PÚBLICO

DECLARACIÓN DE PRÁCTICAS Y POLÍTICA DE SELLADO DE TIEMPO

CENTRO TECNOLÓGICO DEL NOTARIADO

Control Documental

Título del documento:	Declaración de Prácticas y Política de Sellado de Tiempo
Tipo de documento:	Política
Nombre del fichero:	Declaración de Prácticas y Política de TSA.docx
Versión:	1.2
Estado:	Aprobado
Confidencialidad:	Documento de uso interno
Fecha:	22/05/2024
Autor:	Oficina de Seguridad

Revisión, Aprobación		
Revisado por:	Director Seguridad e Innovación	Fecha: 30/05/2024
Aprobado por:	Comité de Seguridad	Fecha: 11/06/2024

Historial de cambios			
Versión	**Fecha**	**Descripción de la acción**	**Páginas**
1.0	23/01/2020	Creación del documento.	Todo
1.1	09/05/2023	Revisión de incorrecciones y actualización del domicilio social	Todo
1.1.1	18/09/2023	Subsanar error domicilio social	9
1.2	22/05/2024	Se incluye referencia e imagen corporativa del Centro Tecnológico del Notariado. Revisión de videncia para la generación del nuevo certificado de la TSA.	Todo

Índice

1. Introducción

Este documento contiene la política de sellado de tiempo y la declaración de prácticas de sellado de tiempo de la Agencia Notarial de Certificación S.L. Unipersonal (en adelante, Centro Tecnológico del Notariado, CTNotariado o ANCERT indistintamente) .

El servicio de sellado de tiempo cualificado forma parte del catálogo de servicios de ANCERT como Prestador Cualificado de Servicios de Confianza en los términos definidos por el Reglamento (UE) 910/2014 [1].

La estructura y numeración de este documento es la misma que la de la norma ETSI EN 319 421 [4]. Este documento complementa con procesos y detalles técnicos para la prestación del servicio de TSA a la "Política General de Certificación" [9] y la Declaración de Prácticas de Certificación (DPC) [9].

Los procedimientos definidos y su correcta implementación son auditados por una entidad externa, según las especificaciones definidas por ETSI a través de la norma EN 319 421 [4].

2. Referencias

Normas legales y técnicas

[1] Reglamento (UE) 910/2014.
[2] Recommendation ITU-R TF.460-6 (2002): "Standard-frequency and time-signal emissions".
[3] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".
[4] ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".
[5] ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".
[6] IETF RFC 3161 (2001): "Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)".
[7] IETF RFC 5816: "ESSCertIDV2 update to RFC 3161".

Políticas y prácticas del prestador

[8] ANCERT: "Política General de Certificación".
[9] ANCERT: "Declaración de Practicas de Certificación de los certificados Notariales".
[10] ANCERT: "Perfiles de Certificados de la Entidad de Certificación".

3. Definiciones y acrónimos

3.1. Definiciones

Autoridad de Sellado de Tiempo (TSA): TSP que emite sellos de tiempo.

Coordinated Universal Time (UTC): escala de tiempo basada en el segundo, según se define en ITU-R TF.460-6 [2].

Declaración de Prácticas de la TSA (DPTSA): declaración de las prácticas que la TSA emplea para la emisión de sellos de tiempo.

Declaración de Prácticas de divulgación de la TSA (DPDTSA): conjunto de declaraciones acerca de la política y las prácticas que requieren de especial divulgación entre los subscriptores y las terceras partes usuarias

Política de sellado de tiempo: reglas que aplican a la TSA cuando se genera un sello de tiempo

Prestador de Servicios de Confianza (TSP): entidad que proporciona Servicios de Confianza según la definición del Reglamento (UE) 910/2014 [1]

Sello de tiempo (TST): objeto de datos que relaciona la existencia de unos datos digitales a un momento concreto. Sirve como evidencia de que un dato existió en un instante determinado en la línea de tiempo.

Servicio de sellado de tiempo: servicio de confianza de emisión de sellos de tiempo.

Suscriptor: persona física o jurídica que utiliza los servicios proporcionado por la TSA y que acepta de forma explícita los términos y condiciones

Terceras partes usuarias: usuario que recibe y confía en un sello de tiempo

Unidad de sellado de tiempo (TSU): componentes hardware y software gestionados como una unidad que proporciona sellos de tiempo desde una única fuente de tiempo. Los componentes pueden ser clonados o implementados en redundancia para conseguir alta disponibilidad.

