Declaración de Prácticas de Certificación de ANF AC

CPS (Certificate Practice Statement) de ANF AC

ANF AC
CIF: G-60865144
Oficina Comercial: Gran Vía Corts Catalanes, 996, 4º 2ª
08018 Barcelona
Teléfono: 93.266.16.14 Fax: 93.303.16.11
E-mail: comercial@anf.es

Certificados de Autenticación | Certificados de Entidad | Certificados ANF Autentic. | Certificados Alta seguridad | Anexo I Código Ético | Anexo II Seguridad Adm

Declaración de Prácticas de Certificación de ANF AC

CPS de ANF AC

Versión 1.1 de fecha 1 de Julio del 2002

Sumario

1. Introducción

1.1 Presentación.

ANF Autoridad de Certificación "ANF AC" es una entidad jurídica sin ánimo de lucro constituida al amparo de la Ley Orgánica 1/2002 del 22 de marzo e inscrita en el Ministerio del Interior con el número nacional 11.465 y CIF G-63287510.

El presente documento constituye una declaración de los criterios que ANF Autoridad de Certificación **("ANF AC"),** se compromete a seguir en la prestación de sus servicios de certificación.

En el ámbito de las Administraciones Públicas, los servicios de esta AC pueden estar regulados por disposiciones adicionales a la presente declaración. Estas disposiciones adicionales serán específicas para cada Administración y se integrarán a este documento como anexos al mismo. En caso de no existir anexo especifico, la firma electrónica, en el ámbito de una Administración Pública, seguirá exclusivamente los criterios generales establecidos.

En esta CPS se exponen las normas y condiciones generales de los servicios de certificación que presta ANF AC, incluyendo la solicitud, identificación, generación, activación, revocación de los certificados, verificación de los sellos de tiempo, garantías patrimoniales, así como gestión y uso de los dispositivos de generación de firma y verificación. Es parte integrante de este documento sus Anexos y las Políticas de Certificación por la que se rigen cada uno de los distintos tipos de certificados que ANF AC emite.

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, receptores que reciben ficheros electrónicos firmados digitalmente por signatarios de ANF AC.

1.2 Identificación.

CPS de ANF AC versión 1
Identidad de la AC = "Distinguished Name" (DN).
País = "Country" (C) = ES = España.
Estado = "State" = ST = Barcelona.
Nombre de la Organización = "Organization Name" = O = ANF.
Nombre Común = "Common Name" = CN = AC.
Netscape-revocation-url = Determina la URL donde está ubicada la Lista de certificados Revocados (CRL) emitidos por esta AC = http://www.anf.es/AC/RC/
Netscape-ca-policy-url = Determina la URL donde está ubicada esta CPS = http://www.anf.es/AC/documentos/
Número de Serie del Certificado de ANF AC = 0271 8C10.
Algoritmo de Firma sha1RSA. Clave Pública (RSA 2048 bits).
Algoritmo de identificación sha1.
Huella Digital del Certificado de ANF AC = `654F 69F9 7557 DA54 1DE1 0E3F 8D7D 29D6 0118 0A10`
Número de versión: Configurado con el número de versión v3.

1.3 Localización.

Cuenta con oficinas centrales en:

Gran Vía de les Corts Catalanes, 996
08018 - Barcelona - España
Tfno.- 932 661 614 FAX.- 933 131 614

Dirección electrónica: ac@anf.es

Dirección web: http://www.anf.es/

Persona de contacto: Florencio Díaz

e-mail: diazdiaz@teleline.es

1.4 Definiciones.

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

Glosario de términos.

Contenedor	=	Soporte del Certificado homologado por ANF AC, denominado Contenedor homologado TID.
Entidad	=	Características relevantes de una persona física o jurídica.
Fichero TID	=	Fichero electrónico que almacena encriptados los datos de creación de firma. Es uno de los contenedores homologados TID.
PKI	=	"Public Key Infrastructure", infraestructura de clave pública. Es La arquitectura, los participantes y el proceso que constituye una comunidad de confianza específica por medio de la criptografía de Clave Pública.
PIN	=	Contraseña secreta que precisa la TID para poder ser activada.
Receptor	=	Tercero de buena fe; persona física o jurídica que recibe un fichero electrónico firmado digitalmente por un signatario de ANF AC. Los requisitos de la buena fe de los receptores se determinan en el apartado 9.3 del presente documento.
Sistema TID	=	Conjunto de programas desarrollados por el Departamento I+ D de ANF. Este software, exclusivo de ANF AC, es el responsable de la seguridad del sistema; asume, además, todo el proceso necesario para la generación de claves y generación y verificación de firma electrónica. En servicios Web ER, asume la seguridad de las comunicaciones, procesos de identificación y autenticación, y posibilita que usuarios de ANF AC puedan firmar electrónicamente de forma remota.
Tarjeta TID	=	Tarjeta de Identificación Digital. Se trata de una tarjeta que integra un microchip; cuenta con un sistema operativo propio, capacidad para efectuar operaciones aritméticas y criptográficas, así como memoria no volátil donde se almacenan los datos de creación de firma. Es un contenedor homologado TID.
Usuario	=	Signatario de ANF AC.

Abreviaturas y acrónimos.

AC	=	Autoridad de Certificación = CA
AR	=	Autoridad de Registro.
CA	=	“Certificate Authority” = AC
CDIP	=	Certificado Digital de Identificación Personal.
CP	=	“Certificate Policy”. Política de Certificación.
CPS	=	“Certificate Practice Statement” - Declaración de Prácticas de Certificación.
CRL	=	Lista de Revocación de Certificados.
DN	=	“Distinguished Name” - Nombre Distintivo
ER	=	Entidad Reconocida.
FTP	=	Protocolo de transferencia de registros “File Transfer Protocol”
GMT	=	Hora del meridiano de Greenwich “Greenwich Mean Time”
HTTP	=	Protocolo de transferencia de hipertexto “Hypertext Transfer Protocol”
IEC	=	“Information Evaluation Criteria”.
ISO	=	Organización Internacional de Normalización.
ITSEC	=	“Information Technology Security Evaluation Criteria”.
NTP	=	“Network Time Protocol”
OID	=	“Digital Object Identifier” - Código por el que se identifica esta CPS.
PC	=	Política de Certificación.
PIN	=	Número de Identificación Personal “Personal Identification Number”
PKCS	=	Estándares de criptografía de Clave Pública “Public Key Cryptography Standards”
PKI	=	Infraestructura de Clave Pública “Public Key Infrastructure”
RSA	=	Algoritmo de Clave Pública - “Rivest, Shamir y Adleman”.
SHA	=	Algoritmo Seguro de Hash.
SSL	=	“Secure Socket Layer”.
TID	=	Tarjeta de Identificación Digital.
URL	=	Localizador de recursos uniforme “Uniform Resource Locator”
UTC	=	“Universal Time Coordinated”. Estándar oficial para contabilizar el tiempo actual
WWW	=	“Word Wide Web”.
X.509	=	Estándar ITU-T para certificados

1.5 Publicación.

Este documento y sus diferentes versiones y anexos puede obtenerse libremente en el Directorio http://www.anf.es/AC/documentos/, o en las oficinas centrales de ANF AC.

ANF AC ha realizado depósito de esta CPS, sus Anexos y Políticas de Certificación en el Registro General de Condiciones Generales de Contratación.

Para facilitar una recuperación de estos documentos en “modo seguro”, previo a su depósito, todos ellos han sido firmados electrónicamente por ANF AC.

1.6 Ámbito de aplicación.

La presente CPS se aplica a todos los Certificados Digitales de Identificación Personal (CDIP) emitidos por ANF AC y a los certificados de Autoridad de Certificación (AC) que la propia ANF

AC emite. Las Políticas de Certificación aplicadas por ANF AC y definidas en estas CPS determinan el uso apropiado que debe darse a los Certificados.

Las presentes CPS no regulan el protocolo “Secure Sockets Layer” (SSL) instalado en los servidores de la AC.

1.7 Control de exportación.

La exportación de determinados elementos empleados dentro de los servicios de certificación pública de ANF AC puede requerir la aprobación por parte del organismo público pertinente. Las partes se ajustarán a la normativa de control de exportación vigente en cada momento, cuando esta normativa sea aplicable.

1.8 Derechos de Propiedad Intelectual.

ANF 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 posee todos los derechos de propiedad intelectual sobre esta CPS, sus ANEXOS, las Políticas de Certificación, los modelos de contrato de prestación de servicios de certificación con las ER y las solicitudes de activación de certificados de usuarios. Todos estos documentos no pueden ser reproducidos total o parcialmente sin el consentimiento expreso de ANF.
Los dispositivos de:

- Generación de Datos de Creación de Firma electrónica.
- Creación de Firma electrónica.
- Verificación de Firma electrónica.

así como el resto del software que compone el **Sistema TID**, es tecnología de propiedad de ANF AC; queda prohibida expresamente su comercialización, modificación o la aplicación de procesos de tecnología inversa. Se autoriza su reproducción y difusión siempre que se reseñe:

-Copyright ANF AC-
Autor: Florencio Díaz Vilches.

Los certificados son propiedad de ANF AC y llevan la pertinente mención relativa a derecho de autor. Se concede un permiso no exclusivo y no retribuido de reproducción y distribución de certificados 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.

Los nombres distintivos son propiedad de las personas que sustentan los derechos de marca correspondiente sobre los mismos, de existir. Si no se conoce esta circunstancia, ANF AC empleará el nombre propuesto por el usuario, bajo la entera responsabilidad de éste. Las claves privadas y públicas son propiedad de los usuarios, con independencia del medio físico empleado para almacenarlas y protegerlas.

2. Seguridad.

La seguridad desarrollada por ANF AC tiene como ejes principales de actuación:

- Los servicios de seguridad que se requiere que el sistema proporcione para satisfacer las necesidades de sus usuarios.

- Los servicios de seguridad que se requiere que el sistema proporcione para satisfacer las necesidades de ANF AC, en especial la protección de sus propias claves privadas, la estructura de las tarjetas TID y código fuente del software empleado por los usuarios y la propia Autoridad de Certificación.

- Los servicios de seguridad que se requiere que el sistema proporcione para satisfacer las obligaciones que le impone la legislación vigente.

- Los elementos del sistema requeridos para implementar esos servicios.

- Los niveles de desempeño que se requiere de los elementos para que interactúen con las amenazas del entorno.

La arquitectura de seguridad contempla los siguientes apartados:

- Seguridad de las comunicaciones.
- Seguridad administrativa.
- Seguridad de los equipos informáticos.
- Seguridad del personal.
- Seguridad física.

Considera tanto amenazas de tipo intencional e inteligente, como de tipo accidental.

ANF AC realiza periódicamente auditorias que controlan el correcto cumplimiento de cada uno de los apartados de Seguridad. Los procedimientos y frecuencia para la realización de auditorias están regulados en el reglamento interno de la Seguridad Administrativa de ANF AC; entre los criterios seguidos para la definición de los procedimientos de auditoria se encuentra el Real Decreto 994/99 ("Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal").

2.1 Seguridad de las comunicaciones.

La comunicación entre los distintos módulos empleados por el dispositivo de generación de firma, tanto localmente como de forma remota, está protegida mediante la aplicación de distintas capas de seguridad "***multilevel secure" (MLS) (*).*** La utilización de técnicas de ataque "***sniffer" (**)*** resultan inviables, **ANF AC** utiliza **"*nonce (***).***

(*) *"**multilevel secure" (MLS) - seguro con multinivel:***

Sistema que tiene recursos en diferentes niveles de seguridad y que permite el acceso concurrente de usuarios con distintas habilitaciones de seguridad y necesidad de saber, pero que puede evitar su acceso a recursos no autorizados.

(**) "sniffer":

Literalmente "Husmeador". Pequeño programa que busca una cadena numérica o de caracteres en los paquetes que atraviesan un nodo con objeto de conseguir alguna información.

(***) "nonce" - ocasional:

Valor aleatorio, no repetitivo que se incluye en los datos intercambiados por un protocolo, que permite garantizar su actualidad y así detectar y proteger contra ataques de repetición.

NOTA IMPORTANTE: Por motivos de seguridad, la información reseñada en el presente apartado debe de ser considerada como mero enunciamiento y sin corresponder la exposición de las operaciones detalladas, al orden en que se realizan.

2.1.a Encriptación.

La información se transmite en todo momento encriptada y, en determinadas operaciones de alta seguridad, en combinación con el sistema “hash” (*), garantizando los siguientes aspectos:

? ????**Integridad:** Cualquier intento de modificación de los datos transmitidos se detecta y rechaza automáticamente por el **Sistema TID**. Queda así garantizada la integridad de los datos recibidos. No es posible su manipulación ***"cut-and-paste attack" (**)*** :

✍✍✍✍✍✍✍✍✍ **Generación:** Se genera resumen hash (*) de los datos a transmitir.
✍✍✍✍✍✍✍✍✍ **Transmisión:** Se empaqueta, encripta y se transmite.
✍✍✍✍✍✍✍✍✍ **Recepción:** Se desempaqueta y se desencripta.
✍✍✍✍✍✍✍✍✍ **Verificación:** Se genera hash (*) de la información recibida y se compara con la huella original.

? ????**Confidencialidad:** Los datos transmitidos son ilegibles.

? ????**Módulo criptográfico:** Combinación de hardware y software ***"key- encrypting key" (KEK) (***)***. Todos los módulos trabajan con el sistema de encriptación 3DES que incorpora el microprocesador de la **tarjeta TID** (caso de utilizar el usuario la TID**)**; además utilizan el algoritmo criptográfico de la librería **Enctid.dll** (desarrollo exclusivo de ANF AC) que genera valores aleatorios en su proceso de encriptación.

(*) ***"Hash function" - función hash:***

Algoritmo que calcula un valor basado en un objeto de datos (como un mensaje o archivo, usualmente de tamaño variable y posiblemente grande) y así mapea el objeto a otro más pequeño el resultado, normalmente de tamaño fijo. Cualquier cambio en el objeto de entrada producirá, un resultado diferente. El **Sistema TID** utiliza **MD5**, “hash” criptográfico, versión mejorada de MD4, que produce un resultado de 128 bits.

