Declaración de Prácticas de Certificación (CPS)

Certificate Practice Statement

Fecha : 12 de diciembre de 2003
Versión: 1.4
OID : 1.3.6.1.4.1.18332.1.4

Declaración de Prácticas de Certificación

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.

Este documento presenta la Declaración de Practicas de Certificación (CPS) de ANF Autoridad de Certificación (ANF AC), y constituye una declaración de los criterios que esta autoridad de certificación se compromete a seguir en la prestación de sus servicios de certificación.

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, 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 a la que se somete cada uno de los distintos tipos de certificados que ANF AC emite.

Esta nueva versión 1.4, contempla los requerimientos que establece el nuevo Real Decreto que aprueba el Reglamento por el que se regulan las obligaciones de facturación, y la LEY 59/2003, de 19 de diciembre, de firma electrónica.

Este documento está dirigido a todos los usuarios de los servicios de ANF AC, entidades con las que se relaciona y, en especial, a los terceros de buena fe, personas que reciben ficheros electrónicos firmados digitalmente por los usuarios de los certificaos emitidos por ANF AC. Caso de que el lector no conozca los conceptos básicos de un sistema de Infraestructura de Clave Pública, certificados digitales y firma digital, ANF AC pone a su disposición un servicio gratuito de Atención al Cliente", y recomienda solicitar esta asistencia antes de continuar con la lectura de este documento.

Esta CPS se ha inspirado en la norma RFC 2527 "*Internet X.509 Public Key Infraestructure Certificate Policy and Certification Practices Framewortk*" propuesto por S. Chokhani y W. Ford, del Internet Engineering Task Force (IETF) como guía de asistencia en la redacción de este tipo de documentos. La CPS de ANF AC contempla todas las secciones esenciales de la especificación, no obstante y dado que la misma sigue las pautas americanas en cuanto a firma electrónica (American Bar Association Digital Signature Guidelines), de menor exigencia que lo establecido en el marco europeo, y más específicamente en el marco legal español, el autor ha estimado necesario incluir otras secciones que a su juicio considera necesarias.

1.2 Identificación.

Nombre del documento	Declaración de Prácticas de Certificación de ANF AC "CPS de ANF AC"
Versión	1.4
Autor	*Florencio Díaz Vilches*
Referencia del documento / OID	1.3.6.1.4.1.18332.1.4
Fecha de emisión	12 de diciembre de 2003
Fecha de expiración	No es aplicable
Localización URL	http://www.anf.es/AC/documentos/

El prefijo del OID de esta CPS es 1.3.6.1.4.1.18332.**1.**

Cualquier modificación que esta Autoridad de Certificación realice sobre este documento, conllevará un cambio de versión y del identificador de objeto (OID). El protocolo a seguir queda determinado en los apartados "*Seguridad en la adecuación a las disposiciones legales*", "*Seguridad a las CP's asociadas*" y "*Procedimiento de Especificación de Cambios*" de este documento.

1.3 Datos de contacto.

1.3.1 Especificación del ente organizador.

Esta CPS es propiedad de ANF AC

ANF Autoridad de Certificación
Gran Vía de les Corts Catalanes, 996
08018 - Barcelona - España
Tfno.-+34 93 2 661614
FAX.-+34 93 3131 614
Dirección electrónica: ac@anf.es
Dirección web: http://www.anf.es/

Esta CPS esta administrada por la Junta Rectora de la PKI de ANF AC.

JRPKI de la ANF Autoridad de Certificación
Gran Vía de les Corts Catalanes, 996
08018 - Barcelona - España
Tfno.-+34 93 2 661614
FAX.-+34 93 3131 614
Dirección electrónica: juntapki@anf.es

1.3.2 Persona de contacto

Para cualquier información relacionada con esta CPS :

Persona de contacto: F. Díaz
e-mail: diazdiaz@anf.es

1.3.3 Determinación de la adecuación de la CPS a las Políticas de Certificación

La Junta Rectora de la PKI de ANF AC es la entidad que determina la adecuación de esta CPS a las distintas Políticas de Certificación de su PKI.

1.4 Definiciones.

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

Glosario de términos.

Certificado	Un certificado electrónico es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.
Contenedor	Soporte homologado por ANF AC, denominado Contenedor homologado TID. Contiene los datos de creación de firma
Fichero TID	Fichero electrónico que almacena cifrados 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 el Contenedor para poder ser activado.
Receptor	Tercero de buena fe; persona física o jurídica que recibe un fichero electrónico firmado digitalmente por un usuario de ANF AC. Los requisitos de la buena fe de los receptores se determinan en el presente documento.
Sistema TID	Conjunto de programas e instrumentos homologados por ANF AC. Esta CA es la responsable de la seguridad del sistema. Este sistema asume, todo el proceso necesario para la generación de claves, creación y verificación de firma electrónica. En servicios telemáticos, 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. TID™ 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	Titular de un certificado emitido por ANF AC.

Abreviaturas y acrónimos.

AC	Autoridad de Certificación = CA
AR	Autoridad de Registro = AR
CA	"Certificate Authority" = AC
CDIP	Certificado Digital de Identificación Personal.
CN	Componente Nombre
CP	"Certificate Policy". Política de Certificación.
CPS	"Certificate Practice Statement" - Declaración de Prácticas de Certificación.
CRL	"Lista de Revocación de Certificados."
CWA	"Cen Workshop Agreements."
DN	"nombre distintivo (DN o distinguished name)"
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 Identificador del Objeto Digital
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 anexos puede obtenerse libremente en la URL 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.

1.6 Comunidad y ámbito de aplicación.

1.6.1 Autoridad de Certificación.

ANF Autoridad de Certificación es la entidad raíz, y única autoridad de certificación de esta infraestructura de clave pública –PKI-.

Su función es la emisión de los certificados digitales de entidad final para los usuarios de este sistema. Así como la administración y control de la infraestructura que se describe en esta CPS.

ANF AC para la prestación del servicio de certificación puede hacerlo directamente o utilizar autoridades de registro. En cualquiera de las modalidades, ANF AC es la única entidad que decide sobre la aceptación o la denegación de una solicitud de certificado, su activación y publicación.

1.6.2 Autoridad de Registro.

Las Autoridades de Registro son personas físicas o jurídicas nombradas por la Autoridad de Certificación, las cuales se comprometen a seguir las normas que al respecto se establecen en esta CPS, así como a las Políticas de Certificación correspondientes a cada tipo de certificado.

Las Autoridades de Registro son competentes para la tramitación de las solicitudes de certificados electrónicos ante ANF AC. Entre otras funciones, están capacitadas para determinar la adecuación de los peticionarios a los tipos de certificados que solicitan. Su responsabilidad principal es la de realizar labores de identificación y autentificación, en ningún caso emiten ni publican certificados.

1.6.3 Entidades finales.

1.6.3.1 Usuarios

El grupo de usuarios que pueden solicitar la emisión de certificados a ANF AC se encuentran definidos en cada Política de Certificación.

1.6.3.2 Terceros de confianza

De forma general son todas aquellas personas físicas o jurídicas que de forma voluntaria, confían en los certificados digitales emitidos por esta autoridad de certificación.

1.6.4 Ámbito de aplicación.

Las Políticas de Certificación aplicadas por ANF AC y definidas en esta CPS determinan el uso apropiado que debe darse a cada tipo de Certificado.

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

ANF AC posee todos los derechos de propiedad intelectual sobre esta 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.

Se autoriza su reproducción y difusión siempre que se reseñe:

-Copyright ANF Autoridad de Certificación-

Los certificados son propiedad de ANF AC. 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. Política de S e g u r i d a d.

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 servicios de seguridad que se requiere que el sistema proporcione, ante ataques conocidos sobre sistemas de certificación y firma electrónica.

- 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.

2.1 Seguridad de las comunicaciones.

La comunicación entre los distintos módulos empleados por el dispositivo de creación 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 Cifrado.

La información se transmite en todo momento cifrada, 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 (*1).
  - ✓ **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 (*1).

- **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 KEY.

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

Identificación y corroboración de que la fuente de los datos recibidos es quién 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 las siguientes etapas:

- **Identificación:** Se utiliza un identificador único y exclusivo de cada operador. Existen dos modalidades:

A. **Tarjeta TID**, personal e intransferible (hardware = SmartCard), que precisa ser activada mediante clave secreta PIN (conocimiento intelectual).
B. **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 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 (caso de que utilice un instrumento de identificación) 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, las necesidades esenciales de los usuarios pueden continuar siendo atendidas: Revocación, verificación del estado de los certificados emitidos, firma electrónica y sellos de tiempo.

El sistema está dotado de un mecanismo de protección adicional de los sistemas de ANF AC, implementando dispositivos de protección "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.

En cumplimiento de lo establecido en la Ley de servicios de la sociedad de la información y de comercio electrónico, ANF AC retiene los datos de tráfico relativos a las comunicaciones electrónicas que se realizan con sus servidores de Internet. Concretamente:

1 ANF AC retiene los datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información por un período máximo de doce meses.
2. Los datos que, en cumplimiento de lo dispuesto en la LSSI, son únicamente los necesarios para facilitar la localización del equipo terminal empleado por el usuario para la transmisión de la información: número de IP, día y hora de acceso, puerto de acceso y servicio al que se ha accedido.

