Como ejemplo de la necesidad de utilización del sellado de tiempo, la LEY 30/2007, de 30 de octubre, de Contratos del Sector Público, en su artículo 42 especifica lo siguiente:

*"Art.42.3. El sistema informático que soporte el perfil de contratante deberá contar con un dispositivo que permita acreditar fehacientemente el momento de inicio de la difusión pública de la información que se incluya en el mismo."*

Por tanto, al especificar que se debe "acreditar fehacientemente el momento", la ley está obligando a que los sistemas de información que la implementen utilicen el sellado de tiempo para indicar "el momento de inicio de la difusión pública", ya que la generación de una marca de tiempo aunque puede ser una marca fiable, no es contrastable y carece de validez jurídica para acreditar la existencia de un documento electrónico antes de un instante determinado.

Procedimiento para la homologación de software de digitalización

El artículo 7 de la Orden EHA/962/2007 contempla de digitalización certificada de facturas. En las disposiciones generales de la Orden se especifican que características se requieren para una digitalización de una factura:

> *"Disposiciones generales*
>
> *Para que la imagen se considere fiel e íntegra ha de ser obtenida en un proceso informático automático en el que sin interrupción del mismo y sin intervención en momento alguno de operador se realicen, en el orden indicado, las siguientes tareas:*
>
> 3.º *Introducir en el fichero de la imagen, como metadatos, la información exigida por la Administración Tributaria que incluye la referencia identificativa de la homologación acordada, una marca de tiempo, así como el nombre y el número de versión del software de digitalización. Para la representación de metadatos, la Agencia Tributaria establece como referencia la especificación estándar denominada XMP (Extensible Metadata Platform).*
>
> 4.º *Firma del fichero que contiene la imagen optimizada y los metadatos, mediante firma electrónica reconocida o mediante cualquier otro sistema de firma electrónica admitido por la Agencia Tributaria con base en un certificado electrónico instalado en el sistema de digitalización e invocado por el software de digitalización certificada. El proceso de firma, en el que puede incluirse sellado de tiempo, conllevará, en cualquier caso, el cálculo previo de la huella o valor resumen del citado fichero. En el cálculo de la huella o valor resumen se podrá utilizar cualquier algoritmo que cumpla los requisitos tecnológicos mínimos, siendo SHA-1 el mínimo que el estado actual de tecnología establece. El fichero, con la imagen resultante y sus metadatos, debe permanecer inalterado desde este instante. "*

Se hace notar que esta orden ministerial es anterior a la aparición de RD 1671/2009 que define marca y sello de tiempo.

En este caso, el procedimiento especifica que, para mayor seguridad, podría incluirse **marca de tiempo** (generada por el Organismo en cuestión). En la actividad de compulsa de documentos en papel, el sello de caucho de la compulsa ha incluido referencia temporal plasmada por el funcionario sin recurrir a reloj externo, por lo que no sería necesario acudir a un prestador de servicios certificados para generar el sello.

Registro Electrónico del Ministerio de Economía y Hacienda

Se trata de un caso particular de Registro Electrónico en la Administración General del Estado. Reproduce lo que determina el RD 1671/2009, sin indicar si es necesario una referencia temporal.

*"Artículo 9. Acuse de recibo.*

1. *El acuse de recibo de los escritos que deban motivar anotación en el Registro Electrónico se realizará por las aplicaciones gestoras de los procedimientos de forma tal que se garanticen plenamente la autenticidad, la integridad y el no repudio por la Administración del contenido de los formularios presentados así como de los documentos anejos a los mismos, proporcionando a los ciudadanos los elementos probatorios plenos del hecho de la presentación y del contenido de la documentación presentada, susceptibles de utilización posterior independiente, sin el concurso de la Administración o del propio Registro.*

2. *El acuse de recibo será proporcionado por las aplicaciones gestoras de los procedimientos en la misma sesión en la que se realice la presentación, estando firmado e incluyendo, al menos, el siguiente contenido:*

   - *El órgano receptor del escrito.*
   - *La fecha y hora de presentación.*
   - *El número o código de registro individualizado.*
   - *La reproducción literal de los datos introducidos en el formulario proporcionado por la aplicación.*
   - *La enumeración y denominación de los ficheros adjuntos al formulario de presentación, seguida de la huella digital de cada uno de ellos. En el caso de que se hubieran presentado ficheros con código malicioso, el documento en formato pdf contendrá el nombre pero no la huella de dichos ficheros.*
   - *La información que permita a los interesados la utilización, validación y conservación correctas de los ficheros entregados, como son la mención del algoritmo utilizado para la creación de las huellas digitales, del estándar de firma utilizado, etc. Dicha información podrá sustituirse por la mención de la dirección electrónica en la que se contenga la mencionada información.*

*A los efectos de lo establecido anteriormente, se entiende por huella digital el resumen que se obtiene como resultado de aplicar un algoritmo matemático de compresión hash a la información de que se trate.*

Registros telemáticos de la Administración de la Comunidad Autónoma de Islas Baleares

En el boletín oficial de la comunidad autónoma de Islas Baleares nº58 de 21 de Abril de 2009 contiene una resolución del director general de tecnología y comunicaciones por la que se determinan los requisitos mínimos de carácter tecnológico que deben cumplir los registros telemáticos en la comunidad:

> *"Requisitos de los Registros Telemáticos de las consejerías y de las entidades autónomas de la Administración de la Comunidad Autónoma de las Illes Balears.*
>
> *Los registros telemáticos regulados por el Decreto 14/2007, de 9 de marzo, deben cumplir los requisitos siguientes:*
>
> 1. *Tendrán que emitir un justificante de recepción firmado electrónicamente con el siguiente contenido:*
>
> – *Fecha y hora de recepción.*
>
> – *Datos de identificación de la persona interesada.*
>
> – *Asunto, donde se incluya una breve referencia a su contenido.*
>
> – *Código de control, que permita verificar la integridad de los documentos registrados.*
>
> – *Sello de tiempo, emitido por un prestador de servicios de certificación."*

En este caso, el primer requisito "fecha y hora de recepción" podría entenderse que se necesita una marca de tiempo obtenida por el sistema que implemente el registro a partir de la hora del servidor. Sin embargo, lo único que se indica es que conste el dato de fecha y hora en el documento que se preparar para la firma.

