

ANF AC Autoridad de Sellado de Tiempo

Declaración de Prácticas de Certificación (DPC)

Certificate Practice Statement (DPC)



Fecha : 1 de septiembre de 2004

Versión: 1

OID : 1.3.6.1.4.1.18332.5.1

Este documento es propiedad de ANF Autoridad de Certificación.

Se autoriza su reproducción y difusión siempre que se reseñe:

- Copyright © ANF Autoridad de Certificación –
- Depósito Legal B.44.547-2005

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 1 de 57

Declaración de Prácticas de Certificación de ANF AC Autoridad de Sellado de Tiempo



Sumario

1. Introducción.

- 1.1 Presentación.
- 1.2 Identificación.
- 1.3 Datos de contacto.
 - 1.3.1 Especificación del ente organizador.
 - 1.3.2 Persona de contacto.
 - 1.3.3 Determinación de la adecuación de la DPC con las restantes DPC y Políticas de ANF AC.
- 1.4 Publicación.
- 1.5 Comunidad, ámbito de aplicación y conceptos generales.
 - 1.5.1 Autoridad de Certificación.
 - 1.5.2 Servicios de Sellos de Tiempo.
 - 1.5.3 Comunidad.
 - 1.5.4 Ámbito de aplicación.
- 1.6 Derechos de Propiedad Intelectual.

2. Información General.

3. Definiciones y abreviaturas.

4. Conceptos Generales.

- 4.1 Servicios de Sellado de Tiempo TSS.
- 4.2 Autoridad de Sellado de Tiempo.
- 4.3 Usuarios
- 4.4 Clientes
- 4.5 Políticas de Sellado de Tiempo y Declaración de Prácticas de la TSA.
 - 4.5.1 El propósito.
 - 4.5.2 Documentación.

5. Políticas de los Sellos de Tiempo.

- 5.1 Características generales.
- 5.2 Identificador de las Políticas de Sellos Digitales de Tiempo.
- 5.3 Conformidad

6. Obligaciones y garantías.

- 6.1 Obligaciones de ANF AC TSA.
 - 6.1.1 Generales.
 - 6.1.2 Obligaciones de la TSA frente a los usuarios.
 - 6.1.3 Obligaciones de la TSA frente a terceras partes.
- 6.2 Obligaciones del Usuario.
- 6.3 Obligaciones de las Terceras Partes.
- 6.4 Garantías financieras.

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 2 de 57

7. Servicios de la TSA.

- 7.1 Manifiesto y prácticas de la TSA.
 - 7.1.1 Prácticas de la TSA.
 - 7.1.2 Manifiesto de la TSA.
- 7.2 Ciclo de vida de las claves.
 - 7.2.1 Generación de la Clave de la TSA.
 - 7.2.2 Protección de la clave privada TSU.
 - 7.2.3 Difusión de la Clave Pública TSA.
 - 7.2.4 Regeneración de la Clave.
 - 7.2.5 Destrucción de la Clave Privada.
 - 7.2.6 Ciclo de vida del módulo criptográfico que firma el TST.
 - 7.2.7 Copia de las Claves.
 - 7.2.8 Periodo de validez.
 - 7.2.9 Cambio de los certificados de la TSA.
- 7.3 Sellos de Tiempo.
 - 7.3.1 Time-Stamp Token
 - 7.3.2 Sincronización del reloj con UTC
 - 7.3.3 Desincronización del Reloj
 - 7.3.4 Coherencia del sistema
- 7.4 Dirección de la TSA y funcionamiento.
- 7.5 Organización.
- 7.6 Dispositivos de obtención de TST.
- 7.7 Dispositivos de verificación de TST.

8. Oficina de Atención al Cliente.

- 8.1 Cometido de la Oficina.
- 8.2 Procedimiento de Consulta.
- 8.3 Procedimiento de Reclamación.

9. Interpretación y Ejecución.

- 9.1 Ley aplicable.
- 9.2 Conflicto de normas
- 9.3 Divisibilidad, supervivencia y notificaciones.
- 9.4 Subrogación.
- 9.5 Administración de la DPC. y Políticas.
- 9.6 Procedimientos de resolución de disputas.

10. Publicación y repositorios.

- 10.1 Publicación de información de la CA.
- 10.2 Frecuencia de publicación.
- 10.3 Control de acceso .
- 10.4 Procedimiento de especificación de cambios.
- 10.5 Procedimiento de Publicación y Notificación.
- 10.6 Procedimientos de aprobación de la DPC.
- 10.7 Repositorio de encadenamientos

11. Información de referencia.

- 11.1 Normas de referencia.
- 11.2 Referencias informativas.

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 3 de 57

1. Introducción.

1.1 Presentación.

ANF 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 CIF G-63287510.

Este documento esta vinculado a la *DPC* de *ANF AC* como entidad prestadora de servicios de certificación. Esta Declaración de Prácticas de Certificación (*DPC*) de ANF Autoridad de Certificación (*ANF AC*) en su Servicio Digital de Sellado de Tiempo, constituye una declaración de los criterios que este prestador de servicios de certificación se compromete a seguir. La denominación completa de este documento es *Declaración de Prácticas de Certificación de ANF AC Autoridad de Sellado de Tiempo (en adelante DPC)*. El término *DPC* se corresponde con el concepto inglés de Certification Practice Statement (*CPS*), y el *TSA* con el concepto inglés de Time-Stamping Authority.

Este documento está dirigido a todos los usuarios de los servicios de *ANF AC*, entidades con las que se relaciona y, en especial, a los terceros de buena fe, personas que reciben ficheros electrónicos que incluyen sellos digitales de tiempo firmados por *ANF AC*. Caso de que el lector no conozca los conceptos básicos de un servicio de estas características, *ANF AC* pone a su disposición un servicio gratuito de Atención al Cliente”, y recomienda solicitar esta asistencia antes de continuar con la lectura de este documento.

Esta *DPC* se ha inspirado en la norma IETF RFC 3628 “Policy Requirements for Time-Stamping Authorities” propuesta como guía de asistencia en la redacción de este tipo de documentos. La estructura y contenidos de este documento es compatible con ETSI TS 102 023 V 1.2.1 (2002-06) [TS 102023].

1.2 Identificación.

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 4 de 57

Nombre del documento	Declaración de Prácticas de Certificación de ANF AC Autoridad de Sellado de Tiempo "DPC TSA de ANF AC"
Versión	1
Autor	<i>Florencio Díaz Vilches</i>
Referencia del documento / OID	1.3.6.1.4.1.18332.5.1
Fecha de emisión	1 de septiembre de 2004
Fecha de expiración	No es aplicable
Localización URL	https://www.anf.es/AC/documentos/

ANF Autoridad de Certificación tiene asignado el código privado de empresa (SMI Network Management Private Enterprise Codes) **18332** por la organización internacional IANA -Internet Assigned Numbers Authority-, bajo la rama iso.org.dod.internet.private.enterprise (1.3.6.1.4.1 -IANA –Registered Private Enterprise-). Esto puede ser consultado en la URL:

<http://www.iana.org/assignments/enterprise-numbers>

El prefijo del OID de esta *DPC* es 1.3.6.1.4.1.18332.5 el sufijo determina la versión de la *DPC* a la que hace referencia el OID. En el caso de este documento versión 1, el OID que lo identifica es 1.3.6.1.4.1.18332.5.1

El protocolo a seguir en el mantenimiento de este OID queda determinado en el apartado "*Procedimiento de Especificación de Cambios*" de este documento.

1.3 Datos de contacto.

1.3.1 Especificación del ente organizador.

Esta *DPC* es propiedad de ANF AC:

ANF Autoridad de Certificación
Gran Vía de les Corts Catalanes, 996
08018 - Barcelona - España
Tfno.- 00 34 932 661 614

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 5 de 57

FAX.- 00 34 933 131 614

Dirección electrónica: ac@anf.es

Dirección web: <https://www.anf.es/>

Esta *DPC* esta administrada por la Junta Rectora de la PKI de *ANF AC*:

JRPKI de la ANF Autoridad de Certificación

Gran Vía de les Corts Catalanes, 996

08018 - Barcelona - España

Tfno.- 00 34 932 661 614

FAX.- 00 34 933 131 614

Dirección electrónica: juntapki@anf.es

1.3.2 Persona de contacto

Para cualquier información relacionada con esta *DPC*:

Persona de contacto: F. Díaz

e-mail: fdiaz@anf.es

1.3.3 Determinación de la adecuación de la *DPC* con las restantes *DPC* y Políticas de *ANF AC*.

Las modificaciones propuestas o las nuevas aportaciones a incluir sobre esta *DPC*, deben ser contrastadas, previa a su aprobación, con las restantes *DPC* y Políticas que *ANF AC* tenga publicadas, a fin de asegurar que soportan estos cambios.

El procedimiento a seguir queda especificado en el apartado “*Seguridad de la adecuación de la DPC a las Políticas asociadas*”, de la *DPC* de *ANF AC*.

1.4 Publicación.

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 6 de 57

Este documento, y restantes asociados puede obtenerse libremente en la URL <https://www.anf.es/AC/documentos/>, o en las oficinas centrales de ANF AC.

La entidad con atribuciones para definir y aprobar sobre cualquier propuesta de modificación de esta *DPC TSA* de ANF AC es la Junta Rectora de la PKI.

El mantenimiento y el control de la correcta aplicación de lo establecido en esta *DPC*, recae sobre la Dirección Ejecutiva de ANF AC.

1.5 Comunidad, ámbito de aplicación y conceptos generales.

1.5.1 Autoridad de Certificación de Sellos Digitales de Tiempo

ANF Autoridad de Certificación es la entidad emisora de Sellos digitales de Tiempo de esta infraestructura de clave pública –PKI-. Time-Stamping Authority (*TSA*),

Su función es la emisión de los sellos digitales de tiempo -*TST*- solicitados por los usuarios de este sistema. Así como la administración y control de la infraestructura de todos los servicios de sellado de tiempo –*TSS*- que se describen en esta *DPC*.

ANF AC en su calidad de *TSA* tiene bajo su responsabilidad la creación y firma de los “time-stamp token” *TST* que emite, siendo posible identificar de forma unívoca cada uno de los sellos emitidos por una unidad de sellado de tiempo –*TSU*-, el cual utiliza un certificado sometido a una Política de Certificación específica.

ANF AC en su calidad de *TSA* asume la responsabilidad global de los servicios de Sellado Digital de Tiempo. Los Sistemas de Certificación, así como las claves privadas utilizadas para la creación de los Sellos de Digitales de Tiempo pertenecen a *ANF AC* y están directamente custodiados por ella.

ANF AC cuenta con diversas unidades desde las que se presta Servicios de Sellos de Tiempo -*TSS*-. Cada unidad –*TSU*- tiene una clave diferente y cuenta con un certificado electrónico exclusivo.

