# Manual de Servicios

TS@ 3.1.3

| | |
|---|---|
| Documento nº: | TSA-Servicios-MAN |
| Revisión: | 007 |
| Fecha: | 21-03-2018 |
| Período de retención: | Permanente durante su período de vigencia + 3 años después de su anulación |

## CONTROL DE MODIFICACIONES

| | |
|---|---|
| Documento nº: | TSA-Servicios-MAN |
| Revisión: | 007 |
| Fecha: | 21-03-2018 |

| | |
|---|---|
| Rev. | 001 |
| Fecha | 11-12-2013 |
| Descripción | Documento inicial. |

| | |
|---|---|
| Rev. | 002 |
| Fecha | 10-10-2014 |
| Descripción | Se hace referencia a los tipos de InputDocument aceptados por los servicios DSS. |

| | |
|---|---|
| Rev. | 003 |
| Fecha | 03-02-2015 |
| Descripción | Actualización de las referencias a la revisión 3.1.0_000. Se elimina el control de aprobación y cualquier referencia a autor. |

| | |
|---|---|
| Rev. | 004 |
| Fecha | 06-02-2015 |
| Descripción | Se incluye la nota aclaratoria indicando que la validación del sello previo es responsabilidad del integrador tal y como indican las especificaciones DSS. |

| | |
|---|---|
| Rev. | 005 |
| Fecha | 07-07-2017 |
| Descripción | Se actualiza el tipo de fuente y la nomenclatura para la versión 3.1.3 de la plataforma. |

| | |
|---|---|
| Rev. | 006 |
| Fecha | 02-01-2018 |
| Descripción | Se incluye el anexo A.1 en el que se informa de la necesidad de revisar la Guía 807 del Esquema Nacional de Seguridad. |

| | |
|---|---|
| Rev. | 007 |
| Fecha | 21-03-2018 |
| Descripción | Se eliminan referencias a la ley 11/2007 y se marcan como discontinuados (deprecated) los servicios de validación y renovación de sello de tiempo |

## CONTROL DE DISTRIBUCIÓN

| | |
|---|---|
| Documento nº: | TSA-Servicios-MAN |
| Revisión: | 007 |
| Fecha: | 21-03-2018 |

### Copias Electrónicas:

La distribución de este documento ha sido controlada a través del sistema de información.

### Copias en Papel:

La vigencia de las copias impresas en papel está condicionada a la coincidencia de su estado de revisión con el que aparece en el sistema electrónico de distribución de documentos.

El control de distribución de copias en papel para su uso en proyectos u otras aplicaciones es responsabilidad de los usuarios del sistema electrónico de información.

Fecha de impresión

### Distribución en Papel:

| Nombre o Cargo y Organización | Nº de Ejemplares | Referencia de la carta de transmisión y fecha |
|---|---|---|
| | | |

# Índice

1 Introducción ..... 5

2 Objetivos ..... 6

3 Siglas y Acrónimos ..... 7

4 Glosario de Términos y Definiciones ..... 9

5 Descripción ..... 10

5.1 Requisitos ..... 10

5.2 Beneficiarios ..... 10

6 Caracterización Técnica y Soporte de la Plataforma ..... 11

6.1 Medidas de Seguridad y Disponibilidad de los Servicios ..... 11

6.2 Red SARA ..... 11

6.3 Servicio de Soporte (CAU) ..... 12

7 Requisitos de Acceso al Servicio ..... 13

7.1 Pasos a Dar para Usar los Servicios ..... 13

7.2 Acceso a la Plataforma ..... 13

7.2.1 WS-Security ..... 13

7.2.2 TCP14

7.2.3 HTTPS ..... 15

8 Servicios del Sistema ..... 16

8.1 Solicitar Sello de Tiempo ..... 16

8.2 Validar Sello de Tiempo. Servicio discontinuado (deprecated) ..... 16

8.3 Solicitar Renovación de Sello de Tiempo. Servicio discontinuado (deprecated). ..... 17

A.1 Guía 807 del Esquema Nacional de Seguridad (ENS). ..... 18

# 1 Introducción

La plataforma TS@, integrada con la plataforma @Firma, es una solución tecnológica que ejerce como una Autoridad de Sellado de Tiempo (TSA), por lo que su función se centra en proporcionar servicios de emisión de sellos de tiempo, validación de sellos de tiempo y renovación de sellos de tiempo, estando estos dos últimos discontinuados (deprecated) en la versión actual.

