

**TSA DISCLOSURE STATEMENT PARA EL
SERVICIO DE SELLADO DE TIEMPO
ELECTRÓNICO**



Control documental

Título del documento:	TSA Disclosure Statement para el Servicio de Sellado de Tiempo Electrónico
Tipo de documento:	Elija un elemento.
Nombre del fichero:	TSADS.docx
Versión:	1.0
Estado:	Aprobado
Confidencialidad:	Público
Fecha:	10/01/2020
Autor:	Área de Seguridad y Firma Electrónica

Revisión, Aprobación		
Revisado por:	Director Área de Seguridad y Firma Electrónica	Fecha: 11/02/2020
Aprobado por:	Comité de Seguridad	Fecha: 02/04/2020

Historial de cambios			
Versión	Fecha	Descripción de la acción	Páginas
1.0	10/01/2020	Creación del documento.	Todo

Índice

1. Introducción	4
2. Texto divulgativo aplicable al Servicio de Sellado de Tiempo.....	4
2.1. Acuerdo completo	4
2.2. Información de contacto.....	4
2.2.1 Organización responsable	4
2.2.2 Datos de contacto de la organización	4
2.3. Tipos de sellos y uso.....	4
2.3.1 Comunidad de usuarios y aplicabilidad	4
2.3.2 Contenido de los sellos de tiempo	5
2.3.3 Solicitud de los sellos de tiempo	5
2.3.4 Verificación de los sellos de tiempo	5
2.4. Límites de fiabilidad	5
2.5. Obligaciones de los subscriptores.....	6
2.6. Obligaciones de las terceras partes	6
2.7. Límites de garantía y responsabilidad	6
2.8. Acuerdos aplicables y declaración de prácticas.....	6
2.9. Política de privacidad.....	7
2.10. Política de reintegro.....	7
2.11. Legislación aplicable, jurisdicción competente y procedimiento de resolución de disputas.....	7
2.12. Acreditaciones y auditorías de conformidad	7

1. Introducción

El presente documento contiene las informaciones esenciales a conocer en relación al servicio de Sellado de Tiempo de la Agencia Notarial de Certificación S.L. Unipersonal (ANCERT).

Este documento sigue la estructura definida en el Anexo B de la norma ETSI EN 319 421-1.

2. Texto divulgativo aplicable al Servicio de Sellado de Tiempo

2.1. Acuerdo completo

El presente documento proporciona declaraciones de alto nivel con respecto al Servicio de Sellado cualificado de tiempo electrónico de ANCERT.

El presente documento no reemplaza ni anula ninguna otra política de ANCERT disponible en <https://www.ancert.com/cps>.

2.2. Información de contacto

2.2.1 Organización responsable

Agencia Notarial de Certificación, S.L. Unipersonal

Paseo General Martínez Campos, número 46.- 6º, Edificio Elcano

28010 Madrid (España)

NIF B-83395988

2.2.2 Datos de contacto de la organización

Cualquier contacto con ANCERT, referente a este documento puede realizarse por los siguientes medios:

- Vía e-mail a la dirección de correo electrónico ancert@ancert.com.
- Por teléfono al número 912187676.

2.3. Tipos de sellos y uso

La política de sellado de tiempo de ANCERT se identifica con el OID 1.3.6.1.4.1.18920.200.2.1.

Los sellos de tiempo emitidos bajo esta política son declarados como cualificados de acuerdo en el Reglamento UE 910/2014 y son conformes con la norma ETSI EN 1319 411-1.

2.3.1 Comunidad de usuarios y aplicabilidad

ANCERT actúa como TSA para el Consejo General del Notariado Español, los Colegios Notariales y los Notarios españoles en el ejercicio de su actividad de función pública.

Otros usuarios deben contratar previamente el servicio con ANCERT para poder acceder al servicio de sellado de tiempo.

2.3.2 Contenido de los sellos de tiempo

Los sellos de tiempo generados por la TSA se adecuan al perfil definido en el apartado 5.2 de la norma ETSI EN 319 422.

El algoritmo de resumen de los sellos de tiempo es SHA-256.

El algoritmo de firma del sello de tiempo es *sha256WithRSAEncryption*.

El sello de tiempo incluye una extensión del tipo *qcStatements* con la declaración *esi4-qtstStatement-1* de acuerdo al apartado 9.1 de ETSI EN 319 422 para indicar que el sello de tiempo es cualificado.

El sello de tiempo incluye el certificado electrónico de la clave pública de firma de la TSU. El certificado de la TSU está emitido por la Entidad de Certificación “ANCERT Certificados Notariales de Sistemas V2” de acuerdo con su Declaración de Prácticas de Certificación. El certificado de la TSU tiene un periodo de validez de 6 años y una longitud de clave RSA de 3072 bits. El uso de clave de la TSU está limitado a 5 años.

2.3.3 Solicitud de los sellos de tiempo

El cliente debe realizar las peticiones de sello de tiempo de acuerdo con la estructura definida en el RFC 3161.