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 7 de 57

ANF AC en su calidad de TSA es un prestador de servicios de certificación que dispone de una amplia gama de servicios, , tal y como queda definido en “EU Directive on Electronic Signaturas (9) - (see article 2(11)).

1.5.2 Servicios de Sellos de Tiempo.

Los servicios de sellado digital de tiempo están basados en la utilización de los siguientes componentes:

- Provisión de Sellos de Tiempo: Componente del Sistema de TSA que genera los Sellos Digitales de Tiempo.
- Time-stamping management: Componente del Sistema de TSA encargado de administrar y supervisar el timbrado de Sellos Digitales de Tiempo. Entre otras funciones asume el control de la procedencia de la hora utilizada para emitir el time-stamping, el correcto funcionamiento de los servicios de acreditación por encadenamiento, el estado de vigencia del certificado de la TSA, y el estado de vigencia del certificado del signatario que solicita el Sello Digital de Tiempo, o la disponibilidad del servicio para clientes autorizados.

1.5.3 Comunidad

1.5.3.1 Usuarios

El servicio de Sellado Digital de Tiempo es prestado a usuarios titulares de certificados digitales vigentes y que han sido emitidos por ANF AC.

1.5.3.2 Clientes

El servicio de Sellado Digital de Tiempo es prestado a personas físicas o jurídicas, que habiendo suscrito un acuerdo específico con ANF Autoridad de Certificación, están autorizados para utilizar el servicio en modalidad: TST Servidor o TST Auditor (*modalidades descritas en este documento*).

1.5.3.3 Terceros de confianza

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 8 de 57

De forma general, son todas aquellas personas físicas o jurídicas que de forma voluntaria confían en los Sellos Digitales de Tiempo –TST- que han sido emitidos por ANF TSA AC.

1.5.4 **Ámbito de aplicación.**

Este documento, la *DPC* a la que se vincula, y las Políticas publicadas por ANF AC determinan el uso apropiado que debe darse a los sellos digitales de tiempo.

1.6 **Derechos de Propiedad Intelectual.**

ANF AC es titular en exclusiva de todos los derechos de propiedad intelectual que puedan derivarse del sistema de certificación que describe y regula este documento.

ANF AC posee todos los derechos de propiedad intelectual sobre esta *DPC*, sus ANEXOS, las Políticas de Certificación y en general el modelo de sistema TSA.

Se autoriza su reproducción y difusión siempre que se reseñe:

-Copyright © ANF Autoridad de Certificación-

Los sellos digitales de tiempo y las actas de encadenamiento son propiedad intelectual de ANF AC. Se concede un permiso no exclusivo y no retribuido de reproducción y distribución de los sellos digitales de tiempo a las partes, siempre y cuando se respete la integridad de los mismos y no se publiquen en un depósito público sin permiso de ANF AC.

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 9 de 57

2. Información General.

Este documento detalla los requisitos que atienden los servicios prestados por esta *TSA* para la emisión de sellos digitales de tiempo. Estos servicios son empleados como apoyo en la generación de firmas electrónicas reconocidas, en línea con la Directiva Europea (1999/93/CE (9)) y de acuerdo con la vigente Ley de Firma Electrónica española, y para atender cualquier otra necesidad que precise demostrar que un dato existió antes de un momento particular.

Los servicios de certificación de *ANF TSA AC* se basan en el empleo del procedimiento de clave pública criptográfica y fuente de tiempo fiable.

Este documento no especifica el protocolo empleado en el timbrado de tiempo *TSP*, el cual está definido en el RFC 3161, conforme al perfil TS 101 861.

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 10 de 57

3. Definiciones y abreviaturas.

A efectos de lo dispuesto en el presente documento, y únicamente cuando los términos comiencen con letra mayúscula y estén en cursiva, se entenderá por:

- *ANF AC* : Es ANF Autoridad de Certificación, entidad raíz y única entidad prestadora de servicios de certificación de esta infraestructura de clave pública.
- *ANF TSA AC* : Corresponde al término utilizado por *ANF AC*, en la prestación de su servicio de sellado de tiempo, como Autoridad de Sellado de Tiempo.
- *ARR* : Es Autoridad de Registro Reconocida, ente colaborador de *ANF AC* en el proceso de solicitud e identificación de los usuarios.
- *Autoridades Intermedias*: Son *PSC Subordinados* que bajo la jerarquía del certificado raíz -ANF Root CA- emiten certificados a usuarios finales.
- *CEN* : Comité Européen de Normalisation
- *Certificado* : Es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad. (*LFE 59/2003, Tit. II Cap. I Art. 6.1*)
- *CP* : Es la contracción del vocablo inglés “Certificate Policy” – en español Política de Certificación - . La Política de Certificación define los requerimientos específicos que deben de ser atendidos para la emisión y uso de un determinado certificado. Cada certificado de *ANF AC* se somete a una *CP* determinada.
- *CWA* : CEN Workshop Agreement
- *Datos de Creación de Firma*: En la *PKI* de *ANF AC* es la clave criptográfica asimétrica privada que el signatario utiliza para crear firmas electrónicas.
- *Datos de Verificación de Firma*: En la *PKI* de *ANF AC* es la clave criptográfica asimétrica pública que se utilizan para verificar las firmas electrónicas.
- *Dispositivo homologado de ANF AC*: Con el fin de garantizar unas garantías homogéneas de seguridad técnica y jurídica, *ANF AC* pone a disposición de sus usuarios y entidades colaboradoras una serie de dispositivos sobre los que ha efectuado las comprobaciones necesarias de calidad. Estos dispositivos gozan de la calificación de homologados y pueden ser empleados en la *PKI* de *ANF AC*.
- *Dispositivo Seguro de Creación de Firma*: Es el dispositivo de creación de firma electrónica que cumple los requerimientos establecidos en la Ley de Firma Electrónica

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 11 de 57

(LFE 59/2003, Tit. IV, Cap. I, Art. 24.3). Los dispositivos homologados por ANF AC cumplen estas exigencias técnicas.

- **Documento electrónico:** Es un conjunto de registros lógicos almacenado en un soporte que permite ser leído por equipos informáticos.
- **DPC** : Declaración de Prácticas de Certificación, en inglés - Certification Practice Statement (CPS)-. Define los procedimientos seguidos por ANF AC en la prestación de sus servicios de certificación, la DPC y su addenda, definen la PKI de ANF AC.
- **Función resumen:** También llamada función hash, es la aplicación de un algoritmo matemático a un documento electrónico, da como resultado un Hash vinculado unívocamente al documento electrónico. Los algoritmos más conocidos son MD5, SHA-1 y SHA-2, el primero de 1.991 y con una longitud de 128 bits, ya esta catalogado como “no seguro”.
- **Hash** : Es un resultado de tamaño fijo que se obtiene tras aplicar una función hash a un documento electrónico. Su propiedad es básicamente que un mismo documento da siempre como resultado el mismo Hash, y documentos distintos dan como resultado Hash diferentes. Sobre esta característica se fundamenta el atributo de Integridad de la Firma Electrónica. También es conocido el Hash por el nombre de “huella digital”.
- **Hashing** : Es la aplicación de una función resumen, a un documento electrónico.
- **JRPKI** : Es la Junta Rectora de la PKI, encargada de supervisar y asesorar a ANF AC.
- **LFE** : Ley 59/2003 , de 19 de diciembre, de firma electrónica. El presente documento se elabora siguiendo lo establecido en esta Ley (LFE 59/2003 Tit. III, Cap. I Art. 19).
- **LOPD** : Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. La Prestación de Servicios de Certificación esta sometida a lo regulado por la citada Ley Orgánica (LFE 59/2003 Tit. III, Cap. I Art. 17).
- **LSSI** : LEY 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de comercio electrónico.
- **OID** : Es la contracción del vocablo inglés “Object Identifier Digital” – en español Identificador Digital de Objetos-. Es un valor de naturaleza jerárquica, siempre formador por enteros no negativos separados por un punto. En esta sistema de certificación son asignados a objetos registrados, y tiene la propiedad de ser únicos entre el resto de OID.

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 12 de 57

- **PKI** : Es la contracción del vocablo en inglés “Public Key Infrastructure” –en español Infraestructura de Clave Pública-. La PKI es el conjunto de entidades, procedimientos, dispositivos ...etc., que conforman un sistema de certificación.
- **PSC** : Prestador de Servicios de Certificación, es la persona física o jurídica que en el ámbito de la legislación en materia de firma electrónica, expide los certificados electrónicos y presta servicios relacionados con la Firma Electrónica. La actual Ley de Firma Electrónica diferencia entre prestadores de servicios de certificación que emiten certificados reconocidos, respecto a los que no los expiden con esta calificación. ANF AC en el presente documento es el PSC, y respecto al marco legal, considerado como entidad emisora de certificados reconocidos.
- **PSC Subordinados**: Son Autoridades Intermedias que bajo la jerarquía del certificado raíz -ANF Root CA- emiten certificados a usuarios finales.
- **Reglamento LOPD** : Reglamento de Medidas de Seguridad de Ficheros que contienen datos de Carácter Personal (BOE 25 de junio de 1999), tal y como consta en la LFE 59/2003 Tit. III, Cap. I Art. 19.3, el presente documento tiene consideración de documento de seguridad a efectos del citado Reglamento.
- **RSA** : Acrónimo de - “Rivest, Shamir y Adleman”. Inventores del criptosistema de clave pública que permite la firma electrónica y el cifrado (1977). Es el criptosistema de clave pública que permite la creación de una firma digital.
- **SHA-1** : “Secure Hash Algorithm” (1994). Este algoritmo de resumen esta en situación de RIESGO. Genera un resumen de 160 bits. Hasta el presente es el algoritmo utilizado por la practica totalidad de prestadores de servicios de certificación, se emplea en “funciones resumen” (hash) que tienen como objetivo dotar de Integridad a los documentos electrónicos durante el proceso de firma.
- **SHA-2** : En el sistema de certificación de ANF AC, este algoritmo esta llamado a sustituir al SHA-1 en aquellos procesos en los que aun se utiliza. Internacionalmente SHA-2 esta catalogado como seguro.
- **SSL** : Contracción del vocablo inglés “Secure Socket Layer”. Es el sistema, de uso común, para garantizar la privacidad de las comunicaciones y garantizar la identidad cierta del servidor al que se conecta.
- **TimeStamping**: Sellado Digital de Tiempo. ANF AC dispone de un servicio de fechado electrónico. Este servicio esta sometido a su propia DPC bajo la denominación de ANF TSA CA
- **TSA**: Contracción del vocablo inglés “Time-Stamping Authority”. Correspondiente al término Autoridad de Sellado de Tiempo, ANF TSA AC administra TSS.