Los servicios de TS@ 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 Entidades Locales. Desde el Ministerio de Hacienda y Administraciones Públicas se ofrece la ayuda y el soporte necesario para que los organismos integren estos servicios de sellado de tiempo sincronizados con la hora oficial del Estado, en los servicios de información de Administración Electrónica. Para ello se ha desarrollado un cliente a integrar dentro de las aplicaciones de aquellos organismos que deseen dotar de una referencia válida de tiempo.

## 2 Objetivos

Cuando la naturaleza de un documento lo requiere, además de la firma electrónica, debe poderse incluir una referencia temporal. Dicha referencia temporal debe ser realizada por medios electrónicos a través de cualquier prestador de servicios de sellado de tiempo admitidos por la Administración General del Estado. En el caso del Ministerio de Hacienda y Administraciones Públicas se dispone para tal labor de la plataforma TS@.

# 3 Siglas y Acrónimos

| | |
|---|---|
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol Secure |
| DSS | Digital Signature Services |
| RFC | Request for Comments |
| SOAP | Simple Object Access Protocol |
| URL | Uniform Resource Locator |
| TCP | Transmission Control Protocol |
| SSL | Secure Sockets Layer |
| IP | Internet Protocol |
| BBDD | Base de Datos |
| SHA | Secure Hash Algorithm |
| XML | eXtensible Markup Language |
| RIPEMD | RACE Integrity Primitives Evaluation Message Digest |
| ASN-1 | Abstract Syntax Notation One |
| SAML | Security Assertion Markup Language |
| HSM | Hardware Security Module |
| WS | Web Service |
| SARA | Sistemas de Aplicaciones y Redes para las Administraciones |
| IPS | Sistema de Prevención de Intrusos |
| IDS | Sistema de Detección de Intrusos |
| SAN | Red de Área de Almacenamiento |
| PNC | Punto Neutro de Comunicaciones |
| AGE | Administración General del Estado |

| | |
|---|---|
| IA | Intranet Administrativa |
| IPsec | Internet Protocol Security |
| DER | Distinguish Encoding Rules |

# 4 Glosario de Términos y Definiciones

| | |
|---|---|
| TS@ | Plataforma de Sellado de Tiempo |
| @Firma | Plataforma de Validación y Firma Electrónica |

# 5 Descripción

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.
- OASIS Digital Signature Service Core Protocols, Elements, and Bindings version 1.0.
- ETSI TS 101 861 Time stamping profile.

TS@ está basada en software libre, estándares abiertos y desarrollada con java.

## 5.1 Requisitos

Para acceder a los servicios es necesario disponer de accesibilidad a la plataforma desde los sistemas de información del organismo en cuestión a través de la red que ofrece servicios de intranet entre las administraciones públicas. Estos sistemas que soportan los servicios de administración electrónica disponibles para los ciudadanos y empresas, accederán a la plataforma a través de servicios web, peticiones HTTPS o mediante peticiones TCP.

## 5.2 Beneficiarios

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 Ministerio de Hacienda y Administraciones Públicas 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.

# 6 Caracterización Técnica y Soporte de la Plataforma

La herramienta externa de importación inicial es una herramienta que se ejecuta a través de consola, generada para poder reutilizar los datos de configuración de la versión 2.1.2 de la TS@ en la versión 3.1.3.

