



Consejería de Hacienda y Administración Pública

Autoridad de Sellado de Tiempo

Política y declaración de prácticas

Versión: v01r01

Fecha: 28/06/2012

Queda prohibido cualquier tipo de explotación y, en particular, la reproducción, distribución, comunicación pública y/o transformación, total o parcial, por cualquier medio, de este documento sin el previo consentimiento expreso y por escrito de la Junta de Andalucía.

HOJA DE CONTROL

Título	Autoridad de Sellado de Tiempo de la Junta de Andalucía		
Entregable	Política y declaración de prácticas		
Nombre del Fichero	TSA_Politica_y_declaración_de_prácticas_v01r01.doc		
Autor	Dirección General de Política Digital		
Versión/Edición	v01r01	Fecha Versión	28/06/2012
		Nº Total Páginas	019

REGISTRO DE CAMBIOS

Versión	Causa del Cambio	Responsable	Área	Fecha
v01r00	Versión con OID	DGTHAE	SCAE	15/03/2012
v01r01	Revisión.	DGPD	SCAE	28/06/2012

CONTROL DE DISTRIBUCIÓN

Nombre y Apellidos	Cargo	Área
Manuel Perera Domínguez <i>manuel.perera@juntadeandalucia.es</i>	Jefe de Servicio	Servicio de Coordinación de Administración Electrónica
José Ignacio Cortés Santos <i>josei.cortes@juntadeandalucia.es</i>	Gabinete de Administración Electrónica	Servicio de Coordinación de Administración Electrónica

ÍNDICE

1	Introducción	4
2	Conceptos generales	6
2.1	Servicio de sellado de tiempo	6
2.2	Servicio de validación de sellos de tiempo	7
2.3	Servicio de resellado de tiempo	7
2.4	Suscriptores.....	8
3	Política de sellado de tiempo	10
4	Obligaciones y responsabilidades.....	13
4.1	Autoridad de Sellado de Tiempo	13
4.2	Cliente	15
5	Requerimientos operacionales	16
5.1	Operación, alta disponibilidad, respaldo y continuidad.	16
5.2	Obtención del tiempo fiable	16
5.3	Certificado de TSA.....	17
6	Glosario de términos y acrónimos	18
7	Normas y estándares de aplicación.....	19

1 Introducción

La Autoridad de Sellado de Tiempo (TSA) de la Junta de Andalucía es un proyecto, puesto a disposición de la Administración de la Junta de Andalucía y otras administraciones andaluzas, para proporcionar un servicio gratuito de sellado de tiempo: emisión de sellos de tiempo, validación de sellos de tiempo y resellado.

La Autoridad de Sellado de Tiempo es una solución tecnológica basada en el software TS@ desarrollado por la Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, del Ministerio de Hacienda y Administraciones Públicas, implantada en la Junta de Andalucía en el marco del artículo 45.1 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. La información sobre este software está disponible en el Centro de Transferencia de Tecnología (CTT) del Portal de Administración electrónica (PAe) de la Administración General del Estado, en la siguiente dirección: <https://administracionelectronica.gob.es/es/ctt/tsa>

El presente documento establece las reglas generales empleadas por la Autoridad de Sellado de Tiempo en la prestación de servicios. Los sellos provistos garantizan y dan fe de la existencia de documentos electrónicos y realización de actuaciones en un instante de tiempo dado, condición que puede resultar necesaria para garantizar la validez de determinadas actuaciones realizadas por medios electrónicos y de acuerdo a la normativa aplicable.

El artículo 27.3 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, dispone que las comunicaciones a través de medios electrónicos serán válidas siempre que exista constancia de la transmisión y recepción, de sus fechas, del contenido íntegro de las comunicaciones y se identifique fidedignamente al remitente y al destinatario de las mismas. En el Anexo se define el sellado de tiempo como la acreditación a cargo de un tercero de confianza de la fecha y hora de realización de cualquier operación o transacción por medios electrónicos.

En el Anexo II del 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 contemplan dos medidas de seguridad de relevancia en esta materia: 5.7.4 (firma electrónica) y 5.7.5 (sellos de tiempo) en las cuales se establecen directrices para la emisión de sellos de tiempo atendiendo a la categorización realizada en materia de seguridad de los sistemas y servicios de acuerdo al Anexo I del Esquema y en función de las denominadas “dimensiones de seguridad”.