Sin embargo, en el último punto del listado de requisitos se determina específicamente de "sello de tiempo, emitido por un prestador de servicios de certificación", por tanto, es necesario acudir a una de las TSAs certificadas por el Ministerio de Industria para la generación del sello. Hay que tener en cuenta que, a la fecha de publicación de la resolución (21 de Abril de 2009) no se disponía del RD 1671/2009.

Este ejemplo sirve para reiterar que solo se debe acudir al servicio de sellado cuando la norma indique explícitamente la necesidad de la generación de un sello de un prestador reconocido.

Reglamento de Gestión electrónica de Documentos, del Ayuntamiento de Arganda del Rey

Este reglamento tiene como objetivo dar seguridad jurídica y regular las condiciones de los distintos procedimientos de administración electrónica ofrecidos por el Ayuntamiento de Arganda del Rey. Trata sobre la integridad a largo plazo y la trazabilidad que se logra mediante la aplicación de referencias temporales sucesivas (la última sobre todo lo anterior):


*"Artículo 15.- Firmas de custodia*

1. *Con el fin de garantizar la autenticidad e integridad del archivo se podrán realizar firmas de custodia sobre los documentos de archivo, individual o conjuntamente. Para extender el período de validez de las firmas de custodia se podrá realizar un resellado periódico de las mismas mediante la actualización de los sellos de tiempo."*

El artículo 15 hace referencia a la actualización de los sellos de tiempo mediante la realización de un **resellado** periódico. El resellado es un servicio definido en el estándar para la generación de sellos de tiempo XML Timestamping Profile of the 2 OASIS Digital Signature Services (DSS) y no se puede realizar para marcas de tiempo, por lo que estamos ante otro ejemplo donde en el procedimiento se exige la utilización de una TSA.

# 4 ASPECTOS GENERALES DEL SELLADO DE TIEMPO

## 4.1 ¿QUÉ ES UN SELLO DE TIEMPO?

Un sello de tiempo es un tipo de firma electrónica que garantiza que cierta información existía antes de un momento determinado. Junto a la existencia del documento, un sello de tiempo sirve para comprobar que dicho documento no se ha modificado desde el momento de la generación del sello.

El sello de tiempo es una parte esencial en el concepto de documento electrónico, definido en la ley 11/2007 Artículo 29, unido a la idea de firma digital y metadatos.

Los protocolos de sellado de tiempo, en los cuales se basa la plataforma, se encuentran especificados en las siguientes normas:

- RFC 3161 "Internet X.509 Public Key Infrastructure Time Stamp Protocols ", estándar definido por la Internet Engineering Task Force (IETF) para el protocolo Time Stamp.
- IETF RFC 3628 Policy Requirements for Time-Stamping Authorities (TSAs).
- ETSI TS 102 023 Policy requirements for time-stamping authorities.
- XML Timestamping Profile of the 2 OASIS Digital Signature Services (DSS) ver. 1.0.
- ETSI TS 101 861 Time stamping profile.

## 4.2 ¿PARA QUÉ SIRVE UN SERVICIO DE SELLADO DE TIEMPO?

Un sello de tiempo sirve para obtener evidencias, técnicas y jurídicas, de que un objeto digital (documento, audio, video, log...) existe y no ha sido modificado desde antes de un instante determinado. Un servicio de sellado de tiempo es una tercera parte de confianza, reconocida por las autoridades pertinentes, que emiten sellos de tiempo verificables y que tienen valor probatorio.

Otras utilidades del servicio de sellado de tiempo:

- Aumentar la confianza en el comercio electrónico. Al incluir sellos de tiempo en los pedidos, facturas y otros documentos implicados en el comercio on-line se garantiza que las transacciones se realizan en un momento particular, disminuyendo las posiblibidadades de fraude y repudio.
- Proteger la identidad intelectual. Cualquier contenido digital puede ser plagiado, pero generando un sello de tiempo asociado a la propiedad intelectual se puede garantizar la existencia de un trabajo antes de un instante determinado. Además, el sello de tiempo puede aplicarse sobre cualquier tipo de documento (ver la sección 4.5 del presente documento), incluyendo imágenes, videos, archivos de sonido, etc.
- Ampliar las funcionalidades de la firma electrónica. Incluir un sello de tiempo en una firma digital es un medio de tener una evidencia del instante en el que el documento se ha firmado, otorgándole a éste medios adicionales para garantizar la propiedad de no repudio.

Los servicios de la Plataforma están disponibles para todo Organismo o Entidad Pública perteneciente a las diferentes Administraciones Públicas sea cual sea su ámbito: Administración General del Estado, Comunidades Autónomas, Diputaciones Provinciales o Entes Locales. Desde el MPTAP se ofrece la ayuda y el soporte necesario para que los Organismos integren estos servicios de certificación de valor añadido en los sistemas de información de Administración Electrónica que admitan autenticación y firma electrónica basada en certificados digitales.

