Declaración de Prácticas TSA y

Política de Sellado de tiempo *(TimeStamping)*

Paseo de la Castellana,79 -28046- Madrid (Spain)

Teléfono: 932 661 614 (Llamadas desde España)

Internacional +34 933 935 946

Web: www.anf.es

Nivel de Seguridad

Documento Público

Aviso Importante

Dirección: Paseo de la Castellana, 79 - 28046 - Madrid (España)

Teléfono: 932 661 614 (llamadas desde España) Internacional (+34) 933 935 946

Web: www.anf.es

ÍNDICE

1. Introducción

1.1. Visión general

El sellado de tiempo electrónico, son datos en formato electrónico que vinculan otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante. Por lo tanto, documenta el "cuándo" y "qué". Una firma electrónica, a menudo referida como la firma personal, documenta el "quién" y "qué". En contraste con la firma electrónica, un sello de tiempo, no está vinculada a las personas y sus acciones. Por lo tanto, se puede integrar mucho más simple y también totalmente de forma automática en los procesos electrónicos.

Con el fin de verificar una firma electrónica, puede ser necesario probar que la firma del firmante se aplica cuando el certificado del firmante era válido. Esto es necesario en dos circunstancias:

1. durante el período de validez del certificado, el firmante puede revocarlo antes del fin de su validez, por ejemplo, porque la clave privada ha sido comprometida;
2. después del final del período de validez del certificado, las entidades emisoras no están obligadas a procesar la información de estado de revocación más allá del final del período de validez de los certificados que hayan expedido.

Un sello de tiempo permite demostrar que un dato existía antes de un tiempo determinado. Esta técnica permite demostrar que la firma o un determinado documento electrónico al que se asocia, se generó antes de la fecha que figura en el sello de tiempo.

ANF AC Autoridad de Certificación *(en adelante, ANF AC)* es una entidad jurídica constituida al amparo de la Ley Orgánica 1/2002 del 22 de marzo e inscrita en el Ministerio del Interior con el número nacional 171.443 y NIF G-63287510, acreditada para la prestación del servicio de sellado de tiempo de ANF AC TSA.

El presente documento especifica la política y requisitos de seguridad relacionados con las operaciones y las prácticas de gestión de ANF AC como **Autoridad de Sellado de Tiempo** *(en adelante, ANF AC TSA),* para la emisión de **sellos cualificados de tiempo electrónico**, así como establecer las condiciones de uso, obligaciones y responsabilidades de las distintas entidades involucradas. Este servicio se ajusta a:

- Reglamento (UE) No 910/2014 (eIDAS), artículo 42.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- ETSI EN 319 421: *"Policy and Security Requirements for Trust Service Providers issuing Time-Stamps."*
- ETSI EN 319 422: *"Time-stamping protocol and time-stamp token profiles."*
- ETSI EN 319 401: *"Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers"*
- ETSI TS 119 312: *"Electronic Signatures and Infrastructures (ESI); Cryptographic Suites"*
- IETF RFC 3628: "*Policy Requirements for Time-Stamping Authorities (TSAs)"*
- IETF RFC 3161: *"Internet X.509 Public Key Infrastructure Time-stamp Protocol"*

La Política de Sellado de Tiempo de ANF AC TSA se basa en la Política de Sellado de Tiempo especificada en ETSI EN 319 421, y se aplica a las TSA que expiden TSTs.

Este documento puede ser utilizado por organismos independientes como base para confirmar que ANF AC TSA, es una entidad de confianza para la emisión de sellos cualificados de tiempo electrónico de acuerdo con el Reglamento eIDAS.

El presente documento no especifica:

- protocolos utilizados para acceder al ANF AC TSA;
- cómo los requisitos especificados en este documento pueden ser evaluados por un órgano independiente;
- los requisitos para poner a disposición la información a dichas entidades independientes;
- los requisitos que deben de cumplir este tipo de organismos independientes;
- los requisitos correspondientes a la custodia de evidencias, preservación cualificada a largo plazo de las firmas y sellos cualificados.

ANF AC no realizará custodia de evidencias y preservación cualificada a largo plazo salvo que se contrate el servicio cualificado correspondiente.

Los certificados de CA raíz y otros certificados necesarios para el funcionamiento de esta PKI, están disponibles en www.anf.es.

En caso de conflicto entre la DPC de ANF AC OID 1.3.6.1.4.1.18332.1.9.1.1 y esta Declaración de Prácticas TSA y Política de Sellado de tiempo (DPC TSA), lo dispuesto en la DPC TSA deberá prevalecer. Además, este documento se publica en versión español e inglés, en caso de conflicto prevalecerá la versión en español.

1.2. Nombre del documento e identificación

Nombre del documento	Declaración de Prácticas TSA y Política de Sellado de tiempo *(Timestamping)*		
Versión	1.6		
OID	1.3.6.1.4.1.18332.15.1		
Fecha de aprobación	02/04/2021	**Fecha de publicación**	02/04/2021

1.2.1. Revisiones

Versión	Cambios	Aprobación	Publicación
1.6.	Revisión e inclusión de TSU.	02/04/2021	02/04/2021
1.5.	Recomendaciones de auditor eIDAS.	18/04/2017	18/04/2017
1.4.	Adaptación a eIDAS.	01/06/2016	01/06/2016
1.3.	Revisión.	02/09/2014	02/09/2014
1.2.	Revisión	01/06/2012	01/06/2012
1.1.	Revisión.	01/05/2010	01/05/2010
1.0.	Versión inicial del documento.	26/10/2004	26/10/2004

1.3. Definiciones y acrónimos

1.3.1. Definiciones

Para efectos del presente documento, se aplican tanto las definiciones dadas en la DPC de ANF AC como las siguientes:

Autoridad de Sellado de Tiempo (TSA): Es el TSP que presta servicios de sellado de tiempo utilizando una o varias unidades de sellado de tiempo (TSUs).

Declaración de divulgación de la TSA: conjunto de declaraciones acerca de las políticas y prácticas de una TSA que requieren especial énfasis en la divulgación a los suscriptores y partes que confían, por ejemplo, para cumplir los requisitos normativos.

Declaración de prácticas de la TSA: declaración de las prácticas empleadas por la TSA en la emisión de sellos de tiempo.

Función Hash: es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales.

Módulo criptográfico hardware (HSM): dispositivo certificado en conformidad con lo establecido en la ETSI EN 319 421, utilizado para realizar funciones criptográficas y almacenar claves en modo seguro.

NTP: Es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable. La norma de referencia es IETF RFC 1305 (Network Time Protocol (NTP v3)).

Política de sello de tiempo: Conjunto de reglas que indica la aplicabilidad de un sello de tiempo a una comunidad y/o clase particular de aplicación de los requisitos de seguridad común. Se trata de un tipo específico de la política de servicio de confianza como se define en la norma ETSI EN 319 421.

Prestador de Servicios de Confianza (TSP): entidad que proporciona uno o más servicios de confianza.

ROA: Real Instituto y Observatorio de la Armada - San Fernando (Cádiz), declarado a efectos legales como Patrón Nacional de dicha unidad, así como del mantenimiento y difusión oficial de la escala "Tiempo Universal Coordinado" (UTC(ROA)), considerado a todos los efectos como la base de la hora legal en todo el territorio nacional (R.D. 23 octubre 1992, núm. 1308/1992). Forma parte de la red de laboratorios del BIPM.[1]

Sello de tiempo *(Time stamp)*: datos en formato electrónico que vinculan otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante.

Servicio de sellado de tiempo: Servicio de confianza para la emisión de sellos de tiempo.

[1] *ROA colabora con el Consejo Superior de Investigaciones Científicas (CSIC), controlando y monitorizando la sincronización de las máquinas principales de distribución de tiempo en España, tres de las cuales (dos localizadas en el INSOB y una tercera en Madrid) pertenecen a la Sección.*
https://armada.defensa.gob.es/ArmadaPortal/page/Portal/ArmadaEspannola/ciencia_observatorio/prefLang-es/06_Hora

Sistema TSA: Conjunto de productos TI y procedimientos empleados para apoyar la prestación de servicios de sellado de tiempo.

Suscriptor: Persona jurídica o física a la que se emite un sello de tiempo y que está obligada a cumplir las obligaciones del suscriptor.

Tercero que confía: Receptor de un sello de tiempo que confía en ese sello de tiempo.

Tiempo Universal Coordinado (UTC): Escala de tiempo basada en el segundo, está definida por el estándar de emisiones de frecuencia y tiempo de la International Telecommunications Union Recommendation (ITU-R TF.460-6).