3.2. Acrónimos

TSA: Time Stamp Authority

TSU: Time Stamp Unit

TST: Time Stamp Token (sello de tiempo)

UTC: Coordinated Universal Time

eIDAS: Reglamento (UE) Nº 910/2014

DPTSA: Declaración de Prácticas de la TSA

DPC: Declaración de Prácticas de Certificación

4. Conceptos generales

4.1. Servicio de sellado de tiempo

Los servicios de sellado de tiempo incluyen dos componentes de servicio:

- **Provisión de sellos de tiempo:** componente técnico encargado de generar los sellos de tiempo.
- **Administración sellos de tiempo:** componente del servicio que monitoriza y controla la operación de los servicios de sellado de tiempo. Este componente es el responsable de la instalación y desinstalación del servicio de provisión de sellos. El servicio de administración asegura que los relojes utilizados en el sellado de tiempo están correctamente sincronizados con UTC.

4.2. Autoridad de sellado de tiempo

Una Autoridad de sellado de tiempo (TSA) es un Prestador de Servicios de Confianza como se describe en ETSI EN 319 401 [3] que proporciona certeza sobre la preexistencia de determinados documentos electrónicos en un momento dado mediante la emisión de sellos de tiempo (TST).

La TSA de ANCERT asume toda la responsabilidad sobre la provisión de los servicios de sellado de tiempo indicados en el apartado 6.5.4. La TSA de ANCERT puede operar varias unidades identificables de sello de tiempo (TSU).

Dentro de un TSU se permite clonar claves y utilizarlas en componentes redundantes para cumplir con requerimientos de alta disponibilidad.

La TSA de ANCERT se identifica con un certificado electrónico usado por su servicio de provisión de sellos de tiempo con las características definidas en el apartado 7.7.1.

4.3. Subscriptor

Los suscriptores son las personas y las organizaciones que se suscriben al servicio de sellado de tiempo y que podrán solicitar sellos durante el periodo de suscripción.

Si el suscriptor es una organización, las obligaciones que aplican a esa organización también aplican a sus usuarios finales asociados. En cualquier caso, la organización será responsable si las obligaciones no son correctamente cumplidas por los usuarios finales. Por lo tanto, esa organización debe informar adecuadamente a sus usuarios finales.

Si el suscriptor es un usuario particular, el usuario final será responsable directamente del cumplimiento de las obligaciones.

4.4. Política de sellado y Declaración de Prácticas de la TSA

La Política de sellado de la TSA define las reglas y procesos que se aplican para la generación de un sello de tiempo, incluyendo todos los requisitos que debe cumplir subscriptor.

La Declaración de Prácticas de TSA es una declaración de cómo está implementado el servicio de sellado de tiempo para cumplir con los requerimientos de la política.

El presente documento complementa y extiende los procesos descritos en la DPC [9] para la prestación del servicio de sellado de tiempo.

5. Política de la TSA y requisitos generales

5.1. General

ANCERT define en el presente documento su propia política para el servicio cualificado de sellado de tiempo con una precisión de la fuente de tiempo de 1 segundo. Esta política es conforme a los requisitos de la norma técnica ETSI EN 319 421 [4].

5.2. Identificación

Los sellos de tiempo (TST) emitidos por la TSA de ANCERT de acuerdo con la presente política incluyen el siguiente identificador (OID):

1.3.6.1.4.1.18920.200.2.1

5.3. Comunidad de usuarios y aplicabilidad

Los usuarios del servicio de sellado de tiempo serán los suscriptores y terceras partes que requieran del servicio.

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 deberán contratar previamente el servicio con ANCERT para poder acceder al servicio de sellado de tiempo.

5.3.1 Límites de uso del servicio y de los sellos de tiempo

Los sellos se emplearán para su función propia y finalidad establecida, sin que puedan emplearse en otras funciones y con otras finalidades.

6. Política y prácticas

6.1. Gestión de riesgos

ANCERT dispone de un plan de gestión de riesgos para identificar, analizar y evaluar los riesgos que pueden afectar al servicio de sellado de tiempo.

ANCERT dispone de un plan de tratamiento de riesgos en el que prioriza, selecciona e implementa las medidas de seguridad oportunas para tratar los riesgos identificados en los análisis de riesgos.

ANCERT actualiza el análisis de riesgo con la periodicidad establecida en su plan de gestión de riesgos y cada vez que se producen cambios substanciales en el servicio.

El Comité de Seguridad de ANCERT aprueba formalmente el plan de tratamiento de riesgos resultante de la actividad de gestión de riesgos y acepta el riesgo residual.