## 4.3 FORMATOS DE SELLOS DE TIEMPO

Existen dos tipos sellos de tiempo generados por la TS@. Cada uno de ellos se basa en un estándar y tiene un formato distinto:

En Agosto de 2001 se publicó el estándar RFC 3161 "Internet X.509 Public Key Infrastructure Time Stamp Protocols", que define un formato de sello de tiempo que se codifica en formato ASN.1.

ASN.1 es una norma para codificar datos de forma que su representación sea independiente de la máquina y el lenguaje de programación que se esté ejecutando. Un sello de tiempo en formato ASN.1 tal y como se especifica en el estándar RFC3161 tiene la siguiente estructura:

```
<TimeStampToken>
    <TSTInfo>
        <Version>
            1
        </Version>
        <Policy>
            OBJECT ID = 1.2.3.4.5.6.7
        </Policy>
        <Message Imprint>
            Hash Algorithm: SHA (1.3.14.3.2.26)
            Hashed Message:
        34:05:EB:AF:8E:4A:D2:59:5F:6C:D0:40:4D:50:D0:1F:83:81:73:A5
        </Message Imprint>
        <SerialNumber (low-order 64 bits)>
            600805
        </SerialNumber>
        <GenTime>
            Tue Sep 28 08:41:20 CEST 2010
        </GenTime>
        <Accuracy>
            Seconds: 1
            Millis: 1
```

```
                Micros: 1
            </Accuracy>
            <Ordering>
                false
            </Ordering>
        </TSTInfo>
    </TimeStampToken>
```

Esta es la representación que da la librería criptográfica iaik para que el sello de tiempo sea legible, ya que la codificación ASN.1 no es formato fácilmente legible.

En Abril 2007 se creó una nueva que especificaba el intercambio de mensajes en la generación, validación y resellado de timestamps y definía un nuevo formato para estos XML: XML Timestamping Profile of the 2 OASIS Digital Signature Services (DSS) ver. 1.0. La principal diferencia entre la norma RFC3161 y la Oasis es que en esta última, los sellos de tiempo tienen formato XML, lo que propicia que se puedan definir los servicios de timestamp como web services con las ventajas de interoperabilidad que conlleva así como posiblitando aplicar mecanismos de seguridad asociados al protocolo: firma de mensajes, cifrado con clave simétrica..

Un sello de tiempo en XML tiene el siguiente formato:

```
<dss:Timestamp xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema">
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Id-b898">
    <ds:SignedInfo Id="Id-45d6cc1d-960a-4185-b80b-38f205cb1bae">
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
    c14n#WithComments"/>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    <ds:Reference Id="Id-bed8bc1e-47be-4813-ba42-972712edc9fb">
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
    <ds:DigestValue>NAXrr45KollfbNBATVDQH4OBc6U=</ds:DigestValue>
    </ds:Reference>
    <ds:Reference Id="Id-771" Type="urn:oasis:names:tc:dss:1.0:core:schema:
    XMLTimeStampToken" URI="#TSTInfo-Id-c57f7f58-9712-4a55-821c-4334d75ab100">
    <ds:Transforms>
    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
    </ds:Transforms>
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
    <ds:DigestValue>IU8FzVDfK7AhkDboTphMypNyeDY=</ds:DigestValue>
    </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>gYxon9Qr..=</ds:SignatureValue>
    <ds:KeyInfo>
    <ds:X509Data>
    <ds:X509Certificate>MII..c=</ds:X509Certificate>
    </ds:X509Data>
```

```
        </ds:KeyInfo>
        <ds:Object Id="TSTInfo-Id-c57f7f58-9712-4a55-821c-4334d75ab100"
        MimeType="application/xml">
        <dss:TstInfo>
        <dss:SerialNumber>600806</dss:SerialNumber>
        <dss:CreationTime>2010-09-28T08:49:02.312+02:00</dss:CreationTime>
        <dss:Policy>urn:oid:1.2.3.4.5.6.7</dss:Policy>
        <dss:ErrorBound>PT1.001001S</dss:ErrorBound>
        <dss:Ordered>true</dss:Ordered>
        <dss:TSA Format="urn:oasis:names:tc:SAML:1.1:nameid-
        nameidformat:X509SubjectName">CN=TSA Pruebas
        SevillaOU=SteriaO=SteriaC=Sevilla</dss:TSA>
        </dss:TstInfo>
        </ds:Object>
        </ds:Signature>
    </dss:Timestamp>
```

Junto al punto anteriormente citado de la seguridad, el formato XML es más legible así como más facilmente ampliable que la codificación ASN.1, aunque su correcto parseo, tratamiento y validación provoca una ligera perdida de rendimiento respecto a la implementación del servicio basado en el estándar RFC.

## 4.4 ¿CÓMO SE OBTIENE UNA FUENTE DE TIEMPO FIABLE?

En el estándar que especifica los requerimientos que deben tener todas las autoridades de sellado de tiempo, se indica que el sistema deberá contar con una fuente de tiempo fiable, sin especificar el mecanismo por el cual se obtiene dicho valor del tiempo, la precisión mínima que se debe garantizar o qué mecanismos han de utilizarse para garantizar la integridad del servicio.