En ningún caso, la obligación de retención de datos afecta al secreto de las comunicaciones.

ANF AC adopta medidas de seguridad apropiadas para evitar la pérdida o alteración y el acceso no autorizado a los datos de trafico retenidos. Estos datos tienen como único fin y destino:

1. Para su utilización en el marco de una investigación criminal o para la salvaguardia de la seguridad pública y la defensa nacional, poniéndose a disposición de los Jueces o Tribunales o del Ministerio Fiscal que así los requieran. La comunicación de estos datos a las Fuerzas y Cuerpos de Seguridad se hará con sujeción a lo dispuesto en la normativa sobre protección de datos personales.
2. Categoría de los datos retenidos:
   Categoría básica:

   a) Servicio de acceso a los repositorios de certificados emitidos.
   b) Servicio de acceso a los repositorios de certificados revocados.

   Categoría crítica

   c) Servicio de revocación de certificados
   d) Servicio de suspensión de certificados
   e) Servicio de reactivación de certificados
   f) Servicio de renovación de certificados
   g) Servicio de recepción de certificados “Request”
   h) Servicio de Sellos de Tiempo

   En todos los casos, los datos serán almacenados en un soporte magnético que se encontrará en lugar custodiado y de acceso restringido. Transcurrido el plazo de retención previsto, los datos se destruirán salvo que fueran necesarios para otros fines previstos por la Ley.

   El plazo de retención será de:

   6 meses para la Categoría básica .
   12 meses para la Categoría Crítica.

   Los datos serán entregados a los órganos autorizados en soporte óptico.

2.3.c Hardware.

2.3.c.a Equipo Informático

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 del sistema, 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 de tarjetas microprocesadas. La modificación de la configuración de seguridad de estos equipos, solo puede ser realizada 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.c.b Dispositivos criptográficos

Parte de los servidores de ANF AC tienen instalados dispositivos criptográficos, sobre estos dispositivos se establecen los siguientes requerimientos:

- Si un dispositivo criptográfico seguro es accesible, y se encuentra permanentemente fuera del servicio, todas las claves privadas de la ANF AC almacenadas dentro del dispositivo que hayan sido utilizadas o potencialmente puedan ser usadas con propósitos criptográficos, son destruidas.

- Si un dispositivo criptográfico seguro está siendo apartado permanentemente del servicio, todas las claves contenidas dentro del dispositivo que hayan sido usadas con propósitos criptográficos, son borradas del mismo.

- Si el contenedor de un dispositivo criptográfico tiene por finalidad proveer evidencia de falsificaciones y el dispositivo se encuentra permanentemente fuera del servicio, dicho contenedor deber ser también destruido.

- El proceso por el cual el hardware criptográfico de ANF AC es desmantelado y retirado del uso se efectúa en presencia de por lo menos dos empleados confiables. Se procede a efectuar la correspondiente anotación en el inventario de la entidad.

- Se exige a los proveedores del hardware criptográfico que procedan a su transporte utilizando un embalaje inviolable. La recepción de este material es encomendada a personal autorizado de ANF AC, el cual revisa que el embalaje y los precintos se encuentren intactos, seguidamente se efectúa un test de aceptación y verificación de los soportes lógicos

- Los dispositivos utilizados para almacenamiento y recuperación de la clave privada y sus interfaces son sometidos a un test de integridad antes de su utilización.

- Se verifica periódicamente el correcto procesamiento del hardware criptográfico de ANF AC.

- Se efectúa un diagnóstico durante el test de verificación de problemas del hardware criptográfico de ANF AC, en presencia de no menos de dos empleados confiables.

Para prevenir fraudes, el hardware criptográfico de ANF AC es almacenado en un sitio seguro, cuyo acceso está limitado a personal autorizado, con las siguientes características:

a) Procesos de control de inventarios y procedimientos para administrar el origen, recepción, condiciones, salida y destino de cada dispositivo.

b) Procesos de control de acceso y procedimientos para limitar el acceso físico a personal autorizado.
c) Todos los intentos de acceso, autorizados o no, a los servicios de la EPSC y al mecanismo de almacenamiento de los dispositivos ingresados en un registro de eventos.
d) Procesos de incidentes y procedimientos para manejar eventos anormales, brechas de seguridad, investigaciones y reportes.
e) Procesos de auditoria y procedimientos para verificar la efectividad de los controles.

El hardware criptográfico de ANF AC es almacenado en embalajes inviolables.

El manejo del hardware criptográfico de ANF AC se efectúa en presencia de no menos de dos empleados confiables.

La instalación del hardware criptográfico de ANF AC se efectúa en presencia de no menos de dos empleados confiables.

La eliminación del hardware criptográfico de ANF AC de producción se efectúa en presencia de no menos de dos empleados confiables.

El proceso de reparación o servicio del hardware criptográfico, utilizando nuevo hardware, software o soportes lógicos, se efectúa en presencia de no menos de dos empleados confiables.

El lugar de prestación del servicio de mantenimiento, soporte técnico o reparaciones es un sitio seguro con control de inventario y acceso limitado a personal autorizado.

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 cifrada).

Todos los ordenadores de ANF AC tienen instalado un 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*", el cual regula la posibilidad de reconstrucción del Depósito, según el sistema descrito en ese apartado este documento

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.

2.3.f .1 Tipos de eventos registrados.

ANF AC registra todos los eventos relacionados con:

- Intentos exitosos o fracasados de cambiar los parámetros de seguridad del sistema operativo.
- Arranque y parada de aplicaciones.
- Intentos exitosos o fracasados de inicio y fin de sesión.
- Intentos exitosos o fracasados de crear, modificar o borrar cuentas del sistema.
- Intentos exitosos o fracasados de crear, modificar o borrar usuarios del sistema autorizados.
- Intentos exitosos o fracasados de solicitar, generar, firmar, emitir o revocar claves y certificados.
- Intentos exitosos o fracasados de generar, firmar o emitir una CRL.
- Intentos exitosos o fracasados de crear, modificar o borrar información de los titulares de certificados.
- Intentos exitosos o fracasados de acceso a las instalaciones por parte de personal autorizado
- Backup, archivo y restauración.
- Cambios en la configuración del sistema.
- Actualizaciones de software y hardware.
- Mantenimiento del sistema.
- Cambios de personal

2.3.f .2 Frecuencia de procesado de logs

Se establecen tres niveles de auditorías de control de los eventos registros con una frecuencia diaria, mensual y anual respectivamente.

2.3.f .3 Periodo de retención para los logs de auditoría

ANF AC retendrá todos los registros de auditoría generados por el sistema por un periodo mínimo desde la fecha de su creación de un (1) años para los pertenecientes a auditorías diarias, dos (2) años para las mensuales y cuatro (4) años para los de auditorias anuales.

2.3.f .4 Protección de los logs de auditoría

Cada histórico de auditoría que contenga esos registros queda cifrada. Las copias de backup de dichos registros se almacena en un dispositivo dentro de las instalaciones seguras de de la CA..

La destrucción de un archivo de auditoría solo se puede llevar a cabo con la autorización del Administrador del Sistema de ANF AC

2.3.f .5 Procedimientos de backup de los logs de auditoría

Se realizará copia de los mismos sobre soporte óptico, grabando además en el mismo soporte el software necesario para poder proceder a su recuperación o consulta.

2.3.f .6 Sistema de recogida de información de auditoría (interno - externo)

El sistema de recolección de auditorías de la PKI es una combinación de procesos automáticos y manuales ejecutados por los sistemas operativos, las aplicación de la PKI, y por el personal que las utiliza.

2.3.f .7 Notificación al sujeto causa del evento

El administrador del sistema determinará en base a la gravedad del incidente detectado, si notifica el suceso a la persona que lo provocó. En caso de tratarse de una evento calificado como grave, será notificado directamente a la Junta Rectora de la PKI.

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. Comprobación de documentos y bastanteo de escrituras y poderes. Dictámenes de aceptación o denegación en la emisión de certificados.
c) Especialista en Protección de Datos y Seguridad Informática TID: 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: Operador que ha recibido la formación básica del sistema y de las normas que lo regulan.

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 a llevar a cabo.

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. 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. Así mismo se detalla:

a) Necesidad de formación continua;
b) Los requerimientos contractuales que incluyen indemnizaciones por daños causados por acciones del personal contratado y,
c) El derecho de ANF AC a la auditoria y el monitoreo de la actividad desarrollada por el personal contratado.

2.4.6 Control de antecedentes del personal contratado.

El Departamento de Recursos Humanos de ANF AC lleva a cabo una verificación de los antecedentes de todo el personal contratado. Como mínimo las comprobaciones a realizar alcanzan los siguientes aspectos:

Personal que desempeña roles confiables:

a. Comprobación de antecedentes profesionales y obtención de referencias.
b. Comprobación de títulos y acreditaciones profesionales.
c. Verificación de datos de residencia.

Resto de personal:

a Comprobación de antecedentes profesionales y obtención de referencias.
b Verificación de datos de residencia.

2.4.7 Acuerdo de confidencialidad.

Los empleados firman un acuerdo de confidencialidad como parte de los términos y condiciones de su incorporación. Este acuerdo contempla además información sobre la labor de control y fiscalización que los responsables de seguridad de ANF AC realizan permanentemente sobre el personal contratado, el fin de esta actividad es garantizar el más alto grado de seguridad de los servicios que esta CA presta, y de los bienes que tiene la obligación de proteger.