La Autoridad de Sellado de Tiempo no es un sistema de “usuario final” sino que sus servicios son invocados por otros sistemas clientes, principal pero no exclusivamente, las implantaciones de la plataforma @firma de identificación y firma electrónica, la plataforma de registro electrónico de la Administración de la Junta de Andalucía y la plataforma de notificaciones telemáticas de la Administración de la Junta de Andalucía.

Las garantías que la TSA proporciona a través de este tipo de servicios están basadas en la certificación, mediante técnicas de firma electrónica, de una representación del conjunto de datos sobre los que proporcionar la evidencia. Así pues, para la prestación del servicio, se requiere una

 <p>JUNTA DE ANDALUCÍA</p>	<p>Consejería de Hacienda y Administración Pública Dirección General de Política Digital</p>	<p>Autoridad de Sellado de Tiempo Política y declaración de prácticas</p>	
---	---	---	---

petición previa por parte del solicitante del fechado (se envía la representación del conjunto de datos) a la que se contestará con el documento electrónico correspondiente (sello de tiempo).

La presente Política y declaración de prácticas es conforme a la norma del ETSI TS 102 023 v1.2.2 “Policy requirements for time-stamping authorities” y a su especificación equivalente RFC 3628.

2 Conceptos generales

Para los propósitos del presente documento, se aplican los siguientes términos y definiciones:

- **Autoridad de Sellado de Tiempo:** Sistema de emisión y gestión de sellos de tiempo.
- **Suscriptor o Cliente:** Persona o entidad que solicita los servicios proporcionados por la Autoridad de Sellado de Tiempo.
- **Token de sello de tiempo:** Estructura de datos empleada en un proceso de creación de firma electrónica, que une la representación de un dato a un tiempo concreto, estableciendo así evidencia de que el dato existía en ese momento.

2.1 Servicio de sellado de tiempo

La TSA genera sellos de tiempo codificados en ASN.1, según el estándar RFC 3161 de la IETF (token RFC 3161 timestamp), o en formato XML/XAdES según el estándar definido por OASIS, Digital Signature Services Versión 1.0 (token dss:TimeStamp).

Los pasos para generar un sello de tiempo son los siguientes:

- El cliente construye una solicitud de sello de tiempo para un documento concreto en uno de los formatos nombrados anteriormente, ASN.1 o XML. Las solicitudes incluirán un resumen del documento.
- Una vez construida la solicitud, el cliente la envía a la URL y puerto que atenderá la petición.
- La TSA recibe la petición, revisa si está completa y es correcta y realiza un control de acceso, para ello se examinan los datos adjuntos a la solicitud, identificador de aplicación, certificado electrónico o usuario y contraseña.
- Si la petición fuese incorrecta o no superase la validación de control de acceso, se envía al cliente un mensaje indicando el error detectado.
- Si la petición fuese correcta y superase la validación de control de acceso, la TSA genera un sello de tiempo incluyendo fecha y hora obtenida de una fuente fiable y la firma electrónica de la TSA. El sello generado tendrá un formato acorde a la solicitud realizada.
- El sello de tiempo se remite al cliente.
- El cliente debe validar la firma del sello y custodiarlo debidamente.

La plataforma almacenará en base de datos todos los sellos emitidos.

2.2 Servicio de validación de sellos de tiempo

A través de este servicio se proporciona la posibilidad de verificar la validez de un sello de tiempo previamente emitido por la propia Autoridad de Sellado de Tiempo.

La validación de sellos de tiempo es una especificación de OASIS enmarcada en sus estándares de Servicios de Firma Digital (DSS).

El proceso de validación de sellos de tiempo es el siguiente:

- El cliente construye una petición de verificación de sello de tiempo según las especificaciones del protocolo DSS de OASIS. En la solicitud se ha de adjuntar el sello de tiempo a validar, datos de identificación de la aplicación solicitante del servicio, certificado electrónico o usuario y contraseña utilizada, el resumen del documento y el algoritmo de resumen empleado.
- Una vez construida la solicitud, el cliente la envía a la URL y puerto que atenderá la petición.
- La TSA recibe la petición, revisa si está completa y es correcta y realiza un control de acceso, para ello se examinan los datos adjuntos a la solicitud, identificador de aplicación, certificado electrónico o usuario y contraseña.
- Si la petición fuese incorrecta o no superase la validación de control de acceso, se envía al cliente un mensaje indicando el error detectado.
- Si la petición es correcta y supera la validación de control de acceso:
 - a) Se compara el resumen del documento con el que consta en el sello de tiempo.
 - b) Se comprueba la firma electrónica del sello de tiempo.
 - c) Se verifica la validez del certificado electrónico firmante del sello de tiempo. Para ello se utilizan los servicios de validación de la implantación corporativa de la plataforma @firma de la Junta de Andalucía.
- La TSA genera una respuesta en la que incluye el resultado de la validación efectuada y la envía al cliente.
- El cliente debe validar la firma de la respuesta recibida.

2.3 Servicio de resellado de tiempo

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 TSA 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:

- 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 software cliente facilitado para interactuar con la TSA.
- El cliente construye una petición de resellado de tiempo según las especificaciones del protocolo DSS de OASIS. En la solicitud se ha de adjuntar el sello de tiempo y el resumen del documento para el cual fue emitido. Asimismo se han de adjuntar datos de identificación de la aplicación solicitante del servicio de resellado, identificación de aplicación, certificado electrónico o usuario y contraseña.
- Una vez construida la solicitud, el cliente la envía a la URL y puerto que atenderá la petición.
- La TSA recibe la petición, revisa si está completa y es correcta y realiza un control de acceso, para ello se examinan los datos adjuntos a la solicitud, identificador de aplicación, certificado electrónico o usuario y contraseña.
- Si la petición fuese incorrecta o no superase la validación de control de acceso, se envía al cliente un mensaje indicando el error detectado.
- Si se superan las validaciones anteriores, la TSA genera un nuevo sello de tiempo incluyendo fecha y hora obtenida de una fuente fiable y la firma electrónica de la TSA. En el nuevo sello de tiempo se incluye el sello anterior, el resumen del documento a resellar y el algoritmo de resumen empleado.
- Se incluye el resumen del documento y el algoritmo de resumen en el nuevo sello de tiempo generado.
- El sello de tiempo se envía de vuelta al cliente.
- El cliente debe validar la firma del sello y custodiarlo debidamente.

2.4 Suscriptores

Los suscriptores son los usuarios del sistema que hayan solicitado y obtenido la autorización de acceso a los servicios de la Autoridad de Sellado de Tiempo de la Junta de Andalucía:

- a) Aplicaciones y sistemas informáticos de la Junta de Andalucía.
- b) Aplicaciones y sistemas informáticos de otras Administraciones Públicas de Andalucía.

 <p>JUNTA DE ANDALUCÍA</p>	<p>Consejería de Hacienda y Administración Pública Dirección General de Política Digital</p>	<p>Autoridad de Sellado de Tiempo Política y declaración de prácticas</p>	
---	---	---	---

Los suscriptores tienen a su disposición un servicio técnico de soporte y atención de consultas, dudas e incidencias, articulado mediante herramienta informática disponible en la siguiente dirección:

<http://www.juntadeandalucia.es/haciendayadministracionpublica/ae>

Los suscriptores deberán utilizar los servicios atendiendo a lo dispuesto en el documento “Guía de uso del sello de tiempo y marca de tiempo. Uso de la TS@ (Time Stamping Authority)” publicado por la Secretaría General Técnica del Ministerio de Hacienda y Administraciones Públicas.

3 Política de sellado de tiempo

La presente Política y declaración de prácticas establece el conjunto de reglas utilizadas durante la emisión y el control de los tokens de sello de tiempo (TST).

El perfil del certificado de la TSA, utilizado en la firma de los TST, se ajusta a lo especificado por el IETF en RFC 3161 y siendo su uso exclusivo para la firma de sellos de tiempo. En la siguiente tabla se detallan los campos básicos de este perfil:

Campo	Contenido
Version	V3
Serial Number	3C:D5:33:0D
Signature Algorithm	sha1RSA
Issuer Distinguished Name	OU = FNMT Clase 2 CA O = FNMT C = ES
Subjet	CN = TSA JUNTA DE ANDALUCIA OU = 500070015 OU = Publicos OU = FNMT Clase 2 CA O = FNMT C = ES
KeyUsage	Firma digital (80)
ExtendedKeyUsage	Impresión de fecha (1.3.6.1.5.5.7.3.8)