En el caso de la TS@ del MPTAP, la obtención de la fuente de tiempo fiable se realiza sincronizando los servidores donde está alojada la aplicación con el Real Instituto y Observatorio de la Armada (ROA) a través del protocolo NTP. A partir de esta fuente de tiempo fiable la TS@ genera los sellos de tiempo.

Asimismo, la Red SARA también obtiene su fuente de tiempo fiable del ROA y la publica a través del servicio NTP. Las administraciones públicas pueden utilizar este servicio para sincronizar sus sistemas con la hora oficial, como establece el articulo 15 del Esquema Nacional de Interoperabilidad (RD 4/2010). De esta forma las aplicaciones que lo deseen pueden generar sus marcas de tiempo sincronizadas con la hora oficial.

*Artículo 15. Hora oficial.*

1. *Los sistemas o aplicaciones implicados en la provisión de un servicio público por vía electrónica se sincronizarán con la hora oficial, con una precisión y desfase que garanticen la certidumbre de los plazos establecidos en el trámite administrativo que satisfacen*

2. *La sincronización de la fecha y la hora se realizará con el Real Instituto y Observatorio de la Armada, de conformidad con lo previsto sobre la hora legal en el 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 y, cuando sea posible, con la hora oficial a nivel europeo*

La Sección de Hora del 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).**

### 4.5 ¿PARA QUÉ TIPO DE ARCHIVOS PUEDO GENERAR UN TIMESTAMP?

Un sello de tiempo se puede generar para cualquier documento electrónico, ya que, como paso previo del envío de la petición al servidor, se aplica un algoritmo de hash que toma como entrada un conjunto de bytes de cualquier tamaño, sin importar a que tipo de archivo corresponden dichos bytes.

Por tanto, se pueden generar sellos sobre documentos ofimáticos, archivos de audio, imágenes, software, trabajos creativos, etc.

### 4.6 ¿EXISTE ALGUNA LIMITACIÓN EN EL TAMAÑO DE LOS DATOS?

No, los dos estándares de generación de sellos de tiempo que cumple el sistema no obligan a la inclusión del documento completo en la petición de generación de sello. Para identificar al documento electrónico se utiliza una función hash.

Una función hash es una operación matemática que se aplica a un conjunto de datos de tamaño arbitrario, de tal manera que como resultado se obtiene una llamada de bits de tamaño fijo llamada 'resumen'. Este resumen tiene la propiedad de encontrarse unívocamente asociado a los datos iniciales, es decir, minimiza la posibilidad de que dos mensajes diferentes tengan un 'resumen' hash identico.

Además, es practicamente imposible generar un documento que sea idéntico a un hash dado.

Por tanto, no existe limitación en el tamaño de los datos ya que estos se van a transformar en un hash de tamaño fijo antes de ser enviados al servidor. La única limitación existente puede venir del tiempo necesario aplicar la función de resumen así como del límite superior que imponga el algoritmo de hash en cuanto al tamaño de la entrada de los datos.

## 5 SELLOS DE TIEMPO EN LA FIRMA ELECTRÓNICA

El concepto de firma electrónica fue introducido en la Ley 59/2003 de Firma Electrónica, que define una firma como un conjunto de datos en forma electrónica, consignados junto a otros o asociado a ellos, que pueden ser utilizados como medio de identificación del firmante.

En la ley se establecen tres tipos de firma electrónica:

1. La **firma electrónica** de es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

2. La **firma electrónica avanzada** es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

3. La **firma electrónica reconocida** es una firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

Es este último tipo de firma electrónica la que tiene el mismo valor para los datos electrónicos que su equivalente firma manuscrita en papel.

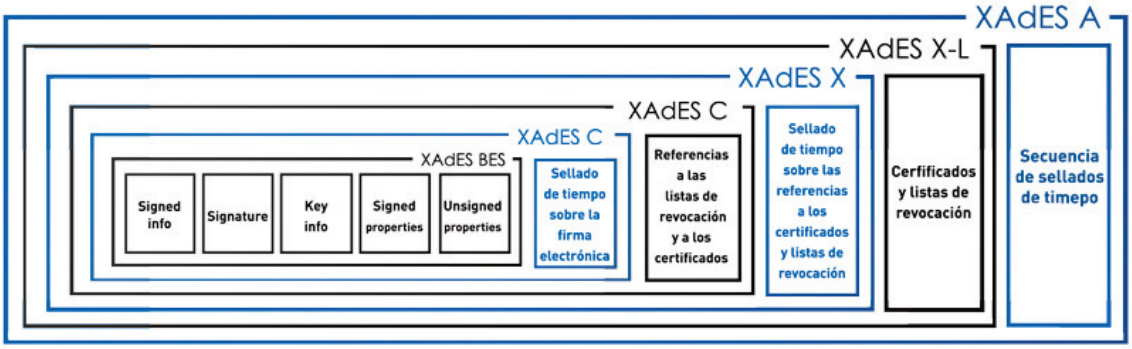
Uno de los requisitos básicos de una firma electrónica es que pueda ser validada. La validación de una firma es un proceso por el cual se asegura que el certificado con el que se firmó era válido en el momento de la operación y la integridad de los datos firmados, es decir, que estos no hayan sufrido ninguna modificación.

XAdES es un conjunto de especificaciones que definen diferentes formatos de firma que pueden ser usadas como **firma electrónica reconocida** y su principal ventaja es que estas firmas XML pueden ser válidas a largo plazo (de forma indefinida) y por tanto poseen plenas garantías juridicas.