(**) "Cut-and-paste attack "- **Ataque de recortar y pegar:**

Ataque activo contra la integridad del texto cifrado, consistente en reemplazar secciones del texto cifrado con otro texto cifrado, de modo que el resultado parece descifrarse correctamente, pero en realidad produce un texto llano fraguado por el atacante.

(***) "***Key encrypting Key" - clave para cifrar claves:***

Clave criptográfica que se usa para cifrar otras claves, sean éstas para datos u otras KEK.

2.1.b Identificación - Autenticación del origen de los datos.

Identificación y corroboración de que la fuente de los datos recibidos es quien declara serlo. ANF AC sigue el sistema ***"identity-based security policy" (*)*** y "***mandatory access control " (MAC) (**).*** Securiza el sistema mediante la combinación de hardware, software y conocimiento intelectual.

Este proceso se divide en tres etapas:

? ????**Identificación:** Se utiliza un identificador único y exclusivo de cada operador. **Tarjeta TID**, personal e induplicable (hardware = SmartCard), que precisa ser activada mediante clave secreta PIN (conocimiento intelectual). **Fichero TID**, precisa ser activado y desencriptado mediante clave secreta PIN y software exclusivo de ANF AC.

? ????**Verificación:** Se corrobora la relación del identificador con la entidad que acoge el módulo correspondiente del **Sistema TID**.

? ????**Atributos:** Se comprueban los atributos del operador en relación con la operación a realizar.

? ????**Autenticación:** En cada conexión se crea un protocolo único e induplicable para cada módulo de los que intervienen en la transacción. Los módulos se autentifican entre sí y se aseguran que la comunicación u orden recibida, nace en ese mismo instante y tiene un origen autorizado. Basado en ***"nonce"*** y ***"challenge-response" (***).***

***(*) "Identity-based security policy"* - política de seguridad basada en la identidad:**

Política de seguridad basada en la identidad y/o atributos de los usuarios, grupos de usuarios o entidades que actúan en nombre de los mismos y los objetos o recursos a acceder.

(**)* "*Mandatory access control" (MAC) - control de acceso obligatorio:

Servicio de control de acceso que impone una política de seguridad basada en comparar rótulos de seguridad (que indican cuán sensibles o críticos son los recursos) con habilitaciones de seguridad (que indican qué entidades del sistema pueden acceder a ciertos recursos). Es obligatorio en el sentido de que una entidad habilitada para acceder a cierto recurso no puede, por su sola voluntad, habilitar a otra para acceder al mismo.

(***)* "*Challenge-response" - desafío-respuesta:

Luego de presentar un desafío impredecible, verifica la identidad al recibir la información computada a partir de ese desafío.

2.1.c Detección.

El **Sistema de seguridad TID** no sólo detecta intentos de violación, sino que tiene la capacidad de impedir los ataques a "fuerza bruta". Además, en caso de que se pretenda utilizar **tarjetas TID** como instrumento de ataque, el sistema está capacitado para detectar la identidad del atacante e, incluso, puede provocar de forma remota la destrucción de la SmartCard utilizada.

- **Detección:** En caso de intento de acceso no autorizado, el sistema registra la dirección IP desde la que se produce el ataque y la identidad del atacante en caso de haber utilizado una **tarjeta TID o fichero TID**.

- **Desconexión:** Los intentos reiterados (máximo de tres), provocan el bloqueo de la SmartCard (caso de que se utilice) y la interrupción de la conexión.

2.2 Seguridad Administrativa.

La Seguridad Administrativa en ANF AC está regulada por un Plan de Seguridad que se ajusta al "Reglamento de medidas de seguridad de los ficheros que contengan datos de carácter personal" (BOE 25 de junio de 1999). Este Plan establece las medidas técnicas y organizativas al **nivel alto**, determinando el cumplimiento del Reglamento y de la LOPD.

El Plan incluye un documento de obligado cumplimiento para el personal con acceso a los ficheros con datos de carácter personal y a los sistemas de información, establece la forma de integración de la normativa y una actividad dedicada a la formación de los responsables de los ficheros y de seguridad.

El detalle del Plan de Seguridad Administrativa queda reseñado en el ANEXO II.

2.3 Seguridad de los equipos informáticos.

2.3.a Fluido eléctrico.

Todos los equipos informáticos están conectados a un estabilizador de corriente que impide que los ordenadores sufran variaciones eléctricas.

En caso de cortes eléctricos por parte de la compañía suministradora, el fluido eléctrico permanece gracias a un sistema de acumuladores que garantizan el servicio durante 24 horas; transcurrido ese periodo, y si el corte eléctrico permanece, el servicio queda asegurado mediante generadores eléctricos que se encuentran permanentemente en las instalaciones donde se ubican los equipo informáticos.

2.3.b Comunicaciones.

El ancho de banda a la Red (Internet), es contratado directamente a las primeras operadoras de comunicaciones.

La accesibilidad de los usuarios al sistema de ANF AC está garantizado mediante un sistema de equipos informáticos que trabajan en espejo; si la dirección principal web queda fuera de servicio, los usuarios pueden continuar atendiendo las necesidades esenciales: Revocación, verificación del estado de los certificados emitidos, firma electrónica y sellos de tiempo.

El sistema está dotado de un servicio de cifrado mediante las claves simétricas de 128 bits y del protocolo "Secure Soket Layer" (SSL) de 128 bits, (ANF AC es miembro de E-PKI Internacional). Un mecanismo de protección adicional de los sistemas de ANF AC es la implementación de dispositivos de protección comercial, denominados "firewalls". Los sistemas y dispositivos de protección ("firewalls") han sido configurados de conformidad con las políticas de seguridad de entidades especialistas en la materia y de reconocido prestigio.

2.3.c Hardware.

Todo el material informático utilizado para dar servicio en la red es estándar. ANF AC cuenta con ordenadores y copias de seguridad, para poder proceder a una sustitución prácticamente inmediata en caso de producirse un fallo en los equipos de atención al público.

La arquitectura de los equipos, está formada por una intranet. Una parte de los ordenadores está conectada a Internet; estos equipos son los que dan servicio Web, Ftp, y posibilitan los procesos de firma electrónica y sellos de tiempo. El resto de los equipos, no tienen conexión a Internet y sólo atienden operaciones llevadas a cabo en la propia intranet; estos ordenadores están destinados a asumir distintas operaciones: copias de seguridad, servicio base de datos, almacén de certificados, sellos de tiempo, códigos fuente de software ...etc.

Cada uno de los ordenadores empleados por ANF AC, servidores y estaciones de trabajo, tienen dedicación exclusiva. En ningún caso se realiza en ellos hospedaje de terceros ni suministro de cuentas de acceso.

Todos los ordenadores tienen instalados lectores especiales de tarjetas microprocesadas; estos lectores tienen almacenadas distintas microtarjetas que contienen información específica que permite autenticar los equipos en que se encuentran instalados, activar los servicios de firma electrónica y sellos de tiempo, así como almacenar claves criptográficas. Estas tarjetas únicamente pueden ser activadas por TID administradoras del sistema.

Todo el personal de ANF AC está dotado de tarjetas que lo identifican y determinan el nivel de accesibilidad que poseen.

2.3.d Software.

ANF AC sólo utiliza software original y de licencia autorizada y se responsabiliza de mantener su sistema operativo actualizado.

Los equipos de ANF AC tienen instalado un sistema de sincronización horaria. La sincronización se realiza con un reloj atómico instalado en EE.UU.
Todos los ordenadores tienen instalado el **Sistema de Seguridad TID**, que garantiza el blindaje de los equipos impidiendo accesos no autorizados. Este software, además, es el encargado de asumir los procesos criptográficos (parte de la información contenida en los equipos de ANF AC se encuentra permanentemente encriptada).

Todos los ordenadores de ANF AC tienen instalado el sistema de supervisión y vigilancia TID.

2.3.e Copias de seguridad.

Diariamente se realizan copias de seguridad del sistema. Se mantiene una copia de cada semana, del mes y un histórico semestral.

Las copias quedan depositadas en las instalaciones donde se encuentran los equipos informáticos, salvo la semestral que queda depositada en caja de seguridad bancaria.
El almacenamiento a largo plazo de los registros se realiza en medios WORM ("escribir una vez leer muchas").

Queda excluido de este sistema de copias de seguridad el Depósito de Almacén y Custodia (ver apartado 7.5), el cual regula la posibilidad de reconstrucción del Depósito mediante el sistema descrito en el apartado 7.5.5 f).

2.3.f Controles de seguridad informática.

ANF AC y sus AR utilizan sistemas de confianza para desarrollar sus respectivas funciones, de conformidad con la presente CPS, Anexos y Políticas de Certificación. Entre los componentes de los controles de seguridad informática se cuentan:

a) Cuentas de usuario individual para cada persona que integra el sistema operativo y el nivel de la administración de las solicitudes.
b) El mantenimiento de los servicios básicos en los "hosts" del sistema para permitir la prestación de servicios en conformidad con las presentes CPS.
c) La realización periódica de un monitoreo de seguridad y de auditorias de las cuentas de usuario y de los "hosts".
d) La comprobación periódica de recursos disponibles y valoración de nuevas necesidades.

2.4 Seguridad del personal.

2.4.1 Requisitos de formación y capacitación.

Todo el personal de ANF AC con acceso al sistema, cuenta con la formación adecuada para la función que tiene encomendada. Esta formación se establece bajo los siguientes criterios:

a) Ingeniero técnico en telecomunicaciones o informática: Servicios de programación, administración de equipos y software.
b) Licenciado en Derecho: Supervisión y comprobación de solicitudes de registro, revocaciones de oficio, derecho de acceso, rectificación y anulación de datos personales de usuarios.
c) Especialista en Protección de Datos y Seguridad Informática TID (Master universitario homologado): Administración y dirección de los distintos departamentos de ANF AC, así como de los operadores que en ellos operan.
Desarrollo y actualización de los planes de seguridad, así como cuantas funciones le son encomendadas en el área de Seguridad Administrativa.
d) Operador Sistema TID (Postgrado universitario homologado): Operador del sistema de seguridad TID y firma electrónica ANF AC.

Se han implementado procedimientos de evaluación del personal para verificar que las aptitudes, la experiencia y la capacitación de cada individuo integrado en ANF AC sean las adecuadas para el cargo ejercido. Con respecto al personal de la AR, cada persona que ejerce dicha función ha recibido la adecuada capacitación para desarrollar las funciones y los procedimientos específicos de su cargo.

2.4.2 Identificación y autenticación para cada función.

Toda persona que tiene funciones de confianza debe obtener autorización para realizarlas, incluida la autorización escrita de su supervisor directo. La asignación de funciones de confianza a un empleado debe ser adecuadamente documentada.

2.4.3 Frecuencia y requisitos de capacitación.

ANF AC desarrolla ejercicios de capacitación cada vez que el personal que integra la AC necesite obtener un mayor grado de conocimiento sobre cualquiera de sus funciones. Anualmente, se llevan a cabo un mínimo de 20 h. de formación en la materia que se considere necesaria para cubrir el adecuado desempeño de sus funciones y, en general, se realizará formación continua en materia de Seguridad Administrativa sobre los siguientes aspectos:

- Control de acceso.
- Gestión de soportes.
- Registro de Incidencias.
- Registro de Usuarios.
- Identificación y autenticación.
- Copias de respaldo y recuperación.
- Análisis de ficheros, datos y sistemas informáticos.
- Sistema de Seguridad TID.
- Seguridad Administrativa. Plan de Seguridad.

2.4.4 Sanciones a las operaciones no autorizadas.

El personal que realice operaciones no autorizadas estará sujeto a medidas disciplinarias de conformidad con la política de recursos humanos de ANF AC existente. Además, la AC tiene el poder de suspender de sus funciones al personal, si se considera que esta medida resulta necesaria para la seguridad de ANF AC.

2.4.5 Documentación entregada al personal.

Todo el personal de ANF AC recibe documentación vinculada con las descripciones, las funciones y las responsabilidades inherentes al cargo ocupado.

2.5 Seguridad física.

Los equipos informáticos que prestan servicio público (principal y espejos) se encuentran instalados en bunker perteneciente a primeras compañías operadoras nacionales y multinacionales.
Las instalaciones cuentan con la garantía AENOR según norma UNE-EN ISO 9002.
Entre las medidas de protección que posee el bunker y cuyo detalle exhaustivo no es posible efectuar en este documento por motivos de seguridad, destacar que:

- Las instalaciones cuentan con servicio de vigilancia y control por circuito de televisión interno permanente.

- La arquitectura y blindaje del edificio corresponden al diseño que comúnmente recibe la calificación de “bunker”.

- Las instalaciones se encuentran protegidas constantemente por personal perteneciente a empresa de seguridad autorizada por el correspondiente departamento del Ministerio del Interior. Este personal tiene relación detallada y actualizada de las personas que ANF AC autoriza a acceder al núcleo central donde se encuentran los equipos informáticos de ANF AC, confeccionan un registro del día y hora de entrada y salida, identidad y firma de la persona que accede y de cada una de las personas que la acompañan, entregando tarjeta de acceso personal. En ningún caso permite la extracción de ordenadores sin autorización expresa.

- El acceso al núcleo central se realiza superando distintos controles con tarjeta de identificación para apertura de puertas. El personal que accede se encuentra en todo momento acompañado por personal responsable de la administración del bunker y cualquier labor que se realiza sobre los equipos informáticos de ANF AC se realiza en presencia constante de un técnico perteneciente al personal responsable de la administración del bunker.

- Todas las instalaciones cuentan con sistemas de energía y aire acondicionado, que cumplen con las normas industriales, a fin de crear un entorno operativo adecuado.

- Todas las instalaciones cuentan con mecanismos de prevención destinados a reducir el efecto del contacto con el agua.

- Todas las instalaciones cuentan con mecanismos de prevención y protección contra incendios. Dichos mecanismos cumplen con las normas industriales.