La Autoridad de Sellado de Tiempo emite los sellos de tiempo acorde a la recomendación ETSI TS 101 861. Los servicios que proporciona son accesibles en las siguientes direcciones y puertos:

Red Corporativa de la Junta de Andalucía (RCJA)

Nombre DNS: tsaexp.chap.junta-andalucia.es

Peticiones según RFC 3161

Peticiones bajo TCP y SSL: 10318

Peticiones bajo HTTPS: 8443

o Solicitudes HTTPS:

<https://tsaexp.chap.junta-andalucia.es/tsa/TspHttpServer>

Peticiones según estándar OASIS (DSS)

- Servicios Web:

- Acceso HTTP (8080):

- <http://tsexp.chap.junta-andalucia.es:8080/tsa/VerifyTimeStampWS>

- <http://tsexp.chap.junta-andalucia.es:8080/tsa/RenewTimeStampWS>

- <http://tsexp.chap.junta-andalucia.es:8080/tsa/CreateTimeStampWS>

- Acceso HTTPS (443):

- <https://tsexp.chap.junta-andalucia.es/tsa/VerifyTimeStampWS>

- <https://tsexp.chap.junta-andalucia.es/tsa/RenewTimeStampWS>

- <https://tsexp.chap.junta-andalucia.es/tsa/CreateTimeStampWS>

Red Interadministrativa de la Junta de Andalucía (NEREA) e Internet

Nombre DNS: ws176.juntadeandalucia.es

Peticiones según RFC 3161

Peticiones bajo HTTPS: 8443

- Solicitudes HTTPS:

- <https://ws176.juntadeandalucia.es/tsa/TspHttpServer>

Peticiones según estándar OASIS (DSS)

- Servicios Web:

- Acceso HTTPS (443):

- <https://ws176.juntadeandalucia.es/tsa/VerifyTimeStampWS>

- <https://ws176.juntadeandalucia.es/tsa/RenewTimeStampWS>

- <https://ws176.juntadeandalucia.es/tsa/CreateTimeStampWS>

Los solicitantes de los servicios de la TSA tendrán a su disposición la información relativa a los servicios prestados y formalizados en la presente Política y declaración de prácticas.

La información de la Política se especifica en la siguiente tabla:



Documento	TSA_Politica_y_declaración_de_prácticas_v01r01.doc
Versión	1.0
Estado del documento	Vigente
O.I.D.	2.16.724.1.6.1.1
Fecha de emisión	15/03/2012
Punto de publicación	http://www.juntadeandalucia.es/haciendayadministracionpublica/ae

El identificador de la política de la Autoridad de Sellado de Tiempo de la Junta de Andalucía está incluido en cada sello de tiempo.

4 Obligaciones y responsabilidades

4.1 Autoridad de Sellado de Tiempo

La Autoridad de Sellado de Tiempo se obliga a:

- Respetar lo dispuesto en esta Política y declaración de prácticas.
- Proteger sus claves privadas de forma segura.
- Emitir sellos de tiempo conforme a esta Política y declaración de prácticas y a los estándares de aplicación.
- Garantizar que la fecha y hora incluida en los sellos de tiempo se ha obtenido a partir de una fuente fiable.
- Emitir sellos de tiempo según la información enviada por el cliente y libres de errores de entrada de datos.
- Emitir sellos de tiempos cuyo contenido mínimo sea el definido por la normativa vigente, cuando sea aplicable.
- Publicar esta Política y declaración de prácticas en el punto de acceso electrónico de la Consejería de la Junta de Andalucía competente en materia de desarrollo de la Administración Electrónica.
- Informar sobre las modificaciones de la Política y declaración de prácticas a los suscriptores.
- Establecer mecanismos de generación, custodia y seguridad de la información relevante en sus actividades.

La TSA no garantiza la veracidad de los contenidos representados por los datos electrónicos objeto del sellado de tiempo, ni su autoría. Asimismo, tampoco los avala, ni participa en su creación en modo alguno, ni es responsable del uso que se pudiera hacer de ellos ni de los efectos que pudiera tener en los interesados y/o terceras partes, ni mantiene vínculo alguno con la procedencia o causalidad de dichos datos electrónicos.