XAdES define seis perfiles (formas) según el nivel de protección ofrecido. Cada perfil incluye y extiende al previo:

- XAdES, forma básica que simplemente cumple los requisitos legales de la Directiva para firma electrónica avanzada,
- XAdES-T (timestamp), añade un campo de sellado de tiempo para proteger contra el repudio,
- XAdES-C (complete), añade referencias a datos de verificación (certificados y listas de revocación) a los documentos firmados para permitir verificación y validación off-line en el futuro (pero no almacena los datos en sí mismos),
- XAdES-X (extended), añade sellos de tiempo a las referencias introducidas por XAdES-C para evitar que pueda verse comprometida en el futuro una cadena de certificados,
- XAdES-X-L (extended long-term), añade los propios certificados y listas de revocación a los documentos firmados para permitir la verificación en el futuro incluso si las fuentes originales (de consulta de certificados o de las listas de revocación) no estuvieran ya disponibles, XAdES-A (archival), añade la posibilidad de times-

tamping periódico (por ej. cada año) de documentos archivados para prevenir que puedan ser comprometidos debido a la debilidad de la firma durante un perido largo de almacenamiento.




Salvo la forma más básica de firma XML, todas las estructuras de firma AdES contiene un sello de tiempo, por lo que el uso de una TSA certificada se hace indispensable para la correcta generación de las firmas electrónicas reconocidas utilizadas en la administración electrónica.

## 6 ENTIDADES QUE INTERVIENEN EN EL PROCESO

En el proceso de la obtención de un timestamp intervienen varias entidades:

Por un lado, la **entidad solicitante** que pide el sello de tiempo que necesita generar una evidencia sobre la existencia de un dato electrónico. Esta entidad, deberá calcular el hash del documento y componer una petición RFC o web service bien formada para invocar al servicio de generación de la TS@.

La **Autoridad de Sellado** (Time Stamp Authority) es quien ofrece el servicio de sellado. Su finalidad es comprobar el correcto formato de las peticiones y generar un sello de tiempo bien formado acorde al estandar RFC3161 o OasisDSS.

De acuerdo con *IETF RFC 3628 Policy Requirements for Time-Stamping Authorities, una TSA* debe:

- Utilizar una fuente de datos fiable
- Incluir un valor de tiempo fiable en cada sello
- Incluir un entero único en cada sello
- Incluir en cada sello un identificador que indique la política de seguridad con la que el sello ha sido creado.
- Firmar cada sello con una clave generada exclusivamente para este proposito.

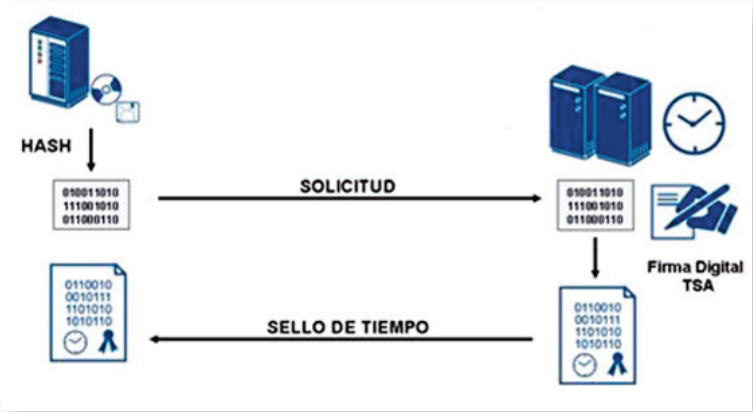
Para cumplir el primer punto (utilizar una fuente de datos fiable) la TSA obtiene el tiempo del Real **Observatorio de la Armada,** mediante el protocolo NTP.

Por último, en el proceso de generación de los sellos intervienen diversos certificados digitales y claves de firma, ya sea para generar el sello o securizar el canal de comunicación entre las distintas entidades. La validez de estos certificados y la caducidad de los mismos se comprueba a través de una plataforma de firma electrónica, siendo @firma el sistema encargado de realizar las validaciones en la TS@ del MPTAP.

## 7 PROCESO DE SELLADO

A continuación se detalla el proceso para la obtención de un sello de tiempo (este proceso puede realizarse mediante el cliente suministrado por la plataforma):

1. El cliente desea generar un sello de tiempo para un documento que posee.
2. Se genera el hash del documento en la máquina del cliente, mediante uno de los algoritmos permitidos por la plataforma.
3. Con el hash, el identificador de política y el identificador de la aplicación se enviará una petición a la plataforma. La estructura de petición será distinta dependiendo del protocolo que se utilice Web-Service, TCP o HTTPS.
4. La plataforma TS@ generará el sello de tiempo con el hash, la fecha y hora, obtenida gracias a un cliente NTP sincronizado con una fuente de tiempo fiable, y la firma electrónica de la TS@.
5. Se envía el sello de tiempo al cliente, al igual que la petición se podrá enviar mediante protocolos diferentes, TCP, Web-Service o HTTPS.