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.

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 de 24 horas y control por circuito de televisión interno permanente.
- La arquitectura y blindaje del edificio corresponden al diseño comúnmente empleado en establecimientos denominados “data center”.
- 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. El personal que accede se encuentra en todo momento acompañado por personal responsable de la administración del “data center” 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 “data center”.
- 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 TID
Se utilizan tarjetas con Microprocesador integrado. Los datos de generación de firma únicamente pueden ser introducidos en la SmartCard 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 Criptográfica TID
Se utilizan tarjetas con Microprocesador integrado, que incluye 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 cifrados. El fichero TID, al contrario que la tarjeta TID, sí que es duplicable, y por tanto, recae una mayor responsabilidad en su usuario, que tiene que extremar la tutela de la clave de activación PIN.

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.

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 usuarios de ANF AC son RSA de 1024 bits.

ANF AC mantiene un seguimiento sobre la evolución de la tecnología eGrid.

La clave de cifrado simétrico de comunicaciones entre módulos es de 1043 bits. Idéntica longitud se emplea en las comunicaciones a través de Internet. Algoritmo simétrico utilizado AES.

2.10 Seguridad a la adecuación a las disposiciones legales.

ANF AC de cada nueva publicación que realiza de sus documentos de prácticas de certificación, solicita un informe jurídico a fin de determinar la correcta adecuación de los mismos a las disposiciones legales vigentes.

ANF AC cuenta con servicios jurídicos que velan por la permanente adecuación de sus prácticas de certificación a las disposiciones legales vigentes. Caso de producirse alguna novedad legislativa o reglamentaria que afecte al sistema PKI de ANF AC, los servicios jurídicos están instruidos para que de oficio eleven a la Junta Rectora de la PKI la correspondiente propuesta de modificación que permita adecuarlos a las nuevas necesidades.

2.11 Seguridad a la adecuación de las CP's asociadas.

Las modificaciones propuestas o las nuevas aportaciones a incluir sobre esta Declaración de Prácticas de Certificación, deberán, previa a su aprobación, ser contrastadas con las Políticas de Certificación asociadas a los certificados emitidos por ANF AC, a fin de asegurar que las CP's soporta estos cambios.

No se podrán realizar cambios que no sean soportados por la CP's asociadas. Deberán, en todo caso, contemplarse simultáneamente con actualizaciones de las CP afectadas.

La Junta Rectora de la PKI de ANF AC es la entidad que determina la adecuación de esta CPS de ANF AC con las que políticas de certificación con las que se relaciona.

2.11 Control de conformidad.

ANF AC realiza periódicamente auditorías que controlan el correcto cumplimiento de cada uno de los apartados de Seguridad. Los procedimientos y frecuencia para la realización de auditorías están regulados en el reglamento interno de la Seguridad Administrativa de ANF AC; los criterios seguidos para la definición de los procedimientos de auditoría se encuentra detallados en el ANEXO III.

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 SmartCard cuenta con este certificado de acreditación internacional.

3.2 ISO 7816.

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

3.3 PC-SC.

Los lectores de SmartCard empleados por 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 ITU-T X.509 de fecha de junio de 1997 (ISO/IEC 9594-8 "Information technology - Open Systems Interconnection - The Directory: Authentication framework", 1997) definida por la Unión Internacional de Telecomunicaciones, Sector de Normalización.

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 que pone a disposición de los usuarios ANF AC que trabajan en un entorno de Microsoft Windows, son dispositivos “Plug and Play” y, por tanto, reconocidos automáticamente por estas plataformas. 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 usuarios de esta PKI, unos niveles básicos de seguridad y calidad, se establece que todos los dispositivos que utilicen deben de estar homologados por ANF AC. Los dispositivos que comprende este apartado son:

a) Contenedor de datos de generación de firma.
b) Dispositivo seguro de creación de firma
c) Dispositivo de verificación de firma.
d) Manejador de las SmartCard

Con el fin de garantizar la más amplia integración del sistema de firma electrónica en los procesos productivos y administrativos de las empresas, ANF 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.

Cualquier empresa o profesional podrá solicitar a ANF AC la homologación de dispositivos por ella desarrollados.

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.
d) Informe favorable del Departamento de I+D de 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, que presupongan una mejora en la prestación de los servicios de certificación o atiendan una necesidad de seguridad técnica. 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 la URL http://www.anf.es/AC/dispositivos.htm

3.8 Dispositivos 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, 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.

ANF AC garantiza que los dispositivos de creación de firma cumplen con los siguientes requerimientos:

1 Los datos de creación de firma son los datos únicos, como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica.
2 El dispositivo de creación de firma es un programa o sistema informático que sirve para aplicar los datos de creación de firma.
3 Que los datos utilizados para la generación de firma pueden producirse sólo una vez y asegura razonablemente su secreto.
4 Que existe una seguridad razonable de que los datos utilizados para la generación de firma no pueden ser derivados de los de verificación de firma o de la propia firma y de que la firma está protegida contra la falsificación con la tecnología existente en cada momento.
5 Que los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros.
6 Que el dispositivo utilizado no altera los datos o el documento que deba firmarse ni impide que éste se muestre al firmante antes del proceso de firma.

Y de acuerdo con la legislación actual, cabe calificarlos como:

"Dispositivos Seguros de Creación de Firma"

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.

ANF AC garantiza que los dispositivos de verificación de firma cumplen con los requerimientos básicos establecidos por la legislación vigente:

1 Los datos de verificación de firma son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica.
2 Un dispositivo de verificación de firma es un programa o sistema informático que sirve para aplicar los datos de verificación de firma.
3 Los dispositivos de verificación de firma electrónica homologados por ANF AC garantizan, que el proceso de verificación de una firma electrónica satisface, al menos, los siguientes requisitos:
    3.3 Que los datos utilizados para verificar la firma corresponden a los datos mostrados a la persona que verifica la firma.
    3.4 Que la firma se verifica de forma fiable y el resultado de esa verificación se presenta correctamente y de forma legible y entendible.
    3.5 Que la persona que verifica la firma electrónica puede, en caso necesario, establecer de forma fiable el contenido de los datos firmados y detectar si han sido modificados.

3.6 Que se muestren correctamente tanto la identidad del firmante o, en su caso, conste claramente la utilización de un seudónimo, como el resultado de la verificación.
3.7 Que se verifican de forma fiable la autenticidad y la validez del certificado electrónico correspondiente.
3.8 Que se detecta cualquier cambio relativo a su seguridad.

4 Asimismo, los datos referentes a la verificación de la firma, tales como el momento en que ésta se produce o una constatación de la validez del certificado electrónico en ese momento, pueden ser almacenados u obtenidos directamente de ANF AC, por la persona que verifica la firma electrónica, si así lo desea.

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 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 usuario 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 y se suscribe el correspondiente Contrato de Prestación de Servicios de Certificación con esta autoridad de certificación.

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.

Cada certificado emitido por ANF AC esta asociado a una Política de Certificación determinada, a la cual esta sometido el titular y los representantes que hacen uso del mismo.

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:

- ***SmartCard TID, SmartCard criptográfica TID y Fichero TID.***

Son propietarios de los contenedores homologados TID, las personas físicas o jurídicas a las que representa la persona física autorizada a utilizar el certificado o, caso de actuar en su propio nombre, el propio usuario.

Las SmartCard TID únicamente son utilizables mediante el uso de manejadores homologados. ANF AC garantiza que estos dispositivos no utilizan la WinsCard de Windows y que están libres del ataque “Trust Winscard”; todos los componentes realizan procesos de autentificación mutua y sus comunicaciones se encuentran cifradas.

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 que el propietario facilite los datos de la persona que será el titular del contenedor y, por tanto, usuario 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) **SamrtCard TID :**
La integración de los datos en la SmartCard, es realizada por el Dispositivo de Generación de Datos de Creación de Firma.

b) **SmartCard Criptográfica TID:**
La propia Smartcard dispone de un Dispositivo de Generación de Datos de Creación de Firma.

c) **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 de los respectivos dispositivos.

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, sino que permite al fabricante dar asistencia técnica y remitir nuevas versiones de su software. Elemento imprescindible para garantizar una adecuación de la seguridad del dispositivo en el transcurso del tiempo.

4.2 Dispositivo de generación de datos de creación de firma.

Las claves de los Usuarios **se generan bajo su exclusivo control** utilizando los instrumentos que ANF AC pone a su disposición. No precisa la intervención de ningún tercero, quedando así garantizado el "no repudio" del usuario (*en combinación con el procedimiento de Sellado de Tiempo de Autoridad en los procesos de creación de firma electrónica descritos en esta CPS*).

Ni esta Autoridad de Certificación ni sus empleados tienen la posibilidad, ni la oportunidad, de copiar o 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 la URL:

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.

El usuario selecciona de forma autónoma cual va a ser su PIN de activación y decide el momento de generar los datos de creación de firma. El dispositivo tiene la capacidad de generar automáticamente el par de claves 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 (datos sobre los que la AR realizará el correspondiente proceso de identificación y autentificación), además de un número de identificación único y exclusivo para ese certificado (certificado de petición – request).