A efectos prácticos UTC es equivalente al tiempo solar medio en el meridiano origen (0 °). Más específicamente, UTC es un compromiso entre el tiempo atómico altamente estable (Tiempo Atómico Internacional- TAI) y la hora solar derivada de la rotación de la Tierra irregular. La Hora Universal Coordinada *(UTC)* constituye el principal estándar de la hora por la cual el mundo regula los relojes y el tiempo.

Unidad de Sellado de Tiempo (TSU): Conjunto de hardware y software que se gestiona como una sola unidad, que tiene una sola clave activa de firma de sello de tiempo a la vez.

UTC(k): Escala de tiempo dada por el laboratorio "k" y que mantiene una estrecha relación con la hora UTC, con el objetivo de alcanzar ±100 ns.

1.3.2. Acrónimos

A los efectos del presente documento, las abreviaturas dadas son las siguientes:

BIPM Bureau International des Poids et Mesures

CA Certification Authority (Autoridad de Certificación)

HSM Hardware Security Module

IT Information Technology (Tecnologías de la Información)

TAI International Atomic Time

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

TSP Trust Service Provider (Prestador de Servicios de Confianza)

TST Time Stamp Token (Token de Sellado de Tiempo)

TSU Time-Stamping Unit (Unidad de Sellado de Tiempo)

UTC Tiempo Universal Coordinado

1.4. Información de contacto

Departamento	Departamento Legal
Correo electrónico 1	soporte@anf.es

Correo electrónico 2	mcmateo@anf.es
Dirección	Paseo de la Castellana, 79
Localidad	Madrid
Código Postal	28046
Número de teléfono	932 661 614 *(Llamadas desde España)* (+34) 933 935 946 *(Internacional)*

2. Conceptos generales

El presente documento hace referencia a la DPC de ANF AC para los requisitos de política genéricos establecidos en ETSI EN 319 401, comunes para todos los servicios de confianza.

Esta política está dirigida a satisfacer los requisitos del sellado de tiempo para validez a largo plazo *(por ejemplo, como se define en la norma ETSI EN 319 122)*, pero generalmente es aplicable a cualquier uso que tiene una exigencia de calidad equivalente.

2.1. Servicios de sellado de tiempo

La prestación de servicios de sellado de tiempo se desglosa en el presente documento en los siguientes componentes para cumplir los requisitos de clasificación:

- **Provisión de sellado de tiempo:** Este componente del servicio genera TSTs.
- **Gestión del sellado de tiempo:** el componente de servicio que monitorea y controla el funcionamiento de los servicios de sellado de tiempo para asegurar que el servicio es prestado tal y como especifica la DPC y Declaración de Prácticas de TSA.

ANF AC TSA se adhiere a las normas y reglamentos establecidos en el apartado 1.1 del presente documento para mantener la fiabilidad de los servicios de sellado de tiempo para suscriptores y usuarios de confianza.

2.2. Participantes del servicio de sellado de tiempo

2.2.1. Prestador Cualificado de Servicios de Confianza (PCSC)

ANF AC es el Prestador de Servicios de Confianza (TSP) que provee de servicios de sellado de tiempo al público, en la prestación de servicio de sellado de tiempo interviene como Autoridad de Sellado de Tiempo.

ANF AC TSA es Prestador Cualificado de Servicios de Confianza como se describe en el Reglamento eIDAS, está incluido en la TSL de España.

ANF AC no se apoya en terceras entidades colaboradoras para la prestación de servicio de sellado de tiempo, mantiene la responsabilidad general y asegura que se cumplen los requisitos de actuación mencionados en el presente documento.

2.2.2. Autoridad de Sellado de Tiempo (TSA)

La TSA tiene la responsabilidad general para la prestación de los servicios de sellado de tiempo y del funcionamiento de una o más TSUs, que crean TSTs.

El servicio cualificado de sello de tiempo electrónico es auditado por lo menos cada 24 meses por un organismo de evaluación de la conformidad, haciendo entrega del informe de evaluación al Organismo de Supervisión en un plazo máximo de 3 días hábiles. Cuando el órgano de control requiere a la TSA subsanar cualquier incumplimiento de los requisitos, la TSA actuará en consecuencia y en el momento oportuno. El órgano de control será informado de cualquier cambio en la disposición de la TSA.

ANF AC TSA puede hacer uso de otras partes para proporcionar partes de los servicios de sellado de tiempo. Sin embargo, la TSA siempre mantiene la responsabilidad general y asegura que se cumplan los requisitos de la política identificados en el presente documento.

La TSA puede operar varias unidades de sellado de tiempo (TSU) identificables. ANF AC TSA está identificada en el certificado TSU utilizado para firmar TST.

2.2.3. Suscriptor / Cliente

El suscriptor es la persona jurídica o física a la que se emite un sello de tiempo y que está obligada a cumplir las obligaciones del suscriptor.

Cuando el suscriptor es una organización, que se compone de varios usuarios finales o un usuario final individual, algunas de las obligaciones que se aplican a esa organización tendrán que aplicarse también a los usuarios finales. En cualquier caso, la organización será la responsable si no se cumplen correctamente las obligaciones de los usuarios finales y, por lo tanto, la organización asume la responsabilidad de informar adecuadamente a sus usuarios finales.

Cuando el suscriptor es un usuario final, el usuario final es responsable directo si no cumple correctamente con sus obligaciones.

2.2.4. Terceros que confían

Un tercero que confía es una persona física o jurídica que actúa confiando es un TST, emitido bajo la Declaración de Prácticas TSA y Política de Timestamping de ANF AC. Una parte que confía puede, o no, ser también un suscriptor.

3. Política de Sellado de Tiempo

3.1. General

ANF AC TSA emite los TSTs, de conformidad con ETSI EN 319 421 y ETSI EN 319 422. ANF AC TSA solo expide sellos de tiempo electrónicos cualificados, las unidades de sellado de tiempo (TSU) no emiten sellos de tiempo electrónicos no cualificados.

Cada TSU está identificada de forma unívoca al encontrarse asociada a un certificado de clave pública el cual utiliza un nombre de sujeto distinto, empleando para ello un número secuencial.

Los TSTs se emiten con una precisión superior a 1 segundo respecto al UTC.

3.2. Identificador

El identificador de la Política de Sellado Cualificado de Tiempo Electrónico, especificado en el presente documento es el:

OID 1.3.6.1.4.1.18332.15.1

Para indicar que el sello de tiempo es cualificado, se incorpora uno de los siguientes OID en el campo “Policy” en el TSTInfo del sello de tiempo:

- 1.3.6.1.4.1.18332.15.1. Correspondiente a esta Declaración de Prácticas TSA y Política de TimeStamping, o
- 0.4.0.2023.1.1. Correspondiente a best-practices-ts-policy definido en el apartado 5.2 de la ETSI EN 319 421

4. Políticas y Prácticas

4.1. Evaluación de Riesgos

ANF AC TSA lleva a cabo evaluaciones de riesgo sobre una base regular para asegurar la calidad y la fiabilidad de los servicios de sellado de tiempo. A fin de asegurar su eficacia, se dispone de medidas de salvaguarda y de controles de seguridad que se definen en un marco de seguridad adecuado a la prestación del servicio de sellado de tiempo. Con una periodicidad mínima anual, y siempre que se produzca un cambio en la infraestructura o procedimientos se realiza una revisión de las políticas de seguridad y se efectúan auditoría contra los estándares internacionales publicados por ISO y ETSI.

4.2. Declaración de Prácticas del Servicio de Confianza

Asegurar la calidad del servicio es uno de los valores más importantes de ANF AC TSA. Por lo tanto, una variedad de controles de seguridad se ha aplicado para asegurar la calidad, el rendimiento y el correcto funcionamiento del servicio de sellado de tiempo. Los controles de seguridad se documentan, los cuales son regularmente revisados por un organismo independiente, empleando personal de confianza y capacitado para comprobar el cumplimiento de los controles de seguridad.

4.2.1. Formato del sello de tiempo

El token de sello de tiempo emitido por ANF AC TSA es compatible con RFC 3161. Con algoritmo RSA y longitud de clave mínima de 2048 bits, se emiten sellos de tiempo que acepten uno de los siguientes algoritmos de hash:

- SHA256
- SHA384
- SHA512

4.2.2. Exactitud del tiempo

El servicio de sellado de tiempo se encuentra en España, donde se proporciona una señal de tiempo a través del ROA (Real Observatorio de la Armada), laboratorio reconocido por el organismo público internacional Bureau International des Poids et Mesures (BIPM). Declarado a efectos legales como Patrón Nacional de dicha unidad, así como del mantenimiento y difusión oficial de la escala "Tiempo Universal Coordinado" *(UTC (ROA))*, considerado a todos los efectos como la base de la hora legal en todo el territorio nacional *(R.D. 23 octubre 1992, núm. 1308/1992)*.