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 13 de 57

- **TSS:** Contracción del vocablo inglés “time-stamp service”. Corresponde al término servicio de sellado de tiempo, que emite *TST*.
- **TST:** Contracción del vocablo inglés “time-stamp token”. Corresponde al sello digital de tiempo emitido por un servicio de sellado de tiempo desde un *TSU*.
- **TSU:** Contracción del vocablo inglés “time-stamp unit”. Corresponde a una Unidad específica de sellado de tiempo, perteneciente a los *TSS* de la *TSA*. Es la unidad desde la que se crean y firman en nombre de la *TSA* los sellos digitales de tiempo.
- **UTC:** Contracción del vocablo inglés “Universal Co-ordinated Time” (anteriormente GMT). Corresponde al término “tiempo universal coordinado” y es el tiempo en el que se basó la emisión del “time-stamp token” *TST*, definido en la Recomendación de ITU-R TF.460-5 [TF.460-5]

Además de las definiciones reseñadas y de las expresadas en la legislación vigente, en la redacción de este documento se emplean:

Glosario de términos.

Tercera parte	Destinatario del Sello Digital de Tiempo que confía en él.
Usuario	Entidad que requiere los servicios de <i>TSA</i> de <i>ANF AC</i> , y que ha aceptado los términos de emisión de los sellos digitales de tiempo.
time-stamp token	Es la impresión digital del sello de tiempo que vincula unos datos a un tiempo particular, estableciendo la evidencia que los datos han existido antes de ese tiempo.
Secuencia ASN	Es la secuencia en la que se incluyen los siguientes valores: hash anterior, hash actual y hash saliente en el servicio de encadenamientos del <i>TSU</i> .
TST info	Son los atributos no firmados del <i>TST</i> , conforme a la recomendación RFC 3161 <i>TST info</i> .
DPC TSA AC	Es la declaración de prácticas de certificación de los servicios de <i>TSA</i> , en la que se describen los sistemas utilizados por <i>ANF AC</i> .

Abreviaturas y acrónimos.

CEN	Contracción del vocablo inglés “Comité Européen de Normalisation”.
------------	--

DPC TSA de ANF AC	Ref. <i>DPC_TSA_ANF_AC_v1.pdf</i>	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 14 de 57

CRL	Contracción del vocablo inglés "Certificate Revocation List" . Lista de Revocación de Certificados suspendidos o revocados, en ella no constan los caducados.
CWA	Contracción del vocablo inglés "Cen Workshop Agreements."
ETSI	Contracción del vocablo inglés "European Telecommunications Standards Institute", Instituto Europeo de Normas de Telecomunicaciones.
FIPS	Normas de seguridad que publica el National Bureau of Standards (NBS). Las normas FIPS (Federal Information Processing Standards) son normas a aplicar en todos los Estados Federales y e1 Departamento de Defensa (DOD -USAF, ARMY y NAVY-) que publica normas en el terreno militar.
HTTP	Protocolo de transferencia de hipertexto "Hypertext Transfer Protocol"
ITSEC	"Information Technology Security Evaluation Criteria".
ITU	"International Telecommunication Union". Unión Internacional de Telecomunicaciones.
OCSP	Contracción del vocablo inglés "Online Certificate Status Protocol" – Protocolo informático que permite determinar la vigencia de un certificado electrónico.
RFC	Contracción del vocablo inglés "Request For Comments".
URL	Localizador de recursos uniforme "Uniform Resource Locator"
WWW	Contracción del vocablo inglés "Word Wide Web".

4. Conceptos Generales.

4.1 Servicio de Sellado de Tiempo -TSS-

El Servicio de Sellado de Tiempo –TSS- emite sellos digitales de tiempo –TST-, mediante los cuales se puede vincular fehacientemente un hecho con la escala universal de tiempo (UTC). El hecho fundamental que se vincula es la existencia de un objeto digital y su reconocimiento por parte de la Autoridad de Certificación en un determinado instante de tiempo.

La infraestructura de ANF AC para generar y emitir sellos digitales de tiempo –TST-, consiste en dos componentes básicos:

- Equipo técnico que genera los TST.
- Sistema logístico que supervisa y dirige la emisión de los TST.

El sistema logístico asegura entre otras cuestiones el acceso a una fuente fiable de tiempo UTC y es responsable de una dirección apropiada de los componentes que constituyen el equipo técnico.

4.2 Autoridad de Sellado de Tiempo.

ANF AC es la Autoridad de Sellado de Tiempo. Es el prestador de servicios de certificación que emite los “time-stamp tokens” -TST-, es la entidad de confianza de las partes respecto a los servicios de sellado digital de tiempo, es decir, los usuarios o los clientes y los terceros de confianza.

ANF AC asume la responsabilidad plena de los Servicios de Sellado de Tiempo -TSS-.

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 16 de 57

4.3 Usuarios.

Son suscriptores de certificados electrónicos emitidos por ANF AC, que requieren los servicios de TSA de ANF AC, y que han aceptado los términos de emisión de los sellos digitales de tiempo.

4.4 Clientes.

Son personas físicas o jurídicas, que en el marco de una relación contractual con ANF Autoridad de Certificación, requieren los servicios de TSA de ANF AC, y han aceptado los términos de emisión de los sellos digitales de tiempo.

4.5 Política de Sellado de Tiempo y Declaración de Practicas de la TSA.

La Política y la Declaración de Prácticas de Certificación regulan el funcionamiento de ANF AC y los servicios de no-repudio asociados.

Esta TSA emite “time-stamp tokens” –TST- de acuerdo con los requerimientos, obligaciones y limitaciones establecidos en los referidos documentos.

4.5.1 El propósito.

De forma general cabe citar que la Política de Sellos de Tiempo declara “lo que será adherido”, mientras que la Declaración de Prácticas de Certificación declara “como se adhiere”, es decir, que procesos realiza para generar y emitir los “time-stamp tokens” –TST-, y como se mantiene la exactitud del reloj de tiempo.

Esta información está disponible al público de forma gratuita. La difusión de este documento está limitada con las restricciones indicadas en el apartado “*Derechos de Propiedad Intelectual*”.

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 17 de 57

4.5.2 Documentación.

Este documento describe solo las reglas generales para emitir y generar sellos digitales de tiempo. La descripción detallada del sistema se describe en documentos adicionales, parte de ellos solo son accesibles a personal autorizado.

La relación de documentos que emplea la organización se detalla en la Tabla 1.

Tabla 1

Nº	Nombre del Documento	Estado	Localización
1	Declaración de Prácticas de Certificación	Público	https://www.anf.es/AC/documentos/
2	Políticas vinculadas	Públicos	https://www.anf.es/AC/documentos/
3	Código ético de protección de datos personales	Públicos	https://www.anf.es/AC/documentos/
4	Seguridad Administrativa	Públicos	https://www.anf.es/AC/documentos/
5	Normas y criterios de auditoria de los Servicios de Certificación	Públicos	https://www.anf.es/AC/documentos/
6	Procedimientos de utilización de los componentes criptográficos.	Públicos	https://www.anf.es/AC/documentos/
7	Documentación técnica de la Base de Datos	No-público	Acceso restringido a personal autorizado
8	Procedimiento de la TSA para el archivo y destrucción de claves.	No-público	Acceso restringido a personal autorizado
9	Documentación técnica del sistema de detección de intrusos.	No-público	Acceso restringido a personal autorizado
10	Documentación técnica del sistema de supervisión permanente de servidores.	No-público	Acceso restringido a personal autorizado
11	Documentación técnica del hardware Servidores.	No-público	Acceso restringido a personal autorizado
12	Documentación técnica del diseño de los TSU	No-público	Acceso restringido a personal autorizado
13	Documentación procedimientos TSS	No-público	Acceso restringido a personal autorizado
14	Documentación técnica del diseño del servicio OCSP	No-público	Acceso restringido a personal autorizado
15	Documentación técnica de los procedimientos de copia y restauración.	No-público	Acceso restringido a personal autorizado
16	Documentación técnica del diseño de los dispositivos ARR.	No-público	Acceso restringido a personal autorizado

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 18 de 57

17	Documentación técnica del diseño de los servicios de notariado y factura delegada.	No-público	Acceso restringido a personal autorizado
18	Documentación técnica del diseño de los dispositivos entidad final.	No-público	Acceso restringido a personal autorizado
19	Documentación técnica del sistema de emisión certificados.	No-público	Acceso restringido a personal autorizado
20	Documentación técnica de los protocolos de comunicaciones.	No-público	Acceso restringido a personal autorizado
21	Normas en la asignación de puertos y reglas de filtrado.	No-público	Acceso restringido a personal autorizado
22	Plan de Contingencias y Seguridad de la Información.	No-público	Acceso restringido a personal autorizado
23	Procedimiento y normas de trabajo del departamento de criptoanálisis.	No-público	Acceso restringido a personal autorizado

5. Política de los Sellos de Tiempo.

5.1 Características generales.

Los datos incorporados en los Sellos Digitales de Tiempo se encuentran firmados electrónicamente. Para la creación de la firma, se utiliza un certificado electrónico emitido por ANF AC para ese único fin, el cual esta sometido a una Política de Certificación específica.

Los sellos digitales de tiempo –TST- se emiten con una exactitud de 1 segundo o superior.

ANF AC garantiza los “time-stamp token” -TST- durante todo el periodo de validez del certificado utilizado por el TSU en su generación, y más allá del extremo del periodo de validez del certificado si en el momento de comprobación se verifica que:

- Los algoritmos de hash usados en la generación del TST siguen siendo seguros, o se ha realizado un re-timbrado de los mismos.
- El algoritmo de firma y el tamaño de la clave sigue ofreciendo requisitos de seguridad en términos criptográficos, o se ha realizado un re-timbrado de los mismos.
- Causas que motivaron la pérdida de validez del certificado, ver apartado “Cambio de los certificados de la TSA”

ANF AC entidad emisora del certificado utilizado por el TSU, garantiza que mantiene la información acerca del estado de revocación de los certificados más allá del periodo de caducidad de los mismos, ver apartado correspondiente en DPC de ANF AC OID: 1.3.6.1.4.1.18332.1

Esta TSA mantiene un servicio público informativo sobre el estado de validez de los algoritmos que emplea y realiza un seguimiento de los ataques criptográficos conocidos. Dispone de un servicio de re-timbrado, el cual permitirá a las partes re-timbrar sus datos

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 20 de 57

en caso de producirse algún quebranto, o si existe sospechas sobre el mantenimiento de la seguridad de los algoritmos. URL:

<https://www.anf.es/AC/algoritmos/>

El perfil del certificado de clave pública utilizado por la TSA cumple con las recomendaciones del IETF RFC 3161, Internet X.509 Public Key Infraestructura Time-Stamp Protocol (TSP), Agosto 2001.