El certificado de petición contiene además del identificador único y los datos del usuario, la clave pública. Este fichero es firmado por el usuario con la clave privada integrada en el contenedor homologado TID. Todo el proceso es realizado de forma automática, sin posibilidad de manipulación por parte del usuario ni de terceros, salvo la inserción del PIN para la activación del proceso. En todo momento siguiendo el protocolo de seguridad de las comunicaciones de ANF AC. No se conoce, hasta la fecha, ningún ataque exitoso a este modelo de procedimiento, por lo cual cabe calificarlo como absolutamente seguro.

ANF AC además de llevar a cabo las correspondientes comprobaciones de identidad del solicitante, las cuales están especificadas en el apartado oportuno de esta CPS, así como contrastar los datos personales con los reseñados en el fichero, procede a la verificación de la firma del certificado con la clave pública en él contenida, estableciendo así la relación del mismo con los datos de generación de firma en posesión del usuario. ANF AC finalmente verifica la integridad del fichero, tras lo cual procede a su emisión. No se conoce ningún ataque de falsificación exitoso a este modelo de procedimiento, este procedimiento garantiza por lo tanto con total certeza, la vinculación de los datos de generación de firma al certificado a emitir.

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:

ANF AC emite las siguientes tipos de certificados, cada uno de ellos cuenta con su respectiva Política de Certificación:

- 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 Clase 1 CA

Los certificados siguientes están sometidos a las Disposiciones que en cada momento establezca la Agencia Tributaria española.

e) Certificados de Clase 2 de Persona física

f) Certificados de Clase 2 de Persona jurídica

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 conforme al estándar X.500.

La AR (Autoridad de Registro) velará de que no puedan emitirse certificados con el mismo nombre de usuario. Proponiendo y aprobando los nombres distintivos para los solicitantes de certificados.

4.4.2 Seudónimo.

Cuando la Política de Certificación del certificado solicitado, permita expresamente el empleo de seudónimos, 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 usuario.

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 Unicidad de nombres.

Todos los certificados requieren un nombre distintivo (DN o distinguished name)

El DN de los certificados contendrá como mínimo los elementos que se citan con el formato siguiente:

> "Se incluirá como parte del nombre común (Common Name) del nombre distintivo, el nombre del usuario seguido de su NIF, con el formato "nombre – número NIF". Caso de que exista un certificado con la misma concordancia de DN (por ejemplo un segundo certificado expedido para una misma persona), la autoridad de registro podrá incluir una numeración correlativa después del NIF, el formato será "nombre – número NIF – número de orden".

Las Políticas de Certificación pueden disponer la sustitución de este mecanismo de unicidad e incluso, no autorizar la emisión de dos certificados de la misma clase a un mismo usuario.

4.4.4 Identidad individual de los Usuarios.

Todos los usuarios que participan en la PKI de ANF AC, son personas jurídicas legalmente constituidas o 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.

Se hace constar que los certificados emitidos por esta Autoridad de Certificación que tengan como titulares a personas jurídicas, contendrán además la identidad de una persona física que será la que esta en posesión del certificado y en disposición de poder utilizarlo.

4.4.5 Identidad de los representantes.

Debe de tratarse de personas físicas. Estas personas tienen que ser mayores de edad y plenamente capacitadas para poder asumir las obligaciones y responsabilidades derivadas de la representación que ostentan.

4.4.6 Nombre alternativo del sujeto.

ANF Autoridad de Certificación tiene asignado el código privado de empresa (SMI Network Management Private Enterprise Codes) 18332 por la organización internacional IANA Internet Assigned Numbers Authority.

Como norma general, los certificados emitidos por esta autoridad de certificación pueden integrar determinados identificadotes OID. Concretamente su equivalencia corresponderá a:

(Prefijo)	iso.org.dod.internet.private.enterprise	ANF.Autoridad de Certificación
1.3.6.1.4.1.18332	**1.3.6.1.4.1**	**18332**

(Prefijo)	Valor	Concepto	Referencia
1.3.6.1.4.1.18332	**10**	Nombre	**persona física representante del titular.**
	11	Primer apellido	
	12	Segundo apellido	
	13	N.I.F.	
	20	Denominación	**persona jurídica titular del certificado.**
	21	C.I.F.	
	30	Nombre	**persona física titular del certificado.**
	31	Primera apellido	
	32	Segundo apellido	

	33	N.I.F.	

A modo de ejemplo y para una mejor comprensión:

	Prefijo + Valor	**Concepto**
O.I.D.	1.3.6.1.4.1.18332.10	Pedro
	1.3.6.1.4.1.18332.11	González
	1.3.6.1.4.1.18332.12	Creus
	1.3.6.1.4.1.18332.13	8769788898F
	1.3.6.1.4.1.18332.20	Comercial Lemas SA
	1.3.6.1.4.1.18332.21	A786769876

Opcionalmente se podrán incluir otros identificadotes de OID que faciliten información complementaria del titular y/o de su representante. La inclusión de estos datos siempre será a requerimiento de los afectados y contando con su expresa autorización.

No obstante, las Políticas de Certificación pueden establecer otros OID e incluso otros procedimientos a seguir, en cuyo caso, prevalecerá lo estipulado en ellas.

4.4.7 Procedimientos de resolución de disputas de nombres, denominaciones comerciales y marcas.

4.4.7.a Nombres

Cualquier disputa concerniente a la propiedad de nombres, será resuelta bajo criterio de la Autoridad de Registro, en caso de que el nombre ya figurará inscrito en ANF AC, prevalecerá el que primero figure registrado.

No obstante ANF AC se reserva el derecho a revocar un certificado en caso de que sobre el mismo se haya establecido una disputa.

4.4.7.b Denominaciones comerciales y marcas

Caso de inclusión de marcas o denominaciones comerciales en el certificado, esta siempre se realizará a petición del titular o del representante del titular del certificado y bajo su exclusiva responsabilidad.

Caso de plantearse una disputa respecto a la propiedad de una denominación comercial o de una marca, siempre prevalecerá la de aquel que acredite ostentar su propiedad en el territorio español.

No obstante ANF AC se reserva el derecho a revocar un certificado en caso de que sobre el mismo se haya establecido una disputa.

4.4.8 Métodos de prueba de posesión de la clave privada.

Dado que el par de claves es generado por el usuario, este deberá probar la posesión de la clave privada correspondiente a la clave pública que solicita que se certifique mediante el envío de la solicitud de certificación en formato PKCS#10.

Esta norma puede verse revocada en caso de que la Política de Certificación que afecta al certificado solicitado, disponga otro tipo de procedimiento.

4.4.9 Autentificación de la identidad de una persona jurídica.

Cada Política de Certificación establece el procedimiento a seguir.

4.4.10 Autentificación de la identidad de una persona física.

Cada Política de Certificación establece el procedimiento a seguir.

4.4.11 Autentificación de la identidad de los representantes.

Cada Política de Certificación establece el procedimiento a seguir.

4.4.12 Renovación rutinaria de un certificado.

Cada Política de Certificación establece el procedimiento a seguir.

4.4.13 Renovación de un certificado después de una revocación

Esta autoridad de certificación no permite la renovación de certificados revocados.

4.4.14 Renovación de un certificado suspendido

Esta autoridad de certificación no permite la renovación de certificados en estado “suspendidos”.

4.4.15 Solicitud de revocación o suspensión

El procedimiento de identificación y autentificación para solicitar una revocación se establece en cada Política de Certificación.

4.5 Revocación y suspensión de certificados.

4.5.1 Procedimiento.

- **Presencial:**

Personándose en las oficinas de ANF AC cuya dirección consta en este documento o en cualquiera de oficinas de las Autoridades de Registro cuya lista figura en la URL http://www.anf.es/ARaeat/ .

- **Telemáticamente:**

a) Enviando solicitud firmada electrónicamente a la cuenta de correo electrónico revocar@anf.es indicando en el asunto *Revocar* y adjuntando el formulario de revocación cumplimentado y firmado.

b) Mediante conexión telemática al Registro de Certificados, de acuerdo con el procedimiento establecido en la sección *"Accesibilidad –Usuarios de ANF AC-"* de esta CPS de ANF AC.

c) Mediante correo electrónico, y desde la cuenta que en el momento de tramitar la solicitud se calificó como segura a la cuenta revocar@anf.es indicando en el asunto *Revocar* más el identificador del certificado. El servidor de ANF AC contestará facilitando un número operacional que deberá ser respondido según las indicaciones que él se detallen.

- **Mediante llamada telefónica:**
  Mediante llamada telefónica a la Oficina de Atención al Cliente 902 902 172, formulando la correspondiente solicitud.

- **Mediante correo tradicional:**
  Enviando el formulario debidamente cumplimentado a las oficinas de ANF AC cuya dirección consta en este documento, firmado y reseñando en el mismo login, password e identificador del certificado.

Los procedimientos reseñados deben de ser complementados con lo especificado en el apartado "*Identificación y autentificación – Solicitud de revocación*" especificados en cada Política de Certificación.

4.5.2 Revocaciones.

Las revocaciones son definitivas. 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, 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 usuario, la persona que lo representa, la propia AC y la Autoridad de Registro que tramitó su identificación. Cuando la revocación no sea solicitada por el usuario, ANF AC le notificará este hecho mediante correo electrónico remitido a la dirección que hizo constar el usuario en su solicitud de certificado, siempre que sea posible de manera previa a la suspensión, o simultáneamente a que se produzca la misma.