## 6.1 Medidas de Seguridad y Disponibilidad de los Servicios

La plataforma presenta las siguientes características sobre seguridad y disponibilidad:

- Arquitectura en alta disponibilidad y escalable.
- Elementos de antivirus, firewalls, IPS/IDS, además de las implícitas medidas de seguridad como cifrado de tráfico disponibles en la red SARA.
- Seguimiento de criterios y guías de seguridad propuestas por el Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI) para la configuración de dichos dispositivos de seguridad, servidores, BBDD, etc.
- Utilización de sistemas almacenamiento masivo externo SAN de alto rendimiento y disponibilidad, donde se hospedan todas las transacciones y ficheros de auditoría.
- Utilización de dispositivos seguros de creación de firmas y almacenamiento de claves criptográficas HSM.
- Centro Espejo de respaldo. Se dispone de un centro espejo de contingencias en estado latente que entraría en operación para ofrecer los servicios de la plataforma principal de servicios de validación y firma electrónica ante una falta de disponibilidad grave y longeva en dicho centro.

## 6.2 Red SARA

El acceso a los servicios de TS@ se realiza a través de SARA, una infraestructura tecnológica que permite y garantiza la comunicación entre las distintas administraciones además de servir de plataforma de intercambio de aplicaciones. Constituye una extranet de comunicaciones que da soporte a la interoperabilidad entre aplicaciones de diferentes organismos públicos.

Incluido dentro de la infraestructura base proporcionada por SARA se dispone de un PNC que posibilita la accesibilidad a los servicios de la plataforma desde múltiples operadores de comunicaciones, dentro de un esquema de direccionamiento IP privado y con las mayores garantías de monitorización.

La red SARA como infraestructura básica de comunicaciones y servicios telemáticos de la AGE se conecta al punto neutro mediante dos enlaces Ethernet (100 Mbps) en alta disponibilidad cada uno de ellos con un operador distinto.

La conexión de un nodo de la AGE con la red troncal de la IA cuenta con un enlace principal y otro de respaldo también con 2 operadores distintos, lo que proporciona un aseguramiento en la fiabilidad y continuidad en el servicio prestado. Adicionalmente y como medida de seguridad la información transita a través de la red troncal cifrada mediante el establecimiento de túneles IPSec.

SARA cuenta con un servicio de soporte 24x7 en el que los tiempos de respuesta y de resolución dependen de la severidad de la incidencias en base a una categorización de los servicios que por ella transitan y de los agentes que participen extremo a extremo.

## 6.3 Servicio de Soporte (CAU)

SARA, y por tanto TS@, disponen de un servicio de soporte 24x7 para atender las posibles incidencias o anomalías que pudieran ocurrir. Este servicio está disponible de lunes a viernes de 8h a 20h para resolver las dudas o consultas de los integradores del sistema.

**Correo Electrónico:** soporte.afirma5@seap.minhap.es

# 7 Requisitos de Acceso al Servicio

## 7.1 Pasos a Dar para Usar los Servicios

A continuación, se detallan los pasos que un organismo debe dar para solicitar el acceso a los servicios de TS@:

1. Ponerse en contacto con el CAU de TS@ indicando qué tipo de organismo es (Ministerio, Comunidad Autónoma o Entidad Local), así como los datos de contacto del mismo.

2. Recibir respuesta del CAU sobre los requisitos que son necesarios para iniciar la integración. Se informará de que los servicios se ofrecen a través de la red SARA, y que es posible realizar pruebas controladas en un entorno de desarrollo habilitado al efecto desde Internet.

3. Recibir la documentación de bienvenida del CAU que consiste en:

   a. ACL (Formulario para el Control de Acceso).

   b. Manual de Servicios de TS@.

   c. Manual del Integrador del Cliente de TS@

4. Remitir al CAU debidamente cumplimentado el ACL.

5. Recibir del CAU los parámetros de conexión con los servicios, esto es, URL de los mismos, identificadores de aplicaciones, etc.