El servicio de sellado de tiempo utiliza esta señal de tiempo ROA, y un conjunto de servidores NTP como fuentes de tiempo. Con esa configuración, el servicio de sellado de tiempo alcanza una precisión de +/- de 100 ms o superior con respecto al UTC.

4.2.3. Limitaciones del servicio

ANF AC se responsabiliza de la variación de la referencia temporal, en relación al tiempo proporcionado por servicio del Real Instituto y Observatorio de la Armada, incluida en el sello cualificado de tiempo electrónico en el momento de la solicitud, pero en ningún caso de la veracidad ni contenido de los datos electrónicos remitidos por los suscriptores del servicio, que son el objeto del Sello de tiempo electrónico emitido.

ANF AC no responderá ante los suscriptores o terceros que confían, cuyo comportamiento en la utilización del servicio cualificado de sellado de tiempo electrónico haya sido negligente, debiendo considerarse a estos efectos y en todo caso como negligencia la falta de observancia de lo dispuesto en la presente Declaración de Prácticas y Política de Sellado de Tiempo, en el Contrato de Servicio, en los Términos y Condiciones, y en especial, en lo dispuesto en los apartados referidos a las obligaciones y a la responsabilidad de los suscriptores y de las partes que confían.

ANF AC no garantiza los algoritmos criptográficos ni responderá de los daños causados por ataques exitosos externos a los algoritmos criptográficos usados, en especial, si guardó la diligencia debida de acuerdo al estado actual de la técnica, el presente documento y su adenda, y lo establecido en el Reglamento eIDAS y Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

ANF AC no responderá por ningún software que no haya proporcionado directamente.

ANF AC no responderá en los supuestos de caso fortuito, fuerza mayor, atentado terrorista, huelga,tumultos sociales, así como en los supuestos que se trate de acciones constitutivas de delito o falta que afecten a su infraestructura.

La cuantía que en concepto de daños y perjuicios que se debiera satisfacer por imperativo judicial, ANF AC a cada tercero perjudicado o miembro de la Comunidad Electrónica en defecto de regulación específica en los contratos o convenios, se limitan a un máximo de CINCO MIL EUROS (5.000€).

4.2.4. Verificación del sello de tiempo

El suscriptor y el tercero que confía, previo a depositar su confianza en el sello de tiempo electrónico, tienen que proceder a su verificación de acuerdo con lo establecido en la cláusula 6.7.5 “Validación de Sello de Tiempo” de este documento.

4.2.5. Ley aplicable

- Reglamento (UE) No 910/2014 (eIDAS), artículo 42.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

4.2.6. Disponibilidad del servicio

ANF AC TSA ha puesto en práctica las siguientes medidas para garantizar la disponibilidad del servicio:

- configuración redundante de sistemas informáticos, con el fin de evitar puntos únicos de fallos,
- conexiones de alta velocidad redundantes con el fin de evitar la pérdida de servicio,
- uso de sistemas de alimentación ininterrumpida.

A pesar de que esas medidas garantizan la disponibilidad del servicio de ANF AC TSA, no se puede garantizar una disponibilidad anual del 100%. ANF AC TSA tiene como objetivo proporcionar una disponibilidad del servicio anual del 99%, y asume con sus suscriptores Acuerdo de Nivel de Servicio (SLA - Service Level Agreement) publicado en, http://www.anf.es

4.3. Términos y condiciones

El documento *"Términos y Condiciones para los Servicios eIDAS de ANF AC” (OID 1.3.6.1.4.1.18332.5.1)* publicado en https://www.anf.es/repositorio-legal/, contiene información, por ejemplo, sobre la limitación

del servicio, las obligaciones de los suscriptores, o limitaciones de responsabilidad. Además, se aplica la siguiente información:

4.3.1. Aplicación de la política de servicio de confianza

Este documento informa sobre la política de servicio de confianza aplicada. Véase el capítulo 5 para más información relativa al alcance de las obligaciones y responsabilidades de las partes.

4.3.2. Periodo de tiempo de retención de los logs

Los registros de logs se retienen durante al menos tres meses. Los protocolos del sello de tiempo, lo que significa cada sello de tiempo emitido, se mantienen durante al menos 15 años.

4.4. Información de la política de seguridad

ANF AC TSA ha puesto en práctica una política de seguridad de la información en toda la empresa. Todos los empleados deben cumplir con las regulaciones establecidas en esta política y los conceptos de seguridad derivados. La política de seguridad de la información se revisa de manera regular y de forma especial cuando se producen cambios significativos. La Junta Rectora de ANF AC TSA aprueba los cambios de la política de seguridad de la información.

5. Obligaciones y responsabilidades

5.1. Obligaciones de la TSA (ANF AC)

5.1.1. Obligaciones

ANF AC, actuando como Autoridad de Sellado de Tiempo *(TSA)*, se compromete a:

- Respetar lo dispuesto en esta Declaración de Prácticas TSA y Política de Sellado de tiempo.
- Proteger sus claves privadas de forma segura.
- Garantizar que su reloj está sincronizado con el UTC dentro de la exactitud declarada de más de (1) segundo utilizando el NTP.
- Supervisar la sincronización de su reloj y garantiza que, si el tiempo que se indica en un TST se deriva o se sale de la sincronización con el UTC, tal caso es detectado.
- En caso de que el reloj del TSA se derive de la precisión, no se emitirán sellos de tiempo hasta que el reloj sea sincronizado.
- El servicio de sellado de tiempo se encuentra en España, donde se proporciona una señal de tiempo a través del ROA (Real Observatorio de la Armada), laboratorio reconocido por el organismo público internacional Bureau International des Poids et Mesures *(BIPM)*.
- Declarado a efectos legales como Patrón Nacional de dicha unidad, así como del mantenimiento y difusión oficial de la escala "Tiempo Universal Coordinado" *(UTC (ROA)),* considerado a todos los efectos como la base de la hora legal en todo el territorio nacional *(R.D. 23 octubre 1992, núm. 1308/1992)*
- El servicio de sellado de tiempo utiliza esta señal de tiempo ROA, y un conjunto de servidores NTP como fuentes de tiempo. Con esa configuración, el servicio de sellado de tiempo alcanza una precisión de +/- de 100 ms o superior con respecto al UTC.
- Los registros de los logs se retienen durante al menos tres *(3)* meses. Los protocolos del sello de tiempo, lo que significa cada sello de tiempo emitido, se mantienen durante al menos quince *(15)* años.
- ANF AC informará a todos los Suscriptores antes de que ANF AC deje de prestar los servicios de sello tiempo y mantendrá la documentación relacionada con los servicios terminados y la información necesaria en concordancia con los procesos establecidos en la DPC ANF AC TSA.

5.1.2. Responsabilidad

- ANF AC, para afrontar el riesgo de la responsabilidad por los daños y perjuicios que pueda ocasionar el servicio de sello de tiempo, ha suscrito el correspondiente seguro de responsabilidad civil, y ha ampliado el importe requerido por la legislación vigente, hasta la cantidad de CINCO MILLONES DE EUROS (5.000.000. €).
- La responsabilidad de ANF AC TSA con los suscriptores está estipulada en los contratos firmados con los suscriptores.
- Se aplican las disposiciones sobre responsabilidad definidas en la DPC de ANF AC, en especial en las secciones 9.6, 9.7 y 9.8.
- Se aplican las limitaciones de servicio, y exoneración de responsabilidad establecidas en este documento.