Las extensiones del certificado raíz ANF Root CA y la subordinada ANF TSA CA, se describen en la Declaración de Prácticas de Certificación de ANF AC OID: 1.3.6.1.4.1.18332.1.

El Perfil básico de los campos del certificado utilizado por la TSA se especifican en la Tabla 2.

Tabla 2

Nombre de los campos	Características
Versión	Versión 3
Número de serie	Identificador, es único para cada certificado emitido en el ámbito de ANF AC.
Algoritmo de Firma	Sha2RSA: (OID: 1.2.840.113549.1.1.13)
Emisor –Issuer- (Nombre Distinguido)	Nombre Común (CN) = ANF TSA CA
	Organización (O) = ANF Autoridad de Certificación
	País (C) = ES
Valido desde	Fecha de emisión
Valido hasta	Fecha de caducidad
Asunto –Subject- (Nombre Distinguido)	Cumple los requerimientos X-501
Información de la Clave Pública del Subject	Figura el código de acuerdo con la recomendación RFC 2459 . Contiene información RSA sobre el tamaño de la clave pública, que es 2048.
Uso de claves mejorado	Impresión de fecha.

Firma	Firma del Certificado. Se generó y se reseña el código de acuerdo con la recomendación RFC 3280.
-------	--

La Autoridad de Sellado de Tiempo que proporciona los servicios dentro de la infraestructura de ANF AC emite los “time-stamp token” –TST- según la recomendación ETSI TS 101.861, Time stamping profile.

5.2 Identificador de las Políticas de Sellos Digitales de Tiempo

El objeto-identificador [X.208] de la Política de Sellos Digitales de Tiempo básica se especifica en la Tabla 3.

Tabla 3

Identificador de Política	Nombre de la Política de Certificación
El ITU (1.3.6.1.4.1), identificación de la organización ANF AC (18332), identificador del documento (5), versión del documento (1)	ANF Autoridad de Sellado de Tiempo. Identidad del documento al que se somete el –TST-

El identificador de la Política que especifica los servicios que proporciona la TSA en el marco de la PKI de ANF AC, es incluido en cada sello digital de tiempo –TST-. Este documento está disponible y es de libre acceso público de acuerdo con lo especificado en el apartado “Documentación”

5.3 Usos del Sello de Tiempo.

No se define ningún límite de uso del “time-stamp token” –TST-. Como ejemplos, meramente enunciativos que no limitativos de los posible usos del –TST-, cabe citar: *todo tipo de transacciones electrónicas, archivos de documentos electrónicos, sistemas de registro de entrada o salida de datos, apoyo en la firma electrónica de acuerdo con las*

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 22 de 57

normas técnicas en esta materia (recomendación IETF RFC 3126, “Electronic Signatura Formats for long term electronic signatures” Septiembre 2001), y apoyo en el atributo “no repudio” de acuerdo con lo citado en la legislación vigente (Ley 59/2003 de firma electrónica).

Además el sello digital de tiempo está especialmente indicado para reunir los requisitos de las firmas electrónicas reconocidas (ver directiva europea sobre Firma Electrónica), y apoyar un plazo extenso de validez (ver P.e. la definición TS 101 733)

5.4 Conformidad.

Esta Autoridad de Sellado de Tiempo incluye el identificador de este documento en todos los sellos que emite. Esta TSA solo apoya “time-stamp tokens” que incluyan este identificador.

Este identificador permite a los usuarios y terceros:

- a) Determinar la conformidad de la TSA con ese sello de tiempo.
- b) La conformidad de los datos contenidos en el sello de tiempo con una determinada Política.

ANF AC garantiza la conformidad de sus servicios de acuerdo con lo especificado en este documento, asume las obligaciones reseñadas en el apartado “Obligaciones de la TSA” , y asegura la realidad de los procedimientos descritos en el apartado “Servicios de la TSA”.

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 23 de 57

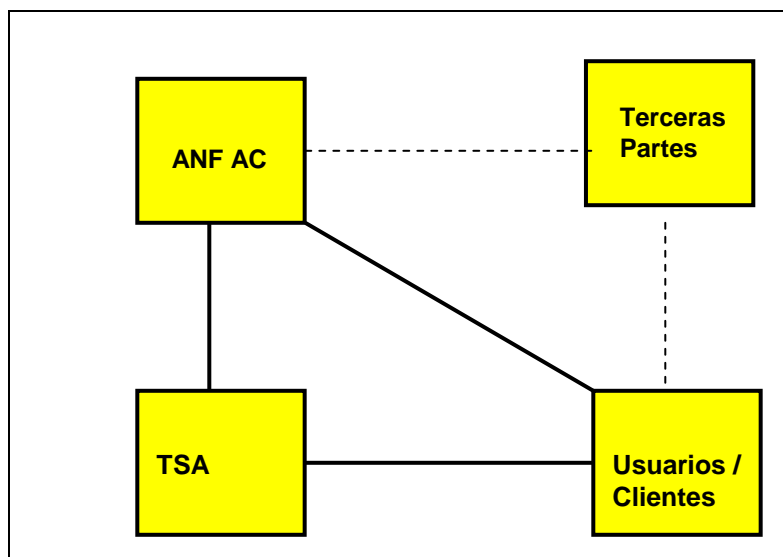
6. Obligaciones y garantías.

6.1 Obligaciones de ANF AC TSA

6.1.1 General

Este apartado incluye todas las obligaciones, garantías y responsabilidades de la TSA frente a los usuarios y terceras partes que voluntariamente confían en los “time-stamp token” *TST*, así como las obligaciones asumidas por las partes en el ámbito de la *PKI* de *ANF AC*. Estas obligaciones y responsabilidades son reguladas por acuerdos mutuos firmados entre *ANF AC* y sus usuarios o clientes, y tácitamente aceptadas por las terceras partes al confiar voluntariamente en los *TST*, tal y como muestra el Diagrama 1.

Diagrama 1



—— Contrato firmado entre las partes.

----- Obligaciones tácitamente aceptadas.

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 24 de 57

Estos acuerdos describen las obligaciones mutuas e incluso las responsabilidades financieras de *ANF AC*.

La Declaración de Prácticas de Certificación de *ANF AC* y *ANF TSA AC*, así como las Políticas, forman parte íntegra de los acuerdos firmados entre *ANF AC* y los usuarios o clientes.

ANF AC tan solo atiende peticiones de servicio de usuarios titulares de certificados vigentes, o clientes que hayan suscrito el correspondiente contrato de prestación de servicios de certificación.

ANF AC genera y firma los “time-stamp token” -*TST*- que emite, asumiendo la responsabilidad global de los sistemas de certificación.

ANF AC garantiza el acceso a la información de las listas de encadenamiento de los sellos digitales de tiempo emitidos por un periodo no inferior a quince años.

ANF AC garantiza el acceso público a los repositorios de encadenamientos de los sellos emitidos.

ANF AC facilita acceso y descarga gratuita de los certificados electrónicos emitidos, a través de repositorio público.

La *TSA* mantiene bajo su exclusivo control, las claves de activación de los datos de generación de firma que emplea para la estampación de los Sellos Digitales de Tiempo. Cada servidor -*TSU*- cuenta con unos datos de generación de firma diferentes del resto, vinculados a certificados digitales que lo identifican de forma unívoca.

La elaboración de los sellos digitales de tiempo -*TST*- que efectúan los Servicios de Certificación -*TSS*-, se realiza de acuerdo con lo especificado en el presente documento.

Previa a la emisión de un Sello Digital de Tiempo solicitado por un usuario de *ANF AC*, los servicios de certificación de *ANF AC* comprueban el estado de vigencia del

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 25 de 57

certificado vinculado al *TSU* y vigencia del certificado del usuario solicitante. Cuando la solicitud proviene de un cliente, el *TSU* determina el estado de vigencia del acuerdo.

La *TSA* garantiza la exactitud de su reloj de tiempo. La *TSA* incluye en el “time-stamp token” –*TST*- la hora *UTC* asegurando una exactitud igual o superior a 1 segundo con numerosas conexiones simultáneas. Esta exactitud pueda variar, por encima de las 200 conexiones simultáneas, hasta alcanzar los 2 segundos.

6.1.2 Obligaciones de la *TSA* frente a los usuarios.

ANF TSA AC garantiza la disponibilidad de sus servicios de certificación digital 24x7x365 excluyendo las paradas por servicios de mantenimiento técnico y otras causas de fuerza mayor. A su vez *ANF TSA AC* se reserva el derecho a efectuar denegación de servicio a aquellos usuarios que hayan incumplido alguna de sus obligaciones.

ANF AC garantiza que sus sistemas de emisión de “time-stamp token” –*TST*- cumplen con los requerimientos establecidos en esta DPC de *TSA* y según lo estipulado en el apartado Política de Sellos de Tiempo.

ANF AC garantiza que cada *TSU* cuenta con un identificador único y utiliza un certificado digital exclusivo, el cual además de la información relativa a la *TSA* y al *TSU*, especifica el país donde se encuentra ubicado el *TSU*.

ANF AC garantiza que los datos contenidos en un *TST* no están vinculados directamente a la identidad del signatario. Garantizando así la independencia del sistema respecto al anonimato de sus usuarios.

ANF AC aceptará las obligaciones emanadas por la emisión de sellos de tiempo por ella firmados.

ANF AC facilita a sus usuarios copia de cada nueva versión de la *DPC* y de las Políticas vinculadas. La documentación se encuentra además permanentemente disponible en repositorio público y gratuito.

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 26 de 57

ANF AC facilita gratuitamente los dispositivos de solicitud de *TST*, así como los dispositivos de verificación homologados por *ANF AC*.

ANF TSA AC garantiza la legalidad de sus servicios, el haber atendido todos los requerimientos establecidos en el actual marco legal, así como el respeto a la propiedad intelectual, licencias y otros derechos relacionados.

ANF TSA AC garantiza que sus servicios de certificación digital se desarrollan siguiendo normas internacionalmente aceptadas, tal y como consta en el apartado “*Características Generales*”.

ANF TSA AC garantiza que el “time-stamp token” –*TST*- emitido, no contiene ningún dato falso o erróneo.

Adicionalmente a lo reseñado, las obligaciones de *ANF TSA AC* se ven complementadas en el correspondiente apartado de Obligaciones de la *DPC* de *ANF AC* OID: 1.3.6.1.4.1.18332.1.

6.1.3 Obligaciones de la *TSA* frente a las terceras partes.

ANF AC garantiza el libre acceso a los repositorios de encadenamientos de los sellos emitidos.

ANF AC facilita el libre acceso a esta *DPC* y de las *Policitas* de Certificación vinculadas. La documentación se encuentra permanentemente disponible en repositorio público y gratuito.

