Política de Autoridad de Sellado de Tiempo y Declaración de Prácticas

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

Teléfono: 902 902 172 (Llamadas desde España)

Internacional (+34) 933935 946

Fax: (+34) 933 031 611 Web: www.anf.es

Nivel de Seguridad

Público

Aviso Importante

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

Teléfono: 902 902 172 (Llamadas desde España) Internacional (+34) 933 935 946

Fax: (+34) 933 031 611. Web: www.anf.es

Control del documento

Control de cambios			
Fecha	Versión	Cambios	Autor
26/10/2004	1.0	Versión inicial	Florencio Díaz
01/05/2010	1.1	Revisión	Florencio Díaz
01/06/2012	1.2	Revisión	Florencio Díaz
02/09/2014	1.3	Revisión	Florencio Díaz
01/06/2016	1.4	Adaptación a eIDAS	Florencio Díaz
18/04/2017	1.5	Recomendación auditor eIDAS	Florencio Díaz

Información básica del documento	
Tipo	Política
Nombre del documento	Política de Autoridad de Sellado de Tiempo y Declaración de Prácticas
Versión	1.5
Autor	Florencio Díaz
Responsable de la auditoria del documento	Mari Carmen Mateo
Nombre del fichero	DPC ANF AC TSA
Fecha de creación	18 de abril de 2017
Estado	Aprobado
Fecha de aprobación	18 de abril de 2017
Aprobado por	Junta Rectora PKI ANF Autoridad de Certificación

Índice

Introducción

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 numero nacional 171.443 y NIF G-63287510.

ANF AC está ofreciendo servicios de confianza y soluciones técnicas relacionadas en UE y LATAM. Estos servicios garantizan la seguridad y comunicación electrónica verificada con instituciones públicas, así como con empresas en su actividad cotidiana.

El Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE contempla la posibilidad de erigirse como Prestador Cualificado de Servicios de Confianza (en adelante, eIDAS). En tal sentido, ANF AC ejecuta su actividad como Prestador Cualificado de Servicios de Confianza.

El presente documento tiene el objetivo de cumplir con los requisitos generales de la comunidad internacional para proporcionar la confianza en las transacciones electrónicas, incluyendo, entre otros, los requisitos aplicables a partir del Reglamento (UE) nº 910/2014.

Inspirado en la serie de normas ETSI EN 319 400, ANF AC ha dividido su documentación en tres partes:

- Declaración de Prácticas de Certificación ANF AC: describe las prácticas generales comunes para todos los servicios de confianza;
- Políticas y Prácticas de Certificación de la Autoridad de Sellado de Tiempo ANF AC: describe las partes específicas para la prestación del servicio de sellado de tiempo;
- Los perfiles técnicos se encuentran en documentos separados.

Con el fin de cumplir con estos requisitos, la información electrónica se ha de proteger, entre otras cosas, contra la manipulación y la pérdida. Es necesario ser capaz de evaluar la observación de los requisitos de cumplimiento en un entorno profesional, la integridad y la confidencialidad son a menudo los principales criterios.

Los sellos electrónicos de tiempo le permitan realizar esta prueba de integridad de una manera que es simple, jurídicamente segura, permanente, de bajo costo y, previa solicitud, en el anonimato.

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 se generó antes de la fecha que figura en el sello de tiempo. Definir los requisitos que se tienen que atender para cumplir este caso, son el objetivo principal del presente documento.

El sellado de tiempo está ganando un creciente interés en el sector empresarial y se está convirtiendo en un componente importante de la firma electrónica; esto se basa normalmente en el protocolo de sello de tiempo [IETF RFC 5816], que se perfila en ETSI EN 319 422. Estas normas establecen los requisitos mínimos de seguridad y calidad necesarios para garantizar la validación de la firma electrónica de confianza a largo plazo.

El servicio de sellado de tiempo de ANF AC TSA se ajusta a eIDAS, al marco legal de España y a ETSI EN 319 421 y ETSE EN 319 422.