2.6 Seguridad de las tarjetas TID.

Una vez que la tarjeta ha salido de la etapa de fabricación, ya no es posible el acceso a los datos físicamente.
Luego de la emisión de la tarjeta, y durante su período de vida, los datos serán accesibles a través de una estructura lógica.

2.6.a Estructura lógica de los datos.

Los datos están organizados en una estructura jerárquica de “directorios” y “sub-directorios”. La tarjeta TID cuenta con un “directorio raíz” denominado "Master File" (MF) debajo del cual existen varios niveles jerárquicos, dos tipos de archivos diferentes: archivos dedicados ("Dedicated Files" - DF) y elementales ("Elementary Files" - EF).
Cada uno de estos tipos de archivos descritos comprenden dos partes fundamentales: el encabezamiento y el cuerpo.

El perfecto conocimiento de la estructura del MF es esencial para poder iniciar el trabajo con el software de ANF AC; esta estructura es considerada materia de máxima seguridad.

2.6.b Control de acceso.

Cada uno de los archivos contenidos en la tarjeta posee un encabezamiento con información relacionada al mismo. Es esta información la que establecerá el estado del archivo y qué condiciones deben cumplirse para poder acceder a los datos que contiene. La base

fundamental del sistema de acceso es la presentación de los PIN ("Personal Identification Number") correctos.

2.6.c Condiciones de acceso.

Las condiciones de acceso a un archivo pueden separarse, en principio, en los siguientes niveles:

- Siempre ("Always" - ALW) - El acceso no tiene restricciones (consulta del ATR y código de autenticación de la tarjeta).
- Verificación de la fecha de caducidad de la tarjeta 1 / 2 / 3 y contador 1 (clave cautiva de TID).
- Verificación del titular de la tarjeta (activación por PIN).
- Verificación del propietario de tarjeta 1 ("Card Holder Verification" 1-CHV1). Puede accederse sólo cuando se presenta la clave de acceso, contador 2 CHV1correcta.
- Verificación de propietario de tarjeta 2 ("Card Holder Verification" 2-CHV2). Puede accederse sólo cuando se presenta la clave de acceso contador 3 CHV2correcta.
- Administrativo ("Administrative" - ADM) - La ubicación de estos niveles y los requerimientos que deben cumplirse, son responsabilidad de la autoridad administrativa.
- Nunca ("Never" - NVR) - El acceso está prohibido.

Es necesario aclarar que los niveles descriptos no son jerárquicos; la presentación de la clave correcta CHV1 no garantiza el acceso a un archivo que requiere la clave CHV2 y, mucho menos, la clave cautiva de TID, la cual tan sólo es válida para los procesos indicados.

2.6.d El PIN ("Personal Identification Number" - Número de Identificación Personal).

Estas claves se almacenan en archivos especiales; archivos que no pueden ser leídos y que validan por comparación interna si la clave introducida es correcta o no (en ningún caso sale el PIN de la tarjeta).

El PIN puede ser cambiado si se ingresa en la terminal el PIN anterior; sin embargo, el sistema operativo bloquea el acceso cuando se ingresan varios PIN incorrectos (3 errores consecutivos).

Una vez que el acceso a los archivos se bloqueó por el ingreso de un PIN erróneo (máximo 3 errores), sólo puede destrabarse con el ingreso de un PIN correcto. Las tarjetas bloqueadas por haber introducido tres PIN erróneos consecutivos se pueden desbloquear mediante la introducción de una clave PUK (esta clave nunca se facilita por el **Sistema de Seguridad TID** y debe desbloquearse en las propias instalaciones de TID).

2.6.e Caducidad.

Las tarjetas TID caducan automáticamente a los dos años de haber sido generadas.

2.6.f Datos de generación de firma.

ANF AC ha homologado tres modelos de creación de datos de generación de firma. Las Políticas de Certificación y el presente documento determinan si existe la obligación de utilizar uno u otro modelo.

Modelo SmartCard
Los datos de generación de firma únicamente pueden ser introducidos en la tarjeta TID por el dispositivo que ANF AC pone a disposición de sus usuarios. El dispositivo es el encargado de crear estos datos; ni ANF AC, ni tan siquiera el usuario, llegarán a conocer nunca los datos de generación de firma, resultando absolutamente imposible que ninguna otra persona pueda suplantar la firma del usuario; únicamente él, en posesión de la tarjeta original y en conocimiento de la clave secreta de activación PIN, puede procesar una firma.
El titular del certificado se generá de forma autónoma su par de claves, sin intervención de terceros.

Modelo SmartCard Critográfica
Se utilizan tarjetas con Chip integrado, con coprocesador matemático, capacidad criptográfica y que tienen integrados los algoritmos RSA necesarios para que la propia tarjeta pueda crear los datos de generación de firma internamente.
Ni ANF AC, ni tan siquiera el usuario, llegarán a conocer nunca los datos de generación de firma, resultando absolutamente imposible que ninguna otra persona pueda suplantar la firma del usuario; únicamente él, en posesión de la tarjeta original y en conocimiento de la clave secreta de activación PIN, puede procesar una firma.
El titular del certificado se generá de forma autónoma su par de claves, sin intervención de terceros.

Modelo fichero TID
Los datos de generación de firma son introducidos en un fichero electrónico que se encuentra cifrado bajo doble llave (clave secreta del software de la Autoridad de Certificación y clave PIN del usuario. Se pone a disposición del usuario un software “dispositivo” que es el encargado de crear estos datos, los algoritmos RSA empleados se encuentran integrados en este software ; ni ANF AC, ni tan siquiera el usuario, llegarán a conocer nunca los datos de generación de firma, resultando absolutamente imposible que ninguna otra persona pueda suplantar la firma del usuario; únicamente él, en posesión de software licenciado por ANF AC y en conocimiento de la clave secreta de activación PIN, puede procesar una firma.
El titular del certificado se generá de forma autónoma su par de claves, sin intervención de terceros.

2.7 Seguridad del fichero TID.

Los datos de generación de firma son creados por el dispositivo que ANF AC pone a disposición de sus usuarios. El dispositivo es el encargado de crear estos datos; ni ANF AC, ni tampoco el usuario, llegarán a conocer nunca los datos de generación de firma. El dispositivo crea automáticamente un fichero electrónico que contiene los datos encriptados. Es ciertamente difícil que otra persona pueda suplantar la firma del usuario; no obstante, el fichero electrónico, al contrario que la tarjeta TID, sí que es duplicable y, por tanto, el mayor peso de la seguridad recaerá en el conocimiento intelectual que presupone saber o desconocer la contraseña de activación.

2.8 Seguridad del PC usuario.

Exclusivamente para usuarios en posesión de tarjetas TID con licencia de instalación.

ANF AC pone a disposición de sus usuarios software de seguridad personal:

- Blindaje capaz de detectar intentos de violación y actuar de forma automática en el mismo instante en que se extrae o introduce la tarjeta TID.

- El blindaje impide el uso del ordenador hasta que no se introduce una tarjeta autorizada y se activa mediante el PIN secreto. Esta protección se extiende al propio sistema de seguridad, el cual sólo puede ser desactivado si se accede con una tarjeta autorizada.

- Protección criptográfica, capaz de encriptar automáticamente importantes volúmenes de ficheros y datos, a selección del usuario de ANF AC.

2.9 Seguridad criptográfica.

La infraestructura de clave pública PKI de ANF AC es de 128 bits y establece los servicios y protocolos necesarios para dar soporte a las aplicaciones de cifrado fuerte enmarcado en los sistemas de clave pública (ver sección 4.13).

La clave de firma de ANF AC tiene una longitud de 2048 bits. Algoritmo de Firma sha1RSA.
Los Pares de Claves de firma de los signatarios de ANF AC son RSA de 1024 bits. Se emplea software criptográfico para su generación.

La clave de encriptación de comunicaciones entre módulos es de 1043 bits. Idéntica longitud se emplea en las comunicaciones a través de Internet, pudiendo operar, además, según la actividad desarrollada sobre línea SSL Se emplea software criptográfico exclusivo de ANF AC.

Para la comunicación SSL se emplea supercertificado SSL de 128 bits. de Thawete (filial Verisign).

El resumen, el “hash” es de 128 bits.

3. Estándares y homologación.

3.1 15408 v.2.1.

Se sigue el estándar ISO 15408 versión 2.1 para criterio común y las especificaciones del (ITSEC) de la Unión Europea. El modelo SmartCar cuenta con este certificado de acreditación internacional Common Criteria emitido por el laboratorio alemán Bundesamt für Sicherheit in der Informationstechnik

3.2 ISO 7816.

Las tarjetas TID que utiliza ANF AC, siguen este estándar internacional.

3.3 PC-SC.

El software de usuario desarrollado por ANF AC cumple este estándar internacional.

3.4 ISO/IEC X-509 v.3.

Los certificados emitidos por ANF AC cumplen este estándar internacional. Normas internacionales en la materia de acuerdo con la (ISO) y las especificaciones (IEC). Y según lo especificado en la Versión 3 de la recomendación UIT-T X.509 de fecha de junio de 1997 (ISO/IEC 9594-8 de 1997) definida por la Unión Internacional de Telecomunicaciones, Sector de Normalización.

Las extensiones utilizadas en los certificados CDIP emitidos por ANF AC están especificadas en sus respectivas Políticas de Certificación. En certificados AC identificadas en el apartado 1.2.

3.5 Protocolos de Sellado de Tiempo.

El Sello de Tiempo de ANF AC cumple las definiciones realizadas por Haber y Stornetta en su artículo: “How to Time-stamp a Digital Document”, propiedades básicas:

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.

3.6 Plug and Play.

Todos los dispositivos digitales que pone a disposición de sus usuarios ANF AC son dispositivos "Plug and Play" y, por tanto, reconocidos automáticamente en plataformas Windows. Cumplen con las especificaciones "Plug and Play" (PnP) para dispositivos COM (comunicación serie) Versión 1.0 de Microsoft.

3.7 Homologación de dispositivos por ANF AC.

Con el fin de garantizar a la comunidad de operadores de esta PKI, unos niveles básicos de seguridad y operatividad entre todos ellos, se establece que todos los dispositivos que utilicen deben de ser previamente homologados por ANF AC. Así mismo, y con el fin de garantizar la mejor integración posible del sistema de firma electrónica en los procesos productivos y administrativos, y siendo conscientes de la amplia gama de tipologías empresariales y profesionales hoy en día existentes, esta AC facilitará tecnología base y asesoramiento técnico a los departamentos informáticos de las ER que se lo requieran, con el fin de crear sus propios dispositivos o integrar los existentes en programas personalizados.

Para poder utilizar y distribuir el software que desarrollen, las ER deberán solicitar la correspondiente homologación con el fin de garantizar el correcto funcionamiento de esta PKI.
La solicitud deberá tramitarse ante la propia ANF AC, la cual la someterá a una comisión formada por responsables del Departamento técnico y jurídico de esta AC.

Se procederá a otorgar la homologación solicitada cuando el dispositivo cumpla:

a) Lo establecido en la legislación vigente.
b) Los criterios y procedimientos reseñados en este documento, sus Anexos y Políticas de Certificación.
c) Ser operacionalmente compatibles con el resto de dispositivos homologados por ANF AC.

La propia evolución de los servicios de certificación de ANF AC, puede conllevar la necesidad de adaptar los dispositivos homologados a los nuevos requerimientos que se establezcan en virtud de la emisión de nuevas versiones de esta CPS, sus Anexos y Políticas de Certificación.

Los nuevos criterios serán siempre objetivos, sobre la base de requerimientos de carácter legal o que presupongan una mejora en la prestación de los servicios de certificación. En caso de producirse nuevos criterios de homologación, todos los dispositivos homologados deberán adaptarse o, en su caso, ANF AC deberá retirarles la homologación otorgada.

Los dispositivos homologados por esta AC figuraran publicados en http://www.anf.es/AC/dispositivos.asp

3.8 Dispositivos seguros de creación de firma electrónica.

Los dispositivos deben de estar homologados por ANF AC y serán suministrados por esta AC a sus Usuarios de forma gratuita.

Entre otros, son dispositivos homologados por ANF AC los integrados en el **Sistema de Seguridad TID,** según la modalidad de instrumento empleado como contenedor de los datos de generación de firma.

Cabe reseñar que cuando el contenedor de los datos de generación de firma es la modalidad SmartCard Criptográfica, el proceso de firma se realiza en el interior de la tarjeta. En el resto de las modalidades de contenedor, las comunicaciones entre los dispositivos se encuentran blindadas de acuerdo con el protocolo establecido en el presente documento y sus anexos de seguridad.

Tanto en la producción de resúmenes de documento (hash) como en la de la firma electrónica propiamente dicha, su desarrollo se basa en la aplicación de algoritmos públicamente conocidos y de los que son de general aceptación por la comunidad internacional. En la actualidad ANF AC emplea los algoritmos reseñados en el presente documento.

3.9 Dispositivo de verificación de firma.

El dispositivo debe de estar homologado por ANF AC y será suministrado por esta AC a sus Usuarios de forma gratuita.

Entre otros, es dispositivo homologado por ANF AC los integrados en el **Sistema de Seguridad TID.**

El proceso de verificación se basa en la aplicación de algoritmos públicamente conocidos y de los que son de general aceptación por la comunidad internacional. En la actualidad ANF AC emplea los algoritmos reseñados en el presente documento.

3.10 Dispositivo de generación de datos de creación de firma.

ANF AC no genera datos de creación de firma. Esta AC pone a disposición de sus usuarios el dispositivo de generación de datos de creación de firma, quedando así plenamente garantizada la confidencialidad del proceso.

El dispositivo debe de estar homologado por ANF AC y será suministrado por esta AC a sus Usuarios de forma gratuita. Entre otros, es dispositivo homologado por ANF AC los integrados en el **Sistema de Seguridad TID.**

3.11 Servidor de Tiempo “stratum 1”.

ANF AC cuenta con un Servidor de Tiempo “stratum 1” para sincronizar su Servidor Digital de Sellos de Tiempo. La comunicación entre ambos servidores se efectúa de acuerdo con el protocolo de seguridad descrito en el apartado 2.1 de este documento.