ANF AC garantiza el acceso a la información de las listas de encadenamiento de los sellos digitales de tiempo emitidos por un periodo no inferior a quince años.

ANF AC facilita libre distribución de los dispositivos de verificación homologados por *ANF AC*. Disponible en repositorio público y gratuito.

6.2 Obligaciones del Usuario

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 27 de 57

El usuario asume la obligación de verificar que “time-stamp token” –TST- ha sido correctamente emitido.

El usuario que recibe un “time-stamp token” –TST-, debe comprobar su validez utilizando dispositivos de verificación homologados por ANF AC. Así mismo y caso de que el dispositivo no pueda establecer conexión OCSP (p.e. proxy o fireware que impide el acceso a la red), el usuario deberá comprobar el estado de vigencia del certificado de la TSA mediante consulta a la CRL de ANF AC.

- En el supuesto de que el certificado haya expirado o haya perdido su validez por revocación deberá:
 - Comprobar que la fecha de revocación o de caducidad es posterior a la fecha en que se emitió el “time-stamp token” –TST-.
 - Que la función criptográfica que se empleo para obtener el hash sigue siendo segura.
 - Que la longitud de la Clave criptográfica empleado por la TSA y el algoritmo de firma electrónica siguen siendo considerados en términos criptográficos como seguros.

El Usuario al remitirlo a terceras partes acepta como válidos los datos incorporados en el Sello Digital de Tiempo.

Aquellos usuarios cuyo volumen de peticiones de Sellos Digitales de Tiempo supere las 2500 unidades al mes, asumen la obligación de solicitar autorización previa e informar a ANF AC sobre sus estimaciones de consumo.

Aquellos usuarios que tengan contratado un Servicio Digital de Tiempo en exclusiva-servidor de notariado electrónico-, asumen la obligación de notificar con carácter prioritario la pérdida de vigencia de su certificado electrónico a su servidor de notariado electrónico, para ello deberán seguir las instrucciones técnicas establecidas en el momento de su contratación.

El Usuario para hacer uso del Sistema de Certificación TSA, asume la obligación de conocer y comprender plenamente las características y limitaciones determinadas en esta Declaración de Practicas de Certificación y de las Políticas vinculadas.

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 28 de 57

La utilización por parte del usuario de servicios de pago de ANF AC, conlleva la obligación inexcusable de pago.

6.3 Obligaciones de las Terceras Partes

Las terceras partes que voluntariamente confíen en los Sistemas de Certificación de esta TSA, asumen la obligación de:

- verificar el estado de activación en que se encuentra el Certificado de la TSA al que se vincula el Sello Digital de Tiempo emitido, mediante consulta a la CRL de ANF AC.
 - En el supuesto de que el certificado haya expirado o haya perdido su validez por revocación deberá:
 - Comprobar que la fecha de revocación o de caducidad es posterior a la fecha en que se emitió el “time-stamp token” –TST-.
 - Que la función criptográfica que se empleo para obtener el hash sigue siendo segura.
 - Que la longitud de la Clave criptográfica empleado por la TSA y el algoritmo de firma electrónica siguen siendo considerados en términos criptográficos como seguros.
 - Comprobar la validez del “time-stamp token” –TST- utilizando dispositivos homologados por ANF AC.

6.4 Garantías financieras.

Las que constan reseñadas en el apartado correspondiente de la DPC de ANF AC OID: 1.3.6.1.4.1.18332.1

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 29 de 57

7. Servicios de la TSA.

Los controles implementados por la TSA, prevén servicios de no-repudio en concordancia con lo regulado en este documento. Dirigen de forma eficaz el funcionamiento de los sistemas de sellado de tiempo, teniendo en cuenta a los usuarios y al personal que desarrolla su actividad en la TSA, registrando todo evento que se produce.

Previa a la estampación del “time-stamp token” –TST- solicitado por un usuario en apoyo en la creación de una firma electrónica, los servicios de la TSA verifican el estado de vigencia del certificado vinculado al usuario solicitante y su conformidad para la utilización de estos servicios.

ANF AC repercute al usuario de sus servicios las tasas correspondientes. Estas tasas pueden variar en función del tipo de servicio recibido y están sometidas a la propia fluctuación de los índices de precios del mercado. Las tarifas correspondientes están publicadas en <https://www.anf.es/AC/tasas/>

ANF AC garantiza que sus sistemas de certificación impiden el uso de los datos de generación de firma, más allá del fin del ciclo de vida del certificado del TSU, o cuando este ha sido revocado.

Los archivos correspondientes a los registros de eventos, son comunicados a la parte interesada adjuntando copia de los mismos. La TSA guarda copia de los eventos registrados fuera del lugar donde se encuentran los servicios que los generaron. El tipo de eventos registrados se describen en esta DPC y documentos vinculados.

En el diseño y desarrollo de los protocolos de los servicios de sellado de tiempo –TSS-, se han seguido las recomendaciones de:

S. Haber y W.S. Stornetta, *Artículo publicado*
- *How to Time Stamp a Digital Document* -,
Journal of Cryptology, vol.3, n 2, pp99-111, 1991

Texto integro disponible en la URL:

http://www.anf.es/security/pdf/Haber_Stornetta.pdf

Cabe destacar del mismo, dos requerimientos básicos:

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 30 de 57

-
1. *Deben sellarse los datos en sí, e independientemente de su continente o soporte, de forma que sea imposible cambiar ni un solo bit del documento sellado sin que este cambio sea detectado e invalide el sello.*
 2. *Debe ser imposible sellar un documento con un tiempo y fecha diferente de la actual*

Con el fin de garantizar la imposibilidad de alterar un sello de tiempo, incluso para la propia TSA que administra el servicio. ANF AC ha integrado en su TSS, dos de las principales opciones propuestas por S. Haber y W.S. Stornetta. Concretamente:

- 1.- Basados en el hecho de que la CA tiene capacidad de Firma Digital. En este modelo el modo de operar es el siguiente:
 - a/ El usuario envía el valor hash de un documento D; es decir, $h(D)$, a la ANF TSA AC,
 - b/ El servicio TSA añade al valor recibido el tiempo t, en la forma de fecha y hora de la recepción, componiendo $(h(D), t)$.
 - c/ ANF TSA AC procede a la firma digital de la asociación anterior calculando $FAC(h(D), t)$, y envía este Sello Digital de Tiempo al usuario que se lo solicitó. De esta forma, el usuario puede verificar el sello y probar ante otros que D existía en el tiempo t, con tan sólo verificar en cualquier momento la firma de la autoridad.

- 2.- ANF TSA AC procede además a realizar un protocolo de enlace. En este caso, lo que se pretende es que cada sello de tiempo emitido se encuentre enlazado con todos los sellos emitidos anteriormente, llegando al extremo de enlazar todos los sellados emitidos en un periodo de tiempo (un día). El modo de actuar es el siguiente:
 - a/ Por cada petición de un sello, la TSA le asigna un numero de serie unico n, identificando esta petición como $H_n = h(D)$,
 - b/ A continuación, la autoridad evalúa el -valor de enlace de orden n-, L_n , a partir de la información aparecida en el sello de tiempo emitido inmediatamente antes (sello n-1). $L_n = (t_{n-1}, U_{n-1}, H_{n-1}, h(L_{n-1}))$

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 31 de 57

-
- c/ Por ultimo, la TSA responde al usuario enviándole el sello de tiempo $T_n = FAC(n, t_n, U_n, H_n, L_n)$ Donde U_n es la identidad del ultimo peticionario, H_{n-1} es el valor hash que compuso el ultimo sello, $FAC()$ es la firma digital de la autoridad, y $h(L_{n-1})$ es el valor hash de enlace del nuevo sello con la secuencia anterior. Por ultimo, se publica periódicamente la secuencia de valores con un acta intervenida por un fedatario público.

7.1 Manifiesto y Prácticas de la TSA

7.1.1 Prácticas de la TSA

La Política de la TSA, forma parte de la DPC de ANF AC, que junto con los documentos internos asociados regula las reglas de funcionamiento de los servicios de Sellos Digitales de Tiempo.

La DPC regula las obligaciones de las operaciones externas relacionadas con la emisión de “time stamp tokens” –TST-. La DPC y Políticas relacionadas son documentos públicos regulados por los derechos de propiedad intelectual reseñados en el apartado correspondiente.

La adecuación de la DPC respecto a las Políticas vinculadas está supervisada de acuerdo con lo reseñado en el apartado correspondiente.

La TSA asume la responsabilidad global respecto a los procedimientos, mecanismos de control e infraestructura técnica, gestionando :

7.1.1.a Controles sobre el desarrollo del sistema

Todas las aplicaciones utilizadas han sido desarrolladas por especialistas de ANF AC. Todas las aplicaciones cuentan con documentación técnica específica, están identificadas mediante un OID exclusivo, el cual identifica a su vez la versión de la aplicación.

Todas las aplicaciones antes de integrarse en los sistemas de certificación de ANF AC son firmadas electrónicamente, y verificada la versión que se va a instalar respecto a la existente.

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 32 de 57

Se aplican igualmente reglas de control sobre el hardware del sistema:

- Todos los dispositivos se encuentran inventariados, determinando su vida útil y fecha de reemplazo.
- El régimen de control permite la trazabilidad del dispositivo, lugar donde se encuentra instalado y evolución del nivel de seguridad que requiere su acceso.
- La sustitución de dispositivos se realiza exclusivamente mediante personal autorizado.

7.1.1.b Seguridad de los equipos, requerimientos técnicos

Los requerimientos técnicos detallados seguidamente protegen a nivel de sistema operativo, aplicaciones y protección física de los sistemas:

- registro autenticado obligatorio en el nivel de sistema operativo y aplicación,
- control de acceso discrecional,
- capacidad para dirigir la auditoria de seguridad,
- los sistemas informáticos solo son accesibles por personal autorizado y de acuerdo con roles de seguridad personalizados,
- se gestiona y registra el momento de entrada en vigor de los roles y los cambios efectuados,
- se establece un sistema jerárquico de adjudicación de roles,
- la reutilización de dispositivos y la descarga de componentes y su instalación requiere autorización expresa,
- se aplica protección criptográfica a los registros de eventos y a los bancos de datos,
- se realiza un archivo histórico de las operaciones realizadas por los equipos informáticos y de todos los datos requeridos para la realización de auditorias de acuerdo con el Anexo III de la *DPC* de ANF AC OID 1.3.6.1.4.1.18332.11.1
- se ha establecido un sistema seguro que garantiza la identificación y autenticación de los roles y del personal que lo realiza,
- métodos de restauración de las claves (exclusivamente en los módulos del hardware de seguridad), aplicaciones y sistema operativo.
- Se monitoriza y se genera una alerta de control en caso de una desautorización de acceso a los sistemas.