6. La plataforma almacenará todos los sellos emitidos en base de datos para una posible verificación posterior.

# 8 PROCESO DE VERIFICACIÓN

La verificación de un timestamp es el proceso por el cual se comprueba la validez de un sello de tiempo. La definición de este proceso así como el formato de los mensajes queda definido en la norma *XML TimeStamping Profile of the OASIS Digital Signature Services* y sus principales pasos son:

1. El cliente construye una petición de verificación de sello de tiempo acorde a la especificación del protocolo DSS de OASIS. Obligatoriamente, dicha petición deberá contener el hash para el cual se quiere verificar el sello (o el documento completo) así como el sello que se quiere validar.
2. Una vez construida la solicitud, el cliente la envía a la URL y puerto que atenderá la petición.
3. La TS@, al recibir la petición, comprueba la corrección del formato del mensaje y realiza un control de acceso basándose en el identificador de la aplicación presente en la petición, y en los mecanismos de seguridad aportados en esta (certificado digital, usuario/password).
4. Suponiendo que la petición está bien formada y el cliente tiene permisos para realizar la petición:
    a. Si se incluyó el documento en la petición, se calcula el resumen con el algoritmo de hash que aparece en el sello de tiempo, para posteriormente verificarlo con el resumen presente en el sello.
    b. Si se incluyó el resumen del documento, se compara este con el hash presente en el sello de tiempo adjunto.
    c. Se verifica la firma del sello.
    d. Se comprueba la validez del certificado firmante del sello de tiempo, para ello se utilizan los servicios web de validación de certificados de la plataforma @firma.
5. La TS@ genera una respuesta acorde a la norma e incluye el resultado de la verificación efectuada.

# 9 PROCESO DE RESELLADO

El resellado de tiempo consiste en la renovación de un sello de tiempo emitido con antelación. Las principales causas que justifican un resellado de tiempo son la necesidad de reemplazo del algoritmo de resumen empleado en el sello de tiempo a renovar o la proximidad de la fecha de caducidad del certificado de la TS@ con que se firmó el sello.

El resellado de tiempo es una especificación de OASIS enmarcada en sus estándares de Servicios de Firma Digital (DSS). El proceso de resellado de tiempo es similar al de sellado con la salvedad de que en el nuevo sello de tiempo generado se incluye el sello de tiempo anterior. El proceso de generación de una renovación de sello es como sigue:

1. El cliente previamente a la solicitud de resellado ha de verificar que el sello de tiempo previo se corresponde con el documento para el que se solicita el resellado. Esta verificación previa al envío de la solicitud de resellado, especificada en el estándar, es realizada de oficio por el cliente TS@ que facilita @firma

2. El cliente construye una petición de resellado de tiempo según las especificaciones del protocolo DSS de OASIS, en la solicitud se ha de adjuntar obligatoriamente el sello de tiempo a renovar y el hash para el que se solicita el resellado o el resumen del documento y el algoritmo de resumen empleado. Asimismo se han de adjuntar datos de identificación de la aplicación solicitante del servicio de resellado, identificación de aplicación, certificado o usuario y contraseña


3. Una vez construida la solicitud, el cliente la envía a la URL y puerto que atenderá la petición.

4. La TS@ recibe la petición, revisa si la petición está completa y correcta y realiza un control de acceso, para ello se examinan los datos adjuntos a la solicitud, identificador de aplicación, certificado digital en peticiones bajo SSL o usuario y contraseña

5. Si la petición fuese incorrecta o no superase la validación de control de acceso, se le envía al cliente un mensaje indicando el error detectado

6. Si se superan las validaciones anteriores, la TS@ genera un nuevo Sello de Tiempo incluyendo fecha y hora obtenida de una fuente fiable y la firma electrónica de la TS@. En el nuevo sello se incluye el sello anterior, el resumen del documento a resellar y el algoritmo de resumen empleado. Si en la petición de resellado se adjunta el documento, la TS@ calcula el resumen a incluir en el nuevo sello de acuerdo con el algoritmo de resumen configurado en la TS@. Si en la petición de resellado se incluyó el resumen del documento y el algoritmo de resumen, se incluyen estos en el nuevo sello de tiempo generado.
7. El sello de tiempo se envía de vuelta al Cliente.

## 10 CONSIDERACIONES DE SEGURIDAD

A continuación se muestran las características de la Plataforma en lo que respecta a la seguridad y disponibilidad:

- Posee una arquitectura de alta disponibilidad y escalable. La aplicación esta construida para que pueda ser desplegada en diferentes cluster, comunicandose entre sí mediante el framework java jgroups. Esto permite aumentar la escalabilidad del sistema horizontalmente y además ser mas tolerante a posibles fallos, ya que existe un balanceador hardware que redirige las peticiones en caso de caida de un nodo.
- Cuenta con elementos de antivirus, firewalls, sistemas de prevención y detección de instrusos (IPS/IDS), además de las implicitas medidas de seguridad como el cifrado de tráfico disponibles en la red SARA de acceso a la Plataforma.
- Igualmente, se han seguido los criterios y guiás de seguridad propuestas por el Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI) para la configuración de los dispositivos de seguridad, sevidores, bases de datos, etc.
- Utilización de dispositivos seguros de creación de firmas y almacenamiento de claves criptográficas HSM. Estos dispositivos se pueden emplear para la firma de los sellos de tiempo solicitado.

### Seguridad Lógica

Además de los controles habituales del sistema operativo respecto a usuarios y listas de control de acceso, se dispone del control de acceso a los servicios ofrecidos mediante un identificador de aplicación.

Adicionalmente, para garantizar que los mensajes intercambiados con la TS@ no se han alterado, el mensaje se cifra siguiendo la especificación estándar XML Encryption y se firma usando XML Signature como estructura de firma.

**Seguridad Física**

Todos los sistemas se encuentran en redundancia n+1 y sin punto único de fallo, se dispone de los siguientes servicios básicos de infraestructuras en el Centro de Proceso de Datos:

- Alimentación eléctrica ininterrumpida
- Suelo técnico
- Sistemas de Control de Temperatura y Humedad (HVAC)
- Protección de incendios
- Control de acceso seguro 24x7
- Doble ruta de acceso a cables.