Este servidor utiliza protocolo de comunicaciones NTP (“Network Time Protocol”). NTP utiliza como tiempo de referencia UTC (“Universal Time Coordinated”).

El nivel de operación es Stratum 1 porque el servidor obtiene sus señales de tiempo a partir de un equipo hardware dedicado (fuente de tiempos *), el cual está sincronizado con la escala UTC con una precisión dentro del microsegundo. El servidor de tiempo tiene instalado un GPS (**).

Stratum 1 es considerado internacionalmente como máximo nivel de sincronización.

(*) Fuente de tiempos: El reloj hardware del servidor de tiempo nos permite conocer el tiempo UTC. Este reloj, que funciona con un oscilador de cuarzo, se mantiene sincronizado cada segundo con las señales de referencia procedentes de varios satélites de la constelación **Navstar (***)** que constituye el alma del sistema GPS y que son visibles desde la ubicación geográfica del servidor.

(**) GPS: Es un sistema de posicionamiento global basado en una constelación de veinticuatro satélites artificiales que orbitan alrededor del planeta en seis órbitas distintas. Cada uno de ellos dispone a bordo de dos relojes atómicos de cesio que en todo momento marcan el tiempo universal y emiten una señal horaria marcando el comienzo de cada segundo de tiempo universal.

(***) Navstar: Este sistema está controlado por diez estaciones de seguimiento terrestres dispuestas alrededor del planeta. Cada una de ellas dispone de varios relojes atómicos sincronizados según UTC. Este proceso de sincronización mantiene la sincronía global del sistema en el rango de los 130 nanosegundos.

4. Certificados ANF AC.

ANF AC ha realizado todos los trámites necesarios para garantizar de forma fiable todos los datos contenidos en cualquier certificado antes de su activación. En certificados en los que el signatario haya consignado un seudónimo, ANF AC garantiza que ha constatado de forma fiable su verdadera identidad y conserva la documentación que lo acredita. ANF AC regula su operativa de acuerdo a lo establecido en la ley española.

ANF AC garantiza la imposibilidad de firmar cuando el certificado no esté activado y que **los efectos de revocación o suspensión de un certificado son inmediatos.**

ANF AC garantiza la confidencialidad y privacidad de sus usuarios. Sus datos personales son sólo accesibles por personas por ellos autorizadas.

ANF AC no emitirá un certificado sin el consentimiento del solicitante del certificado. El consentimiento para la emisión se entiende prestado desde el momento en que se realiza la solicitud del certificado.

ANF AC se reserva el derecho a negarse a emitir un certificado a cualquier persona, a su discreción, sin incurrir en responsabilidad alguna por cualquier pérdida o lucro cesante que pueda producir tal negativa.

Los certificados de ANF AC únicamente pueden ser solicitados por personas mayores de edad para ser utilizados en su propio nombre, o en representación de terceras personas físicas o jurídicas. La generación de los datos de creación de firma por parte del usuario, y la tramitación de la correspondiente solicitud del certificado, presupone su aceptación y consentimiento para la emisión del certificado por parte de ANF AC.

4.1 Contenedores homologados TID.

Los datos de creación de firma únicamente pueden ser almacenados en contenedores homologados por ANF AC. Esta Autoridad de Certificación reconoce por la máxima seguridad y fiabilidad que ofrecen, los siguientes:

- ***Tarjeta microprocesada TID, Tarjeta criptográfica TID y Fichero encriptado TID.***

Son propietarios de los contenedores homologados TID, las personas físicas o jurídicas a las que representa el signatario o, caso de actuar en su propio nombre, el propio signatario.

4.1.a Dispositivo de Generación del Contenedor TID.

ANF AC facilita de forma gratuita este dispositivo, el cual tiene la capacidad de generar el contenedor homologado TID. Durante el proceso se requiere del propietario que facilite los datos de la persona que será el titular del contenedor y, por tanto, signatario de ANF AC.
Estos datos son sobre los que, posteriormente, se realizará el proceso de solicitud, identificación y autenticación por parte de la AR. Clases de dispositivos:

a) Tarjeta TID y Tarjeta Criptográfica TID:
Estos dispositivos se encuentran integrado en el Sistema de Seguridad TID.

b) Fichero TID:
La generación del fichero TID se realiza por el Dispositivo de Generación de Datos de Creación de Firma.

4.1.b Obtención de Licencia de generación de contenedor.

De carácter gratuito.

Durante el proceso de generación, se crea un fichero electrónico que permite Licenciarse en línea con el fabricante del **Sistema TID**, NetMCP Tecnology, SL.

Es imprescindible remitir este fichero al fabricante para obtener una licencia de generación. Esta licencia no sólo habilita al contenedor para procesar un certificado de ANF AC ante la AR, sino que permite al fabricante dar asistencia técnica y remitir nuevas versiones de su software.

4.2 Dispositivo de generación de datos de creación de firma.

Las claves de los Usuarios **se generan bajo su exclusivo control** utilizando este dispositivo que ANF AC pone a su disposición. No precisa la intervención de ningún tercero, quedando así garantizado el "no repudio" del signatario y se establece la necesaria confiabilidad en el sistema, tanto de él mismo, como de los receptores.

Esta Autoridad de Certificación, ni sus empleados, tienen la posibilidad, ni la oportunidad, de copiar ni de almacenar, en ningún momento, los datos de creación de firma.

4.2.a Difusión.

ANF AC pone a disposición gratuita de sus usuarios el dispositivo de generación de datos de creación de firma electrónica. Las actualizaciones de este software son igualmente gratuitas y se encuentran disponibles en:

http://www.anf.es/TID/software/

4.2.b Instalación.

El usuario de ANF AC debe de proceder a la instalación del dispositivo siguiendo sus instrucciones técnicas.

4.2.c Procedimiento.

Este dispositivo genera automáticamente el par de claves asimétricas necesarias para poder procesar con total garantía técnica firmas electrónicas avanzadas.
.
Los datos de generación de firma son introducidos automáticamente en uno de los contenedores homologados TID. Simultáneamente, el dispositivo crea un autocertificado de usuario en el cual constan los datos personales por él reseñados, además de un número de identificación único y exclusivo para ese certificado (certificado de petición - request).

Para posibilitar su activación, el usuario deberá remitir a ANF AC el autocertificado, así como tramitar su identificación y autenticación ante la Autoridad de Registro. El usuario puede remitir el autocertificado utilizando el propio dispositivo de creación de firma o a la dirección de correo electrónico:

ac@anf.es

4.3 Modalidades:

Cada tipo de certificado cuenta con su respectiva Política de Certificación, salvo el certificado de ANF Autoridad de Certificación que se regula de acuerdo con los criterios establecidos en el presente documento, sus Anexos y Políticas de Certificación. ANF AC emite las siguientes clases de certificados:

- Certificados CDIP (Certificado Digital Identificación Personal):

  a) Certificado de alta seguridad. Código 1

  c) Certificado de entidad. Código 2

  d) Certificado de Autenticación. Código 3

- Certificados ANF AC:

  e) ANF Autoridad de Certificación. Código 4

  f) ANF Autenticación. Código 5

- Certificados de Administración Pública

  Esta modalidad de certificados puede estar sometida a Disposiciones Adicionales incorporadas a esta CPS como anexos a la misma.
  Los certificados emitidos bajo esta modalidad, poseen su propia Política de Certificación. Cada Política de Certificación establece código de identificación, denominación del certificado, sus normas de uso y especifica, caso de existir, la vinculación a determinada Disposición Adicional.

4.4 Identificación y autenticación.

Este apartado se desarrolla de manera específica para cada tipo de certificado a través de su respectiva Política de Certificación. Registro inicial, de forma general se establece:

4.4.1 Tipos de nombres.

ANF AC ha establecido una sola jerarquía de nominación, sobre la base del formulario de Nombre Distintivo (DN). La AR (Autoridad de Registro) velará de que no puedan emitirse certificados con el mismo nombre de Usuario.

.

4.4.2 Seudónimo.

Los Usuarios podrán solicitar de ANF AC que el certificado sea emitido con un seudónimo una vez que la AR haya confirmado la identidad cierta del signatario.

Podrá ser rechazado por la AR seudónimos que, por similitud a otros ya existentes, puedan inducir a confusión; así mismo se podrán rechazar seudónimos peyorativos, de carácter grosero, que correspondan a marcas comerciales conocidas o cuyo significado considere la AR inadecuado para esta AC.

4.4.3 Exclusividad de nombres.

Todos los Signatarios que participan en la PKI de ANF AC se identifican inequívocamente en la jerarquía de nominación. Personas con idéntico nombre o Usuarios en posesión de varios certificados, tendrán registrado en su certificado DN = su nombre más el número que por orden cronológico le corresponda. Por ejemplo:

Juan Pérez García	= Primer solicitante
Juan Pérez García (1)	= Segundo solicitante
Juan Pérez García (2)	= Tercer solicitante y sucesivos...
Juan Pérez García (3)	

4.4.4 Identidad individual de los Signatarios.

Todos los Signatarios que participan en la PKI de ANF AC, son personas físicas, mayores de edad y plenamente capacitadas para asumir las obligaciones y responsabilidades que son inherentes a la posesión y uso de un certificado de ANF AC.

4.4.5 Identidad de los representados.

Puede tratarse de personas físicas o jurídicas. Respectivamente, estas personas tienen que ser mayores de edad o estar legalmente constituidas y, en ambos casos, plenamente capacitadas para poder asumir las obligaciones y responsabilidades derivadas de la representación que otorgan a sus signatarios.

4.5 Revocación y suspensión de certificados.

4.5.1 Procedimiento.

Los procedimientos que posibilitan al signatario o la persona a la que representa, para proceder a la revocación o suspensión del certificado son:

Mediante conexión telemática directa al Registro de Certificados:

Las establecidas en las secciones 4.12.b y 4.12.c del presente documento.

Mediante comunicación con ANF AC:

a) Mediante correo electrónico o correo tradicional, formulando la correspondiente solicitud en la que se reseñará (login y password) e identificador del certificado.
b) Mediante llamada telefónica a la Oficina de Atención al Cliente, formulando la correspondiente solicitud y en la que se deberá indicar (login y password) e identificador del certificado.

c) Mediante llamada telefónica a la Oficina de Atención al Cliente, declarando haber olvidado su login y password. Siguiendo el procedimiento especificado en el apartado 4.12.c.3 b) del presente documento.
d) Mediante presencia física en la Oficina de Atención al Cliente, identificándose mediante Documento Nacional de Identidad, Pasaporte o tarjeta de residente vigente.

4.5.2 Revocaciones.

Las revocaciones son definitivas y presupone la pérdida de eficacia de los certificados e impide al usuario el uso legítimo del mismo.

La revocación tiene efectos inmediatos, imposibilitando que el Dispositivo seguro de creación de firma electrónica pueda procesar esta función.

La referencia de todo certificado revocado será incluida en el Registro de Certificados (ver 4.12), teniendo como efecto la información a terceros que lo consulten, de que el certificado ha sido revocado.

Tiene la capacidad de revocar los certificados el signatario, persona a la que representa o la propia AC y la Autoridad de Registro que tramitó su identificación. Cuando la revocación no sea solicitada por el signatario, ANF AC le notificará este hecho mediante correo electrónico remitido a la dirección que hizo constar el usuario en su solicitud de certificado.

Se procederá a la revocación del certificado a petición del signatario, la persona a la que representa, ANF AC o AR por incumplimiento de las obligaciones impuestas en esta CPS (ver 9.2), sus ANEXOS, Políticas de Certificación o en cualquiera de los supuestos que establece la legislación vigente.

En cualquier caso sí:

a. Ha existido pérdida, robo, modificación, divulgación no autorizada u otro compromiso de la clave privada asociada al certificado.
b. Se conoce o se tienen motivos para creer razonablemente que uno de los hechos representados en el certificado es falso.
c. Se conoce que alguno de los requisitos de emisión del certificado no fue cumplido.

d. El sistema de certificación se vio comprometido de modo tal que afecta a la fiabilidad del certificado.
e. Cese en la actividad de la AC, salvo que los certificados sean transferidos a otro prestador de servicios de certificación.
f. Cuando el certificado ha sido emitido en fecha posterior a que la clave privada de la ANF AC se haya visto comprometida y por tanto revocada.

4.5.3 Suspensiones.

Las suspensiones presuponen la pérdida de eficacia de los certificados durante el periodo en que está vigente esta suspensión e impide al usuario el uso legítimo del mismo.

La referencia de todo certificado en suspenso será incluida en el Registro de Certificados (ver 4.12), teniendo como efecto la información a terceros que lo consulten, de que el certificado ha sido suspendido.

Se procederá a la suspensión del certificado a petición del Signatario, la persona a la que representa o en cualquiera de los supuestos que establece la legislación vigente y en los especificados en su respectivas Políticas de Certificación. Cuando la suspensión no sea solicitada por el signatario, ANF AC le notificará este hecho mediante correo electrónico remitido a la dirección que hizo constar el Usuario en su solicitud de certificado.

En cualquier caso sí:

- Se sospecha la pérdida, robo, modificación, divulgación no autorizada u otro compromiso de la clave privada asociada al certificado.

- Si existe duda sobre la veracidad de alguno de los datos representados en el certificado.

Reactivación : La reactivación de un certificado suspendido deberá llevarla a cabo el mismo operador que provocó la suspensión. O ANF AC, a instancias del Signatario, si éste acredita de forma suficiente que las causas que provocaron la suspensión han desaparecido.

4.5.4 Acreditaciones.

Independientemente del procedimiento seguido para efectuar la revocación o suspensión del certificado por parte del Usuario o persona a la que representa, éstos podrán requerir de ANF AC que le sea expedida de forma inmediata acreditación del estado de suspensión o revocación en que se encuentra su certificado. Esta acreditación será firmada por ANF AC, estampando sello de tiempo.