Se procederá a la revocación del certificado a petición del usuario, la persona a la que representa, ANF AC o AR por incumplimiento de las obligaciones impuestas en esta CPS, 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 del usuario, o al del certificado que AC empleo para su emisión.
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.
g. El mal uso deliberado de claves y certificados, o falta de observación de los requerimientos operacionales del acuerdo de suscripción.
h. La negligente actuación del usuario en el ámbito de esta PKI, aunque se haya producido con otro certificado distinto al que se va a revocar.
i. Resolución judicial o administrativa que lo ordene.
j. Fallecimiento o extinción de la personalidad jurídica del firmante; fallecimiento, o extinción de la personalidad jurídica del representado; incapacidad sobrevenida, total o parcial, del firmante o de su representado; terminación de la representación; disolución de la persona jurídica representada o alteración de las condiciones de custodia o uso de los datos de creación de firma que estén reflejadas en los certificados expedidos a una persona jurídica.

Si la solicitud de revocación es a instancias del propio titular o de su representante legal, deberá, tanto si se realiza en papel o en formato electrónico, contener la información que se especifica en el "Formulario de Solicitud de Revocación" incluido en cada Política de Certificación a la que se asocia ese certificado.

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.

Se establece un periodo máximo de 6 meses para el mantenimiento de una suspensión, transcurrido ese plazo el certificado será revocado de oficio.

La referencia de todo certificado en suspenso será incluida en el Registro de Certificados, 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 usuario, la persona que lo 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 usuario, ANF AC le notificará este hecho mediante correo electrónico remitido a la dirección que hizo constar el Usuario en su solicitud de certificado, siempre que sea posible de manera previa a la suspensión, o simultáneamente a que se produzca la misma.

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.

Si la solicitud de suspensión es a instancias del propio titular o de su representante legal, deberá, tanto si se realiza en papel o en formato electrónico, contener la información que se especifica en el "Formulario de Solicitud de Suspensión" incluido en cada Política de Certificación a la que se asocia ese certificado.

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.

4.6 Solicitud, emisión y aceptación de los Certificados.

4.6.1 Solicitud.

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

4.6.2 Emisión.

El mecanismo que determina el procedimiento a realizar es la Política de Certificación aplicable a cada certificado.

4.6.3 Aceptación.

El mecanismo que determina el procedimiento a realizar es la Política de Certificación aplicable a cada certificado.

4.7 Caducidad y renovación.

Cada Política de Certificación establece el procedimiento a seguir.

4.8 Atributos.

Definen documentos y operaciones homologadas por esta AC. Su exclusión en el momento de generar el certificado incapacita al usuario 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, Registro de Entrada de Documentos o procesar firmas en "Modo Autofirma" 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 usuario, 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.

Esta norma puede verse revocada en caso de que la Política de Certificación que afecta al certificado solicitado, disponga otro tipo de consideración.

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 usuario.
c) Utilizar un contenedor de datos de creación de firma homologado por ANF AC.
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, emisión 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.

Toda la información y documentación relativa a los certificados emitidos por esta Autoridad de Certificación, así como los propios certificados y sus circunstancia históricas, especialmente incidencias de suspensión, reactivación, renovación y revocación, deberá ser conservadas y accesibles al menos por un periodo mínimo de **quince años**.

El Registro de Certificados se localiza en la siguiente URL :

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

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 completo del usuario 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/LDAP: Repositorio donde se almacenan copias de los certificados de los Usuarios de ANF AC y los propios certificados de AC de ANF AC en formato x.509 v.3.

Servicio SOAP, que permite la actualización incremental telemática de la lista de certificados revocados.

Servidor Delegado. Que contiene una lista actualizada de todos los certificados emitidos por ANF AC, con información relativa a su estado de vigencia, suspensión o revocación.

Servicio OCSP, (**Online Certificate Status Protocol**), según el estándar RFC – 2560 que permite obtener el estado de un certificado evitando tener que descargar la Lista de Certificados Revocados (CRL).

d) CRL: "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:

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

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 identificador del certificado o login del usuario, 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 completo del usuario 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.

Otras entidades, mediante acuerdo específico con ANF AC se podrán habilitar otros sistemas de consulta e incluso, la implantación de servidores externos de la CA.

4.12.c Tasas de acceso a los certificados, e información de su estado de activación, revocación o suspensión.

El acceso a la información mediante consulta World Wide Web o CRL es libre y gratuita, y por tanto, no se aplicará ninguna tarifa. Cualquier otra modalidad de consulta se regulará mediante acuerdo específico y tendrá consideración de Condiciones Particulares del presente documento.

4.12.d 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.d.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 usuario:
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 usuario 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.d.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 usuario.

4.12.d.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.d.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.e Administración.

4.12.e.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.e.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 usuarios 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.
4) El informe será firmado por ANF AC y se estampará sello de tiempo que acredita el momento en que se ha efectuado la verificación.El soporte en el que se emite el informe será electrónico.

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

4.12.f 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 15 años contados desde el momento de su expedición, sin perjuicio del derecho de cancelación sobre aquellos datos de carácter personal que establezca la legislación vigente.

4.12.g Frecuencia de la emisión de CRLs.

ANF AC publicará una nueva CRL en su repositorio, de forma simultanea a que se produzca cualquier revocación.

ANF AC mantendrá este tipo de ficheros cuando la legislación vigente así lo requiera.

4.12.h Requisitos de comprobación de CRLs.

Los terceros de confianza deberán comprobar el estado de validez del certificado de ANF AC empleando los dispositivos de verificación homologados por ANF AC.

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 de forma telemática. Los interesados deberán acceder a la Web de ANF AC, URL: http://www.anf.es/ , teniendo conocimiento del identificador del certificado en cuestión, o el login del usuario titular del mismo.

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 usuario.

4.15 Certificados de ANF AC.

4.15.a Protección de las Claves Privadas.

Control redundante de la Clave Privada:

La Clave Privada de estos certificados se encuentra integrada en un ordenador y debidamente cifrada. Para su uso se requiere realizar el correspondiente proceso de descifrado y activación mediante PIN secreto.

Para el uso de la clave se requiere el empleo de un software específico, software que a su vez tiene que ser activado mediante una SmartCard de alta seguridad, al igual que el ordenador que lo contiene, el cual esta blindado mediante una segunda SmartCard.

Las tarjetas de activación del software y del hardware se encuentran en poder de personas distintas, y la activación de los dispositivos requiere la presencia de ambos responsables.

4.15.b Objetivos del uso de claves.

La clave de firma de ANF AC se utilizan para Emitir Certificados.

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 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 la Junta Rectora de la PKI.

Todas las copias y fragmentos de la clave privada de ANF AC se destruyen al finalizar el ciclo de vida de su par de claves.

4.15.d 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 la URL: http://www.anf.es/AC/certificados.htm

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.

4.16 Perfiles de Certificado y CRL.

4.16.a Perfil de Certificado.

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

4.16.b Perfil de CRL.

4.16.b.1 Numero de versión.

El formato de las CRLs es el especificado en la versión 2 (v2).

4.16.b.2 CRL y extensiones.

La presente CPS y sus Políticas de Certificación soportan y utilizan CRLs conformes al estándar ITU - x509

5 Autoridad de Registro.

Para llevar a cabo la Prestación del Servicio de Certificación, ANF AC podrá realizarla de forma autónoma o utiliandor a **Autoridades de Registro** "AR" cuya relación se especifica en cada Política de Certificación (CP) que se asocia a cada uno de los certificados emitidos por esta CA.

Las funciones a realizar por las Autoridades de Registro quedan especificadas en cada Política de Certificación asociada a los certificados emitidos por esta autoridad de certificación. De forma general y siempre en concordancia con lo especificado en cada (CP) cabe señalar que

- Las Autoridades de Registro reconocidas (AR) llevarán a cabo la identificación y autentificación de los solicitantes de Certificados de acuerdo con las estipulaciones reseñadas en las Políticas de Certificación asociadas al certificado solicitado. Así mismo, le corresponde a la Autoridad de Registro comprobar la identidad y autorización de la persona física que representa al usuario.

- La valoración final de la suficiencia o no de la comprobación realizada por la AR, así como de los documentos aportados, siempre correrá a cargo de ANF AC.

- Las Autoridades de Registro reconocidas 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.

- Las Autoridades de Registro reconocidas analizarán toda la documentación aportada por el solicitante, compulsarla con las copia que se incluyan en el formulario de petición (numerándolas y visándolas una a una), estimar su capacidad para ostentar el certificado solicitado, la adecuación de la clase de certificado solicitado a las características del solicitante, determinar la suficiencia y validez de las acreditaciones que acompaña a la solicitud y rechazar en caso de duda su tramitación. En general aceptar o denegar la tramitación de solicitudes de certificados.

- Serán las Autoridades de Registro Reconocidas las encargadas de comunicar a los Usuarios la decisión que por su parte adopten sobre su solicitud. No obstante es la Autoridad de Certificación la que adopta la última decisión de aceptación o denegación a emitir un certificado, y notificar al titular la emisión del certificado y la forma de obtener copia del mismo.