## 7.2 Acceso a la Plataforma

Como se ha indicado anteriormente, el acceso a los servicios de la plataforma puede llevarse a cabo mediante servicio web (de ahora en adelante, interfaz web), o mediante TCP o HTTPS (de ahora en adelante, interfaz RFC 3161):

### 7.2.1 WS-Security

WS-Security es un protocolo de comunicación entre plataformas, que provee diversos métodos para asegurar 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 es desarrollado a través del comité OASIS-OPEN. La

comunicación en este sentido con la TS@ se hará mediante mensajes SOAP que siempre deberán incluir el identificador de aplicación cliente, asignado por el soporte de @Firma.

WS-Security incorpora características de seguridad en el encabezado de un mensaje SOAP, así, para permitir una conexión segura con la TS@, toda aplicación que requiera hacer uso de los servicios de TS@ deberá autenticarse frente a la misma. Para ello la plataforma permite dos métodos de autenticación para el emisor de la petición:

- Usuario/Contraseña: Es el modo de autenticación menos seguro. Las peticiones SOAP contendrán el tag de seguridad "UserNameToken" de manera que el usuario y la contraseña alojados en dicho tag deben estar registrados en la TS@ para la aplicación que hace uso del servicio web.

- Certificado: Es el modo de autenticación más seguro y por tanto el recomendado. La petición SOAP se encontrará firmada haciendo uso de un certificado X.509. El certificado correspondiente a la clave utilizada para generar la firma debe estar registrado en la TS@.

Si se desea cifrar los mensajes SOAP enviados hacia la plataforma se permite el uso de una clave simétrica conocida tanto por la aplicación cliente como por la plataforma TS@. Igualmente es posible asegurar los mensajes SOAP enviados hacia la plataforma mediante afirmaciones SAML.

Por su parte, la plataforma TS@ permite también asegurar los mensajes SOAP que devuelve a los clientes firmando las respuestas SOAP y cifrándolas con clave simétrica.

La configuración de todas estas características se lleva a cabo desde la herramienta de administración de la TS@. El proceso de integración de la aplicación cliente con la plataforma a través de servicios Web se encuentra ya implementado en el cliente de la TS@. Más información sobre cómo integrar una aplicación cliente con el cliente se encuentra en el documento "*TSA-@Firma-Manual Usuario Cliente*".

### 7.2.2 TCP

La plataforma a través de la interfaz TCP posibilita la petición y obtención de sellados de tiempo. El protocolo utilizado se encuentra definido en la especificación *RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol*.

La plataforma dispone de dos interfaces distintas para recibir este tipo de peticiones, una sin securización y otra securizada mediante SSL. Los puertos donde se encontrarán desplegados los dos servicios serán ofrecidos por los administradores de la plataforma.

Dentro de cada petición, debe incluirse el identificador de aplicación cliente, asignado por el soporte de @Firma. Este identificador se incluirá como extensión dentro de la estructura "TimeStampRequest" enviada a la plataforma.

Para facilitar este proceso de inclusión de extensiones y generación de estructuras, se ha desarrollado el cliente de la TSA, puede dirigirse al documento *"TSA-@Firma-Manual Usuario Cliente*" para más información al respecto.

### 7.2.3 HTTPS

La plataforma despliega el servicio de generación de sellos por el protocolo HTTPS admitiendo peticiones *requestTimeStampHTTPS*. Dentro de cada petición, debe incluirse el identificador de aplicación cliente, asignado por el soporte de @Firma.

Los administradores del sistema informarán del puerto donde se encuentra desplegada esta interfaz.

El cliente de la TS@ facilita la interacción con la plataforma encapsulando la generación de las peticiones. Para más información se encuentra el manual de integración del cliente "*TSA-@Firma-Manual Usuario Cliente*".

# 8 Servicios del Sistema

Actualmente, TS@ publica los servicios de sello de tiempo de las formas siguientes:

- ✓ Notación abstracta ASN.1, cumpliendo con las especificaciones de la IETF RFC3161, utilizando sintaxis de peticiones y respuestas en notación abstracta ASN.1 codificado en DER.
- ✓ Servicios web utilizando la especificación de mensajes XML-SOAP.