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 33 de 57

7.1.2 Manifiesto de la TSA

La *DPC* de la *TSA* y Políticas relacionadas son documentos disponibles al público tal y como consta en el apartado correspondiente.

La *DPC* de la *TSA* está administrada según lo reseñado en este documento. El mantenimiento y control de la correcta aplicación de la *DPC* recae en la Junta Directiva de *ANF AC* según consta en el apartado correspondiente.

La identificación de la Política queda formulada en el apartado Política de Sellos de Tiempo de este documento y de la *DPC* de la *TSA* en el apartado correspondiente.

La función criptográfica del hash, usada en los procesos de sellado de tiempo, es conforme a los requisitos NIST FIPS PUB 180-1, Secure Hash Standard, 17 de Abril de 1.995. El periodo de validez del “time stamp token” –*TST*- después de la fecha de caducidad del certificado de la *TSA* vinculado al *TST*, queda regulado en los apartados “*Obligaciones de la TSA frente a los usuarios*” y “*Obligaciones de las Terceras partes*”.

Las limitaciones establecidas de los sistemas de la *TSA*, queda especificadas en este documento.

7.2 Ciclo de vida de las claves.

7.2.1 Generación de la Clave de la TSA.

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 34 de 57

Los datos de creación de firma son generados siguiendo los requerimientos establecidos en la Declaración de Prácticas de Certificación de ANF AC OID 1.3.6.1.4.1.18332.1. y su respectiva Política de Certificación.

En cualquier caso esta TSA asegura que entre otros requerimientos de seguridad caben destacar:

- Los datos de creación de firma se generan en un ambiente de seguridad, directamente controlado por personal de alta dirección de ANF AC.
- La generación de los datos de creación de firma se realiza bajo supervisión de al menos dos altos directivos de la TSA.
- La generación de los datos de creación de firma se han realizado dentro de un módulo criptográfico que reúnen los requisitos FIPS 140-1 nivel 3.

7.2.2 Protección de la clave privada TSU.

La TSA garantiza la confidencialidad e integridad de la clave privada instalada en cada TSU. En particular:

- Los datos de creación de firma están custodiados en módulos criptográficos que reúnen los requisitos FIPS 140-1 nivel 3 y siguen los requerimientos CWA-14167-2
- La activación de los datos de creación de firma se realiza bajo supervisión de al menos dos altos directivos de la TSA.
- El acceso a los módulos criptográficos de los TSU está restringido a personal autorizado de ANF AC, se realiza en todo momento de forma dual y en presencia de un responsable del área de seguridad.
- Las instalaciones donde quedan instalados los TSU son instalaciones que reúnen los requerimientos de seguridad física establecidos en la DPC de ANF AC OID: 1.3.6.1.4.1.18332.1

7.2.3 Difusión de la Clave Pública de la TSA.

Los certificados de TSA son de acceso público, sin restricción alguna. Se encuentra publicado en la URL:

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 35 de 57

El certificado de *TSA* se incluye en cualquiera de los dispositivos homologados de esta *ANF AC*.

7.2.4 Regeneración de la clave.

Transcurrido el periodo de validez del certificado vinculado a la clave privada, ésta se destruye, mientras que el certificado que contiene la clave publica es guardado por un periodo mínimo de 15 años para permitir la comprobación de los sellos de tiempo emitidos en el pasado.

7.2.5 Destrucción de la clave privada.

Una vez finalizado el ciclo de vida de las claves privadas, esta *TSA* procede a su destrucción y a la destrucción de cualquier copia de las mismas, siguiendo procedimientos que imposibilitan su recuperación.

7.2.6 Ciclo de vida del modulo criptográfico empleado para la firma de los *TST*.

La *TSA* garantiza la seguridad del hardware criptográfico a lo largo de su ciclo de vida.

En particular se responsabiliza que:

- el hardware criptográfico que firma del *TST* no puede ser manipulado durante el proceso de generación,
- el hardware criptográfico que firma del *TST* no puede ser manipulado durante el proceso de emisión,
- la instalación, activación y administración de los *TSU* se realiza por personal especialmente autorizado de acuerdo con los roles definidos por *ANF AC* . Siempre bajo presencia dual y además, siendo supervisado por un responsable del área de seguridad,
- el *TSU* funciona correctamente y,
- finalizado el ciclo de vida del *TSU*, las claves son borradas siguiendo procedimientos que imposibilitan su recuperación.

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 36 de 57

7.2.7 Copia de las Claves

Esta TSA con el fin de garantizar la continuidad del sistema ante cualquier posibilidad de siniestro, cuenta con una copia de las Claves Privadas de la entidad y de los Token que permiten su activación en Caja de Seguridad bancaria. Antes de guardarse en el contenedor de transporte, las claves han sido cifradas bajo triple clave y se ha custodiado durante todo el trayecto por dos altos cargos de ANF AC.

7.2.8 Periodo de validez

El periodo de validez de los certificados empleados por la TSA en el desarrollo de sus actividad, es el adecuado al tipo de algoritmo escogido y a la longitud de la clave según normas internacionalmente aceptadas. Cada certificado está sometido a una Política de Certificación la cual especifica el algoritmo empleado, la longitud de clave y plazo de vida.

7.2.9 Cambio de los certificados de la TSA

Todos los datos relativos al cambio de los Certificados de la TSA están descritos en la DPC de ANF AC OID: 1.3.6.1.4.1.18332.1 “Cambio de los Certificados de ANF Autoridad de Certificación” y documentos vinculados-

7.3 Sellos de Tiempo

7.3.1 Time-stamping token

- Todos los TST emitidos por esta TSA incluyen un identificador único y un identificador correspondiente a la DPC a la que se someten, tal y como consta en el apartado correspondiente.

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 37 de 57

- Cada *TST* incluye el certificado del *TSU* que lo generó, permitiendo determinar entre otros valores: la identificación del *TSU* y país en el que se encuentra ubicado.
- Cada *TST* incorpora el tiempo *UTC*, momento en que el *TSU* lo generó de acuerdo con la hora de referencia tomada de uno de los laboratorios reconocidos por Bureau International des Poids et Mesures (BIPM) website (www.bipm.org)
- El tiempo incluido en el “time-stamp token” –*TST*- se sincroniza con *UTC* de acuerdo con la exactitud definida en este documento, apartado correspondiente.
- Si se comprueba que el reloj del proveedor de tiempo esta fuera de la exactitud declarada, se cesará en la emisión de *TST*.
- El *TST* incluye un hash del tiempo reseñado en el *TST*.
- La clave generada para la firma de *TST* se utiliza exclusivamente para este fin. El sistema de certificación sigue las recomendaciones definidas en el RFC 3631 “*Protocol for a time-stamp token*”.
- Todos los *TST* emitidos por cada *TSU* están vinculados entre sí mediante el procedimiento de encadenamiento a través de una secuencia ASN.1 *. En la construcción del encadenamiento se incluye el identificado único del *TST* (serial number), la fecha del *TST* (día y hora), el hash (hash saliente) del sello inmediatamente anterior que cronológicamente se emitió (llamado hash entrante en este nuevo encadenamiento), el hash correspondiente al *TST info** (llamado hash actual) y el hash saliente que se construye en base a los dos hash (entrante y actual).

TST info es un atributo no firmado correspondiente conforme a las recomendaciones establecidas en el RFC 3161.

Esta secuencia de encadenamiento garantiza la imposibilidad de realizar manipulación alguna en el registro de *TST* emitidos.

Diariamente se genera un acta firmada por *ANF AC* de los encadenamientos que se han producido en el transcurso del día. Periódicamente, el conjunto de actas pertenecientes a ese periodo son incorporadas a un soporte óptico que queda protocolizado notarialmente.

* Secuencia ASN.1 = (Hash entrante, Hash actual, Hash Saliente)

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 38 de 57

7.3.1.a Tipos de Sellos Digitales de Tiempo.

Esta *TSA* emite las siguientes tipos de sellos digitales de tiempo:

- **TST cliente**
Sello Digital de Tiempo emitido a requerimiento de un usuario de esta *TSA* en apoyo de la generación de una firma electrónica avanzada.

- **TST Servidor**
Sello Digital de Tiempo emitido a requerimiento de un equipo informático en apoyo de la generación de una firma electrónica avanzada. Sistema habitualmente utilizado por clientes y por ANF *TSA* AC en la prestación de sus servicios de certificación.

- **TST Auditor**
Sello Digital de Tiempo emitido con el fin de atender cualquier otra necesidad que precise demostrar que un dato existió antes de un momento particular. Sistema habitualmente utilizado por clientes.

7.3.2 Sincronización del Reloj con UTC

El Servicio Digital de Tiempo de la *TSA* se conecta a un Servidor NTP Stratum I, sincronizando periódicamente (cada minuto) el reloj del sistema.

El Servidor NTP Stratum I consiste en un emisor de paquetes IP con información horaria sobre el valor del tiempo universal actual *UTC* a través del protocolo NTP (Network Time Protocol). El nivel de operación es Stratum I porque el servidor obtiene sus señales de tiempo a partir de un equipo hardware dedicado que está sincronizado con la escala *UTC* (Universal Time Coordinates) con una precisión dentro del microsegundo.

ANF AC garantiza que su reloj se sincroniza con *UTC* dentro de la exactitud declarada.

DPC <i>TSA</i> de ANF AC	Ref. DPC_ <i>TSA</i> _ ANF_ AC_ v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 39 de 57

Como fuente de tiempos, se toma como referencia de tiempo la hora facilitada por uno de los laboratorios reconocidos por el organismo público internacional Bureau International des Poids et Mesures (BIPM). BIPM publica mensualmente a través de su website (www.bipm.org) la lista del conjunto de grandes relojes atómicos en los institutos del metrología nacionales y los observatorios astronómicos nacionales que cubren todo el planeta. El laboratorio seleccionado por ANF AC es el Real Instituto y Observatorio de la Armada - San Fernando (Cádiz), "ROA", que es el responsable del mantenimiento de la unidad básica de Tiempo, 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)), considerada a todos los efectos como la base de la hora legal en todo el territorio nacional (R.D. 23 octubre 1992, núm. 1308/1992). Este laboratorio mantiene en funcionamiento varios servidores que distribuyen el tiempo a través del protocolo NTP. Este sistema de alta estabilidad y precisión utiliza un conjunto de patrones atómicos de cesio, que permiten conocer el tiempo UTC con una precisión superior al microsegundo, y con una estabilidad de 32 s/año 5 .