5.1.3. Exoneración de responsabilidad

ANF AC no será responsable de:

- Los errores en la verificación de la validez de los sellos de tiempo o de las conclusiones erróneas condicionadas por omisiones o por las consecuencias de tales conclusiones erróneas.
- El incumplimiento de sus obligaciones si dicho incumplimiento se debe a fallos o problemas de seguridad del organismo de supervisión (Ministerio de Industria, Energía y Turismo), la autoridad supervisora de protección de datos (Agencia Española de Protección de Datos), la Lista de Confianza o cualquier otra entidad pública.
- El incumplimiento si dicho incumplimiento fue ocasionado por fuerza mayor.
- Por la interrupción del servicio en cumplimiento con la sección 7.7.2. de la ETSI EN 319 421, por la que si ANF AC TSA detecta que la hora a introducir en un sello de tiempo se desvía o pierde la sincronización con el UTC, está obligada a detener la emisión. Cuando la parada del servicio se realice en cumplimiento con dicha norma, el suscriptor no tendrá derecho de reclamación.
- El Suscriptor, con la aceptación del sello de tiempo, exime de toda responsabilidad a ANF AC, y en especial, se compromete a mantener indemne a ANF AC de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del sello de tiempo, cuando concurra alguna de las siguientes causas:
    i. Falsedad o manifestación errónea realizada por el usuario del sello de tiempo.
    ii. Error del usuario del sello de tiempo al facilitar los datos de la solicitud, si en la acción u omisión medió dolo o negligencia con respecto a ANF AC, la entidad de registro o cualquier Tercero que Confía en el sello de tiempo.
    iii. Negligencia en la protección de la clave privada, en el empleo de un sistema fiable o en el mantenimiento de las precauciones necesarias para evitar el compromiso, la pérdida, la divulgación, la modificación o el uso no autorizado de dicha clave.
    iv. Empleo por el Suscriptor de un nombre u otra información en el certificado, que infrinja derechos de propiedad intelectual o industrial de terceros.
    v. Uso indebido de la clave privada del certificado, para operaciones que no están autorizadas en el mismo.
    vi. Incumplimiento en el pago de las tasas de emisión, renovación, pago del Dispositivo Criptográfico, firmas electrónicas o cualquier otro que el suscriptor haya contratado.
- El Tercero que Confía en el certificado se compromete a mantener indemne a ANF AC de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño, pérdida o gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:
    i. Incumplimiento de las obligaciones del tercero que confía en el certificado.
    ii. Confianza temeraria en un sello de tiempo, a tenor de las circunstancias.
    iii. Falta de comprobación del estado de un certificado, para determinar que no se encuentra suspendido o revocado.
    iv. Comprobación del certificado utilizando dispositivos no homologados por ANF AC.
    v. No utilizar el servicio de retimbrado de firmas, cuando alguno de los componentes criptográficos entre en situación de riesgo en conformidad con la publicación que al efecto ANF AC realiza en el Sitio Web.

5.2. Obligaciones de los suscriptores / clientes

Las obligaciones generales especificadas en este documento y en la cláusula 9.5.3 de la DPC ANF AC son aplicables:

- El suscriptor está obligado a no utilizar el servicio cualificado de sellado de tiempo electrónico de ANF AC, hasta haber formalizado el correspondiente contrato de uso del servicio. El disponer de un programa cliente de consumo de sellos de tiempo de ANF AC, o incluso, disponer de credenciales de control de acceso al servicio no le da derecho a utilizarlo.
- El suscriptor respetará lo establecido en la DPC de ANF AC y en este documento, así como lo acordado en los documentos contractuales y, en especial, los Términos y Condiciones de ANF AC.
- El suscriptor está obligado a:
    - verificar la firma del TST,
    - que la firma ha sido elaborada con un certificado TSU de ANF AC, y
    - comprobar que el certificado empleado para firmar el TST estaba vigente.

  Para realizar estas comprobaciones, se deberá utilizar un servicio cualificado de firma y sellos electrónicos cualificados.

- El suscriptor debe tomar las medidas necesarias para garantizar la validez del TST más allá del tiempo de vida de los certificados empleados por ANF AC TSA.
- Si no utiliza un cliente de sellos de tiempo de ANF AC, deberá comprobar que el hash contenido en el sello de tiempo coincide con el hash que envió en su solicitud de TST.
- Si no utiliza un cliente de sellos de tiempo de ANF AC, el suscriptor está obligado a utilizar las funciones criptográficas seguras para las solicitudes de sellado de tiempo.
- El suscriptor está obligado a comprobar la veracidad y contenido de los datos electrónicos remitidos al sellado de tiempo electrónico de ANF AC.
- Si no ha contratado el servicio de custodia de evidencias y preservación a largo plazo de firmas y sellos electrónicos, el almacenamiento y conservación de los sellos de tiempo entregados por la TSA es responsabilidad del suscriptor.
- El suscriptor está obligado a informar a sus usuarios finales *(por ejemplo, los terceros que confían)* sobre el uso correcto de sellos de tiempo y las condiciones de ANF AC y ANF AC TSA.
- El suscriptor no hará valer los sellos de tiempo electrónicos como referencia temporal fuera de los límites establecidos para estos en su correspondiente política.

5.3. Obligaciones de los terceros que confían

Las obligaciones generales especificadas en este documento y en la cláusula 9.5.4 de la DPC ANF AC son aplicables:

- Los terceros que confían antes de depositar su confianza en un sello de tiempo electrónico (TST) de ANF AC, deben:
    - comprobar la correspondencia del TST con los datos electrónicos a los que se asocia,
    - verificar que el TST ha sido firmado con la clave correspondiente del certificado del TSU de ANF AC, y
    - que el certificado empleado para firmar el TST estaba vigente.

Para realizar estas comprobaciones, se deberá utilizar un servicio cualificado de firma y sellos electrónicos cualificados.

- Los terceros que confían deben tomar las medidas necesarias para garantizar la validez del TST más allá del tiempo de vida de los certificados empleados por ANF AC TSA.
- Deben de tener en cuenta cualquier limitación de uso de acuerdo con la política indicada en el sello de tiempo.
- Los terceros que confían no harán valer los sellos de tiempo electrónicos como referencia temporal fuera de los límites establecidos para estos en su correspondiente política.
- Deben tener en cuenta cualquier otra obligación prescrita en esta Declaración de Prácticas y su adenda, así como en los Términos y Condiciones correspondientes al servicio de sellado de tiempo electrónico.

6. Gestión y operación de la TSA

6.1. Introducción

ANF AC TSA ha implementado un sistema de gestión de seguridad de la información para mantener la seguridad del servicio.

La provisión de un TST en respuesta a una solicitud es a discreción de ANF AC TSA, dependiendo del contrato del suscriptor.

6.2. Organización interna

Todas las prácticas de ANF AC TSA están descritas en el apartado 9 de la DPC de ANF AC. La estructura organizativa, las políticas, procedimientos y controles de ANF AC se aplican a ANF AC TSA.

Los procedimientos de organización cumplen con las normas y reglamentos definidos en la cláusula 1.1 del presente documento.

a) **Entidad legal**: La Autoridad de Sellado de Tiempo es gestionada por ANF AC TSA.
ANF AC TSA, es una entidad de tecnología especializada en el desarrollo y fabricación de productos electrónicos inteligentes, complejos y seguros:
   - ANF Autoridad de Certificación
   - Paseo de la Castellana, 79 – 28046 - Madrid (España)
   - Tfno: +34 932 661 614 *(España)*
   - Tfno: +34 933 935 946 *(International)*
   - Web: www.anf.es

b) Gestión de la información de seguridad y gestión de la calidad del servicio se lleva a cabo dentro del concepto de seguridad del servicio.

6.3. Personal de confianza

Se aplican las prácticas definidas en las cláusulas 5.2 y 5.3 de la DPC de ANF AC.

ANF AC TSA ha entendido que los empleados con talento y motivación son un factor clave para el éxito del negocio. Por lo tanto, las prácticas de contratación es un proceso muy importante en la organización. Sólo un buen conocimiento, con respecto a su puesto de trabajo, y personal de confianza permiten cumplir con las operaciones en el servicio de sellado de tiempo.

El concepto “rol” hace cumplir la segregación de funciones para garantizar que sólo el personal titulado realice las tareas operativas importantes.

Antes del nombramiento de personal en puestos de confianza, ANF AC comprueba que cuente con los conocimientos necesarios o, en su caso, se realiza transferencia de conocimiento a través de cursos de formación y estos deben superar las pruebas de adquisición de conocimiento.

El personal de ANF AC se encuentra libre de conflictos de intereses que pudieran perjudicar la imparcialidad de las operaciones de ANF AC TSA.

6.4. Gestión de activos

Se aplican las prácticas definidas en las cláusulas 5, 6.4 y 6.5 de la DPC de ANF AC.

Todos los sistemas informáticos utilizados en el servicio están claramente identificados, clasificados y registrados en una base de datos de gestión de activos.

Todos los recursos se manejan de forma correcta.

La información contenida en los equipos se elimina de forma segura, ya sea por un proceso de borrado de los datos electrónicos o destruyendo físicamente a los medios dispuestos.

6.5. Control de accesos

Las prácticas identificadas en las cláusulas 6.4 y 6.5 de la DPC de ANF AC son aplicables.

Las diferentes barreras de seguridad con respecto al acceso físico y acceso lógico, garantizan un funcionamiento seguro del servicio de sellado de tiempo. Por ejemplo:

- Entorno físico seguro
- Segregación de los segmentos de red
- Segregación de responsabilidades
- Firewalls
- Monitorización del Servicio de Red
- Fortalecimiento de los Sistemas IT

En caso de que una persona lleve a cabo operaciones en ANF AC TSA, y esta cambie de rol o deje de prestar sus servicios a la entidad, le serán retirados todos sus tokens de seguridad.