6.2. Declaración de Prácticas de la TSA

ANCERT, en calidad de TSA, desarrolla, implementa, hace cumplir y actualiza el presente documento que contiene la Declaración de Practicas de TSA para cumplir con los requerimientos de su política sellado de tiempo.

Los procedimientos definidos y su correcta implementación son auditados anualmente por una entidad externa independiente.

La Declaración de prácticas de divulgación de TSA se publica de forma independiente a este documento y está disponible 24x7 en https://www.ancert.com/cps .

6.3. Requisitos generales de la Declaración de Prácticas

El presente documento con la política y Declaración de Prácticas de sellado de TSA y otra documentación relevante está disponible 24x7 en https://www.ancert.com/cps .

Organización que administra el documento

Agencia Notarial de Certificación, S.L. Unipersonal

Calle Campezo 1, Edificio 6, planta 2, 28022 Madrid (España)

NIF B-83395988

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.
- Directamente en el domicilio social de ANCERT: Agencia Notarial de Certificación, S.L. Unipersonal, Calle Campezo 1, Edificio 6, planta 2, 28022 Madrid (España)

Las alteraciones que se produzcan sobre los anteriores datos como Web, correo, dirección o teléfono constarán debidamente reflejadas en la página web www.ancert.com que ANCERT mantiene en vigor en Internet.

Procedimientos de gestión de la documentación

Quien determina la idoneidad de esta Declaración de Prácticas y se encarga de su aprobación es el Comité de Seguridad de ANCERT.

ANCERT dispone de un procedimiento interno de creación, revisión y aprobación formal de este documento.

6.4. Política de Seguridad de la Información

ANCERT dispone de una política de seguridad de la información, aprobada por su Comité de Seguridad, que define cómo la organización gestiona la seguridad de la información.

6.5. Obligaciones y responsabilidades

6.5.1 Obligaciones de la Entidad Emisora de Sellos de Tiempo

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

ANCERT es la única entidad responsable del cumplimiento de los procedimientos descritos en esta política, incluso cuando una parte o la totalidad de las operaciones sean subcontratadas externamente.

ANCERT presta sus servicios de certificación conforme con su Declaración de Prácticas de Certificación vigente, en la que se detallan sus funciones, procedimientos de operación y medidas de seguridad.

6.5.2 Obligaciones del suscriptor de sellos de tiempo

El subscritor del servicio de sellado de tiempo debe:

- Respetar lo dispuesto en los documentos contractuales firmados con ANCERT.
- Cumplir con la presente política de sellado de tiempo de ANCERT.
- Utilizar el servicio según las especificaciones de ETSI EN 319 422 [5].
- 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.
- 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.

6.5.3 Obligaciones de terceras partes usuarias de sellos de tiempo

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.

6.5.4 Responsabilidades de la Entidad Emisora de Sellos de Tiempo

ANCERT opera su TSA de acuerdo con la política de TSA, su declaración de prácticas, y los términos de cualquier otro acuerdo vinculante entre ANCERT y los subscriptores del servicio de sellado de tiempo.

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

ANCERT no responderá en los supuestos de caso fortuito, fuerza mayor, atentado terrorista, huelga salvaje, así como en los supuestos que se trate de acciones constitutivas de delito o falta que afecten a sus infraestructuras prestadoras, salvo que hubiera mediado culpa grave de la entidad. En cualquier caso ANCERT realizará todas las medidas razonables para mitigar los efectos de tales eventos.

7. Gestión y operación de la TSA

7.1. Introducción

Esta sección incluye los controles de seguridad y de operación implantados por ANCERT para la prestación del servicio de sellado de tiempo. Los siguientes apartados referencian apartados y secciones de la Política General de Certificación [8] y cuando es necesario completan y extienden el mismo documento para el ámbito de la prestación del servicio de sellado de tiempo.

7.2. Gestión de la seguridad

La gestión de la seguridad de la TSA está descrita en la sección 5 “Controles de seguridad física, de gestión y de operaciones” de la Política General de Certificación [8].

7.3. Seguridad del personal

Según lo especificado en el apartado 5.3 “Controles de personal” de la Política General de Certificación [8].

7.4. Gestión de activos

ANCERT realiza una gestión adecuada de todos sus activos y les asigna medidas de protección en función de su nivel de riesgo.

En particular, ANCERT dispone de un inventario de activos de información y asigna una clasificación a sus activos de acuerdo con su normativa interna de clasificación de la información y su análisis de riesgos.