Si el procedimiento ha sido telemático, la acreditación se descargará vía Web en el ordenador del Usuario; si se ha realizado a través de la Oficina de Atención al Cliente, se remitirá por e-mail a la dirección electrónica de esta persona.

4.6 Solicitud de Certificados.

Este apartado se desarrolla de manera específica para cada tipo de certificado a través de su respectiva Política de Certificación.

4.7 Caducidad y renovación.

4.7.1 Caducidad.

Los certificados caducan a los dos años de su creación o por caducidad del Contenedor homologado TID. La caducidad de un certificado es definitiva y presupone su pérdida de eficacia e impide al usuario el uso legítimo del mismo.

4.7.2 Renovación.

Los certificados pueden ser renovados por un nuevo y único periodo de dos años, transcurrido el cual el usuario deberá efectuar un nuevo proceso de solicitud de certificado.

El proceso de renovación se realiza telemáticamente en:

http://www.anf.es/TID/administracion/

El usuario deberá firmar la solicitud de renovación y pagar las correspondientes tasas (ver 4.11). Sólo pueden ser renovados certificados activos; los certificados caducados no son renovables.

4.8 Atributos.

Definen documentos y operaciones homologadas por esta AC. Su exclusión en el momento de generar el certificado incapacita al signatario para poder firmarlos. Así mismo se determina el importe límite de firma expresado en € (euros).

No se pueden establecer restricciones de atributos que presupongan la imposibilidad de gestionar los servicios de Almacén y Custodia (apartado 7.5), Registro de Entrada de Documentos (apartado 8) o procesar firmas en “Modo Autofirma” (apartado 7.1.c b) a certificados emitidos en la modalidad “Certificado de Autenticación” o “ANF Autenticación”.

Los atributos son configurados por el propietario del contenedor TID y es obligación del receptor la comprobación de los mismos para establecer la capacidad de firma de un signatario, teniendo en consideración lo expresado en el párrafo anterior. Cuando el receptor es una ER, el dispositivo seguro de generación de firma homologado por ANF AC tiene la capacidad de procesar esta comprobación en tiempo real y de forma automática, siempre y cuando la ER haya codificado de forma correcta sus páginas WWW.

4.9 Limitaciones de uso.

Las reseñadas en sus respectivas Políticas de Certificación.

4.10 Condiciones de uso.

Para poder utilizar los certificados expedidos por ANF AC se requiere:

a) Que el certificado esté activado por la AC.
b) Que el contenedor de datos de creación de firma esté activado por el signatario.
c) Utilizar un Dispositivo seguro de creación de firma electrónica homologado por ANF AC.
d) Debe de estar conectado a Internet.

4.11 Tasas de activación y renovación.

Este apartado se desarrolla de manera específica para cada tipo de certificado a través de su respectiva Política de Certificación.

4.12 Registro de Certificados.

El Registro de Certificados se localiza en la siguiente URL :

http://www.anf.es/AC/Registro.asp

4.12.a Contenido.

a) Documental:

Documentación original relativa al proceso de identificación y autenticación que acredita la identidad de los usuarios de ANF AC.
Documentación o informes realizados por el Departamento Jurídico de ANF AC o por la Autoridad de Registro.
En general, escritos y documentos relacionados con los usuarios de ANF AC y sus certificados.

b) Informatizado:

World Wide Web, acceso a base de datos**:** Identificador del certificado, fecha de emisión, fecha de caducidad, fecha de renovación, fecha de activación, revocación (fecha y causa), histórico de suspensiones y reactivaciones (fecha y causa), atributos, importe límite de firma electrónica, estado (activado, caducado, revocado, suspendido), Nombre y apellidos del signatario y seudónimo. Así mismo, registrará la dirección de correo electrónico, DNI, dirección personal, población, provincia, país, teléfono y cuantos datos consten caso de tratarse de un certificado de entidad, o el usuario actúe en representación de terceras personas físicas o jurídicas.
Directorio X500: Repositorio donde se almacenan copias de los certificados de los Usuarios de ANF AC y los propios certificados de AC de ANF AC.

d) CRL: Si bien la tecnología utilizada por esta AC no hace preciso el empleo de "Listas de Certificados Revocados", ANF AC mantendrá este tipo de ficheros cuando la legislación vigente así lo requiera.

4.12.b Accesibilidad.

Se permitirá el acceso al Registro de Certificados en todos los supuestos que contempla la legislación vigente, sobre firma electrónica. El sistema de accesibilidad telemático es:

Los Usuarios de ANF AC pueden acceder de forma telemática y en tiempo real, al contenido informatizado completo de sus respectivos datos. El Usuario debe de tener la posibilidad de configurar el proceso de seguridad que controla el acceso a esta información en base a las siguientes posibilidades:

a) Exclusivamente mediante Tarjeta TID.
b) Habilitando el sistema de login y contraseña
(ver efectos en sección 4.12.c.2).

El contenido documental original puede ser accesible concertando visita personal con la Oficina de Atención al Cliente. El usuario deberá acreditar de forma suficiente su identidad en el momento de la personación en las oficinas centrales de ANF AC. Los usuarios podrán solicitar por escrito, acreditando su identidad de forma suficiente, copia firmada por ANF AC de la documentación relativa al proceso de identificación y autenticación, así como de los escritos intercambiados con la AC, corriendo a su cargo los gastos de confección y envío, el cual se realizará contra reembolso y certificado con acuse de recibo.

Las consultas de terceros se realizará determinando de forma concreta identificados del certificado o login del signatario, no son permitidas consultas por aproximación. Pueden acceder de forma telemática y en tiempo real, al siguiente contenido:

> Identificador del certificado, fecha de emisión, fecha de caducidad, fecha de renovación, fecha de activación, fecha de revocación, fechas de suspensión y reactivación, estado (activado, caducado, revocado, suspendido), atributos, importe límite de firma electrónica, nombre y apellidos del signatario o seudónimo (según la identidad que conste consignada en el certificado). Así mismo registrará, caso de que conste en el certificado, la dirección de correo electrónico, DNI, dirección personal, población, provincia, país, teléfono y cuantos datos consten caso de tratarse de un certificado de entidad, o el usuario actúe en representación de terceras personas físicas o jurídicas. Pueden descargarse copia del certificado.

Personal autorizado de ANF AC y AR pueden acceder de forma telemática y en tiempo real, al contenido del Registro de Certificados y efectuar labores de mantenimiento dentro de las funciones que le son encomendadas. El control de acceso se realizará exclusivamente mediante tarjetas TID y utilizando el Sistema de Seguridad e identificación TID.

4.12.c Claves de Identificación reconocidas.

Cada operador frente al sistema informático cuenta con sus propias claves de acceso: login y contraseña.
Cada certificado cuenta con un código único y exclusivo que lo identifica en el Registro de Certificados.
El nombre y apellidos de cada Usuario junto con su número de: Documento Nacional de Identidad o Pasaporte o tarjeta de residencia, es un código de identificación único y exclusivo que lo identifica en el Registro de Certificados.
El conjunto de respuestas correctas a las preguntas que configuró el operador en su momento, es una clave de acceso.

4.12.c.1 Creación:

a) Por el propietario:
Durante el proceso de generación del contenedor homologado TID realizado personalmente por su propietario, éste crea su login y contraseña de acceso al Registro de Certificados. Durante el mismo proceso puede configurar los datos que permitirán vía Web recordarle sus claves por el sistema de preguntas–respuestas(hasta un máximo de cinco preguntas y sus respectivas respuestas).

b) Por el signatario:

En el caso de que el titular del certificado no sea el propietario del contenedor, es decir, que actúe en representación de éste, el dispositivo de generación de datos de creación de firma posibilita que el signatario pueda crear su propio login y contraseña, así como configurar el sistema de preguntas - respuestas (hasta un máximo de cinco preguntas y sus respectivas respuestas).

4.12.c.2 Efectos de la configuración:

La accesibilidad al sistema mediante claves de identificación por parte de los Usuarios, viene determinada por el estado de activación o desactivación en que cada operador lo configura.

Si está activado, el usuario puede acceder al Registro de Certificados, visualizar completamente sus datos personales e, incluso, efectuar las labores de mantenimiento, utilizando estas Claves.

Si está desactivado, podrá utilizar estas claves para acceder al Registro de Certificados con la única posibilidad de revocar o suspender su certificado.

En ambos casos, activado o desactivado, la utilización del login junto con el identificador del certificado, determina ante el sistema que se trata de una persona autorizada por el signatario (ver apartado 4.12.b).

4.12.c.3 Sistema de Preguntas y Respuestas:

En caso de olvido de login y contraseña, el sistema informático tiene la capacidad de recordar al operador estas claves de identificación.

a) Procedimiento telemático:
El operador debe de introducir su nombre, apellidos y el nº de documento que reseñó al generar el Contenedor homologado TID y responder correctamente a las preguntas que le efectuará el sistema.

b) Mediante llamada a la Oficina de Atención al Cliente:
Personal de esta Oficina seguirá idéntico protocolo al procedimiento telemático antes descrito. Efectuando las preguntas e introduciendo las respuestas.

4.12.c.4 Modificación:

El usuario mediante su tarjeta TID o utilizando login y contraseña (si está activada esta modalidad), puede modificar cuando lo desee los datos relativos a las claves de identificación o reconfigurar el sistema de claves de identificación (activarlo o desactivarlo).

4.12.d Administración.

4.12.d.1 Administración de los registros.

El Usuario de ANF AC o la persona física o jurídica a la que representa, tienen la capacidad de desactivar temporalmente (suspender) o definitivamente (revocar) siempre que lo deseen su certificado. Los servidores Web de esta AC posibilitan el acceso directo al Registro de Certificados para la desactivación o reactivación (en caso de suspensión) de su certificado, siendo los efectos de suspensión o revocación inmediatos.
El resto de operaciones de administración están reservadas a personal autorizado por ANF AC o las AR.

4.12.d.2 Expedición de acreditaciones.

Sobre el sistema informático, esta AC tiene la capacidad de autenticar "on line" páginas Web, información en base de datos, formularios ...etc. estampando sobre ellos la firma electrónica avanzada de esta AC y sello de tiempo. Estas acreditaciones son gratuitas.

Sobre ficheros firmados por signatarios de esta AC, ANF AC expedirá a cualquier persona o entidad que se lo solicite, un informe que determine sí:

1) La firma ha sido creada durante el periodo operativo de un certificado válido,
2) La firma digital puede ser adecuadamente verificada por confirmación de la cadena de sellos de tiempo emitidos por ANF AC,
3) La firma digital corresponde al documento al que se la vincula.
   Y haga constar:
   a) el día y la hora en que se firmó el documento.
   b) la identidad del firmante.
   c) tipo de certificado al que se vincula la clave privada utilizada.
   d) atributos y limitaciones de uso.

Esta labor realizada por la AC correrá a cargo del solicitante.

4.12.e Mantenimiento de los datos.

ANF AC mantendrá los datos y documentos relativos a la emisión de certificados, evolución e incidencias, por un plazo mínimo de 5 años, sin perjuicio del derecho de cancelación sobre aquellos datos de carácter personal que establezca la legislación vigente.

4.13 Difusión Certificados CDIP (Certificado Digital de Identificación Personal).

ANF AC se encargará de difundir copia de los Certificados CDIP a todas las Entidades Reconocidas por esta AC. La transmisión se realizará una vez al día y utilizando el Sistema de Transmisión Segura de los Servicios de Comunicación TID.

ANF AC facilitará copia de los Certificados CDIP a Personas Autorizadas por los Usuarios (ver 4.12.b) mediante alguno de los siguientes sistemas:

a) Mediante conexión al Registro de Certificados, utilizando el login o el identificador del certificado.

b) Introduciendo en el navegador la dirección URL http://www.anf.es/certificado.exe?clave=login del Usuario.
El Dispensador de Certificados de ANF AC descargará en el ordenador remoto copia del certificado de Usuario.

c) Introduciendo en el navegador la dirección URL http://www.anf.es/certificado.exe?identificador=identificador del certificado.
El Dispensador de Certificados de ANF AC descargará en el ordenador remoto copia del certificado de Usuario.

4.14 Cifrado de Datos.

Si bien ANF AC dota a sus Usuarios del software del **Sistema TID** el cual incluye servicios y protocolos de encriptación, se hace constar que el cifrado de datos está fuera del ámbito de aplicación de los certificados emitidos por esta AC. El uso de certificados de ANF AC para el cifrado de datos se realizará bajo exclusiva responsabilidad del Signatario.

4.15 Certificados de ANF AC y Certificados de Autenticación.

4.15.a Protección de las Claves Privadas.

Doble control de la Clave Privada:

La Clave Privada de estos certificados se almacena en un dispositivo desmontable que impide la alteración de los datos y está protegida por tres de las cuatro llaves hardware que contienen componentes de la clave. Para su activación es imprescindible el empleo de la cuarta llave con el máximo nivel de acreditación en caso del certificado modalidad -ANF Autoridad de Certificación 4.3.e- y exclusivamente por el propio titular del certificado, para activar claves correspondientes a certificados tipo -ANF Autenticación 4.3.f- y -Certificado de Autentificación 4.3.d-.

4.15.b Objetivos del uso de claves.

La clave de firma de ANF AC se utilizan para firmar Certificados CDIP.

Las claves de firma de -ANF Autenticación- y -Certificado de Autenticación- se utiliza para firmar en “modo autofirma” documentos o ficheros electrónicos existentes en servidores web autorizados (ER) y autenticar procesos de firma llevados a cabo por Usuarios de esta AC (ver sección 7.1.c b).

4.15.c Cambio de los Certificados de ANF Autoridad de Certificación.

La clave de la raíz de la AC tiene un período de validez de 10 años.

ANF AC maneja todos los aspectos relativos al cambio de claves. Cuando se haya superado cuatro quintos del tiempo de vida del certificado de la Autoridad de Certificación, se generará una nueva identidad raíz. A partir de ese momento, las nuevas inscripciones se harán

firmando certificados con esa nueva identidad. De esta forma, los certificados CDIP emitidos y vigentes, cuentan con el plazo de tiempo suficiente para operar con normalidad.