6.6. Certificado de TSA *(TSU)*

ANF AC dispone y sigue procedimientos que garantizan la seguridad criptográfica del servicio, estas practicas están documentadas en “Controles de Seguridad Criptográfica CA - TSA” OID: 1.3.6.1.4.1.18332.57.1.2

Los certificados de TSA no se renuevan.

6.6.1. Generación de claves TSA

Las claves privadas de la TSA se generan y custodian en un dispositivo criptográfico seguro (HSM) que cumple los requerimientos que se detallan en FIPS 140-2 nivel 2 o superior, o con un nivel EAL 4+ o superior de acuerdo con ISO/IEC 15408, no siendo esta importada a otros módulos criptográficos.

La generación de las claves de firma de la TSA (TSU) se lleva a cabo en un entorno físicamente protegido (según la cláusula 5.8 de este documento) por personal en puestos de confianza (según la cláusula 5.3 de este documento), bajo al menos el control de dos personas de confianza. Esta clave privada de firma se utiliza solo para firmar TSTs.

El algoritmo de firma es RSA y la longitud de clave mínimo es de 2048 bit. Los certificados tendrán una duración adecuada a la seguridad criptográfica de acuerdo con las recomendaciones publicadas en ETSI TS 119 312, contando desde el momento de inicio del periodo validez del certificado asociado.

Cada Unidad de Sellado de Tiempo (TSU) tendrá una única clave privada de firma de sello de tiempo activa cada vez.[2]

En la utilización de sellos de tiempo para procedimientos de nivel alto del Esquema Nacional de Seguridad se seguirán las indicaciones de la norma de seguridad CCN-STIC-807

6.6.2. Protección de la clave del TSU

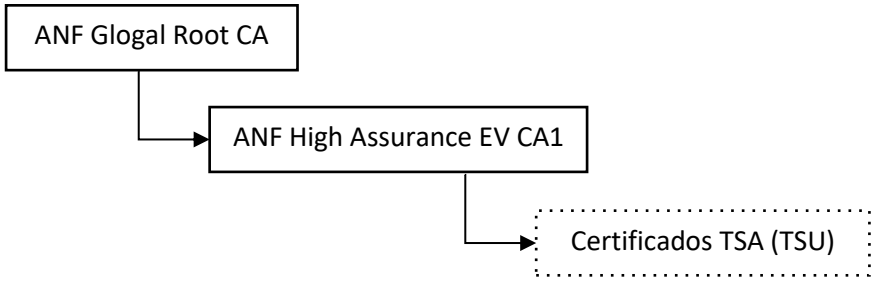
Se aplican las prácticas de protección de claves de TSU, almacenamiento, backups y recuperación descritas en las cláusulas 6.2 y 6.3 de la DPC de ANF AC.

La clave privada del TSU se encuentra protegida en un módulo criptográfico HSM certificado en ISO 15408, Common Criteria EAL 4+.

6.6.3. Publicación de los Certificados de la TSA

Los Sellos de tiempo electrónicos emitidos bajo esta política son firmados por certificados específicos, que a su vez han sido emitidos bajo la Cadena de Certificación de la Autoridad de Certificación raíz con CN= ANF Global Root CA

El certificado del servicio TSA se adjunta en la respuesta de cada sello de tiempo que se emite y está publicado en https://www.anf.es/certificados-ca-raiz/



Certificado Autoridad de Certificación Raíz (Root CA), **ANF Global Root CA**:

ANF Global Root CA *(caducidad 2036)*			
Sujeto	CN = ANF Global Root CA	**Serial number**	01 64 95 ee 61 8a 07 50
	SERIALNUMBER = G63287510		
	O = ANF Autoridad de Certificación	**Clave Pública**	RSA (4096 Bits)
	C = ES	**Algoritmo de firma**	Sha256RSA
Periodo de vigencia	Válido desde el 2016-05-20 hasta el 2036-05-15		
Fingerprint SHA-1	FC9843CC9922615001A17374CE8A3D79580FEA51		
Fingerprint SHA-256	E0AFBD2C0EE95A68CD9A3C590B2D3FE07C0A6D0BE796AE5291E424D47792178E		

[2] *Apartado 7.6.2. f) ETSI EN 319 421*

Certificado Autoridad de Certificación Intermedia, **ANF High Assurance EV CA1**:

ANF High Assurance EV CA1			
Sujeto	CN = ANF High Assurance EV CA1	**Serial number**	06 5d 66 65 46 a4 59 00
	SERIALNUMBER = G63287510	**Clave Pública**	RSA (4096 Bits)
	OU = ANF Autoridad Intermedia Tecnicos		
	O = ANF Autoridad de Certificación	**Algoritmo de firma**	Sha256RSA
	C = ES		
Periodo de vigencia	Válido desde el 2016-05-20 hasta el 2026-05-18		
Fingerprint SHA-1	67939B3CA77E5F6FDEC07EC96371A87C77197962		
Fingerprint SHA-256	1C28A8C009F25850B9155533D4A9A14C534B24DA84756E82D6150B5062D63704		

El servicio cualificado de Sellado de Tiempo empleará los siguientes certificados electrónicos de TSU para prestar el servicio:

ANF Qualified Time-Stamping Unit 1360			
Subject	CN = ANF Qualified Time-Stamping Unit 1360	**Serial number**	996112230137107613581495663
	OI = VATES-G63287510	**Clave Pública**	RSA (2048 Bits)
	OU = TSU		
	O = ANF Autoridad de Certificación	**Algoritmo de firma**	Sha256RSA
	C = ES		
Identificador Política	1.3.6.1.4.1.18332.15.1		
Periodo de vigencia	Válido desde el 2021-04-15 hasta el 2025-04-14		
Periodo de uso de la clave privada	2024-04-14		

Fingerprint SHA-1	05:D6:BC:52:B9:81:73:4C:90:3A:7A:F8:0A:D3:1D:82:93:EE:76:11
Fingerprint SHA-256	2E:C5:A6:1B:5D:77:2E:10:9F:BB:76:A1:D6:6C:0F:B2:C6:06:A2:A2:34:BF:9D:F3:A0:97:B8:5E:AA:65:09:24

ANF Qualified Time-Stamping Unit 1361			
Sujeto	CN = ANF Qualified Time-Stamping Unit 1361	**Serial number**	996750780693200761702941647
	OI = VATES-G63287510	**Clave Pública**	RSA (2048 Bits)
	OU = TSU		
	O = ANF Autoridad de Certificación	**Algoritmo de firma**	Sha256RSA
	C = ES		
Identificador Política	1.3.6.1.4.1.18332.15.1		
Periodo de vigencia	Válido desde el 2021-04-15 hasta el 2025-04-14		
Periodo de uso de la clave privada	2024-04-14		

Fingerprint SHA-1	34:4E:E2:0D:ED:5F:E7:5A:37:A6:2C:A5:69:84:39:07:68:27:FB:3F
Fingerprint SHA-256	92:3F:7F:DD:D5:A0:EB:17:B4:C2:4A:48:27:D1:AD:F5:BA:BF:D3:F6:96:B7:C3:FD:D6:DF:9B:2C:0B:76:6B:A8

ANF Qualified Time-Stamping Unit 1362			
Sujeto	CN = ANF Qualified Time-Stamping Unit 1362	**Serial number**	996426365797221774638995437
	OI = VATES-G63287510	**Clave Pública**	RSA (2048 Bits)
	OU = TSU		
	O = ANF Autoridad de Certificación	**Algoritmo de firma**	Sha256RSA
	C = ES		
Identificador Política	1.3.6.1.4.1.18332.15.1		
Periodo de vigencia	Válido desde el 2021-04-15 hasta el 2025-04-14		
Periodo de uso de la clave privada	2024-04-14		

Fingerprint SHA-1	B4:C8:83:6A:35:AE:14:08:60:15:37:C5:E3:03:51:57:E1:8D:52:28
Fingerprint SHA-256	88:18:5A:3E:D9:95:53:9E:B9:EA:7C:4B:D9:6D:6F:85:96:0D:5A:13:2E:DB:6D:77:01:DF:67:0F:5C:AC:B4:E7

Los certificados electrónicos de TSU incluyen, siguiendo las recomendaciones de las normas ETSI EN 319 421 y ETSI EN 319 422, la extensión privateKeyUsage, que limita el uso de la Clave privada estableciendo una fecha de cese de uso de la clave, anterior a la caducidad de la clave pública, de manera que se asegure un tiempo suficiente para la renovación de los TST emitidos por una TSU antes de la caducidad de su certificado.