En el caso de los servicios de sellado ofrecidos mediante web-services (aquellos especificados en el estándar XML Timestamping Profile of the OASISDigital Signature Services Version 1.0), la comunicación se realiza haciendo uso de servicios web seguros.

WS-Security es un protocolo de comunicación entre plataformas, que provee diversos métodos para la securización de las comunicaciones.

La versión actual del protocolo fue publicada el 17 de febrero de 2006 por OASIS, con el identificador de versión 1.1. Desarrollado originalmente, de manera conjunta por IBM, Microsoft y Verisign, actualmente es denominado como WSS y desarrollado a través del comité OASIS-OPEN.

El protocolo provee medios para autenticar quién realizó la petición. Los métodos principales utilizados son usuario-password y mediante certificado (incluyendo un certificado con formato X.509 en la cabecera del mensaje).

Además de permitir la autenticación del emisor de la petición, permite la firma del mensaje, de manera que el receptor pueda validar que el contenido del mensaje no ha sido alterado durante su envío y el emisor es quien dice ser. La firma se realizará con la clave privada de la TS@, el certificado correspondiente a la clave estará en posesión de todas las aplicaciones que se integren con la TS@.

Para la identificación de la aplicación cliente, la plataforma permite la utilización del token userNameToken, o certificado X.509. Se recomienda utilizar certificado para au-

tenticar al cliente. Tanto los usuarios como los certificados habrán sido previamente asociados a la aplicación solicitante.

Si se desea cifrar los mensajes enviados entre la aplicación cliente y la plataforma se permite el uso de una clave simétrica conocida por ambas partes. Esta clave les será asociada a las aplicaciones a través de la herramienta de administración.

Para la respuesta se podrá solicitar que la plataforma firme los mensajes devueltos, haciendo uso de su clave privada, y habiéndose publicado previamente, para las aplicaciones, su certificado.

# 11 CONSIDERACIONES LEGALES

Como consecuencia de la incorporación de medios telemáticos a la administración pública y para facilitar y agilizar trámites, se ha desarrollado una normativa que permite el uso de la tecnología para el intercambio de documentación y realización de trámites administrativos. Además de las mejoras que esto implica, se intenta garantizar la seguridad y veracidad de la información que se está gestionando.

La plataforma TS@-@firma se realiza con la finalidad de facilitar estos trámites cumpliendo con los requerimientos legales expuestos a continuación.

## 11.1 MARCO LEGAL

- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- 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
- Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica

### 11.2 FUNDAMENTOS JURÍDICOS

A continuación se detallan las referencias a marcas temporales presentes en las leyes anteriormente citadas:

**LEY 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.**

Expone una definición de documento electrónico donde se especifica que, en caso de que el tipo de documento lo requiera, se le podrá asociar una referencia temporal. Además, índica que la Administración General del Estado especificará las entidades válidas para la emisión de sellos de tiempo reconocidos.

*"Artículo 29. Documento administrativo electrónico.*

2. *Los documentos administrativos incluirán referencia temporal, que se garantizará a través de medios electrónicos cuando la naturaleza del documento así lo requiera.*

3. *La Administración General del Estado, en su relación de prestadores de servicios de certificación electrónica, especificará aquellos que con carácter general estén admitidos para prestar servicios de sellado de tiempo."*

*"ANEXO*

*Definiciones*

s) *Sellado de tiempo: Acreditación a cargo de un tercero de confianza de la fecha y hora de realización de cualquier operación o transacción por medios electrónicos."*

**Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos**

Expande la definición de referencia temporal citada en la ley 11/2007 y categoriza estas posibles referencias en sello de tiempo y marca de tiempo, añadiendo una definición de cada uno de estos conceptos. Adicionalmente, determina que la inclusión de un tipo u otro de referencia temporal será dictada por el procedimiento.

Con relación a los prestadores de servicios de certificación, se nombra al Ministerio de la Presidencia (actualmente Ministerio de Política Territorial y Administración Pública) y el Ministerio de Industria y Comercio como responsables de publicar aquellos prestadores admitidos así como de controlar los requisitos que éstos deben cumplir.

*"Artículo 47. Referencia temporal de los documentos administrativos electrónicos.*

1. *La Administración General del Estado y sus organismos públicos dependientes o vinculados asociarán a los documentos administrativos electrónicos, en los términos del artículo 29.2 de la Ley 11/2007, de 22 de junio, una de las siguientes modalidades de referencia temporal, de acuerdo con lo que determinen las normas reguladoras de los respectivos procedimientos:*

   a) *«Marca de tiempo» entendiendo por tal la asignación por medios electrónicos de la fecha y, en su caso, la hora a un documento electrónico. La marca de tiempo será utilizada en todos aquellos casos en los que las normas reguladoras no establezcan la utilización de un sello de tiempo.*

   b) *«Sello de tiempo», entendiendo por tal la asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento.*

*La información relativa a las marcas y sellos de tiempo se asociará a los documentos electrónicos en la forma que determine el Esquema Nacional de Interoperabilidad.*

2. *La relación de prestadores de servicios de certificación electrónica que prestan servicios de sellado de tiempo en la Administración General del Estado, conforme a lo dispuesto en el artículo 29.3 de la Ley 11/2007, de 22 de junio, así como los requisitos que han de cumplirse para dicha admisión, serán regulados mediante el real decreto a que se refiere el artículo 23.3.*