ANF AC se encargará de notificar a los Usuarios y ER sobre el cambio de las claves correspondientes dentro de un plazo razonable anterior a la fecha de vencimiento del Certificado.

Se realizará un informe del cambio de certificados, remitiéndolo a los departamentos correspondientes del Ministerio de Justicia y Ministerio de Fomento, solicitando, además, la actualización de los datos de ANF AC respecto a las nuevos certificados de AC que utiliza.

4.15.d Duración de los Certificados de Autenticación.

Seguirá lo establecido como norma general en el apartado 4.7.1 Caducidad.

4.15.e Difusión.

Los certificados de ANF Autoridad de Certificación, ANF Autenticación y Certificados de Autenticación, son de acceso público, sin restricción alguna. Se encuentra publicado en:

http://www.anf.es/AC/certificados.asp

El certificado de ANF AC se incluye en el software del **Sistema TID** y se instala automáticamente con cualquiera de los dispositivos de esta AC.

5 Autoridad de Registro.

Para llevar a cabo la Prestación del Servicio de Certificación, ANF AC utilizará las **Autoridades de Registro** que se especifican en cada Política de Certificación (CP). En aquellas CP que no conste ninguna en particular, ANF AC puede valerse de una o varias Autoridades de Registro.

Las Autoridades de Registro (AR) llevarán a cabo la identificación de los solicitantes de Certificados de acuerdo con las estipulaciones reseñadas en las Políticas de Certificación de cada uno de los tipos de Certificados que ANF AC emite. Así mismo, le corresponde a la Autoridad de Registro comprobar la identidad y autorización de la persona física o jurídica a la que representa el signatario.

Las Autoridades de Registro podrán valerse de los medios que consideren necesarios para comprobar la veracidad de los datos y documentos aportados, incluso requerir al solicitante acreditación o información complementaria.

Les corresponde a las AR analizar toda la documentación aportada por el solicitante, determinar la suficiencia y validez de la misma, comprobar en caso de duda su veracidad y aprobar o denegar las solicitudes de certificados.

Serán las AR las encargadas de comunicar a los Usuarios la decisión adoptada sobre su solicitud.

Las Autoridades de Registro únicamente podrán tramitar solicitudes de Usuarios cuyos contenedores homologados TID cuentan con la oportuna licencia de generación (ver apartado 4.1.b).

Las Autoridades de Registro velarán para impedir que puedan emitirse certificados con nombres de usuarios idénticos, todos ello sobre la base de “Nombre Distintivo” (ver apartado 4.4.1)

Los criterios de valoración que seguirá la AR para valorar la documentación que garantiza la correcta identificación del signatario serán los aceptados según la legislación vigente.

6 Entidades Reconocidas

Son personas físicas o jurídicas a las que ANF AC ha licenciado e instalado tecnología Web del Sistema TID en sus equipos informáticos.

Las Entidades Reconocidas (ER), han suscrito con ANF AC una serie de obligaciones y compromisos, que garantizan a los usuarios de esta AC máximas garantías de operatividad con los contenedores homologados TID, reconocimiento de su firma electrónica y seguridad de datos y servicios.

Las Entidades Reconocidas (ER), reconocen esta CPS, sus Anexos y Políticas de Certificación.

7 Firma Electrónica y Sello de Tiempo

ANF AC garantiza que la firma electrónica de los usuarios de esta AC es “Firma Electrónica Avanzada”.

ANF AC garantiza su intervención durante el proceso de firma. Verificando el estado del certificado y avalando la operación mediante su firma electrónica y estampación de sello de tiempo.

7.1 Dispositivos seguros de creación de firma electrónica.

Los dispositivos de ANF AC tienen la capacidad de firmar cualquier tipo de fichero electrónico que se encuentre en el propio ordenador del signatario “modo local”, o cualquier página WWW de forma remota “modo Web” o bien, que el servidor firme automáticamente en “modo Autofirma”, acreditando la existencia de una determinada página web, en un determinado sitio web, en un determinado momento. La modalidad de “Autofirma”, es también necesaria para la prestación del Servicio de Almacén y Custodia (apartado 7.5.) y el Registro de Entrada de Documentos.

Para procesar la firma deben de utilizarse dispositivos homologados por ANF AC (ver sección 3.8).

7.1.a Difusión.

ANF AC pone a disposición gratuita de sus Usuarios los dispositivos seguros de creación de firma electrónica "modo local" y "modo Web". Las actualizaciones de este software son igualmente gratuitas y se encuentran disponibles en:

http://www.anf.es/TID/software/

El dispositivo seguro de creación de firma en "modo Autofirma", así como la tecnología necesaria para posibilitar la firma de Usuarios de ANF AC en "modo Web" está restringida a Entidades Reconocidas (ER) y requiere de acuerdos específicos con cada una de ellas.

7.1.b Instalación.

El usuario de ANF AC debe de proceder a la instalación de los dispositivos siguiendo sus instrucciones técnicas.

7.1.c Procedimiento según modalidades de firma.

ANF AC tiene configuradas las siguientes modalidades de firma:

?? Modo Local.
?? Modo Web.
?? Modo Auto firma.

Los procedimientos seguidos por los dispositivos seguros de creación de firma electrónica en cada una de estas modalidades son los siguientes:

a) En "Modo Local":

El documento o fichero electrónico queda firmado por el usuario y por la Autoridad de Certificación, la cual estampa sello de tiempo y verifica, en tiempo real, el estado del certificado al que se vincula la firma del signatario.

?? **Fase previa.**

- El signatario selecciona el fichero o documento a firmar.
- El dispositivo posibilita la verificación previa del documento.
- Introducción del PIN (en un plazo máximo de 60 segundos).

?? **Validación.**

- Verificación del PIN.
- Autenticación del contenedor homologado TID.

?? **Hash.**

- Generación del resumen "hash".

- Valoración de las limitaciones de uso del certificado para poder firmar el documento o fichero.

?? **Comunicación.**

- El dispositivo establece comunicación con ANF AC.

- ANF AC procede a autenticar la conexión (ver protocolo 2.1),

?? **Comprobación.**

- ANF AC verifica el estado del certificado (activado - revocado - caducado).
- ANF AC autoriza o deniega que el usuario pueda firmar electrónicamente el fichero (durante el proceso de firma se integra la identidad del firmante por reseña del identificador único de su certificado y el nombre del fichero).

(NOTA IMPORTANTE: en ningún caso la Autoridad de Certificación recibe el documento o fichero a firmar. Ver servicio Guarda y Custodia, apartado 7).

?? **Sello de tiempo (caso de autorización de firma).**

- ANF AC genera hash **de los datos relativos a la firmas generada por la ER,** incluyendo el tiempo t, en la forma de fecha y hora de la recepción, componiendo [h(D), t].

ANF 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, publicándolo simultáneamente en un Registro Público. 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.(ver 6.3).

Cada sello de tiempo que emite la Autoridad se encuentra enlazado con todos los sellos emitidos anteriormente, llegando al extremo de enlazar todos los sellados emitidos por la Autoridad; de esta forma, se logra determinar todos los sellos emitidos por la misma o solicitados por un firmante en concreto. El modo de actuar es el siguiente:

1. A cada petición de un sello, ANF AC asigna un número de serie único n, identificando esta petición.

2. Se registra el número de transacción en base de datos, junto al identificador del certificado instante de la firma y nombre del fichero firmado.

El modo de generar el número de serie único es el siguiente:

1. Por cada petición de un sello, ANF AC toma el valor del “hash” saliente (Hs) del sello inmediatamente anterior que emitió. Siendo éste el valor “hash” entrante en esta operación (He).

2. Seguidamente toma el valor del “hash” actual, más todos los datos relativos a las firmas electrónicas generadas, así como de los certificados a los que se las vincula, y la fecha y hora de la recepción [h(D), t] según protocolo A, e incluye He.

3. ANF AC procede a la firma digital de la asociación anterior y envía este Sello Digital de Tiempo firmado por la AC al usuario que se lo solicitó. Ha obtenido así un nuevo Hs; "hash" saliente que servirá de cabecera He para la siguiente petición de sello que reciba.

El detalle completo de la operación es depositado en un registro público, ordenado cronológicamente. Si los operadores desean verificar el correcto funcionamiento de la Autoridad de Certificación sobre los sellos recibidos, únicamente deben de localizar el sello recibido de la AC y comprobar la correcta correlación de "hash" entrante y "hash" saliente, con los inmediatamente anteriores y posteriores sellos de tiempo que la AC ha emitido. El anterior siempre existirá y será cronológicamente de tiempo pasado y el posterior, si existe, será cronológicamente de tiempo más actual.

?? **Comprobante de firma.**

La firma electrónica queda automáticamente depositado en:

Ordenador del Signatario.

?? **Fin de la conexión.**

ANF AC cierra automáticamente la conexión.

Cada uno de estos procesos es monitorizado por los dispositivos.

b) En "Modo Web":

El documento o fichero electrónico queda firmado por el usuario, por la Entidad Reconocida (Web) y por la Autoridad de Certificación, la cual estampa sello de tiempo y verifica, en tiempo real, el estado de los certificados a los que se vinculan las firmas generadas. Automáticamente se envían las firmas a todas las partes.

?? **Fase previa.**

- El signatario selecciona el fichero o documento a firmar.
- El dispositivo posibilita la verificación previa del documento.
- Introducción del PIN (en un plazo máximo de 60 segundos).

?? **Validación.**

- Verificación del PIN.
- Autenticación del contenedor homologado TID.

?? **Hash.**

- Generación del resumen "hash" (E.R. y usuario).
- Valoración de las limitaciones de uso del certificado para poder firmar el documento en Web.

?? **Comunicación.**

- El dispositivo establece comunicación con ANF AC.

- ANF AC procede a autenticar la conexión (ver protocolo 2.1), tanto del Usuario como de la Entidad Reconocida. La tecnología empleada por ANF AC en "modo web", garantiza:

a) Al **Usuario**: el origen cierto del documento que va a firmar, la imposibilidad de que suplanten su identidad y su presencia cierta en ese momento.

b) A la **Entidad Reconocida** (ER): la imposibilidad de que suplanten su identidad, el origen cierto del Usuario y su presencia cierta en ese momento.

?? **Comprobación.**

- ANF AC verifica el estado de los certificados de ER y usuario (activado - revocado - caducado).
- ANF AC autoriza o deniega que el usuario pueda firmar electrónicamente el fichero (durante el proceso de firma se integra la identidad del firmante por reseña del identificador único de su certificado) y autoriza o deniega la firma de la ER.

?? **Sello de tiempo (caso de autorización de firma).**

- ANF AC genera hash **de los datos relativos a las firmas generadas por la ER y usuario,** incluyendo el tiempo t, en la forma de fecha y hora de la recepción, componiendo [h(D), t].

ANF AC procede a la firma digital de la asociación anterior calculando FAC(h(D), t), envía este Sello Digital de Tiempo al usuario que se lo solicitó y a la ER, publicándolo simultáneamente en un Registro Público. 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.(ver 6.3).

Cada sello de tiempo que emite la Autoridad se encuentra enlazado con todos los sellos emitidos anteriormente, llegando al extremo de enlazar todos los sellados emitidos por la Autoridad; de esta forma, se logra determinar todos los sellos emitidos por la misma o solicitados por un firmante en concreto. El modo de actuar es el siguiente:

1. A cada petición de un sello, ANF AC asigna un número de serie único n, identificando esta petición.

2. Se registra el número de transacción en base de datos, junto al identificador del certificado instante de la firma.

El modo de generar el número de serie único es el siguiente:

1. Por cada petición de un sello, ANF AC toma el valor del "hash" saliente (Hs) del sello inmediatamente anterior que emitió. Siendo éste el valor "hash" entrante en esta operación (He).

2. Seguidamente toma el valor del "hash" actual, más todos los datos relativos a las firmas electrónicas generadas, así como de los certificados a los que se las vincula, y la fecha y hora de la recepción [h(D), t] según protocolo A, e incluye He.

3. ANF AC procede a la firma digital de la asociación anterior y envía este Sello Digital de Tiempo firmado por la AC al usuario que se lo solicitó y a la ER que tramitó el proceso de firma. Ha obtenido así un nuevo Hs; "hash" saliente que servirá de cabecera He para la siguiente petición de sello que reciba.

El detalle completo de la operación es depositado en un registro público, ordenado cronológicamente. Si los operadores desean verificar el correcto funcionamiento de la Autoridad de Certificación sobre los sellos recibidos, únicamente deben de localizar el sello recibido de la AC y comprobar la correcta correlación de "hash" entrante y "hash" saliente, con los inmediatamente anteriores y posteriores sellos de tiempo que la AC ha emitido. El anterior siempre existirá y será cronológicamente de tiempo pasado y el posterior, si existe, será cronológicamente de tiempo más actual.

?? **Documento y comprobante de firma.**

El documento firmado queda automáticamente depositado en:

Ordenador del Signatario junto con los datos relativos al certificado al que se vincula la firma.

?? Ordenadores WWW que establezca la ER, incluso en el repositorio de ANF AC si tiene contratado el servicio de Almacén y Custodia (ver apartado 7.5)

?? Se envía informe de la transmisión al ordenador que originó la operación.

?? **Fin de la conexión.**

ANF AC cierra automáticamente la conexión.

Cada uno de estos procesos es monitorizado por los dispositivos.

c) En "Modo Autofirma":

El documento o fichero electrónico queda firmado por la Entidad Reconocida (Web) y por la Autoridad de Certificación, la cual estampa sello de tiempo y verifica, en tiempo real, el estado del certificado al que se vincula la firma generada.

1) Fase previa y Validación.

Según lo establecido en el apartado 4.15 (Certificados de ANF AC y Certificados de Autenticación) de este documento.

2) Solicitud de Firma.

El dispositivo genera el “hash” del documento y procesa su firma.

3) Comunicación.

El dispositivo establece comunicación con ANF AC.
ANF AC procede a autenticar la conexión (ver protocolo 2.1). La tecnología empleada por ANF AC, garantiza:

a) **Al Usuario:** el origen cierto del documento que recibe firmado.

b) **A la Entidad Reconocida** (ER) **:** la imposibilidad de que le atribuyan documentos Web que no corresponden a la realidad.