Si bien las normas de referencia no establecen ningún requisito técnico al respecto, con objeto de garantizar la fiabilidad del sistema para que la captación de tiempos sea precisa y disponible, y no esté sujeta a las fallas de disponibilidad en la sincronización con el ROA, ANF AC se ha dotado de un servidor que se sincroniza cada segundo con las señales de referencia procedentes de varios satélites de la constelación Navstar. Este servidor cuenta con relojes hardware redundantes y está destinado exclusivamente a la captación de la fecha y hora UTC de señales satelitales (mediante GPS) para su posterior transmisión a la TSA mediante protocolo NTP.

El sistema UTC utiliza la hora del meridiano de Greenwich, ignorando los desplazamientos provocados por el horario de verano. Desde el 1 de enero de 1.972 UTC es el estándar internacional de tiempo y si bien "Coordinated Universal Time" (UTC) ha reemplazado "Greenwich Mean Time" (GMT), en la práctica nunca existe más de 1 segundo de diferencia.

La escala de tiempo UTC, basada al segundo, es definida y recomendada por International Telecommunications Radio Committee (ITU-R), Recommendation TF.460-4.

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 40 de 57

La hora cero (0) *UTC* es de la media noche en Greenwich, Inglaterra en la que queda, en cero el meridiano longitudinal. El tiempo universal está basado en 24 horas, por consiguiente, horas de tarde de reloj como 4 pm en *UTC* se expresan como 16:00 *UTC* (dieciséis horas, cero minutos).

El Tiempo Atómico Internacional (TAI) es calculado por Bureau International des Poids et Mesures (BIPM), de la lectura de una red de 200 relojes atómicos localizados en laboratorios de institutos y observatorios de metrología repartidos en más de 30 países del mundo. ROA es parte integrante de la red descrita.

7.3.3 Desincronización del reloj.

En caso de que se produzca una falla de disponibilidad del servicio suministrado por el proveedor principal de hora (ROA), el sistema procede temporalmente a sincronizar su tiempo con el sistema GPS, emitiendo una alarma a los servicios técnicos de ANF AC. Estos servicios evalúan las características de la incidencia, a fin de establecer la necesidad de cambiar la obtención de la hora de referencia a otro laboratorio del BIPM.

Caso de producirse simultáneamente una falla del servicio ROA y GPS, lo cual imposibilita la sincronización horaria de los servidores, los sistemas de certificación de ANF AC proceden parar los servicios de emisión de *TST*.

7.3.4 Coherencia del sistema.

Los servicios de certificación de *ANF AC* están dotados de sistemas de protección ante incidencias de manipulación horaria fortuitas (altas de tensión, fallo de hardware) o intencionadas (atacantes externos o internos), que afecten la coherencia del sistema o que provoquen saltos cronológicos irregulares.

7.4 Dirección de la *TSA* y funcionamiento.

DPC <i>TSA</i> de ANF AC	Ref. DPC_ <i>TSA</i> _ ANF_ AC_ v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 41 de 57

7.4.1 Seguridad de la Dirección

Todos los datos relativos a la Seguridad de la Dirección están descritos en la *DPC* de ANF AC OID: 1.3.6.1.4.1.18332.1 y documentos vinculados-

7.4.2 Estimación de riesgos

Todos los datos relativos a la valoración de riesgos están descritos en la *DPC* de ANF AC OID: 1.3.6.1.4.1.18332.1 y documentos vinculados, en especial en el Plan de Contingencias de ANF AC.

7.4.3 Seguridad del personal

Todos los datos relativos a la Seguridad del Personal están descritos en la *DPC* de ANF AC OID: 1.3.6.1.4.1.18332.1 y documentos vinculados.

7.4.4 Seguridad Física y del entorno

Todos los datos relativos a la Seguridad Física y del entorno están descritos en la *DPC* de ANF AC OID: 1.3.6.1.4.1.18332.1 y documentos vinculados.

7.4.5 Operaciones de control

Esta TSA posee procedimientos de seguridad de acuerdo con los requerimientos ETSI TS 102 023 v.1.2.11 (2002-06) Policy Requirements for time-stamping authorities. La compañía realiza periódicamente auditorias internas siguiendo la directrices establecidas en el ANEXO III de la *DPC* de ANF AC OID 1.3.6.1.4.1.18332.11.1

7.4.6 Control de acceso a los sistemas

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 42 de 57

Todos los datos relativos al control de acceso a los sistemas están descritos en la *DPC* de ANF AC OID: 1.3.6.1.4.1.18332.1 y documentos vinculados.

7.4.7 Entorno de confianza

Toda la actividad desarrollada por la TSA se realiza en un ambiente de confianza adecuado a su actividad, basado en la utilización de medios físicos que ofrecen plenas garantías de seguridad y personal capacitado. Se realizan procesos de control permanentes, los sistemas están dotados de procedimientos de auditoria permanente y se registran los eventos que se producen, siendo éstos evaluados diariamente.

7.4.8 Servicios comprometidos

La TSA cuenta con un Plan de Contingencias y la *DPC* de ANF AC OID: 1.3.6.1.4.1.18332.1, especifica medidas de actuación ante la posible rotura de seguridad de los sistemas de certificación.

7.4.9 Conformidad con los requerimientos legales

Todos los datos relativos a la conformidad con los requerimientos legales están descritos en la *DPC* de ANF AC OID: 1.3.6.1.4.1.18332.1 y documentos vinculados.

7.4.10 Registro diario de eventos

ANF AC incorpora en sus sistemas mecanismos que registran diariamente los eventos que se han producido. Los eventos registrados y niveles de seguridad afectados quedan recogidos en la *DPC* de ANF AC OID: 1.3.6.1.4.1.18332.1 y documentos vinculados.

7.5 Organización

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 43 de 57

ANF Autoridad de Certificación

Gran Vía de les Corts Catalanes, 996
08018 - Barcelona - España
Tfno.- 00 34 932 661 614
FAX.- 00 34 933 131 614
Dirección electrónica: ac@anf.es
Dirección web: <https://www.anf.es/>

7.6 Dispositivos de obtención de TST.

Para la obtención de Sellos Digitales de Tiempo los usuarios deben emplear dispositivos homologados por ANF AC.

Estos dispositivos son distribuidos por la Autoridades de Registro, de acuerdo con lo establecido en la DPC de ANF AC OID: 1.3.6.1.4.1.18332.1

Las actualizaciones de este software, están digitalmente firmadas, son gratuitas y se encuentran disponibles en la URL:

<https://www.anf.es/AC/dispositivos/>

7.7 Dispositivos de verificación de TST.

Para verificar los Sellos Digitales de Tiempo se deben de utilizarse dispositivos homologados por ANF AC.

Estos dispositivos tiene la capacidad de verificar la integridad del Sello Digital de Tiempo, la identidad de la TSA y el estado de vigencia de los certificados. Concretamente se garantiza que:

- a) La firma digital fue creada por la clave privada vinculada a la clave pública perteneciente al certificado de la TSA.

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 44 de 57

-
- b) * Estado del certificado y capacidad de firma en relación a la Polícita a la que se somete.
 - c) Que el documento no ha sido alterado desde que se creó.
 - d) Identidad de la AC que emite el certificado y garantiza la firma.
 - e) * Caso de encontrarse el certificado de la TSA revocado, determina la causa de revocación.
 - f) El informe de verificación facilita detalle de la Secuencia ASN.1.

* Se requiere que el dispositivo de verificación pueda efectuar una conexión OCSP con los servidores de ANF AC.

Caso de que el dispositivo de verificación no pueda establecer conexión OCSP, es responsabilidad del receptor del sello digital de tiempo verificar personalmente a través de consulta a la Web de ANF AC el estado de vigencia de todos los certificados vinculados al TST.

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 45 de 57

8. Oficina de Atención al Cliente.

ANF AC se compromete a tener plenamente operativo un servicio gratuito de atención de Usuarios y Receptores.

8.1 Cometido de la Oficina.

Este servicio atenderá cuantas consultas comerciales, jurídicas y técnicas estén relacionadas con:

- La actual legislación vigente sobre firma electrónica.
- Esta *DPC* y las Políticas relacionadas.
- Instalación y utilización de los dispositivos relacionados con la firma electrónica.
- Instalación y utilización del software de verificación.
- Consultas generales sobre los conceptos básicos de Infraestructura de Clave Pública, certificados digitales y firma electrónica.

Así mismo, realizará en nombre del Usuario o de la persona a la que éste representa, las distintas operaciones que esta *DPC* y sus Políticas de Certificación le encomienden.

8.2 Procedimiento de Consulta.

Las consultas se realizarán mediante correo electrónico dirigido a :

consultas@anf.es

en ellas se reseñará el identificador del usuario que consulta o, en caso de ser receptor, el identificador de la firma recibida.

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 46 de 57

Todas las consultas serán contestadas por este mismo medio a la dirección electrónica del remitente.

8.3 Procedimiento de Reclamación.

En caso de desear presentar una reclamación, esta entidad prestadora de servicios de certificación cuenta con formularios al efecto. Éstos pueden ser libre y gratuitamente descargados a través de Internet, en la URL:

<https://www.anf.es/AC/reclamaciones/>

Posteriormente tramitar su reclamación por correo electrónico a: ac@anf.es

O también se puede dirigirse personalmente ante la Oficinas de Atención al Cliente.

ANF AC contestará por escrito a la reclamación formulada en un tiempo no superior a 15 días hábiles.

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 47 de 57

9. Interpretación y Ejecución.

9.1 Ley aplicable.

La legislación aplicable a este documento y a las relaciones jurídicas subyacentes es la del Reino de España.

Esta *DPC* debe interpretarse con arreglo a la legislación vigente, sus disposiciones de desarrollo y la legislación específica que afecta a sus servicios, especialmente en materia de protección de datos personales y legislación sobre protección de los consumidores y usuarios.

9.2 Conflicto de normas.

Cada sello digital se emite bajo una *DPC* y una Política de Sellos de Digitales de Tiempo, identificadas por un número de versión, de modo que, en cada caso, deberá acudirse a esa concreta versión, con independencia de posteriores versiones de tales documentos.

La *DPC* y las Políticas de Sellos Digitales de Tiempo se incorporan por referencia a los certificados bajo las cuales se emiten tales certificados, a fin de que el receptor de los mismos disponga de elementos suficientes para valorar si decide confiar en los mismos.

9.3 Divisibilidad, supervivencia y notificaciones.

Cada cláusula de esta *DPC* y sus Políticas, es válida en sí misma y, en caso de anulación no invalidará el resto. La cláusula inválida o incompleta podrá ser sustituida por otra equivalente y válida por acuerdo de las partes.

Las normas sobre obligaciones y responsabilidades, y todas aquéllas relacionadas a la confidencialidad y privacidad de los datos que han sido confiados a *ANF AC*, permanecerán en vigor tras la finalización de la vida de esta *DPC*.