- Las Autoridades de Registro reconocidas únicamente podrán tramitar solicitudes de Usuarios que ya hayan generado sus datos de creación de firma, que los mismos se encuentren integrados en contenedores homologados TID y hayan enviado los certificados de petición a la Autoridad de Certificación. Instruirán a los solicitantes en el uso de los certificados, en sus obligaciones y deberes y especialmente, en lo especificado en este documento, sus Anexos y CPs

- Si de las manifestaciones realizadas por el solicitante, la AR reconocida llega a conocer o sospechar que la seguridad de los datos de creación de firma o que el PIN de activación esta comprometido, ya sea por la intervención de terceros durante el proceso de generación o bien, que se ha producido una transferencia de conocimiento del PIN a terceros, la AR tiene la obligación de rechazar la tramitación de la solicitud de certificado, aunque todo ello se haya realizado de forma voluntaria por el propio titular. Igualmente la AR rechazará la tramitación de la petición, si sospecha que la petición se efectúa bajo presión, o en cualquier caso presuma que el procedimiento de solicitud no se ejercita bajo el principio del libre consentimiento.

- Las Autoridades de Registro reconocidas velarán para impedir que puedan emitirse certificados con nombres de usuarios idénticos, todos ello sobre la base de "Nombre Distintivo".

Los criterios de valoración que seguirá la AR para valorar la documentación que garantiza la correcta identificación del usuario serán los normalmente 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 Avanzada y Sello de Tiempo

ANF AC garantiza que la firma electrónica asociada a los certificados emitidos por esta autoridad de certificación y generada por los dispositivos de creación de firma electrónica homologados por ANF AC, permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere, y que ha sido creada por medios que el firmante puede y debe de mantener bajo su exclusivo control.

Y de acuerdo con la legislación actual, cabe calificarla como:

"Firma Electrónica Avanzada"

La Junta Rectora de la PKI es el órgano que controla y tutela que el producto resultante de la aplicación de los datos de generación de firma, utilizando dispositivos homologados por ANF AC, cumpla con la calificación expresada.

La Ley obliga a los prestadores de servicios de certificación a efectuar una tutela y gestión permanente de los certificados electrónicos que expiden.

ANF AC para llevar a cabo la Prestación del Servicio de Certificación emplea tecnología de Notariado electrónico -**NA (Notary Authority)- o -TSA (Time Stamp Authority)-,** este procedimiento además de atender el mandato legal de "tutela y gestión permanente", permite garantizar el "**no repudio**" de las firmas generadas. ANF AC en "tiempo real" verifica el estado del certificado electrónico, autorizando o denegando la generación de la firma según su estado de vigencia, avala 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 usuario "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 y el Registro de Entrada de Documentos.

Para procesar la firma deben de utilizarse dispositivos homologados por ANF AC.

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 la URL:

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 usuario.

	Modo Local
• **Fase previa.**	- Arranque del software (autentificación mutua de los dispositivos), **el sistema esta protegido contra el ataque "Change Scard".** - El usuario 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.**	- Comunicaciones cifradas entre dispositivos. - Autenticación del contenedor homologado TID. - Verificación del PIN.
• **Hash.**	- Valoración de las limitaciones de uso del certificado para poder firmar el documento o fichero. - Generación del resumen "hash". **El sistema esta protegido contra el ataque "Trust NSA".**
• **Comunicación.**	- El dispositivo establece comunicación con servidor de notariado de ANF AC. - ANF AC procede a autenticar la conexión, dispositivos y usuario.
• **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 firmado
NOTA IMPORTANTE: *en ningún caso la Autoridad de Certificación recibe el documento o fichero a firmar. Ver servicio "Guarda y Custodia".*	

• **Generación** *(autorización de firma).*	- ANF AC en caso de autorización, permite al usuario el empleo de los datos de generación de firma con el dispositivo de creación de firma electrónica.
• **Sello de tiempo** *(autorización de firma).*	- ANF AC genera hash **de los datos relativos a la firmas generadas,** incluyendo el tiempo t, en la forma de fecha y hora de la recepción, componiendo [h(D), t].
	Protocolo
	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. 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.** Además del número de petición único, cada servidor de notariado, adjudica un número de transacción único de las peticiones de firma recibidas. Se registra entre otros datos el número de transacción, junto al identificador del certificado instante de la firma y el número de serie único n. **El modo de generar el número de serie único:** **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. Dado que esta Autoridad de Certificación puede tener n servidores de notariado funcionando simultáneamente, cada sello de tiempo incorpora el identificador del servidor que ha intervenido en la transacción. Es en este servidor contra el que se debe de efectuar el proceso de comprobación anteriormente reseñado.	
• **Comprobante de firma.**	La firma electrónica avanzada queda automáticamente depositado en: **Ordenador del usuario.**
• **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 además estampa sello de tiempo tras verificar, el estado de los certificados a los que se vinculan las firmas electrónicas. Todas las partes reciben una copia de las firmas creadas.

	Modo Web
• **Fase previa.**	- El usuario selecciona el fichero o documento a firmar. - El dispositivo posibilita la visualización previa del documento. - Introducción del PIN (en un plazo máximo de 60 segundos).
• **Validación.**	- Comunicaciones cifradas entre dispositivos. - Verificación del PIN. - Autenticación del contenedor homologado TID.
• **Hash.**	- Generación del resumen "hash". **El sistema esta protegido contra el ataque "Trust NSA".** - 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, 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.
	Durante el proceso de firma se integra la identidad del firmante por reseña del identificador único de su certificado y el nombre del fichero firmado
NOTA IMPORTANTE: *en ningún caso la Autoridad de Certificación recibe el documento o fichero a firmar. Ver servicio "Guarda y Custodia".*	

• **Generación** *(autorización de firma).*	- ANF AC en caso de autorización, permite al usuario y a la ER el empleo de los datos de generación de firma con el dispositivo de creación de firma electrónica.
• **Sello de tiempo** *(autorización de firma).*	- ANF AC genera hash **de los datos relativos a la firmas generadas,** incluyendo el tiempo t, en la forma de fecha y hora de la recepción, componiendo [h(D), t].
	Protocolo

	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. 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.** Además del número de petición único, cada servidor de notariado, adjudica un número de transacción único de las peticiones de firma recibidas. Se registra entre otros datos el número de transacción, junto al identificador del certificado instante de la firma y el número de serie único n. **El modo de generar el número de serie único:** **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. Dado que esta Autoridad de Certificación puede tener n servidores de notariado funcionando simultáneamente, cada sello de tiempo incorpora el identificador del servidor que ha intervenido en la transacción. Es en este servidor contra el que se debe de efectuar el proceso de comprobación anteriormente reseñado.	
• **Documento y comprobante de firma.**	El documento firmado queda automáticamente depositado en: • Ordenador del usuario. • Ordenadores WWW que establezca la ER, incluso en el repositorio de ANF AC si tiene contratado el servicio de "*Almacén y Custodia*" 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.

	Modo Autofirma
• **Fase previa y validación.**	Según lo establecido en el apartado "*Certificados de ANF AC y Certificados de Autenticación"* de este documento.
• **Solicitud de firma.**	El dispositivo genera el "hash" del documento y procesa su firma. **el sistema esta protegido contra el ataque "Trust NSA".**

• **Hash.**	- Generación del resumen "hash". **El sistema esta protegido contra el ataque "Trust NSA".** - 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. 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.
• **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).
• **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 se encapsula para poder ser descargado vía Web.
• **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 usuario, 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 usuario y de la AC que emite el certificado y garantiza la firma.

Es responsabilidad del receptor del documento firmado, verificar y valorar la adecuación del tipo de certificado vinculado a la firma electrónica, así como 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 la URL: 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 los dispositivo homologados de verificación de firma electrónica de ANF AC:

1) **Fase previa.**

   Selección del fichero firmado.

2) **Verificación.**

   a) Los datos utilizados para verificar la firma corresponden a los datos mostrados a la persona que verifica la firma.
   b) Se verifica la integridad del fichero electrónico con relación a la firma electrónica a la que se le vincula (comparación de la huella digital del fichero firmado, con la que contiene la firma electrónica).
   c) El resultado de verificación muestra la identidad del usuario y en caso de seudónimos, se hace constar claramente.
   d) Se verifica de forma fiable la autenticidad y la validez del certificado electrónico. La tecnología empleada imposibilita la falsificación de certificados, **el sistema esta protegido contra el ataque "Trust Clonation".**
   e) Se valida o deniega la relación de la firma electrónica con el certificado al que se la vincula.
   f) 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.
   g) Se determina el estado del certificado: activado, revocado o suspendido, en el momento en que se generó la firma electrónica asociada al mismo.
   h) 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 usuarios.
      h. Posible representación que ostentan los usuarios.
      i. Tipos de certificados empleados.
      j. Resto de firmas estampadas.

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

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

Asimismo, el destinatario del documento o fichero electrónico firmado, puede requerir que el proceso de verificación sea realizado por la propia autoridad de certificación, en cuyo caso, el informe de verificación contendrá además de los datos anteriormente reseñados:

- Sello de tiempo que determina el momento en el que se ha realizado la verificación.
- Información del estado en el que se encuentra en ese momento el certificado asociado a las firmas electrónicas verificadas.

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 usuarios 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 este documento.
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.

b) Directorio exclusivo.
Cada directorio es exclusivo de la entidad contratante del servicio.

c) 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.

d) Copias de seguridad.
Con el fin de garantizar lo establecido en el apartado anterior (*c) 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.