4) Comprobación.

ANF AC verifica el estado del certificado de la Entidad Reconocida -ER- (activado - revocado - caducado), y determina la correspondencia cierta de la firma electrónica recibida con el certificado de la ER.

Superada la anterior comprobación, procede a estampar sello de tiempo, insertar identificador de firma de la ER y número de transacción (este último a efectos meramente estadísticos y sin valor relevante).

5) Documento y comprobante de firma.

Se transmite el fichero de firma a la ER; el dispositivo se encarga de insertarlo al pie del documento original, junto con los datos relativos al certificado al que se vincula la firma.

Finalmente, el dispositivo encapsula el documento para poder ser descargado vía Web por el usuario remoto.

6) Descarga del documento.

Se transmite el documento firmado vía Web a requerimiento del usuario.

7.2 Dispositivo de verificación de firma.

Este dispositivo tiene la capacidad de verificar automáticamente la identidad e integridad de un fichero electrónico firmado. Determina si:

a) La firma digital fue creada por la clave privada vinculada a la clave pública perteneciente al certificado del signatario, el estado del certificado y
b) Estado del certificado y capacidad de firma: atributos e importe límite de firma.
c) Que el documento y el sello de tiempo asociado al mismo, no han sido alterados desde que se creó la firma digital.
d) Identidad del signatario y de la AC que emite el certificado y garantiza la firma.

Es responsabilidad del receptor del documento firmado, verificar en el propio certificado del signatario, o en el Registro de Certificados, sus posibles limitaciones de uso.

7.2.a Difusión.

ANF AC pone a disposición pública y gratuita el dispositivo de verificación de firma. Las actualizaciones de este software son igualmente gratuitas y se encuentran disponibles en:

http://www.anf.es/TID/software/

7.2.b Instalación.

El usuario de ANF AC debe de proceder a la instalación del dispositivo siguiendo sus instrucciones técnicas.

7.2.c Procedimiento.

Procedimiento seguido por el dispositivo de verificación de firma electrónica de ANF AC:

1) **Fase previa.**

   Selección del fichero firmado.

2) **Verificación.**

   a) Se verifica la integridad del fichero electrónico con relación a la firma electrónica a la que se le vincula.
   b) Se verifica la identidad del signatario. Validando o denegando la relación de la firma electrónica con el certificado al que se la vincula.
   c) Se verifica la identidad de la autoridad de certificación. Validando o denegando la relación de la firma electrónica, estampada en el sello de tiempo, con el certificado AC al que se la vincula.
   d) Se determina el estado del certificado: activado, revocado o suspendido.

   e) Se verifica la integridad de los datos firmados por la autoridad de certificación:
      a. Hash anterior
      b. Hash actual
      c. Hash siguiente
      d. Día y hora de firma
      e. Identificador de firma de los firmantes.
      f. Importe límite de los certificados empleados.
      g. Atributos de los certificados empleados por los signatarios.
      h. Posible representación que ostentan los signatarios.
      i. Tipos de certificados empleados.
      j. Según modalidad:
         - Modo Web: Verificación de firma y certificado de la ER y usuario.
         - Modo Autofirma: Verificación de firma y certificado de la ER.
         - Modo Local: Verificación de firma, nombre del documento y certificado del usuario.

3) **Emisión del informe de verificación.**

Se emite informe detallado del protocolo de verificación seguido y, resultado obtenido.

Es especialmente necesario consultar los atributos e importe límite de firma del certificado y, en su caso, el tipo de certificado para determinar la capacidad de firma del signatario.

7.3 Registro de transacciones.

7.3.a Contenido.

En base de datos: Identificador del certificado, identificador de la firma (código de la transacción), fecha de firma, "hash" del documento o fichero firmado (hash anterior, actual y siguiente), resultado de la operación (firma aceptada o rechazada por la AC).

7.3.b Accesibilidad.

De libre acceso por vía telemática.

7.3.c Mantenimiento de los datos.

ANF AC mantendrá los datos por un plazo mínimo de 5 años.

7.4 Depósito de Sellos de Tiempo.

7.4.a Contenido.

En servidor: Espacio en disco duro donde se almacenan copias de los sellos de tiempo enviados a los signatarios al procesar una firma electrónica. Esta información se reseña en una relación que, con orden cronológico, el sistema genera diariamente de forma automática.

7.4.b Accesibilidad.

De libre acceso por vía telemática.

7.4.c Mantenimiento de los datos.

ANF AC mantendrá los datos por un plazo mínimo de 5 años.

7.5 Almacén y Custodia.

ANF AC dispone en sus servidores WWW de un espacio especialmente diseñado para la guarda y custodia de ficheros electrónicos.

Normas y operativa de funcionamiento:

1. **Contratación.**

Este servicio únicamente puede ser contratado por Entidades Reconocidas o por Usuarios de ANF AC.

2. Contenido.

Cualquier tipo de fichero electrónico (documentos, pág. Web, fotografías, código fuente, programas...etc). Estos ficheros pueden estar en formato legible o encriptados.

3. Finalidad del servicio.

Almacenar y custodiar copias de seguridad de ficheros electrónicos. Acreditar la existencia de un determinado fichero en un determinado momento.

4. Restricciones de uso.

a) Queda prohibido el depósito de ficheros que por su naturaleza o titularidad puedan presuponer una violación de la legalidad vigente o de los derechos de terceros que ostenten su legítima propiedad intelectual.

b) Queda prohibida la utilización de este depósito por parte de los contratantes a modo de servicio WWW, debiendo respetar su utilización para los fines para los que ha sido creado.

5. Recepción.

Los servidores de ANF AC procederán a efectuar las siguientes operaciones:

a) Recepción.

1) Verifica la identidad cierta del emisor, según el procedimiento descrito en el apartado 2.1.

2) Verifica que el fichero no ha sufrido modificación durante la transmisión mediante procedimiento “hash”.

3) Se procede a renombrar los ficheros siguiendo un patrón numérico y transformarlo a formato X25.

4) Lo deposita en el repositorio del propietario del fichero.

b) Registro de entrada.

Los servidores de ANF AC gestionan una relación de los ficheros recibidos. En esta relación se anota:

1) Nombre original del fichero.
2) Nuevo nombre otorgado.
3) Hash del fichero.
4) Fecha y hora de recepción.

La relación es diaria, por contratante y, al finalizar el día, ANF AC procede a firmarla y estampar sello de tiempo.

6. Seguridad y Control.

Además de las enumeradas en el apartado 2 de esta CPS:

a) Ejecución.

El directorio donde quedan depositados los ficheros no tiene capacidad de ejecución.

d) Directorio exclusivo.

Cada directorio es exclusivo de la entidad contratante del servicio.

e) Garantía de destrucción.

Se garantiza la destrucción automática del fichero en todos los ordenadores de ANF AC en -tiempo real- (en ese mismo momento), cuando así lo ordene el contratante.

f) Copias de seguridad.

Con el fin de garantizar lo establecido en el apartado anterior (*e) Garantía de destrucción*), ANF AC no realizará copias de seguridad de este Depósito. No obstante, y con el fin de garantizar la reconstrucción del repositorio en caso de siniestro, ANF AC gestionará el servicio en modo distribuido con otros servidores espejo que mantiene bajo su exclusivo control y que, como mínimo, cuentan con niveles de seguridad idénticos a los especificados en esta CPS.

g) Modificaciones.
Queda prohibida la modificación de ficheros depositados en este almacén. ANF AC garantiza la identificación del fichero original que le ha sido confiado.

h) Operadores autorizados.
Sólo operadores autorizados por el contratante pueden acceder a este servicio.

i) Registro de destrucción.

Se registrarán las operaciones de destrucción ordenadas, anotando: Día y hora, nombre original del fichero e identidad del operador.

j) Control de acceso.
Se seguirán los mismo parámetros en materia de seguridad a los reseñados en el apartado 4.12 (Registro de certificados).

7. Accesibilidad.

La realización de consultas, la destrucción de ficheros e, incluso, la obtención de copias de los ficheros y listas de recepción firmadas, se realizará de forma telemática vía WWW. El

depósito de ficheros electrónicos debe de realizarse mediante dispositivos de transmisión homologados por ANF AC.

8. Dispositivos de verificación y recuperación.

ANF AC facilitará gratuitamente los dispositivos necesarios para verificar la integridad de los ficheros electrónicos recuperados del repositorio, así como para transformarlos del formato X25 a su estado original.

9. Tasas.

Almacén y custodia:

a) Tasa por Fichero. Se facturará de acuerdo con las tarifas vigentes en ese momento.

b) Incrementos por Peso de Fichero. Se facturará de acuerdo con las tarifas vigentes en ese momento.

7.6 Codificación de documentos.

Los dispositivos seguros de creación de firma electrónica homologados por esta autoridad de certificación, permiten automatizar un proceso de control previo de atributos e importe límite de firma exigibles a los usuarios. Este control previo, no tiene otro valor que el de imposibilitar el proceso de firma por evidente incoherencia de codificación. En firmas efectivamente procesadas, el receptor deberá verificar la capacidad de firma del signatario, de acuerdo con sus atributos de firma e importe límite de firma de su certificado digital.

7.6.a Codificación en Modalidad Firma Local.

Al nombre del fichero se debe de incluir:
Nombre del fichero, guión (-) **nombre TID (TID) guuion (-) cada uno de los dígitos, correspondientes a los atributos exigibles para poder firmar el documento separados por una coma(,) y, caso de tratarse de un documento con valor económico, incluir punto y coma (;) seguido del valor. Finalmente, punto (.) y la extensión del fichero electrónico.**

Por ejemplo:
El documento en cuestión se trata de un fichero electrónico en formado *.doc que incorpora un contrato de transporte, que incluye la contratación de un seguro . El importe de la operación son 2.000 €. Por ello, el firmante tiene que tener atributos :

- Contrato transporte **30**
- Solicitar seguros **22**
- Límite de importe de firma igual o superior a los **2000**.

IMPORTANTE: No incluir separador de millares. La etiqueta puede no incluir importe limite, en cuyo caso no se debe reseñar el separador (punto y coma ;) o bien, puede tratarse de una etiqueta que reseñe únicamente cantidad, en cuyo caso no se debe de incluir el separador (coma ,) pero si el de punto y coma que es identificativo de cantidad.

Los certificados de esta autoridad, integran el importe límite de firma siempre expresado en euros €.

Etiqueta:

Contrato-TID-30,22;2000.doc

7.6.b Codificación en Modalidad Firma Web y Modalidad Autofirma.

7.6.b.1 Modalidad Firma Web

En la cabecera del documento se debe de incluir la siguiente etiqueta:

<!— nombre TID (TID) guuion (-) cada uno de los dígitos, correspondientes a los atributos exigibles para poder firmar el documento separados por una coma(,) y, caso de tratarse de un documento con valor económico, incluir punto y coma (;) seguido del valor -->

Por ejemplo:

El documento en cuestión se trata de una página Web que incorpora un contrato de transporte, que incluye la contratación de un seguro . El importe de la operación son 2.000. Por ello, el firmante tiene que tener atributos :

- Contrato transporte **30**
- Solicitar seguros **22**
- Límite de importe de firma igual o superior a los **2000**.

IMPORTANTE: No incluir separador de millares. La etiqueta puede no incluir importe limite, en cuyo caso no se debe reseñar el separador (punto y coma ;) o bien, puede tratarse de una etiqueta que reseñe únicamente cantidad, en cuyo caso no se debe de incluir el separador (coma ,) pero si el de punto y coma que es identificativo de cantidad.

Los certificados de esta autoridad, integran el importe límite de firma siempre expresado en euros €.

Etiqueta:

<!— TID-30,22;2000 -->

7.6.b.1 Modalidad Firma Autofirma

La única diferencia con el procedimiento de modalidad firma web, es que en este formato no están permitidas restricciones de atributos.

7.6.c Tabla de codificación de atributos.

Los establecidos en cada una de las Políticas de Certificación.

8 Registro de Entrada de Documentos.

Con el fin de atender las necesidades operativas que imponen los nuevos procesos de trabajo telemático a profesionales, instituciones y empresas en general, en materia de recepción y envío de documentos, ANF AC pondrá a disposición exclusiva de sus ER el “Registro de Entrada de Documentos ” (RED). RED es un dispositivo cuya operativa debe de seguir los siguientes criterios:

a) Trabajar en modo automático y, por lo tanto, en materia de firma, seguir el procedimiento reseñado en el apartado 7.1.c b) y relacionados con el tipo “Modo Autofirma”.

b) Ser capaz de procesar lotes de documentos, firmándolos de forma individual, creando una relación de envío firmada y sellada electrónicamente. En esta relación debe de constar como mínimo:

1. Número de lote.
2. Número de orden del documento en esa relación.
3. Nombre del fichero electrónico correspondiente al documento.
4. Resumen "hash" del documento.
5. Dirección IP del RED que genera y procesa el lote.
6. Firma y sello de tiempo de la relación.
7. Empaquetar los documentos y la relación en un solo lote.
8. Encriptar el lote según los niveles criptográficos descriptos en esta CPS.

c) Ser capaz de transmitir los lotes de acuerdo con los niveles de seguridad en las comunicaciones descrito en el apartado 2.1 de esta CPS.

d) Ser capaz de desencriptar y desempaquetar lotes de documentos.

e) Ser capaz de verificar identidad e integridad de la relación y de los documentos recibidos, así como verificar la existencia de todos los documentos de acuerdo con la relación correspondiente a su lote.

f) Ser capaz de depositarlos en Almacén seguro.

g) Ser capaz de firmar un acuse de recibo de la relación recibida, indicando, en caso de necesidad, las discrepancias detectadas.

h) Ser capaz de transmitirla de acuerdo con los niveles de seguridad en las comunicaciones descrito en el apartado 2.1 de esta CPS.