1 Alcance

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. Estos sellos de tiempo se pueden utilizar en apoyo de las firmas electrónicas o para cualquier aplicación que requiera de probar que un dato existió antes de un tiempo determinado.

El presente 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 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.

ANF AC emite los tokens de sello de tiempo en conformidad con la norma ETSI EN 319 421 "Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".

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 y la DPC TSA, lo dispuesto en la DPC TSA deberá prevalecer. En caso de conflicto entre el documento original en inglés y la traducción española, prevalecerá el original en inglés.

2 Referencias

2.1 Referencias normativas

1. Reglamento (UE) No 910/2014 del Parlamento Europea y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.
2. Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
3. [LPDCP] Ley de Protección de Datos de Personas Físicas
4. [DPC] Declaración de Prácticas de Certificación de ANF AC
5. IETF RFC 3161 “Internet X.509 Public Key Infrastructure Time-stamp Protocol”
6. ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers”
7. ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps”
8. ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".

2.2 Referencias informativas

1. Recommendation ITU-R TF.460-6 (2002): "Standard-frequency and time-signal emissions".
2. IETF RFC 5905: “Network Time Protocol Version 4: Protocol and Algorithms Specification”
3. Términos y Condiciones para los Servicios de Sello de Tiempo. Este documento se puede descargar en www.anf.es
4. ISO/IEC 19790:2012: "Information technology -- Security techniques -- Security requirements for cryptographic modules".
5. ISO/IEC 15408 (secciones de la 1 a la 3): "Information technology – Security techniques -- Evaluation criteria for IT security".
6. FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Modules".

3 Definiciones y Abreviaturas

3.1 Definiciones

- **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.
- **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.
- **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.
- **Sello de tiempo**: Sello 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.
- **Servicio de sellado de tiempo**: Servicio de confianza para la emisión de sellos de tiempo.
- **Sistema TSA**: Conjunto de productos TI y procedimientos empleados para apoyar la prestación de servicios de sellado de tiempo.
- **Suscriptor**: Persona física o jurídica para la que se emite un sello de tiempo.
- **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 (Temps Atómico Internacional- TAI) y la hora solar derivado 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.

3.2 Abreviaturas

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)*

- **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

4 Conceptos Generales

4.1 Conceptos y requerimientos generales

Sigue los requerimientos establecidos en la DPC de ANF AC.

4.2 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 DPC TSA.

ANF AC TSA se adhiere a las normas y reglamentos establecidos en el apartado 2 del presente documento para mantener la fiabilidad de los servicios de sellado de tiempo para suscriptores y usuarios de confianza.

4.3 Partes del servicio de sellado de tiempo

4.3.1 Autoridad de sellado de tiempo (TSA)

El Prestador de Servicios de Confianza (TSP) que provee de servicios de sellado de tiempo al público, se denomina Autoridad de Sellado de Tiempo (TSA). La TSA tiene la responsabilidad general para la prestación de los servicios de sellado de tiempo señalados en la cláusula 4.2. La TSA tiene la responsabilidad del funcionamiento de una o más TSU's, que crean y firman en nombre de la TSA. La TSA responsable de la emisión de un sello de tiempo es identificable.

ANF AC TSA confirma, que la TSA es auditada 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 terceras entidades colaboradoras para apoyarse para la prestación de servicio de sellado de tiempo. Sin embargo, la TSA siempre mantiene la responsabilidad general (según la cláusula 6.5) y asegura que se cumplen los requisitos de actuación mencionados en el presente documento.

ANF AC TSA puede operar varias unidades de sellado de tiempo (TSU) identificables.

ANF AC TSA es un Prestador Cualificado de Servicios de Confianza como se describe en eIDAS, que emite sellos de tiempo.

ANF AC TSA está identificada en el certificado TSU utilizado para firmar TST.