La TSA no se hace responsable de la veracidad ni de los contenidos representados por los datos electrónicos objeto del sello de tiempo que emite.

La TSA, a través de su servicio de sellado de tiempo, exclusivamente garantiza la existencia de unos datos, que bien pudieran ser una representación particular de otros, en el instante de tiempo en el que recibe la solicitud y determinado por la referencia temporal empleada. Esta garantía se expresa a través de la firma electrónica conjunta de dichos datos y dicha referencia temporal con un certificado electrónico específicamente emitido para la TSA. No resultará válida cualquier interpretación de las

garantías que proporcionan los sellos de tiempo que emite más allá de lo expresado anteriormente. La Autoridad de Sellado de Tiempo es una tercera parte de confianza sin un interés particular en los documentos que se han fechado en el tiempo.

La TSA no garantizará los algoritmos y estándares criptográficos utilizados ni responderá de los daños causados por ataques externos a los mismos.

La TSA no será responsable de los daños y perjuicios y/o funcionamiento defectuoso que los sellos de tiempo emitidos por ella puedan producir en los usos que puedan realizarse, ya sean estos por responsabilidad de los interesados o por defectos de origen de los elementos.

La TSA no responderá ante personas, entidades y sistemas cuyo comportamiento en la utilización de los servicios y/o los propios sellos de tiempo, haya sido negligente, debiendo considerarse a estos efectos y en todo caso como negligencia la falta de observancia de lo dispuesto en el presente documento, en la documentación técnica para el acceso y utilización de los servicios y en la normativa aplicable.

La responsabilidad financiera no es aplicable por no tratarse de un servicio de emisión de certificados electrónicos reconocidos según lo estipulado en el artículo 20.2 de la Ley de 59/2003, de 19 de diciembre, de firma electrónica. La TSA no será responsable en caso de pérdidas de transacciones o procesos de cualquier índole.

La TSA no será responsable en ningún caso cuando se encuentre ante cualquiera de estas circunstancias:

- Estado de guerra, desastres naturales, funcionamiento defectuoso de los servicios eléctricos, las redes telemáticas o de los equipos informáticos utilizados por el cliente u otros terceros, o cualquier otro caso de fuerza mayor.
- Por el uso indebido o fraudulento de los sellos de tiempo.
- Por el uso indebido de la información.
- Por el contenido de los mensajes o documentos sellados.
- Las acciones u omisiones de los suscriptores de los servicios de la TSA.
- Falta de veracidad de la información suministrada para emitir el sello.
- Negligencia en la conservación de los datos de acceso a los servicios, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación.
- Extralimitación en el uso del sello de tiempo, según lo dispuesto en la normativa vigente y en este documento.
- Falta de comprobación de la suspensión o pérdida de vigencia del certificado electrónico de la TSA o falta de verificación de la firma electrónica.

Cese de la actividad

El cese de actividad de la TSA se comunicará a los suscriptores de sus servicios con antelación mínima de dos meses, o el periodo que establezca la legislación vigente.

La TSA efectuará la transmisión de todo el registro de log y evidencia a quien se considere para poder demostrar la correcta operación del servicio durante un periodo de tiempo al menos de 5 años.

La TSA procederá a la destrucción de las claves privadas con las que firma los sellos de tiempo y de las copias de respaldo que de ellas poseyese.

La TSA procederá asimismo a la revocación del certificado con el que firma los sellos de tiempo y que en el momento fuera vigente, finalizando la validez del mismo a partir de ese momento.

4.2 Cliente

El cliente o usuario de los servicios prestados por la TSA estará obligado a cumplir con lo dispuesto por la normativa aplicable y además a:

- Con carácter general, seguir los procedimientos y directrices expresadas en el presente documento y en la documentación técnica de acceso y utilización de los servicios.
- Respetar lo dispuesto en las condiciones de suscripción a los servicios de la TSA y su utilización.
- Verificar la corrección de la firma electrónica de los sellos de tiempo.