Los certificados electrónicos de TSU incluyen la extensión "id-kp-timestamping" que indica que este certificado se utilizará con el fin exclusivo de expedir sellos de tiempo electrónico.

6.6.4. Cambio del Certificado de TSA

Se establecen los controles para garantizar el cese de uso de la clave privada antes de la extinción de su vigencia.

El certificado de la TSA puede ser cambiado en cualquier momento por otro certificado de TSA, previo aprobación de la Junta Rectora de la PKI de ANF AC.

En caso de cambio de certificado, las claves asociadas serán destruidas de forma que no puedan ser recuperadas, conforme a las instrucciones del fabricante del HSM que las genera y alberga.

El certificado de la TSA tendrán una vida útil máxima de 5 años. La duración del certificado del TSU está limitado por:

- El tiempo de validez del certificado de CA emisora.
- El tiempo de vigencia establecido en el propio certificado.

- Si un algoritmo o la longitud de clave entra en situación de riesgo, éste deja de ser adecuado; la TSA cesará en el uso de los certificados afectados, procediendo a la emisión de nuevos certificados con algoritmos y longitudes seguras.
- Cese de la actividad. Se aplicará lo establecido en el apartado Finalización de TSA y Plan de Cese de este documento.

6.6.5. Gestión del ciclo de vida del hardware criptográfico

Las prácticas de gestión del ciclo de vida del HSM se describen en la cláusula 6.2 de la DPC de ANF AC.

El hardware criptográfico utilizado es inspeccionado por personal de confianza (en presencia de dos personas) en el control de transporte y almacenamiento. En concreto, en cuanto al hardware se comprueba lo siguiente:

a) Daños en los sellos de seguridad
b) Daños en el equipamiento hardware (por ejemplo: arañazos, golpes…)
c) Daños en el embalaje del hardware

La inspección es protocolizada. Además, se aplica lo siguiente:

a) La instalación, y activación de claves de firma de TSU en hardware criptográfico se realiza únicamente por personal de confianza según sus roles utilizando, al menos, el control dual en un entorno protegido físicamente.
b) La clave privada de firma almacenada en el módulo criptográfico del TSU, se borra al retirarse el dispositivo de una forma que prácticamente imposibilita su recuperación.

6.6.6. Fin del ciclo de vida de la Clave del TSU

Después de la expiración de las claves privadas, se destruyen de una manera tal que las mismas no se puedan recuperar siguiendo el procedimiento establecido por el fabricante del módulo criptográfico que las almacena.

6.7. Sellado de tiempo

ANF AC TSA solo emite los sellos electrónicos de tiempo cualificados, y no emite sellos electrónicos de tiempo no cualificados.

El TSU no emite un sello de tiempo antes de su verificación de firma (clave pública). Cuando el certificado se carga en el TSU, la TSA verifica que este certificado ha sido firmado correctamente (incluyendo la verificación de la cadena de certificados de una autoridad de certificación de confianza).

6.7.1. Emisor de sello de tiempo

ANF AC TSA ofrece servicios de sellado de tiempo utilizando el RFC 3161 “Time-Stamp Protocol (TSP)”, que se perfila en ETSI EN 319 422. La URL del servicio se especifica en los contratos de suscripción. Cada TST contiene el identificador de la política de sellado de tiempo, un número de serie único y un certificado que contiene la información de identificación del TSU de ANF AC TSA.

El TSU, en las solicitudes de sello de tiempo, acepta algoritmos de hash SHA256, SHA384, SHA512 y, para firmar el TST se utiliza la función de hash criptográfica mínimo de SHA-256.

Las claves del TSU son claves RSA con una longitud mínima de 2048 bits. La clave se utiliza sólo para la firma del TST. La TSA registra todos los TST emitidos, los cuales son almacenados por tiempo indefinido.

ANF AC TSA gestiona un servicio de encadenamiento de hash relativo a todos los TST emitidos por cada TSU, sin incluir información que pueda determinar la identidad del solicitante. Y, por lo tanto, puede probar la existencia de un TST en concreto, y su correcta correspondencia cronológica respecto al conjunto de TST emitidos por un determinado TSU. Además, realiza depósito notarial de las actas de resumen general de los hash entrante-actual-saliente asociados a los TST emitidos. ANF AC TSA podrá pedir al tercero que confía cubrir los costos de comprobación de existencia de hash, en caso de solicitud de evidencia.

El TSU no emite ningún TST cuando la clave privada alcanza el fin de uso.

6.7.2. Sincronización de la hora con UTC

ANF AC TSA asegura que su reloj está sincronizado con UTC [ROA] dentro de la precisión de 1 segundo o mejor, utilizando el protocolo NTP.

ANF AC TSA supervisa la sincronización de su reloj y asegura que, si el tiempo de un TST está fuera de sincronización con UTC, esto es detectado. En el caso de que el reloj de la TSA pierda su exactitud, se procederá a la paralización del servidor hasta recuperar la sincronización del reloj.

En concreto, los aspectos siguientes se regulan:

- Calibración permanente del reloj TSU
- El control de la precisión del reloj TSU
- Análisis del hilo contra los ataques a tiempo de la señal
- Comportamiento mientras se saltan / añaden segundos intercalados
- Comportamiento mientras se deriva más de un 1s del UTC

6.7.3. Solicitud de Sellos de Tiempo

ANF AC TSA presta el servicio de Sellado de Tiempo Electrónico a clientes del mismo. El servicio es prestado en dos modalidades:

- Utilizando un cliente TST de ANF AC,
- Consulta directa al servidor TSU, para ello las solicitudes de sellos cumplirán la sintaxis de la especificación “RFC 3161 Time Stamp Protocol (TSP)” y precisarán superar el correspondiente control de autenticación acceso.

ANF AC TSA facilta soporte técnico en cualquiera de los supuestos.

6.7.4. Formato de las respuestas de Sellos de Tiempo

Las respuestas no incluyen extensiones, no se incluye la TSA al incluir el certificado TSU en la respuesta, y el TSP se envía en el siguiente formato:

> Content type: application/timestamp-reply
> Method: POST
> Content-length: required
> <<*Contiene la respuesta de sello de tiempo en ASN.1 (en su caso especifica el código de error)*, codificado en DER >>

Campo	Tratamiento
Policy	1.3.6.1.4.1.18332.15.1
Ordering	Falso
Nonce	Si la petición lo contiene se devuelve el mismo valor Sino se crea uno nuevo
Certificados adjuntos	<Certificado de TSA> <Certificado de CA Subordinada>
Accuracy	La correspondiente, no permitido TST superior a 1

Si la solicitud se ha podido procesar, TimeStampToken Secuencia. Estructura firmada del tipo CMSSignedData en la que se incluye el sellado de tiempo y el sello electrónico del mismo. Incluye el certificado de TSU que lo firma:

TSTInfo ::= SEQUENCE {
version INTEGER { v1(1) },
messageImprint MessageImprint,
-- OID del algoritmo hash y el valor hash de los datos sellados---
reqPolicy TSAPolicyId OPTIONAL,
certReq BOOLEAN DEFAULT FALSE,
nonce INTEGER OPTIONAL,
extensions [0] IMPLICIT Extensions OPTIONAL
}

El campo *reqPolicy* corresponde al OID de la *TSAPolicyId*. Los OIDs aceptados son OID 1.3.6.1.4.1.18332.15.1 correspondiente a la DPC de ANF AC TSA, y OID 0.4.0.2023.1.1 correspondiente a best-practices-ts-policy definido en el estándar europeo ETSI EN 319 421.

Si la solicitud no se puede procesar, se devuelve una respuesta indicando un código de error cuando no puede responder con un time-stamp. A continuación, se describen los códigos de error del campo PKIFailureInfo, que se incluyen al generar una respuesta fallida por cada tipo de posible error:

1. badRequest: Cuando la política de la solicitud no coincide con la política de la TSA.
2. badAlg: Cuando el algoritmo del messageImprint no está soportado o no es válido.
3. badTime: Cuando la exactitud es superior o igual a un segundo o 1000 milisegundos.
4. timeNotAvailable: Cuando la fecha actual no es válida porque no es superior a la última fecha registrada en la base de datos.
5. systemFailure: Cuando el encadenamiento anterior es incorrecto, o no se puede obtener el nuevo encadenamiento. También se incluye en la respuesta producida por una excepción o error que no permite seguir con el procesamiento de la solicitud.