9 Sistema de Intercambio de facturas telemáticas.

En este proceso se emplearan como instrumentos de creación de datos de generación de firma electrónica, así como creación y verificación de firma electrónica, el modelo SmartCard Criptográfica descrito en el punto 2.6.f y siguientes.

El procedimiento establecido es el siguiente:

1. Por cada factura intercambiada se adjuntará la firma electrónica de la misma, generada con los datos de firma del emisor, y todos los datos que permitan al receptor verificar la

integridad de lo firmado y la autenticidad del firmante. La firma electrónica podrá integrarse en el propio fichero electrónico o en un fichero independiente, sin que ello afecte a la integridad del documento original ni a la modalidad del proceso de verificación.

2. En el propio fichero de firma se incluirá el vinculo desde el cual el receptor de la factura telemática se puede descargar gratuitamente el software de verificación de firma.
3. De acuerdo con el protocolo de firma establecido en esta Declaración de Practicas de Certificación, toda factura electrónica incorpora en su firma como mínimo:
    a. Identidad del emisor
    b. Sello de tiempo en el que se indica el instante exacto en el que se firmo la factura.
    c. Firma electrónica de ANF AC que acredita que la Autoridad de Certificación ha verificado el estado del certificado digital que se vincula al emisor y que ha permitido su utilización al encontrarse con plena vigencia y atributos de firma. Es decir no ha perdido su eficacia por revocación, caducidad o cualquier causa establecida en el ordenamiento jurídico
    d. Identificador del certificado al que se vincula la firma empleada, tanto por parte del emisor como de la Autoridad de Certificación. Así como vinculo para descargar de Internet copia de estos certificados.
    e. Claves públicas vinculadas a las privadas empleadas para firmar el hash del documento, tanto del emisor como de la Autoridad de Certificación.
    f. Número de transacción, único y exclusivo de cada firma realizada y que esta vinculada a ese certificado.

4. Este procedimiento además asegura que:
    a. ANF AC guarda un registro de todas las transacciones realizadas y los hash firmados. Este registro es público y se gestiona bajo el sistema de encadenamiento de hash.
    b. Los dispositivos desarrollados por ANF AC, para llevar a cabo el Sistema de Facturas Telemáticas, garantizan el almacenaje de los datos tal y como fueron transmitidos para posibilitar posteriores verificaciones de firma y contenido de las facturas.

10 Obligaciones y Responsabilidades.

10.1 ANF AC.

10.1.1 Generales.

Se responsabiliza en cumplir todas las obligaciones exigibles a los prestadores de servicios de certificación. Así como todas las derivadas del presente documento, sus anexos y Políticas de Certificación.

ANF AC se compromete a proteger las Claves Privadas contra el peligro de usurpación.

10.1.2 Ubicación segura luego de haberse producido accidentes o algún tipo de daño.

En el caso de que se deba establecer un sitio de procesamiento alternativo por la existencia de daños, el nuevo sitio tendrá, como mínimo, el mismo nivel de seguridad física y lógica que el sitio de procesamiento original. La nueva ubicación se hará de forma diligente y en el menor plazo de tiempo posible. El Plan de Reanudación de las Operaciones Comerciales de ANF AC, se encuentra disponible para todo el que justifique la necesidad de conocerlo, en la Oficina de Atención al Cliente.

10.1.3 En caso de que los recursos, el software y/o los datos informáticos estén gravemente dañados.

En el caso de que se dañen gravemente los recursos, el software y/o los datos informáticos, se detendrá el funcionamiento de la AC y el sistema será restablecido una vez que se hayan incorporado nuevos componentes de eficiencia comprobable. Simultáneamente, se llevará a cabo una investigación para identificar la causa de los daños y se evaluará la integridad de la PKI. Se notificará a los Usuarios y ER acerca de los daños producidos.

10.1.4 En caso de que la clave de la entidad pueda ser usurpada.

Si la Clave Privada de la AC es usurpada, o está expuesta a dicho riesgo, se revocará inmediatamente el Certificado correspondiente, se actualizará y publicará la CRL, se detendrá el funcionamiento del sistema de la AC y se llevará a cabo un nuevo proceso de generación de claves de ANF AC. Además, se notificará a los Usuarios y ER acerca de esta situación. Los Certificados emitidos antes de que se usurpara la Clave serán firmados nuevamente y aquellos que fueron emitidos luego de que se identificara la usurpación serán revocados. Se solicitará a los usuarios que generen un nuevo Par de Claves y que vuelvan a realizar el proceso de solicitud.

Se realizará un informe de lo acontecido, remitiéndolo a los departamentos correspondientes del Ministerio de Justicia y Ministerio de Fomento, solicitando además la actualización de los datos de ANF AC respecto a las nuevos certificados de AC que utiliza.

10.1.5 Cese de las actividades de la AC.

Las actividades de ANF AC sólo pueden ser suspendidas por su propia Junta Rectora. En el caso de que esto ocurra, ANF AC podrá ejercer su derecho de subrogación (ver apartado 11.2) o bien, revocar todos los Certificados emitidos por ANF AC, suspendiendo de forma inmediata, a su vez, la emisión de nuevos Certificados.

ANF AC, se encargará de comunicar esta situación a todas los usuarios y ER con la antelación que establezca la legislación vigente y en la forma que en ella se requiera.

10.1.6 Garantías Patrimoniales de ANF AC.

ANF AC garantiza su responsabilidad frente a sus usuarios y terceros afectados mediante aval bancario y/o seguro de responsabilidad civil, cuyo importe asciende de forma suficiente a lo establecido en la legislación vigente.

10.2 Usuarios.

Se responsabiliza en cumplir todas las obligaciones derivadas del presente documento, sus anexos y Políticas de Certificación.

Asegurarse de que toda la información contenida en el Certificado es cierta.
Utilizar el certificado respetando las restricciones que le vienen impuestas según sus "Atributos y Limitaciones de uso" (ver sección 4).

Se obliga a custodiar, de forma diligente, el contenedor TID que contiene los datos de creación de firma y la clave secreta de activación, así como login y contraseña secreta de acceso al Registro de Certificados.

Se compromete a solicitar la suspensión / revocación del Certificado cuando se vea comprometida la seguridad de los datos de creación de firma o la clave secreta de activación o sus datos personales hayan sufrido alguna modificación.

Los usuarios garantizan que la propuesta y posterior uso de un dominio y nombre distintivo por su parte, no infringe los derechos de terceros en ninguna jurisdicción con respecto a derechos de propiedad industrial y marca, y que no emplearán el dominio y nombre distintivo para propósitos ilícitos; entre ellos, competencia desleal, suplantación, usurpación y actos de confusión en general. Los solicitantes y, en general, los usuarios de certificados, indemnizarán a ANF AC por los daños que le pueda causar en la realización de estas actividades.

10.3 Receptor.

Tiene la consideración de receptor, el tercero de buena fe que confía en el fichero electrónico que está firmado digitalmente por un signatario de ANF AC y que, además de depositar la confianza en esa firma electrónica, cumpla con las siguientes obligaciones:

- Debe de verificar la firma utilizando el Dispositivo de Verificación de firma electrónica homologado por ANF AC.
- Debe de comprobar y valorar posibles restricciones según las indicaciones establecidas en el apartado "Atributos y Limitaciones de Uso" (ver sección 4).
- Debe de haber leído este apartado y cuantos de él se deducen o, en su caso, solicitar asesoramiento a la "Oficina de Atención al Cliente" de ANF AC (ver apartado 11).

Los receptores que no cumplan los requisitos indicados no podrán ser considerados de buena fe.

10.4 Entidades Reconocidas.

Se comprometen a codificar según homologación de la AC, los documentos o ficheros que habiliten para ser firmados por usuarios de ANF AC.

Se responsabiliza en cumplir todas las obligaciones derivadas del presente documento, sus anexos y Políticas de Certificación.

10.5 Autoridad de Registro.

Las AR están obligadas a:

- Verificar la exactitud y autenticidad de la información suministrada por el Usuario al momento de la solicitud, en conformidad con la Política de Certificación pertinente.
- Proteger las Claves Privadas de la AR contra peligro de usurpación.
- Validar y enviar en forma segura una solicitud de Revocación a ANF AC al tener constancia de inexactitudes en la información reseñada en el Certificado del Usuario.
- Verificar la exactitud y autenticidad de la información suministrada por el Usuario al momento de la renovación de clave, de conformidad con la Política de Certificación pertinente.
- Comunicar oportunamente a ANF AC la existencia de solicitudes relacionadas con la firma de Certificados.

11 Protección de Datos Personales.

A los efectos de lo dispuesto en la normativa sobre tratamiento de datos de carácter personal (*), se informa a los usuarios de ANF AC de la existencia de un fichero automatizado de datos de carácter personal creado y bajo la responsabilidad de ANF AC. Este fichero que recibe el nombre de "Registro de Certificados", tiene la finalidad de servir a las necesidades previstas en esta CPS,

sus anexos y Políticas de Certificación. El usuario consiente expresamente la cesión de sus datos en la medida que sea necesario para llevar a cabo las acciones previstas en los servicios de certificación.

Es responsable de este fichero ANF AC, quién informa a todos los Usuarios de esta AC de su derecho de información, oposición, acceso, rectificación y cancelación de los datos. Este derecho se extiende a las personas físicas a las que representan los Usuarios de esta AC.

ANF AC ha desarrollado y suscrito voluntariamente un código de practicas en el tratamiento de datos de carácter personal, en colaboración con la Agencia de Protección de Datos y que le autoriza a utilizar el Sello de Garantía de Protección de Datos (Código de Practicas de Tratamiento de Datos de Carácter Personal en el ANEXO I).

(*) Regulado por la Ley Orgánica 15/1999, de 13 de diciembre, sobre Protección de Datos de Carácter Personal y Real Decreto 994/1999, de 11 de junio por el que se aprueba el Reglamento de medidas de Seguridad de los ficheros Automatizados que contengan datos de carácter personal.

12 Oficina de Atención al Cliente.

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

12.1 Cometido de la Oficina.

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

- Real Decreto Ley 14/1999, de 17 de septiembre, sobre firma electrónica. Esta CPS, ANEXOS, Políticas de Certificación y documento de solicitud de certificados.
- Instalación y utilización de los dispositivos relacionados con la firma electrónica.
- Instalación y utilización del software del Sistema TID.
- Generación y uso de los contenedores homologados TID y, en general, todo lo relacionado con la prestación de servicios de certificación que esta AC realiza.

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

12.2 Procedimiento de Consulta.

Las consultas se realizarán mediante correo electrónico dirigido a :

consultas@anf.es

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

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

12.3 Procedimiento de Reclamación.

En caso de desear presentar una reclamación ante ANF AC, esta oficina dispone de servicio Web para poder confeccionarla y obtener en tiempo real copia firmada y sellada:

http://www.anf.es/AC/reclamaciones/

13 Interpretación y Ejecución.

13.1 Ley aplicable.

La legislación aplicable a este documento y a las relaciones jurídicas subyacentes es la española. Este documento, junto con sus Anexos y Políticas de Certificación aplicables a cada tipo de Certificado, se considera Condiciones Generales de Contratación (*), anexas a los contratos que firman los usuarios al solicitar la emisión de certificados y se incluyen por referencia en todos los certificados electrónicos emitidos por ANF AC.

Esta CPS 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.

13.2 Conflicto de normas.

Cada certificado se emite bajo una CPS y una Política de Certificación, 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 CPS y las Políticas de Certificación se incorporarán 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 certificados y las firmas digitales vinculadas a los mismos.

Dado el carácter de Condiciones Generales de la Contratación de la CPS y las Políticas de Certificación, caso de mediar Condiciones Particulares, éstas se impondrán sobre aquéllas en caso de conflicto.

13.3 Divisibilidad, supervivencia y notificaciones.

Cada cláusula de esta CPS, sus Anexos y Políticas de Certificación, 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 CPS.

Las notificaciones a ANF AC podrán realizarse mediante mensajes de correo electrónico firmados digitalmente, de acuerdo con las prescripciones de esta CPS, 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

13.4 Subrogación.

ANF AC, en caso de cese de su actividad, se reserva el derecho, y los usuarios consienten expresamente, la posibilidad de transmitir en el futuro todos los certificados que ha expedido junto con todas las obligaciones y derechos que se deriven de ello a otro prestador de servicios de certificación.

13.5 Administración de la CPS y Políticas de Certificación.

La propia evolución de los servicios de certificación de ANF AC, conlleva que esta CPS, sus Anexos y Políticas de Certificación 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 integro 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.

Las nuevas versiones entrarán en vigor en el momento de ser inscritas en el Registro de Condiciones Generales de la Contratación (*).

(*) Regulado por la Ley 7/1998 de abril, sobre Condiciones Generales de la Contratación.

14 Preguntas Frecuentes.

X.509 v 3 Extensiones de Servicio Estándar.

Estándar ITU-T (Unión Internacional de Telecomunicaciones). La "Enmienda 1ª X.509 a ISO/IEC 9594-8:1995" define un número de extensiones. Éstas proporcionan varios controles de gestión y administrativos útiles para la autenticación a gran escala y multipropósito.

Los certificados de entidad permiten a los usuarios definir extensiones "privadas" (información que deberá ser contrastada de acuerdo con las especificaciones de su Política de Certificación).

¿ QUÉ ÉS HASH -FUNCION RESUMEN- ?

Algoritmo que mapea o traduce un conjunto de bits a otro (generalmente menor) de forma que:

a). Un mensaje proporciona el mismo resultado siempre que el algoritmo es ejecutado utilizando el mismo mensaje como entrada.

b) Es computacionalmente inviable que se pueda inferir o reconstituir un mensaje a partir del resultado producido por el algoritmo.

c) Es computacionalmente inviable encontrar dos mensajes diferentes que produzcan el mismo resultado resumen utilizando el mismo algoritmo.

¿ QUÉ ÉS UNA INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI) ?

Es la arquitectura, los participantes y el proceso que constituye una comunidad de confianza específica por medio de la criptografía de Clave Pública.

¿ QUÉ ÉS RSA ?

Es un Sistema de criptografía de clave pública inventada por Rivest, Shamir & Adelman.