5 Requerimientos operacionales

5.1 Operación, alta disponibilidad, respaldo y continuidad.

La operación tecnológica de la Autoridad de Sellado de Tiempo se desarrolla al amparo del Proceso de Planificación y Gestión de Infraestructuras Digitales, en el marco del Plan Estratégico de Sistemas y Tecnologías de la Información de la Consejería de Hacienda y Administración Pública como instrumento que vertebra y pone en práctica la estrategia corporativa y la estrategia sectorial de los sistemas de gestión para la prestación de servicios de la Consejería, sirviendo de impulso a un proceso continuo de modernización en el ámbito de las Tecnologías de la Información y Comunicación que permita alinear la infraestructura tecnológica actual y futura de la Consejería al marco competencial.

La arquitectura tecnológica de la TSA es de naturaleza escalable y de alta disponibilidad. Está construida para que pueda ser desplegada en diferentes cluster. Esto permite aumentar la escalabilidad del sistema horizontalmente y además ser más tolerante a posibles fallos, disponiéndose de un balanceador hardware que redirige las peticiones en caso de caída de un nodo. Se dispone de los servicios básicos de infraestructura en el centro de infraestructuras digitales de la Consejería de Hacienda y Administración Pública: alimentación eléctrica ininterrumpida, suelo técnico, sistemas de control de temperatura y humedad, protección de incendios y control de acceso permanente.

Existe un servicio técnico 24x7 para la atención a problemas en la prestación de servicios de la plataforma y garantía de la alta disponibilidad.

El sistema está incorporado en los servicios de respaldo y continuidad del Centro de Respaldo de la Junta de Andalucía.

5.2 Obtención del tiempo fiable

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, para dar cumplimiento a lo dispuesto en el artículo 15 del 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.

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" considerada a todos los efectos como la base de la hora legal (Real Decreto 1308/1992, de 23 octubre).

5.3 Certificado de TSA

El certificado empleado por la TSA ha sido generado por la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda (FNMT-RCM) de acuerdo con las políticas de certificación de este tipo de certificados. La FNMT – RCM, como entidad emisora de dicho certificado, no adquiere por ello responsabilidad adicional alguna en lo relativo a la Autoridad de Sellado de Tiempo ni los servicios prestados.

La clave privada de la TSA reside en un almacén de claves seguro en software protegido mediante contraseña.

El certificado de la TSA puede ser cambiado en cualquier momento por otro certificado de TSA igualmente válido. Este cambio no se comunicará obligatoriamente a los suscriptores de los servicios, los cuales deberán confiar en todos los sellos emitidos por la TSA y firmados con certificados válidos de TSA dentro de la jerarquía de certificación.

6 Glosario de términos y acrónimos

@firma: Plataforma de identificación y firma electrónica

<http://www.juntadeandalucia.es/haciendayadministracionpublica/ae>

CEN: Comité Europeo de Normalización.

CWA: CEN Workshop Agreement.

ETSI: European Telecommunications Standards Institute.

<http://www.etsi.org/>

HTTPS: Hypertext Transfer Protocol Secure

IETF: Internet Engineering Task Force.

<http://www.ietf.org>

NEREA: Red Interadministrativa de Andalucía

<http://www.rednerea.es>

NTP: Network Time Protocol

OASIS: Organization for the Advancement of Structured Information Standards

<http://www.oasis-open.org/>

RFC: Request For Comments.

<http://www.ietf.org/rfc.html>

SOAP: Simple Object Access Protocol.

SSL: Secure Sockets Layer

TSA: Time Stamping Authority (Autoridad de Sellado de Tiempo)

TST: Time Stamping Token (Token de Sellado de Tiempo)

URL: Uniform Resource Locator (Localizador Uniforme de Recursos). También se usa URI.

UTC: Universal Time Coordinated.

XAdES: XML Advanced Electronic Signature.

7 Normas y estándares de aplicación

CWA 14170 Security Requirements for Signature Creation Applications.

CWA 14171 General Guidelines for electronic signature verification.

CWA 14172-1 EESSI Conformity Assessment Guidance - Part 1: General introduction.

CWA 14172-3 EESSI Conformity Assessment Guidance - Part 3: Trustworthy systems managing certificates for electronic signatures.

CWA 14172-8 EESSI Conformity Assessment Guidance - Part 8: Timestamping Authority services and processes.

ETSI TS 102 023 Policy requirements for time-stamping authorities.

ETSI TS 101 861 Time stamping profile.

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

RFC 3628 Policy Requirements for Time-Stamping Authorities (TSAs)

XML Timestamping Profile of the OASIS Digital Signature Services (DSS) ver. 1.0.