Los servicios disponibles son:

## 8.1 Solicitar Sello de Tiempo

La solicitud de sellos de tiempo a la TS@ se podrá realizar a través de cualquiera de las dos interfaces:

- Interfaz Web: Permite generar sellos de tiempo en formato XML y ASN.1. Los algoritmos de resumen que soporta para la generación son SHA-1 y SHA-256. Los datos a sellar (elemento *InputDocuments*) pueden ser incluidos en un elemento del tipo *dss:Document*, *dss:TransformedData* o *dss:DocumentHash*, tal y como se indica en el estándar Digital Signature Service Core Protocols, Elements, and Bindings version 1.0 de OASIS. El tipo *dss:AnyType* no está permitido.
- Interfaz RFC 3161: Permite generar sellos de tiempo en formato ASN.1. Los algoritmos de resumen que soporta para la generación son SHA-1, SHA-256, SHA-512 y RIPMED-160.

Tanto el algoritmo de resumen como el certificado a usar para generar el sello de tiempo serán definidos en la Administración de la TS@ para cada una de las aplicaciones cliente.

## 8.2 Validar Sello de Tiempo. Servicio discontinuado (deprecated).

La solicitud de validación de sellos de tiempo a la TS@ sólo podrá realizarse a través de la interfaz web. Al igual que para la generación de sello de tiempo, los datos a validar (elemento *InputDocuments*) pueden ser incluidos en un elemento del tipo *dss:Document*, *dss:TransformedData* o *dss:DocumentHash*, tal y como se indica en el estándar Digital Signature Service Core Protocols, Elements, and Bindings version 1.0 de OASIS. El tipo *dss:AnyType* no está permitido.

## 8.3 Solicitar Renovación de Sello de Tiempo. Servicio discontinuado (deprecated).

La utilidad más importante del servicio de renovación de sello de tiempo consiste en preservar la longevidad de la validez de los sellos generados sobre los documentos o transacciones, en caso de que se pueda poner en cuestión la validez de un sello emitido.

Por medio de este servicio se proporciona la funcionalidad de generar un nuevo sello de tiempo para una acción de firma de datos o de documento. Sólo se podrá realizar una petición de renovación de sello de tiempo a través de la interfaz web usando un algoritmo de resumen SHA-1 o SHA-256 y únicamente para generar un nuevo sello de tiempo en formato XML. Los datos a sellar (elemento *InputDocuments*) pueden ser incluidos en un elemento del tipo *dss:Document*, *dss:TransformedData* o *dss:DocumentHash*, tal y como se indica en el estándar Digital Signature Service Core Protocols, Elements, and Bindings version 1.0 de OASIS. El tipo *dss:AnyType* no está permitido.

Según las especificaciones DSS, antes de solicitar una renovación de un sello de tiempo, se debe proceder a validar el sello de tiempo que se enviará a la plataforma para ser renovado. Dicha responsabilidad de la validación del sello de tiempo es exclusiva del integrador, es decir, la plataforma TS@ no llevará a cabo una validación del sello de tiempo enviado en el servicio de renovación de sello de tiempo.

## A.1 Guía 807 del Esquema Nacional de Seguridad (ENS).

Les comunicamos que los productos de la Suite de @firma pueden contener entre los algoritmos disponibles, algunos no recomendados por la Guía 807 del Esquema Nacional de Seguridad (ENS; editada por el Centro Criptológico Nacional, CCN) vigente en el momento de publicación de este documento. Por lo que queda bajo la responsabilidad de las aplicaciones que hacen uso de estos productos el configurar adecuadamente las llamadas a los mismos para generar el resultado esperado, válido y adecuado para ese momento y el nivel de seguridad deseado, utilizando para ello algoritmos de la familia SHA-2 tal y como especifica dicha norma para la generación de firmas electrónicas.

Pueden consultar la norma vigente en el siguiente enlace:

https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file.html