6.7.5. Validación del sello de tiempo electrónico

Para validar un sello cualidicado de tiempo electrónico, las partes confiantes verificarán el TST haciendo uso de un sistema cualificado de validación de firmas y sellos electrónicos cualificados que disponga de verificación de TST. ANF AC pone a disposición pública y gratuita este servicio.

El servicio de verificación de TST, hace uso del campo “messageImprint” descrito en el apartado anterior, así como el estado de validez del Certificado de la TSU a través del servicio de validación del estado de los

certificados (protocolo OCSP) de ANF AC. El punto de acceso al servicio OCSP se encuentra incluido en el certificado TSU.

La verificación del sello de tiempo incluye las siguientes operaciones:

- **Operación I Verificación del emisor del sello de tiempo:** El emisor es ANF AC TSA, una Autoridad de Sellado de Tiempo inscrita en la TSL de España en conformidad con el Reglamento eIDAS, que utiliza los certificados electrónicos adecuados para emitir el sellos cualificados de tiempo electrónico. Las claves públicas de los certificados utilizados, están incluidas en los certificados de TSU y CA, y se publican para permitir una verificación de que el sello de tiempo se ha firmado correctamente por la TSA. Los certificados se pueden encontrar en: www.anf.es

- **Operación II Verificación del estado de revocación del certificado TSU:** Un servicio OCSP que cumple IETF RFC 6960, está disponible con el fin de comprobar el estado de revocación de los certificados utilizados en el sello de tiempo. La dirección de acceso al servicio respondedor OCSP está incluida en el certificado empleado para firmar el sello de tiempo.

- **Operación III Verificación de la integridad del sello de tiempo:** La integridad criptográfica del sello de tiempo, por ejemplo, la estructura ASN.1 es correcta, y los datos *(los datos que han sido fechados)* pertenecen a la solicitud. Esto puede ser verificado mediante dispositivos de validación cualificada disponible publicamente en: www.anf.es

El servicio de validación podrá determinar la asociación del TST con los datos electrónicos sellados mediante obtención del hash de los datos electrónicos sellados, comprobando su correspondencia con el hash que ha sido sellado por la TSA.

Además, se puede comprobar la existencia e imposibilidad de manipulación del sello de tiempo electrónicio por parte de la TSA, comprobando:

- la existencia del hash del TSP en las actas de encadenamiento, y
- su correcta correspondencia de la fecha y hora estampada, respecto a la relación cronológica del conjunto de TST emitidos por el TSU de interés.

La relación general de actas de encadenamiento hash son protocolizadas mediante intervención de notario.

6.8. Seguridad física y ambiental

Se aplican las prácticas identificadas en las cláusulas 5.1 y 6.5 de la DPC de ANF AC.

Un entorno físico de alta seguridad es necesario; éste alberga la TSA. Las instalaciones de gestión de sellado de tiempo se operan en un entorno que protege física y lógicamente los servicios de transacción con controles de acceso no autorizados a sistemas o datos. Cada entrada en el espacio físicamente seguro está sujeto a supervisión independiente de la TSA. En el área de seguridad se acompaña a la persona que accede a las instalaciones, registrando identidad, hora de entrada y salida.

La protección física se logra mediante la creación de perímetros de seguridad claramente definidos (es decir, barreras físicas) en torno a la gestión de sellado de tiempo.

Los controles físicos y ambientales de seguridad protegen la instalación que alberga los recursos del sistema.

La política de seguridad física y ambiental de la TSA, para los sistemas que se emplean en la gestión del servicio de sellado de tiempo, se dirige al control del acceso físico, protección de desastres naturales, factores de seguridad contra incendios, fallo en los suministros (por ejemplo, energía, telecomunicaciones), colapso de la estructura, fugas de agua o inundaciones, protección contra robo, allanamiento y recuperación de desastres.

Los controles físicos y de organización protegen contra el acceso desde el exterior a servidores, información, medios de comunicación y software relacionados con los servicios de sellado de tiempo.

6.9. Seguridad de las operaciones

Se aplican las prácticas identificadas en las cláusulas 6.3, 6.4 y 6.5 de la DPC de ANF AC.

ANF AC TSA ha implementado un sistema avanzado de seguridad para garantizar la calidad y disponibilidad del servicio. En particular, estos controles son:

a) Se lleva a cabo un análisis de los requisitos de seguridad en las especificaciones de diseño, y los requisitos para cualquier etapa del proyecto de desarrollo de sistemas emprendida por el TSP o en nombre de la TSP, para asegurar que la seguridad se integra adecuadamente en los sistemas de tecnología de la información.
b) Como procedimiento de control de cambios, se aplica un control de versionado para modificaciones y correcciones del software.
c) La integridad de los sistemas y la información TSP está protegido contra virus, software malicioso y software no autorizado.
d) Los medios empleados en los sistemas TSP son seguros y protegen contra daños, robo, acceso no autorizado y la obsolescencia.
e) Dentro del período de tiempo que se requiere que deben conservarse los registros, los procedimientos de gestión de medios hacen que la información se proteja contra la obsolescencia y el deterioro de los medios de comunicación.
f) La aplicación de procedimientos adecuados para todas las funciones de confianza y administrativos que tienen un impacto en el suministro de servicios.
g) El TSP ha especificado y aplicado procedimientos para asegurar que los parches de seguridad se aplican dentro de un tiempo razonable después de que estén disponibles. La aplicación de un parche de seguridad no será obligatoria si introduce vulnerabilidades o inestabilidades adicionales que superan a los beneficios de aplicar dicho parche. Se debe documenta la razón por la cual no se aplica un parche de seguridad
h) Se monitoriza la correcta calibración del reloj de su TSU. En caso de detectar una desviación superior a 1 segundo, el servicio de TSA se detendrá automáticamente.

6.10. Seguridad de la red

Se aplican las prácticas identificadas en las cláusulas 6.5 de la DPC de ANF AC. El TSP protege su red y los sistemas de los ataques. En particular:

a) La red TSP está segmentada en redes o zonas en función de la evaluación de riesgos teniendo en cuenta la relación funcional, lógica y física (incluyendo la ubicación) entre los sistemas y servicios de confianza.
b) El TSP restringe el acceso y la comunicación entre las zonas a las necesarias para el funcionamiento de la TSP. No se necesitan conexiones y los servicios están prohibidos o desactivan de forma explícita. El conjunto de reglas establecido se revisa de manera regular.
c) Todos los elementos de los sistemas críticos del TSP (por ejemplo, los sistemas de CA raíz, TSU) se mantienen en una zona segura.
d) Se ha establecido una red dedicada para la administración de sistemas de TI que se separa de la red operativa. Los sistemas utilizados para la administración no serán utilizados con fines no administrativos.
e) La plataforma de test y la plataforma de producción se separan. La plataforma de test se encuentra en un entorno no encargado de operaciones vivas (por ejemplo, de desarrollo).
f) La comunicación entre los distintos sistemas de confianza sólo puede establecerse a través de los canales de confianza que son distintos lógicamente de otros canales de comunicación, y proporcionan la identificación segura de sus puntos finales y protegen los datos de la modificación o de la divulgación.
g) La conexión a la red externa de Internet es redundante para asegurar la disponibilidad de los servicios en caso de un solo fallo.
h) El TSP lleva a cabo regularmente un análisis de vulnerabilidades de direcciones IP públicas y privadas previamente identificadas por el TSP, el análisis de cada vulnerabilidad es realizado por una persona o entidad con las habilidades, herramientas, conocimientos, código de ética, y la independencia necesaria para proporcionar un informe fiable.
i) El TSP, después de configurar la infraestructura con actualizaciones o modificaciones que el TSP considera que son significativas, lleva a cabo una prueba de penetración en los sistemas. El TSP obtiene registros de evidencia de que cada prueba de penetración realizada por una persona o entidad con las habilidades, herramientas, conocimientos, código de ética, y la independencia necesaria para proporcionar un informe fiable.

6.11. Gestión de incidentes

Se aplican las prácticas identificadas en la cláusula 4.15 de la DPC de ANF AC. Para una información más detallada acudir al Documento de Seguridad “Procedimiento de gestión de las incidencias”.