Todos los medios de información son gestionados de forma segura de acuerdo con los requisitos establecidos en la política de seguridad de la información. ANCERT dispone de

procedimientos para destruir de forma segura los medios de información que pueden contener información confidencial cuando finaliza su vida útil.

7.5. Control de acceso

La TSA de ANCERT dispone de los controles de acceso adecuados según se define en el apartado 5.2. “Controles de procedimientos” y 6.5 “Controles de seguridad informática” de la Política General de Certificación [8].

7.6. Controles criptográficos

7.6.1 General

ANCERT dispone e implementa una política de seguridad criptográfica que regula el uso de controles criptográficos y la duración, el uso y la protección de las claves criptográficas a lo largo de todo su ciclo de vida.

7.6.2 Generación de la clave de la TSU

ANCERT genera las claves criptográficas de la TSU en un entorno físico seguro. Solo el personal autorizado designado con roles de confianza puede llevar a cabo la operación de generación de claves y siempre bajo condiciones de control dual.

ANCERT dispone de un procedimiento específico de generación de claves de la TSU y genera un acta de creación de las mismas.

La generación de las claves se realiza en un módulo criptográfico certificado de acuerdo con ISO/IEC 15408 contra el perfil de protección EN 419 221-5 o que cumpla con les requisitos de FIPS PUB 140-2 nivel 3.

El algoritmo criptográfico de la clave es RSA de 3072 bits y su uso se limita a 5 años.

7.6.3 Protección de la clave privada de la TSU

ANCERT mantiene la confidencialidad e integridad de la clave privada de la TSU mediante el uso de un módulo criptográfico certificado de acuerdo con ISO/IEC 15408 contra el perfil de protección EN 419 221-5 o que cumpla con les requisitos de FIPS PUB 140-2 nivel 3 para todas las operaciones de firma.

La administración del módulo criptográfico requiere necesariamente del concurso simultáneo de dos (2) dispositivos criptográficos protegidos por una clave de acceso, de entre cuatro (4) dispositivos.

La clave de acceso será conocida únicamente por una persona responsable de ese dispositivo. Ninguna de ellas conocerá más que una de las claves de acceso.

ANCERT puede contar una copia de respaldo de la clave privada de la TSU, almacenada en una dependencia independiente de aquélla donde se almacena habitualmente, y recuperada en su

caso, por personal sujeto a la política de confianza del personal. Este personal debe ser expresamente autorizado a estos fines, y debe limitarse a aquel que necesite hacerlo.

Los controles de seguridad a aplicar a las copias de respaldo de la TSU son de igual o superior nivel a los que se aplican a las claves habitualmente en uso.

7.6.4 Certificado de la clave pública de la TSU

ANCERT garantiza la integridad y autenticidad de la clave pública de la TSU mediante un certificado electrónico emitido por ANCERT.

El certificado de la TSA se encuentra publicado en la página web de la ANCERT www.ancert.com .

El certificado de la TSA tiene el perfil detallado en la sección 7.7.1.

7.6.5 Regeneración de la clave de la TSU

Las claves de la TSA son reemplazadas antes de que finalice su periodo de uso, expire su certificado electrónico o sea necesario substituir el algoritmo o longitud de la clave.

La regeneración de una nueva clave implica la emisión de un nuevo certificado electrónico. ANCERT genera una nueva clave de TSU cada 4 años.

7.6.6 Gestión del módulo criptográfico

ANCERT dispone de un procedimiento interno para la gestión del ciclo de vida de los módulos criptográfico, que aseguran que los mismos no son manipulados durante su envío y recepción, almacenamiento, puesta en funcionamiento y que garantizan su borrado cuando son retirados del uso. Todos los procedimientos de gestión de claves en los módulos criptográficos son realizados por personal autorizado designado con roles de confianza, bajo control dual, en un entorno físicamente seguro.

7.6.7 Finalización del uso de la clave de la TSU

ANCERT define un periodo de uso de la clave privada de la TSU de 5 años. El periodo de validez del certificado asociado a la pública de la TSU es de 6 años.

ANCERT no utiliza una clave privada de TSU una vez se supera su periodo de validez.

ANCERT dispone de procedimientos operativos para asegurar que la TSU utiliza una nueva clave antes de que la anterior expire y que ésta es destruida cuando llega al final de su uso.

7.7. Sellado de tiempo

7.7.1 Emisión de sellos de tiempos

La emisión de sellos de la TSA de ANCERT es conforme al protocolo y el perfil definido en la norma ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles". [5]

Petición de un sello de tiempo

El cliente debe realizar las peticiones de sello de tiempo de acuerdo con la estructura definida en el RFC 3161 [6].