Información de contacto:

ANF Autoridad de Certificación
Paseo de la Castellana, 79 – 28046 – Madrid (España)
Tfno: 902 902 172 (España) (+34) 933 935 946 (International)
Fax: (+34) 933 031 611 Web: www.anf.es

4.3.2 Subscriptor

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

4.3.3 Tercero que confían - TSA

Un tercero que confía es una persona física o jurídica que actúa confiando es un TST, emitido bajo la política de ANF AC TSA [ETSI ES 319 421]. Una parte que confía puede, o no, ser también un subscriptor.

4.4 Política de Sellado de Tiempo y Declaración de Prácticas TSA

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 TST's.

La Declaración de Prácticas de ANF AC TSA forma parte de la Declaración Prácticas de Confianza de ANF AC, especificada en ETSI EN 319 421, aplicable por ANF AC TSA como emisora de TST's.

5 Política del Sello Tiempo

5.1 General

ANF AC TSA emite los TST's, 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 TST's se emiten con una precisión del 1 segundo respecto al UTC o mejor.

5.2 Identificación

El identificador de la política de sello de tiempo especificado en el presente documento es el OID:

1.3.6.1.4.1.18332.15.1

{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) ANF Autoridad de Certificación (18332) TSA(15) CPS-PC-EU-Regulation 910/2014 (1)}

- Iso (1)
- Org (3)
- Dod (6)
- Internet (1)
- Private (4)
- Enterprise (1)
- ANF AC Autoridad de Certificación (18332)
- Autoridad de Sellado de Tiempo (15)
- Declaración de Prácticas de Certificación y Política de Sello de Tiempo en conformidad con el Reglamento (UE) 910/2014 (1)

Con la inclusión de este identificador de objeto (OID) al generar los sellos de tiempo, ANF AC TSA estipula conformidad con esta política de sello de tiempo.

5.3 Comunidad de usuarios y aplicabilidad

Esta política está dirigido 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.

Esta política puede ser utilizada por servicios públicos de sellado de tiempo o servicios de sellado de tiempo utilizados dentro de una comunidad cerrada.

6 Políticas y Prácticas

6.1 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. Los controles de seguridad que se definen en un marco de seguridad de los servicios de sellado de tiempo, son revisados cada tres meses con el fin de asegurar su eficacia.

Una explicación detallada respecto a este tema se describe en el concepto de seguridad:
"Análisis de las amenazas y medidas a adoptar" y "Evaluación de Riesgos".

6.2 Declaración de Prácticas de 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.

Además de respetar la norma ETSI TS 119 421, se han aplicado las siguientes medidas especificadas respectivamente en los siguientes servicios:

6.2.1 Formato de 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 2048 se emiten sellos de tiempo que acepten uno de los siguientes algoritmos de hash:

- SHA256
- SHA384
- SHA512

6.2.2 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.

6.2.3 Limitaciones del servicio

El servicio de sello de tiempo de ANF AC TSA sólo puede ser utilizado para transacciones legales cuyo valor, en el momento de su uso, no supere 500.000 euros en el caso individual, y un total de 5.000.000.- de euros por año natural.

6.2.4 Obligaciones de los suscriptores

Para información detallada consulte el apartado “Términos y Condiciones para los Servicios de Sello de Tiempo.

6.2.5 Obligaciones de las partes que confían

Para información detallada consulte el apartado “Términos y Condiciones para los Servicios de Sello de Tiempo.

6.2.6 Verificación del sello de tiempo

La verificación del sello de tiempo incluye las siguientes operaciones:

Operación I *Verificación del emisor del sello de tiempo*
El emisor es una Autoridad de Sellado de Tiempo que utiliza los certificados electrónicos adecuados para emitir el sello de tiempo. 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 sello de tiempo*
Un servicio OCSP 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 a través del servicio web de ANF AC TSA, que se ofrece de forma gratuita en: www.anf.es

6.2.7 Ley aplicable

Para información detallada consulte el apartado “Términos y condiciones para los Servicios de Sello de Tiempo”.

6.2.8 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%.