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 48 de 57

Las notificaciones a *ANF AC* podrán realizarse mediante mensajes de correo electrónico firmados digitalmente, de acuerdo con las prescripciones de esta *DPC*, o por escrito.

Las comunicaciones electrónicas serán efectivas tras la recepción por parte del emisor del correspondiente acuse de recibo firmado digitalmente.

Las comunicaciones escritas deben ser enviadas por servicio certificado con acuse de recibo o equivalente, a la siguiente dirección:

ANF AC

Gran Vía de les Corts Catalanes, 996 planta 4ª
08018 – Barcelona - ESPAÑA

9.4 Administración de la *DPC* y Políticas.

La propia evolución de los servicios de certificación de *ANF AC*, conlleva que esta *DPC* y sus Políticas estén sujetas a modificaciones. Se establece un sistema de versiones numeradas para la correcta diferenciación de las sucesivas ediciones que de estos documentos se produzcan.

ANF AC se compromete a notificar a todos sus usuarios, Autoridades de Registro y Entidades Reconocidas, con una antelación de 30 días a la entrada en vigor de las nuevas versiones, el texto íntegro de las mismas.

Toda necesidad de modificación debe estar justificada desde el punto de vista técnico, legal o comercial, debiendo, por lo tanto, estar avalada por la firma de los responsables de *ANF AC*.

Se deberán contemplar todas las implicaciones técnicas y legales de la nueva versión de especificaciones. Se establecerá un control de modificaciones para garantizar, en todo caso, que las especificaciones resultantes cumplen con los requisitos que se intentaban cumplir y que dieron pie al cambio.

9.5 Procedimientos de resolución de disputas.

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 49 de 57

9.5.a Procedimiento aplicable para la resolución extrajudicial de los conflictos.

ANF Autoridad de Certificación se somete voluntariamente para la solución de cualquier cuestión litigiosa que pudiera surgir por el ejercicio de su actividad, al arbitraje institucional del Tribunal Arbitral del Consejo Empresarial de la Distribución (TACED), al que se le encarga la designa del Árbitro – que será único – y la administración del arbitraje – que será de equidad – con arreglo a su Reglamento, obligándose desde ahora, al cumplimiento de la decisión arbitral. Caso de que la alguna de las partes contrarias a ANF AC no acepte este procedimiento arbitral, se seguirá lo establecido en el apartado correspondiente.

9.5.b Procedimiento judicial.

Todas las partes se someten expresamente a los Juzgados y Tribunales de la ciudad de Barcelona, con renuncia a su propio fuero si fuese otro.

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 50 de 57

10. Publicación y repositorios.

10.1 Publicación de información de la CA.

Es obligación de esta autoridad de certificación publicar información relativa a sus prácticas, sus certificados y el estado en que se encuentran dichos certificados. Todo el histórico de esta documentación esta conservado y es accesible al menos por un periodo mínimo de quince años.

Este documento y sus anexos son públicos y se encuentran disponibles en el sitio Web de la autoridad de certificación <https://www.anf.es/AC/documentos/>.

Las Políticas de Sellos Digitales de Tiempo son públicas y se encuentran disponibles en el sitio Web de la autoridad de certificación <https://www.anf.es/AC/documentos/>.

El certificado de la TSA de ANF AC es público y se encuentra disponible en el sitio Web de la autoridad de certificación <https://www.anf.es> en formato x.509 v.3

La lista de certificados revocados por ANF AC es pública y se encuentra disponible en el sitio Web de la autoridad de certificación <https://www.anf.es> . Su consulta sobre base de datos está regulada en este documento, al igual que la obtención de una copia en formato CRL v2 del repositorio.

Todos los documentos se encuentran firmados electrónicamente por ANF AC. La integridad y autenticidad de los mismos debe de ser comprobada mediante dispositivo de verificación homologado por ANF AC, de libre distribución, puede ser descargado a través de la URL:

<https://www.anf.es/AC/dispositivos.htm>

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 51 de 57

10.2 Frecuencia de publicación.

La *DPC* y las Políticas de Sellos Digitales de Tiempo se publicarán en el momento de su creación.

Los Sellos de Tiempo se integran en el repositorio de *ANF AC* de forma simultanea a su creación.

10.3 Controles de acceso.

El acceso a lectura de la información del repositorio de *ANF AC* y de su Web es libre.

Solo *ANF AC* está autorizada a modificar, sustituir, añadir o eliminar información de su repositorio y sitio Web. *ANF AC* utiliza medios de control adecuados para restringir la capacidad de escritura o modificación de estos elementos.

10.4 Procedimiento de especificación de cambios.

Esta Declaración de Prácticas de Certificación y las Políticas de Sellos Digitales de Tiempo pueden sufrir cambios en el transcurso del tiempo.

La entidad con atribuciones para analizar los cambios sobre esta *DPC* es la Junta Rectora de la PKI “JRPKI”, cuyos datos constan en el “*Especificación del ente organizador*”. La JRPKI determinará en cada caso, los elementos que le servirán de soporte para efectuar los análisis de los cambios propuestos, aunque deberá contar siempre con un informe jurídico que establezca que estos cambios se adecuan a lo establecido en la legislación vigente.

La entidad con atribuciones para definir y aprobar sobre cualquier propuesta de modificación de esta *DPC* es la Junta Rectora de la PKI. No obstante, si el informe jurídico recibido durante la fase de análisis es negativo, deberá rechazar el cambio propuesto.

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 52 de 57

Cuando se produzca un cambio en la *DPC* se modificará el número de versión del documento afectado, incrementando en uno el número menor del valor de la versión existente (inmediatamente posterior al prefijo). Asimismo se podrá variar el número mayor de la versión (prefijo), si a juicio de la JRPKI los cambios efectuados son de tal importancia que recomienden realizar esa modificación. El nuevo prefijo es determinado por la propia JRPKI.

El mantenimiento y el control de la correcta aplicación de lo establecido en la Declaración de Prácticas de Certificación y sus Políticas, recaen sobre la Dirección Ejecutiva de ANF AC.

10.5 Procedimiento de Publicación y Notificación.

Cuando se produzca un cambio de versión, se comunicará a todos los usuarios de esta PKI y a las Autoridades de Registro mediante correo electrónico. Así mismo se publicará del repositorio de documentos de la Web de esta autoridad de certificación.

10.6 Procedimientos de aprobación de la *DPC*

La entidad con atribuciones para aprobar los cambios sobre esta *DPC* es la Junta Rectora de la PKI. Cuyos datos constan en el apartado “*Especificación del ente organizador*”.

La Junta Rectora de la PKI, notificará los cambios al equipo ejecutivo de ANF AC para que confeccionen una nueva *DPC* según el caso. Proceda a su publicación, notificación, y en caso de necesidad realizar las operaciones logísticas y operativas que adecuen la actividad de la autoridad de certificación a los nuevos requerimientos.

10.7 Repositorio de encadenamientos

Cada *TSU* gestionan un repositorio público de los encadenamientos que ha realizado. Cada día el *TSU* genera, firma y estampa sello de tiempo en un acta en la que se agrupan los encadenamientos realizados durante ese periodo. Aquellos encadenamientos que aun

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 53 de 57

no han sido integrados en el fichero autenticado, pueden ser consultados por acceso al listado general.

Periódicamente, el conjunto de actas pertenecientes a ese periodo son incorporadas a un soporte óptico que queda protocolizado notarialmente.

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 54 de 57

11. Información de referencia.

Documentos que se han tomado como referencia para la elaboración de este documento y en el desarrollo de la infraestructura tecnológica empleada por esta TSA.

11.1 Normas de referencia

- [TF.460-5]** ITU-R Recommendation TF.460-5 (1997): Standard-frequency and time-signal emissions.
- [TF.536-1]** ITU-R Recommendation TF.536-1 (1998): Time-scale notations.
- [CWA 14167-1]** CEN Workshop Agreement CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electrónica Signatura – Part. 1: System Security Requirements.
- [CWA 14167-2]** CEN Workshop Agreement 14167-2: Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP).
- [FIPS 140-1]** FIPS PUB 140-1 (1994): Security Requirements for Cryptographic Modules.
- [ISO 15408]** ISO/IEC 15408 (1999) (parts 1 to 3): Information technology - Security techniques and Evaluation criteria for IT security.

11.2 Referencias informativas

- [CWA 14172]** CEN Workshop Agreement 14172: EESSI Conformity Assessment Guidance.
- [Dir 95/46/EC]** Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 55 de 57

-
- [Dir 99/93/EC]** Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
- [Ley 59/2003]** Ley de Firma Electrónica de España. Ley 59/2003 de 19 de diciembre.
- [LO 15/1999]** Ley Orgánica de Protección de Datos de España 15/1999, de 13 de diciembre.
- [ISO 17799]** ISO/IEC 17799: Information technology Code of practice for information security management
- [RFC 3126]** Pinkas, D., Ross, J. and N. Pope, "Electronic Signature Formats for long term electronic signatures", RFC 3126, September 2001.
- [RFC 3161]** Adams, C., Cain, P., Pinkas, D. and R. Zuccherato, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)", RFC 3161, August 2001.
- [RFC 3628]** Adams, P., Pinkas, Bull, N. Pope, J. Ross, "Policy Requirements for Time-Stamping Authorities (TSAs)", RFC 36128, November 2003.
- [TS 101733]** ETSI Technical Specification TS 101 733 V.1.2.2 (2000-12) Electronic Signature Formats. Note: copies of ETSI TS 101 733 can be freely downloaded from the ETSI web site www.etsi.org.
- [TS 101861]** ETSI Technical Specification TS 101 861 V1.2.1. (2001-11). Time stamping profile. Note: copies of ETSI TS 101 861 can be freely downloaded from the ETSI web site www.etsi.org.
- [TS 102023]** ETSI Technical Specification TS 102 023. Policy requirements for Time-Stamping Authorities. Note: copies of ETSI TS 102 023 can be freely downloaded from the ETSI web site www.etsi.org.
- [X.208]** CCITT Recommendation X.208: Specification of AbstractSyntax Notation One (ASN.1), 1988.
- [X.509]** RFC 3647 "*Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*".
- [X.501]** ITU-T RECOMMENDATION X.501 TC2 (08/1997)
| ISO/IEC 9594-2:1998

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 56 de 57

[TF.460-4] ITU-R RECOMMENDATION UTC Time scale, based on the second International Telecommunications Radio Committee (ITU-R), Recommendation TF.460-4.

Relación permanentemente actualizada y públicamente disponible en la URL:

<http://www.anf.es/AC/normas/>

DPC TSA de ANF AC	Ref. DPC_TSA_ANF_AC_v1.pdf	Versión: 1
	OID: 1.3.6.1.4.1.18332.5.1	Página 57 de 57