*(Artículo 23. Obligaciones de los prestadores de servicios de certificación.*

3. *Las condiciones generales adicionales a que se refiere el artículo 4.3 de la Ley 59/2003, de 19 de diciembre, se aprobarán mediante real decreto aprobado por el Consejo de Ministros a propuesta conjunta de los Ministerios de la Presidencia y de Industria, Turismo y Comercio, previo informe del Consejo Superior de Administración Electrónica.*

*Corresponde a los Ministerios de la Presidencia y de Industria, Turismo y Comercio publicar la relación de prestadores de servicios de certificación admitidos y de controlar el cumplimiento de las condiciones generales adicionales que se establezcan.)"*

**Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.**

Se especifica que el sello de tiempo será de obligado uso en aquellas aplicaciones que se definan con un nivel de seguridad ALTO (según se establece en el ENS), y que la utilización del servicio se realizará con el fin de garantizar la seguridad en la dimensión correspondiente a la trazabilidad.

*"Artículo 33. Firma electrónica.*

1. *Los mecanismos de firma electrónica se aplicarán en los términos indicados en el Anexo II de esta norma y de acuerdo con lo preceptuado en la política de firma electrónica y de certificados, según se establece en el Esquema Nacional de Interoperabilidad.*

2. *La política de firma electrónica y de certificados concretará los procesos de generación, validación y conservación de firmas electrónicas, así como las características y requisitos exigibles a los sistemas de firma electrónica, los certificados, los servicios de sellado de tiempo, y otros elementos de soporte de las firmas, sin perjuicio de lo previsto en el Anexo II, que deberá adaptarse a cada circunstancia.*

   *Los sellos de tiempo solo aplican en el apartado de seguridad realativo a la trazabilidad e los sistemas y solo en los sistemas de información con un nivel alto de seguridad.*

   *El sello de tiempo actará como una protección en los sistemas de información de nivel alto de seguridad, concretamente en el ámbito de la trazabilidad.*

   *5.7.5 Sellos de tiempo*

| dimensiones | T | | |
|---|---|---|---|
| nivel | bajo | medio | alto |
| | no aplica | no aplica | aplica |

*Los sellos de tiempo prevendrán la posibilidad del repudio posterior:*

1. *Los sellos de tiempo se aplicarán a aquella información que sea susceptible de ser utilizada como evidencia electrónica en el futuro.*

2. *Los datos pertinentes para la verificación posterior de la fecha serán tratados con la misma seguridad que la información fechada a efectos de disponibilidad, integridad y confidencialidad.*

3. *Se renovarán regularmente los sellos de tiempo hasta que la información protegida ya no sea requerida por el proceso administrativo al que da soporte.*

4. *Se utilizarán productos certificados servicios externos admitidos."*

**Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica**

En su Capitulo X se establecen las condiciones que un sistema debe cumplir para custodiar debidamente y recuperar documentos electrónicos. En el punto g) del Artículo 21 especifica que el sello de tiempo, en caso de este existir, debe almacenarse asociado al documento electrónico para el cual fue generado.

*"Artículo 21. Condiciones para la recuperación y conservación de documentos.*

*g) El acceso completo e inmediato a los documentos a través de métodos de consulta en línea que permitan la visualización de los documentos con todo el detalle de su contenido, la recuperación exhaustiva y pertinente de los documentos, la copia o descarga en línea en los formatos originales y la impresión a papel de aquellos documentos que sean necesarios. El sistema permitirá la consulta durante todo el período de conservación al menos de la firma electrónica, incluido, en su caso, el sello de tiempo, y de los metadatos asociados al documento."*

*"Artículo 29. Actualización permanente.*

*b) Documento electrónico: tratará los metadatos mínimos obligatorios, la asociación de los datos y metadatos de firma o de sellado de tiempo, así como otros metadatos complementarios asociados; y los formatos de documento."*

*Glosario de términos:*

***Marca de tiempo:** La asignación por medios electrónicos de la fecha y, en su caso, la hora a un documento electrónico.*

***Sello de tiempo:** La asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento.*

## 12 GLOSARIO DE TÉRMINOS

- **MPTAP:** Ministerio de Política Territorial y Administración Pública.
- **Timestamp o Sello de tiempo:** Asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento.
- **Marca de tiempo:** Asignación por medios electrónicos de la fecha y, en su caso, la hora a un documento electrónico.
- **Fehaciente:** Que da fe de algo. Que asegura autenticidad ante terceros.
- **RFC3161:** Estándar que define el protocolo de comunicación y mensajes de un servicio de sellado de tiempo.
- **RFC3628:** Estándar que define los requerimientos que ha de cumplir una autoridad de sellado de tiempo.
- **IETF:** Internet Engineering Task Force.
- **ROA:** Real Instituto y Observatorio de la Armada.
- **NTP:** Network Time Protocol. Protocolo de red para sincronizar relojes informáticos.
- **Hash:** Función para generar claves que identifican casi unívocamente un documento.
- **@firma:** Plataforma de validación y firma electrónica.
- **TCP:** Transmission Control Protocol.
- **HTTPS:** Hypertext Transfer Protocol Secure. Protocolo de red seguro basado en HTML.
- **URL:** Uniform Resource Locator (Localizador Uniforme de Recursos). También se usa URI.
- **Red SARA:** Sistema de Aplicaciones y Redes para las Administraciones.
- **HSM:** Hardware Security Module.
- **ETSI:** European Telecommunications Standards Institute.

# ÍNDICE