6.3 Términos y condiciones

Dentro del documento "Términos y Condiciones para los Servicios de Sello de Tiempo" se contiene información, por ejemplo, sobre la limitación del servicio, las obligaciones de los suscriptores, o limitaciones de responsabilidad. Además, se aplica la siguiente información:

6.3.1 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.

6.3.2 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.

6.4 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.

6.5 Obligaciones

6.5.1 Obligaciones de la TSA

Las obligaciones de la TSA con respecto a los suscriptores y terceros que confían están especificadas en este documento, y en la cláusula 9.5.1 de la DPC ANF AC.

6.5.2 Obligaciones de los suscriptores – TSA

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 verificar la firma del TST y garantizar que la clave privada utilizada para firmar el TST no ha sido revocada.
- El suscriptor está obligado a utilizar las funciones criptográficas seguras para las solicitudes de sellado de tiempo.
- 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.

6.5.3 Obligaciones de los terceros que confían – TSA

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 deben de verificar que el TST ha sido firmado con la clave correspondiente del certificado del TSU, y que la clave privada utilizada para firmar el TST no ha sido revocada.
- Los terceros que confían deben tomar las medidas necesarias para garantizar la validez del TST más allá del tiempo de vida de los certificados de ANF AC TSA.
- Deben de tener en cuenta cualquier limitación de uso de acuerdo con la Política indicada en el sello de tiempo.
- Deben tener en cuenta cualquier otra precaución prescrita en los contratos o en otros documentos.

6.6 Responsabilidad

Las disposiciones de responsabilidad están detalladas en las secciones 9.6, 9.7 y 9.8 de la DPC de ANF AC:

- Se aplican las disposiciones sobre responsabilidad definidas en la DPC ANF AC.
- La responsabilidad de ANF AC TSA con los suscriptores está estipulada en los contratos firmados con los suscriptores.
- ANF AC no se hace 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.
- ANF AC no asume ninguna responsabilidad por la pérdida del valor de la prueba de confirmación de validez debido a fuerza mayor.

7 Gestión y Operaciones TSA

7.1 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 subscriptor.

7.2 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 2.1 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 2016
   Paseo de la Castellana, 79 – 28046 - Madrid (España)
   Tfno: 902 902 172 (España) +34 933 935 946 (International)
   Fax: +34 933 031 611 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.

7.3 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.

7.4 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.

7.5 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.

7.6 Controles criptográficos

7.6.1 Generación de la clave del TSU

En los controles del personal se aplican las restricciones descritas en las cláusulas 5.2 y 5.5 de la DPC de ANF AC. La activación del TSU se realiza mediante control dual.

El TSU usa un par de claves RSA de longitud de 2048-bit. Este par de claves se utiliza solo para firmar TST's.

a) La generación de la clave de firma de la TSU (s) se lleva a cabo en un entorno físicamente protegido (según la cláusula 7.8 de este documento) por personal en puestos de confianza (según la cláusula 7.3 de este documento), bajo al menos el control de dos personas de confianza.
b) La generación de la clave de firma de la TSU (s) se lleva a cabo dentro de un módulo criptográfico, que es conforme a FIPS PUB 140-2, el nivel 3, o ISO 15408 Common Criteria EAL 4+, no siendo esta importada a otros modulos criptográficos.
c) El algoritmo de generación de claves TSU, el algoritmo de firma, la longitud de clave usada para firmar los sellos de tiempo, es reconocido por la autoridad nacional de control, y es reconocido por el estado actual de la técnica como adecuado para la firma de sello de tiempo que realiza una TSA, como se especifica en ETSI TS 119 312.

7.6.2 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+.

No se realizan copias de la clave privada del TSU.

7.6.3 Certificado de clave pública

El TSA garantiza la integridad y la autenticidad de la verificación de la firma TSU (clave pública) como a continuación se describe.

a) La verificación de la firma del TSU (claves públicas) están a disposición de los terceros que confían en un certificado de clave pública. Los certificados se publican en: www.anf.es
b) La 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).
c) Solo se emite un certificado de TSU con su clave privada específica.
d) Los certificados TSU no se renuevan.
e) La información sobre el estado de los certificados de TSU se renueva periódicamente y están disponibles los servicios OCSP y CRL, con los enlaces indicados en los certificados.