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 [6].

Los algoritmos de resumen criptográfico aceptados por la TSA de ANCERT son: SHA-256, SHA-512 y SHA-1. ANCERT desaconseja a sus subscriptores el uso de SHA-1 como algoritmo de resumen, que mantiene por motivos de compatibilidad.

Respuesta a una petición de sello de tiempo

Los sellos de tiempo generados por la TSA se adecuan al perfil definido en el apartado 5.2 de ETSI EN 319 422 [5].

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 el apartado 9.1 de ETSI EN 319 422 [5] 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.

Perfil del certificado

El certificado de la TSU está emitido por la entidad de certificación “ANCERT Certificados Notariales de Sistemas V2”.

El perfil de certificación se define en el apartado “Certificado de Autoridad de Sellado de tiempo Cualificada” del documento ANCERT: "Perfiles de Certificados de la Entidad de Certificación". [10]

La duración del certificado es de 6 años y el certificado contiene la extensión *PrivateKey Usage Period* para especificar el periodo de uso de la clave privada a 5 años.

7.7.2 Sincronización del reloj

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.

ANCERT mantiene controles para asegurar que el reloj de las TSU cumple los siguientes requisitos:

- Se encuentra sincronizado con UTC con la precisión declarada de 1 segundo.
- La calibración se mantiene de forma que no resulte previsible un desplazamiento en la fecha y hora de los mismos.
- Los relojes están protegidos contra amenazas que pudieran resultar en un cambio no detectado que descalibre el reloj.

- Se asegura que se detectan los desplazamientos y saltos del reloj, que impidan su sincronización con UTC.
- Se asegura que se mantiene la sincronización del reloj cuando se notifica un segundo de salto, notificado por el órgano competente.

En caso de detectarse una pérdida de sincronización de la fuente de tiempo o saltos mayores a la precisión declarada, ANCERT detiene la emisión de sellos de tiempo.

7.8. Seguridad física

Según lo especificado en el apartado 5.1 “Controles de seguridad física” de la Política General de Certificación [8].

7.9. Gestión de operaciones

Según lo especificado en el apartado 6.6 “Controles técnicos del ciclo de vida” de la Política General de Certificación [8].

7.10. Seguridad de red

Según lo especificado en el apartado 6.7 “Controles de seguridad de red” de la Política General de Certificación [8].

7.11. Gestión de incidentes

Según lo especificado en el apartado 5.7. “Compromiso de claves y recuperación de desastre” de la Política General de Certificación [8].

7.12. Recogida de evidencias

Según lo especificado en el apartado 5.4. “Procedimientos de auditoría de seguridad” de la Política General de Certificación [8].

Adicionalmente a estos requisitos, ANCERT recoge evidencias de los siguientes registros:

- Todos los eventos que tienen relación con la gestión del ciclo de vida de las claves de la TSU y de su certificado asociado.
- Todos los eventos relacionados con la sincronización del reloj de la TSU con UTC.
- Todos los eventos relaciones con la detección de la pérdida de sincronización.

7.13. Continuidad de negocio

Según lo especificado en el apartado 5.7. “Compromiso de claves y recuperación de desastre” de la Política General de Certificación [8].

Adicionalmente a estos requisitos, en caso de pérdida o compromiso de la calibración del reloj de la TSU, ANCERT realizará las siguientes acciones:

- Detendrá la emisión de sellos de tiempos hasta que se recupere del incidente.

- Notificará a los subscriptores, terceros usuarios de los sellos y a la autoridad de competente el incidente. En caso de que antes de detectarse el incidente se hayan emitido sellos de tiempo que se encuentre afectados por el mismo se informará a todas las partes de cuáles son los sellos afectados (mediante sus números de serie y/o periodo de emisión).

7.14. Terminación del servicio

Según lo especificado en la sección 5.8 “Terminación del servicio” de la Política General de Certificación [8].

Adicionalmente a los requisitos anteriores, cuando finaliza el servicio de TSA el certificado de la TSU es revocado.

7.15. Cumplimiento

Los servicios de la TSA de ANCERT cumplen con los requerimientos del Reglamento (UE) 910/2014. [1].

Según lo especificado en la sección 9.4 “Protección de datos personales” de la Política General de Certificación [8] en lo referente al establecimiento de las medidas de seguridad adecuadas para evitar el procesamiento no autorizado de datos de carácter personal de los usuarios y la confidencialidad de los mismos.