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

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

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

h) Control de acceso.
Se seguirán los mismo parámetros en materia de seguridad a los reseñados en el apartado "*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 usuario, 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) guión (-) 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) guión (-) 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 anterior apartado 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 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 esta CPS.

9 Obligaciones y Responsabilidades.

9.1 ANF AC.

9.1.1 Generales.

Se responsabiliza en cumplir con todas las obligaciones exigibles a los prestadores de servicios de certificación de acuerdo con la legislación vigente. Así como todas las derivadas del presente documento, sus anexos y Políticas de Certificación. La siguiente relación es meramente enunciativa y no limitativa.

ANF AC se compromete a:

- Proteger las Claves Privadas contra el peligro de usurpación.
- Emitir certificados en conformidad con las Políticas de Certificación que le sean aplicables.
- Emitir certificados de acuerdo con los requerimientos expresados en la solicitud, siempre que estos requerimientos sean compatibles con los términos expresados en esta CPS, sus Anexos y Políticas de Certificación.
- Conservar registrada toda la información y documentación relativa a un certificado emitido por ANF AC por un plazo no inferior a cuatro años a contar desde la fecha de caducidad del mismo.

9.1.2 Del repositorio.

- Mantener accesible vía Web para toda la comunidad que participa en esta PKI un repositorio con el conjunto de certificados emitidos en formato x.509.v3, con información actualizada y detallada sobre su estado: vigencia, suspensión o revocación.
- Mantener accesible para el público en general el repositorio de sellos de tiempo.
- Mantener accesible para el público en general el repositorio de CRL.

9.1.3 Limitaciones de las responsabilidades.

ANF AC no responderá de otros daños y perjuicios que los expresamente reseñados en la Ley de Firma Electrónica vigente.

9.1.4 Deslinde de responsabilidades y limitaciones de pérdidas.

En ningún caso responderá de daños o perjuicios comerciales, profesionales o empresariales, salvo que exista contrato de prestación de servicios expreso, que como Condiciones Particulares vinculadas a esta CPS, hayan sido previamente aceptadas por ANF AC.

9.1.5 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.

9.1.6 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.

9.1.7 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 la Junta Rectora de la PKI.

ANF AC procederá al borrado de la clave comprometida de todos los dispositivos que la contienen, y en aquellos que la clave este integrada en una SmartCard, se procederá a la destrucción física de la misma.

9.1.8 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 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, a las ER y a la Administración Pública, con la antelación que establezca la legislación vigente y en la forma que en ella se requiera, en cualquier caso con una antelación mínima de un mes.

9.1.9 Garantías Patrimoniales de ANF AC.

ANF AC garantiza su responsabilidad frente a sus usuarios y terceros afectados de forma suficiente a lo establecido en la legislación vigente .

9.1.10 Subcontratación.

Aunque ANF AC puede optar por delegar una parte de sus roles y de sus respectivas funciones, siempre seguirá siendo igualmente responsable final por el cumplimiento de las funciones definidas y por la definición y mantenimiento de su CPS..

9.2 Usuarios.

Se responsabiliza en cumplir todas las obligaciones derivadas del presente documento, sus anexos y Políticas de Certificación. Limitando y adecuando el uso del certificado y de los sistemas de firma electrónica contemplados en el ámbito de esta PKI, a propósitos lícitos y acordes con una honesta y leal actuación con toda la comunidad: ANF AC, Autoridades de Registro, otros usuarios y terceros de confianza. La siguiente relación es meramente enunciativa y no limitativa.

El usuario se compromete a:

- Asegurarse de que toda la información contenida en el Certificado es cierta.
- Utilizar el certificado respetando las restricciones que le vienen impuestas según su Política de Certificación
- Emplear exclusivamente dispositivos homologados por ANF AC, tanto para el almacenamiento de los datos de generación de firma, como para la creación de firmas electrónicas, como su posterior verificación.
- Caso de que el certificado reseñe “Atributos y Limitaciones de uso” , deberá atenerse a lo ahí indicado.
- 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.
- Suministrar a las Autoridades de Registro documentación original e información que consideren exacta y completa. Así como a notificar cualquier modificación que sobre la misma se produzca.
- Abonar las tasas de los servicios que le sean prestados por parte de la Autoridad de Certificación, o por parte de la Autoridad de Registro.
- Y en general, a todas las derivadas de la Ley de Firma Electrónica, es especial la reseñadas en el artículo 23 apartado 1º.

9.3 Terceros de confianza.

Tiene la consideración de receptor, el tercero de buena fe que confía en el fichero electrónico que está firmado digitalmente por un usuario 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 un dispositivo de verificación de firma electrónica homologado por ANF AC.

- El destinatario del documento o fichero electrónico firmado debe de actuar de forma diligente. Se considerará que si actuación ha sido negligente si incurre en alguno de los supuestos contemplados en la Ley de Firma Electrónica en su artículo 23 apartado 4 puntos a y b.

- Debe de valorar la adecuación del certificado asociado a la firma electrónica, de acuerdo con el tipo de certificado y las limitaciones de uso que en el mismo se reseñan.

- Debe de solicitar el asesoramiento de la "Oficina de Atención al Cliente" de ANF AC en caso de duda..

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

9.4 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.

9.5 Autoridad de Registro.

9.5.1 Generales.

Las AR están obligadas a realizar todas sus operaciones en conformidad con los establecido en esta CPS y la Política de Certificación aplicable en cada caso. La siguiente relación es meramente enunciativa y no limitativa:

- 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.

- Admitir únicamente documentación original en el proceso de identificación, obteniendo copia de la documentación aportada por los usuarios. Documentación que será remitida a la autoridad de certificación para su guarda y custodia.

- Utilizar exclusivamente formularios homologados por ANF AC. Cumplimentándolos de la forma más exhaustiva posible y sin errores.

- Formalizar el Contrato de Certificación con el suscriptor.

- No autorizar la emisión de certificados a personas que presenten o, sobre las que existan, dudas de minusvalía síquicas. Cuando las causas hayan sobrevenido y enterada la AR, procederá a la revocación de oficio del certificado del afectado.

- Mostrar la máxima diligencia y esfuerzo en informar y facilitar todo el soporte posible a los usuarios peticionarios, a cerca de los conceptos básicos de un sistema PKI, y en

especial de la correcta interpretación de esta CPS. Caso de evidente incapacidad del usuario peticionario, la AR deberá denegar la expedición del certificado.

- Informar, a los usuarios que soliciten sus servicios, de su precio, de las condiciones precisas para la utilización del certificado, de sus limitaciones de uso y los derechos que le asisten de acuerdo con la Ley Orgánica de Protección de Datos. En especial, notificando la transmisión de datos y el almacenamiento que se van a realizar de los mismos en los sistemas informáticos de ANF AC.

- 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 de emisión de Certificados.

- No almacenar ni copiar los datos de creación de firma de la persona a la que haya prestado sus servicios.

- Almacenar de forma segura y permanente, copia de la documentación aportada por el usuario para realizar su petición, así como de la documentación generada por la AR, durante el proceso de petición, registro, renovación, suspensión o revocación.

- La comprobación de la documentación aportada, así como la valoración de la suficiencia o insuficiencia de la misma, para emitir un dictamen de autorización o denegación en la emisión de un certificado, deberá ser efectuada por un Licenciado en Derecho.

- Colaborar con las auditorias dirigidas por ANF AC para validar la renovación de sus propias claves.

- Solicitar la revocación de un certificado cuando tenga conocimiento o sospecha de que la seguridad de la clave privada ha quedado comprometida.

9.5.2 Deslinde de responsabilidades y limitaciones de pérdidas.

Las Autoridades de Registro no responderán de otros daños y perjuicios que los expresamente reseñados en la Ley de Firma Electrónica vigente. En ningún caso responderán de daños o perjuicios comerciales, profesionales o empresariales, salvo que exista contrato de prestación de servicios expreso, que como Condiciones Particulares vinculadas a esta CPS, hayan sido previamente aceptado por la Autoridad de Registro.

10 Responsabilidad Financiera.

10.1 Indemnización a las partes confiantes.

ANF AC de acuerdo con lo establecido en la Ley de Firma Electrónica, ha solicitado la contratación de un seguro de responsabilidad civil por importe de TRES MILLONES DE EUROS (3.000.000.-) para afrontar el riesgo de la responsabilidad por los daños y perjuicios que pueda ocasionar el uso de los certificados que emita. Este trámite se realiza ante compañías de seguros de solvencia acreditada radicadas en España.

Los datos relativos a la póliza contratada constarán publicados en la URL: http://www.anf.es/AC/seguro/

10.1 Relaciones fiduciarias.

ANF AC no se desempeña como agente fiduciario ni representante en forma alguna de los usuarios ni de los terceros de confianza en los certificados que emite.

10.2 Procesos administrativos.

ANF AC garantiza la realización de auditorías de los procesos y procedimientos de forma regular.

11 Política de Confidencialidad.

11.1 Protección de Datos de Personales

A los efectos de lo dispuesto en la normativa sobre tratamiento informatizado de los datos de personas físicas LOPD (*), 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 "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).