El protocolo para el envío de la petición de sello de tiempo al servicio será HTTP o HTTPS de acuerdo con la definición del apartado 3.4 del RFC 3161.

Los algoritmos de resumen criptográfico aceptados por la TSA de ANCERT son: SHA-256, SHA-512 y SHA-1.

2.3.4 Verificación de los sellos de tiempo

La comprobación del estado de revocación de los certificados se puede realizar mediante consulta OCSP en la URL: <http://ocsp.ac.ancert.com/ocsp.xuda>

Alternativamente se puede comprobar mediante descarga y consulta de la CRL de la Entidad de Certificación “ANCERT Certificados Notariales de Sistemas V2” en la URL: http://www.ancert.com/crl/ANCERTNOT_V2.crl.

Las URLs de acceso a los servicios OCSP y de descarga de CRL se encuentran en las extensiones del certificado de la TSU.

2.4. Límites de fiabilidad

ANCERT obtiene el tiempo de sus sistemas de una conexión al Real Observatorio de la Armada (ROA) siguiendo el protocolo NTP a través de Internet.

La exactitud de la fuente de tiempo de ANCERT es de 1 segundo respecto a UTC.

ANCERT mantiene registros de todas las operaciones de la TSA durante 15 años desde la emisión de cada sello de tiempo.

2.5. Obligaciones de los subscriptores

El suscriptor del servicio de sellado de tiempo debe:

- Respetar lo dispuesto en los documentos contractuales firmados con ANCERT.
- Cumplir con la política de sellado de tiempo de ANCERT.
- Utilizar el servicio según las especificaciones de ETSI EN 319 422.
- Verificar la firma electrónica del sello de tiempo y comprobar que el certificado asociado a la clave privada con la que la TSA firma el sello no ha sido revocado con cualquiera de los métodos detallados en el apartado 2.3.4.
- Comprobar que el resumen criptográfico y el identificador de política contenidos en del sello de tiempo se corresponden con los solicitados.
- Almacenar y conservar los sellos de tiempo entregados por la TSA en caso de que para él sean necesarios en el futuro.

2.6. Obligaciones de las terceras partes

Cuando recibe un de sello de tiempo la tercera parte debe verificar la firma electrónica del sello de tiempo y comprobar que el certificado asociado a la clave privada con la que la TSA firma el sello no estaba revocado en el momento de la generación del sello con cualquiera de los métodos detallados en el apartado 2.3.4.

2.7. Límites de garantía y responsabilidad

ANCERT garantiza, bajo su plena responsabilidad, que cumple con todos los requisitos establecidos en la política con la que emite sellos de tiempo.

ANCERT limita su responsabilidad a la producción de sellos de tiempo en las condiciones de su política, y en ningún caso aceptará responsabilidad alguna por el uso de dichos sellos.

ANCERT no responderá en los supuestos de caso fortuito o fuerza mayor salvo que hubiera mediado culpa grave de la entidad.

2.8. Acuerdos aplicables y declaración de prácticas

Los acuerdos aplicables al sello cualificado de tiempo electrónico alto son los siguientes:

- Contrato de servicios de certificación, que regula la relación entre ANCERT y la entidad suscriptora de los sellos cualificados de tiempo electrónico.
- La Declaración de Prácticas del servicio de sellado de tiempo (DPTSA) de ANCERT.
- La Política General de Certificación (PG) y la Declaración de Prácticas de Certificación (DPC) de ANCERT.

La PG, DPC, DPTSA y todo el resto de documentación complementaria está accesible en <https://www.ancert.com/cps> donde se actualiza periódicamente.

2.9. Política de privacidad

Ver el apartado de 11.4 de la DPC de los Certificados Notariales, disponible en <https://www.ancert.com/cps>.

2.10. Política de reintegro

ANCERT no reintegrará el coste del servicio de sellado en ningún caso.

2.11. Legislación aplicable, jurisdicción competente y procedimiento de resolución de disputas

Las relaciones con ANCERT se regirán por la ley española en materia de servicios de confianza vigente en cada momento, así como por la legislación civil y mercantil en lo que sea de aplicación.

La jurisdicción competente es la que se indica en la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

En caso de discrepancia entre las partes, las partes intentarán la previa resolución amistosa. A tal fin, las partes deberán dirigir una comunicación a ANCERT por cualquier medio que deje constancia a la dirección de contacto indicada en el punto 2.2.2 de este documento.

2.12. Acreditaciones y auditorías de conformidad

Los servicios de la TSA de ANCERT cumplen con los requerimientos del Reglamento (UE) 910/2014.

ANCERT y su servicio de sellado de tiempo se encuentran en la lista de prestadores de confianza (TSL) española.

De acuerdo con lo indicado en el Reglamento UE 910/2014, ANCERT realiza auditorías anuales de sus servicios de confianza con una entidad acreditada como CAB (Conformity Assessment Body) y renueva con periodicidad bienal el CAR (Conformity Assessment Report) de sus servicios.