7.6.4 Renovación de clave TSU's

El tiempo de vida del certificado de TSU, se corresponde con el período de tiempo del algoritmo elegido y la longitud de la clave (véase la cláusula 7.6.1c).

Las claves del TSU tendrán la vida útil máxima de 5 años. Un certificado puede ser emitido por todo el tiempo de vida esperado. La duración de la clase del TSU está limitada por:

- El tiempo de validez del certificado de entidad emisora raíz.
- Una vez al año o cuando se producen cambios significativos, la persona que posea la función "Supervisor de Criptografía" verifica todos los algoritmos criptográficos utilizados en la TSA comprobando que cada algoritmo es reconocido como adecuado, tal y como se indica en la cláusula 7.6.1c).
- Si un algoritmo entra en situación de riesgo, éste deja de ser adecuado; el Responsable de Seguridad encargará a la TSA cesar en el uso de las claves afectadas y cargar nuevas claves.

7.6.5 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 módulo criptográfico del TSU, se borra al retirarse el dispositivo de una forma que prácticamente imposibilita su recuperación.

7.6.6 Fin del ciclo de vida de la Clave del TSU

Después de la expiración de las claves privadas, éstas son almacenadas en el módulo criptográfico y se destruyen de una manera tal que las mismas no se puedan recuperar.

El Supervisor de Criptografía define la validez de la clave de acuerdo con lo expresado en la cláusula 7.6.1c).

7.6.7 Autoridad de Certificación Raíz

ANF AC TSA opera con una infraestructura de clave pública propia, que consiste en una "Autoridad de Certificación Raíz" y servicio de respuesta OCSP.

La CA Raíz opera sin conexión (fuera de línea); todos los aspectos relacionados con la seguridad física y técnica están detallados en la Declaración de Prácticas de Certificación de ANF AC, publicada en repositorios públicos y de libre acceso en: www.anf.es

7.7 Sellado de tiempo

7.7.1 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 subscripción. 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 SHA-256.

Las claves del TSU son claves RSA 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 puede probar la existencia de un TST en concreto para comprobar su confianza. ANF AC TSA podrá pedir al tercero que confía cubrir los costos de tal servicio.

El TSU no emite ningún TST cuando se ha alcanzado el fin de la validez de la clave privada TSU.

7.7.2 Sincronización de la hora con UTC

ANF AC TS 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

7.8 La 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 autorizado 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.

7.9 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 protege 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

7.10 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, lógico y físico (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 necesita 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.

7.11 Administración de incidencias

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 accesos a los sistemas informáticos, sistemas de usuario de la misma, y las solicitudes de servicio son monitoreados. En particular:
Las actividades de seguimiento toman en cuenta la sensibilidad de cualquier información recogida y analizada.

a) 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.
b) Los sistemas IT del TSP controla los siguientes eventos: Puesta en marcha y parada de las funciones de registro; disponibilidad y utilización de los servicios necesarios con la red TSP.
c) 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.
d) 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.
e) La autoridad nacional de control es informada dentro de las 24 h siguientes del descubrimiento de un fallo de seguridad crítico.
f) Los registros de auditoría son monitoreados y revisados con regularidad para identificar evidencia de actividad maliciosa.
g) 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.
h) 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.

7.12 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).

7.13 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 dañar. 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 7.7.1 de este documento.

7.14 Finalización de TSA y plan de terminación

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 retirados 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.

7.15 Conformidad

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

En concreto, esta Política está en conformidad con:

a) Regulación (EU) N°910/2014
b) Ley 59/2003, del 19 de diciembre, de firma electrónica.
c) ETSI TS 119 312
d) ETSI EN 319 401
e) ETSI EN 319 421
f) ETSI EN 319 422
g) IETF (RFC 3161)

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.