Las actividades de acceso a los sistemas informáticos, sistemas de usuario de la misma, y las solicitudes de servicio son monitoreados. En particular:

a) Las actividades de seguimiento toman en cuenta la sensibilidad de cualquier información recogida y analizada.
b) Las actividades anormales del sistema que indican una posible violación de seguridad, incluyendo la intrusión en la red TSP, son detectados y reportados como alarmas.
c) Los sistemas IT del TSP controlan los siguientes eventos: Puesta en marcha y parada de las funciones de registro; disponibilidad y utilización de los servicios necesarios con la red TSP.
d) El TSP actúa de una manera oportuna y coordinada con el fin de responder rápidamente a los incidentes y para limitar el impacto de las violaciones de la seguridad. El TSP designa a personal de

confianza y según roles, para dar seguimiento a las alertas de eventos de seguridad potencialmente críticos, y garantizar que los incidentes relevantes se recogen en consonancia con los procedimientos del TSP.

e) El TSP notifica a las partes correspondiente, de acuerdo con las normas reglamentarias aplicables, cualquier violación de seguridad o pérdida de la integridad que tiene un impacto significativo en el servicio prestado, y la confianza en los datos personales mantenidos en ella.
f) La autoridad nacional de control es informada dentro de las 24 h siguientes del descubrimiento de un fallo de seguridad crítico.
g) Los registros de auditoría son monitoreados y revisados con regularidad para identificar evidencia de actividad maliciosa.
h) El TSP resolverá las vulnerabilidades críticas en un plazo razonable después del descubrimiento. Si esto no es posible, el TSP crea e implementa un plan para mitigar la vulnerabilidad crítica, o el TSP documentará la base fáctica de la determinación del TSP que la vulnerabilidad no requiere de remediación.
i) Los procedimientos de información y respuesta a incidentes, se aplican de tal manera que el daño de los incidentes de seguridad y problemas de funcionamiento se reducen al mínimo.

6.12. Gestión de evidencias

Se aplican las prácticas identificadas en la cláusula 4.12 de la DPC de ANF AC.

En el momento en el que se ha detectado un incidente de seguridad, puede ser que no sea obvio, si ese incidente de seguridad es objeto de nuevas investigaciones. Por lo tanto, es importante, que cualquier prueba, el estado del sistema o la información se guarde de forma segura antes de que sean inutilizables o se destruyan.

Los registros del TSP se mantienen accesibles durante un período adecuado de tiempo, incluso después de que las actividades de la TSP han cesado. Toda la información pertinente relativa a los datos emitidos y recibidos por el TSP son custodiados con el fin de proporcionar pruebas en los procedimientos legales y con el fin de garantizar la continuidad del servicio. En particular:

a) La confidencialidad y la integridad de los registros actuales y de archivo relativos a la operación de los servicios se mantiene.
b) La información relativa a la gestión de servicios es confidencial y archivada de conformidad con las prácticas comerciales descritas.
c) La información relativa a la gestión de servicios, en caso necesario, se pone a disposición a los efectos de proporcionar pruebas del correcto funcionamiento en un procedimiento judicial.
d) El TSP registra en el momento preciso, los acontecimientos significativos del medio ambiente, gestión de claves y sincronización de reloj. El tiempo utilizado para registrar los acontecimientos, como se requiere en el registro de auditoría, está sincronizado con UTC continuamente.
e) La información relativa a los servicios se salvaguarda durante un período de tiempo después de la expiración de la validez de las claves de firma, o de cualquier servicio de token como la confianza adecuada para proporcionar la evidencia jurídica como se estipula en el presente documento.
f) Los eventos se registran en una forma que no pueden ser borrados o destruidos (excepto si se transfieren de forma fiable a los medios de comunicación de largo plazo).

6.13. Gestión de la Continuidad del Negocio

Se aplican las prácticas identificadas en la sección 4.15 de la DPC de ANF AC.

Las copias de seguridad de la base de datos de todos los TST emitidos por ANF AC TSA se mantienen en almacenamiento fuera del sitio.

Si la clave privada del TSU se ve comprometida o se sospecha que se vea comprometida, ANF AC TSA informará a los suscriptores y terceros que confían, y dejarán de usar la clave comprometida.

En caso de revocar el certificado de TSU, las acciones se llevan a cabo de conformidad con la decisión del Comité de Crisis y Plan de Recuperación.

En caso de pérdida de sincronización del reloj, ANF AC TSA suspende sus operaciones para evitar una mayor daño. El Plan de Recuperación se activa para restaurar la sincronización y el servicio.

El servicio de sellado de tiempo en sí, está situado en un entorno físico asegurado que minimiza el riesgo de desastres naturales (por ejemplo, incendios).

Las claves privadas de la TSU se almacenan en un módulo de seguridad criptográfica.

En caso de que las claves privadas puedan verse en peligro, el archivo de los sellos de tiempo registrados ayuda a diferenciar entre los sellos de tiempo correctos y los falsos en una pista de auditoría.

El HSM está aislado de la red pública y en caso de necesidad se tomarán las siguientes medidas correctoras:

- Notificar al Responsable de Seguridad para que coordine todas las medidas a adoptar.
- Poner en marcha una auditoría de seguridad de las restantes claves privadas (comprobaciones de integridad, análisis de registros del archivo).
- Notificar la incidencia a los terceros que confían.
- Iniciar el procedimiento de sustitución con el fin de volver a una redundancia N + 1 En los casos de desastres naturales (por ejemplo, incendios, terremotos, tormentas) si ocurre una pérdida de las instalaciones, podría suspenderse el servicio de sellado de tiempo hasta que se haya reconstruido y un órgano independiente haya realizado una evaluación de la instalación. La pérdida de calibración o sincronización del reloj de un TSU está cubierta en la cláusula 5.7.1 de este documento.

6.14. Finalización de TSA y Plan de Cese

Se aplican las prácticas identificadas en la sección 4.16 y 4.17 de la DPC de ANF AC. Adicionalmente:

- En el caso de que la TSA termine sus operaciones por cualquier motivo, se notificará a la autoridad nacional de control antes de la terminación.
- Se proporcionará un aviso oportuno para todos los terceros que confían, con el fin de minimizar cualquier perjuicio que pueda ser causado debido a la terminación de los servicios.
- Además, en colaboración con el órgano de control, el TSP coordinará las medidas necesarias con el fin de asegurar la retención de todos los registros archivados pertinentes antes de la terminación del servicio.

- Además, se aplica lo siguiente:
  a) El TCP mantiene un plan de terminación actualizado.
  b) Antes de que el TSP de por finalizados sus servicios, al menos, se aplican los siguientes procedimientos:
     i. el TSP informará de la terminación a las siguientes partes: todos los suscriptores y otras entidades con las que el TSP tiene acuerdos u otras formas de relaciones que se establecen. Además, se pondrá a disposición esta información a los terceros que confían;
     ii. el TSP terminará la autorización de todos los subcontratistas para actuar en nombre de la TSP, y llevar a cabo cualquiera de las funciones relacionadas con el proceso de emisión de tokens de servicio de confianza;
     iii. el TSP transferirá a una entidad fiable, por un período razonable, las obligaciones para mantener toda la información necesaria para proporcionar evidencias de las operaciones de la TSP, a menos que pueda demostrarse que el TSP no ser titular de dicha información;
     iv. Las claves privadas del TSP incluyendo las copias de seguridad, serán destruidas o retiradas de su uso, de tal manera que no se pueden recuperar.
     v. ANF AC TSA realiza los pasos necesarios para revocar los certificados del TSU.
     vi. siempre que sea posible el TSP utilizará un sistema que permita la transferencia de prestación de servicios de los clientes existentes a otro TSP.
  c) El TSP tiene un acuerdo para cubrir los costos y cumplir con estos requisitos mínimos en caso de que el TSP se declara en quiebra, o por otras razones que le impidan ser capaz de cubrir los costos por sí misma, en la medida de lo posible dentro de las limitaciones de la legislación aplicable en materia de quiebra.
  d) El TSP mantendrá o transferirá a una entidad fiable su obligación de poner a disposición, su clave pública o sus tokens de servicio de confianza, a los terceros que confían durante un período razonable.

6.15. Conformidad

ANF AC TSA asegura el cumplimiento de la legislación aplicable en cada momento.

En concreto, esta Política está en conformidad con:

- Reglamento (UE) No 910/2014 (eIDAS), artículo 42.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- ETSI EN 319 421: *"Policy and Security Requirements for Trust Service Providers issuing Time-Stamps."*
- ETSI EN 319 422: *"Time-stamping protocol and time-stamp token profiles."*
- ETSI EN 319 401: *"Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers"*
- ETSI TS 119 312: *"Electronic Signatures and Infrastructures (ESI); Cryptographic Suites"*
- IETF RFC 3628: "*Policy Requirements for Time-Stamping Authorities (TSAs)"*
- IETF RFC 3161: *"Internet X.509 Public Key Infrastructure Time-stamp Protocol"*

La validación del cumplimiento de estas normas se lleva a cabo durante la evaluación de conformidad como se describe en el apartado 8 de la DPC de ANF AC.