(*) *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.*

11.2 Tipos de información confidencial

Se declara expresamente como información confidencial y no podrá ser divulgada a terceros, excepto en los casos en que la ley exija lo contrario:

- La identidad de los titulares de certificados que han sido emitidos bajo un seudónimo.
- Cualquier información o dato, que habiendo sido aportado por el usuario a la autoridad de certificación o la autoridad de registro, no conste en el certificado digital.
- Toda información relativa a los parámetros de seguridad, control y procedimientos de auditoría.
- Las claves privadas de ANF AC, de las Autoridades de Registro y de los usuarios.
- Cualquier otra información que ANF AC o la Junta Rectora de la PKI de ANF AC clasifique como “Confidencial”.

11.3 Envío a la autoridad judicial y/o policial

Como norma general ningún documento o registro perteneciente a ANF AC se envía a las autoridades judiciales o policiales, excepto cuando:

- El agente de la ley se identifica adecuadamente

- Se proporcione una orden judicial debidamente redactada

- La Autoridad de Certificación o de Registro tengan conocimiento que los certificados emitidos, o alguno de los instrumentos pertenecientes a esta PKI, están siendo utilizados para la comisión de un delito.

11.4 Divulgación a petición del propietario

El propietario de la información podrá requerir a ANF AC la emisión de un informe de la información de su propiedad, que esta almacenada o depositada en la Autoridad de Certificación o en la Autoridad de Registro. ANF AC facilitará presupuesto de la tasa correspondiente a ese servicio, y tras la aceptación, expedirá el mencionado informe.

11.5 Otras circunstancias de publicación de información

No esta permitida la divulgación de información bajo ninguna otra circunstancia de las reseñadas en los puntos expresados en este documento.

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:

- La actual legislación vigente 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.
- Consultas generales sobre los conceptos básicos de Infraestructura de Clave Pública, certificados digitales y firma electrónica.

Así mismo, realizará en nombre del Usuario o de la persona a la que éste representa, las distintas operaciones que esta 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 usuario 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, esta entidad prestadora de servicios de certificación, cuenta con formularios al efecto. Estos pueden ser libre y gratuitamente descargados a través de Internet, en la URL: http://www.anf.es/AC/reclamaciones/

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

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

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

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.

13.6 Procedimientos de resolución de disputas.

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

ANF Autoridad de Certificación se somete voluntariamente para la solución de cualquier cuestión litigiosa que pudiera surgir por el ejercicio de su actividad, al arbitraje institucional del Tribunal Arbitral del Consejo Empresarial de la Distribución (TACED), al que se le encarga la designa del Árbitro – que será único – y la administración del arbitraje – que será de equidad – con arreglo a su Reglamento, obligándose desde ahora, al cumplimiento de la decisión arbitral. Caso de que la alguna de las partes contrarias a ANF AC no acepte este procedimiento arbitral, se seguirá lo establecido en el apartado 14.6.b.

13.6.a Procedimiento judicial.

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

14 Publicación y repositorios.

14.1 Publicación de información de la CA.

Es obligación de esta autoridad de certificación publicar información relativa a sus practicas, sus certificados y el estado en que se encuentran dichos certificados. Toda el histórico de esta documentación deberá estar conservada y accesible al menos por un periodo mínimo de quince años.

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

Las Políticas de Certificación son públicas y se encuentran disponibles en el sitio Web de la autoridad de certificación http://www.anf.es/AC/documentos/.

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

El certificado emitidos por ANF AC son públicos y se encuentran disponible en el sitio Web de la autoridad de certificación http://www.anf.es . Su consulta sobre base de datos esta regulada en este documento, al igual que la obtención de una copia en formato x.509 v.3 del repositorio.

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

14.2 Frecuencia de publicación.

La CPS y las Políticas de Certificación se publicarán en el momento de su creación.

Los certificados emitidos por la CA se publican de forma inmediata a su emisión.

La autoridad de certificación creará simultáneamente al acto de revocación del certificado, una nueva CRL que lo incluye.

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

14.3 Controles de acceso.

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

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

14.4 Repositorios.

El repositorio LDAP ANF AC es un servicio de directorio LDAP, en alta disponibilidad, accesible en: ldap://ldap.anf.es:389.

El repositorio de LDAP ANF AC no contiene ninguna información de naturaleza confidencial.
.

El repositorio de Sellos de Tiempo es un directorio Web, accesible en la URL http://www.anf.es/timestamp/

El repositorio de Sellos de Tiempo de ANF AC no contiene ninguna información de naturaleza confidencial.

14.5 Procedimiento de especificación de cambios.

Esta Declaración de Practicas de Certificación y las Políticas de Certificación pueden sufrir cambios en el transcurso del tiempo.

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

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

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

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

La entrada en vigor de la nueva versión será en el momento en que se produzca su inscripción en el Registro General de Condiciones Generales de Contratación

14.6 Procedimiento de Publicación y Notificación.

Cuando se produzca un cambio de versión, se comunicará a todos los usuarios de esta PKI y a las Autoridades de Registro mediante correo electrónico, se procederá a inscribirla en el Registro General de Condiciones Generales de Contratación y se colgará del repositorio de documentos de esta autoridad de certificación.

La notificación se realizará con anterioridad a la entrada en vigor de esta nueva versión.

14.7 Procedimientos de aprobación de la CPS

La entidad con atribuciones para aprobar los cambios sobre esta CPS o en alguna de las CP de ANF AC es la Junta Rectora de la PKI. Cuyos datos constan en el apartado "*Especificación del ente organizador".*

La Junta Rectora de la PKI, notificará los cambios al equipo ejecutivo de ANF AC para que confeccionen una nueva CPS o CP según el caso. Proceda a su publicación, notificación, y en caso de necesidad realizar las operaciones logísticas y operativas que adecuen la actividad de la autoridad de certificación a los nuevos requerimientos. Asimismo, tramitará la inscripción del nuevo documento en el Registro General de Condiciones Generales de Contratación.

15 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.

¿ Es obligatorio seguir una determinada norma técnica o estándar ISO por parte de una Autoridad de Certificación?
No. Ni la legislación española, ni la directiva europea en materia de firma electrónica exige nada al respecto.

No obstante, debemos hacer constar que en el mes de junio del año 2.003, la Comisión Europea decidió la publicación de los números de referencia de las normas que gozan de reconocimiento general para productos de firma electrónica, de conformidad con lo dispuesto en la Directiva 1999/93/CE del Parlamento Europeo y del Consejo.
Lista de normas que gozan de reconocimiento general para productos de firmas electrónicas considerados conformes por los Estados miembros con los requisitos del anexo II (f) y III:
— CWA 14167-1 (Marzo 2003): Requisitos de seguridad de sistemas fiables que controlan los certificados de firmas electrónicas — Parte 1: Sistema de condiciones de seguridad
— CWA 14167-2 (Marzo 2002): Requisitos de seguridad de sistemas fiables que controlan los certificados de firmas electrónicas — Parte 2: Módulo criptográfico para las operaciones de firmas CSP — Perfil de protección (MCSO-PP)
— CWA 14169 (Marzo 2002): Dispositivos protegidos de creación de firma electrónica."

Así mismo hay que señalar que el sistema fiscal español, concretamente en el ámbito de la facturación telemática, se establecen determinados requerimientos de estándares técnicos. ANF AC cumple todos los establecidos en este marco regulador.

¿ANF AC en su procedimiento de firma atiende las garantías ineludibles de un sistema de firma electrónica?

Si. El procedimiento de firma de ANF AC en cualquier de sus modalidades garantiza los tres requisitos de la firma electrónica avanzada:

1. **Identidad**. Garantiza poder determinar sin lugar a dudas la identidad de la persona que firmó.
2. **Integridad**. Garantiza que el documento no puede ser falsificado. El sistema es capaz de determinar con absoluta seguridad si el documento corresponde al original firmado o se ha producido en él una modificación por pequeña que sea.
3. **No repudio**. Garantiza que el usuario del documento no puede negar que ha sido él el que ha firmado el documento.

¿La confidencialidad o privacidad no es un requerimiento exigible a la firma electrónica?

No. No se debe de confundir el hecho de que se puedan emplear las claves privada y publica para circularizar mensajes o ficheros, con el hecho de que sea un elemento imputable al procedimiento de firma electrónica.

¿Una identificación basada en el certificado digital de acceso a un determinado espacio Web en Internet, puede considerarse como un procedimiento de firma electrónica?

No. Son diversas las Web que han incorporado un proceso de identificación del visitante basado en los certificados digitales, incluso por desconocimiento, hablan de emplear sistemas de firma electrónica. En realidad se debe de enmarcar y considerar como un procedimiento de seguridad informática, aunque en si el mismo se incluya procesos criptográficos similares al sistema SSL, es decir empleando el par de claves.

¿Qué información aporta un OID?

OID = “Digital Object Identifier” - Código Identificador del Objeto Digital, incluye la siguiente información
Son identificadotes administrados por la institución internacional IANA, en el marco de SMI Network Management Private Enterprise Codes.

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

La estructura de composición del código es la siguiente:

Prefijo común IANA = iso.org.dod.internet.private.enterprise (1.3.6.1.4.1)
Al prefijo se le añade en número exclusivo de la entidad, ANF AC tiene otorgado el 18332.
El número parcialmente confirmado será 1.3.6.1.4.1.18332
A partir de esta raíz, la entidad identifica libremente los diferentes objetos digitales que desee. De esta forma, independientemente en que lugar del planeta nos encontremos, siempre podremos saber a quién pertenece un objeto digital (evidentemente si esta vinculado a un OID).