Declaración de Prácticas de Certificación (CPS)

Certificate Practice Statement

Fecha : 8 de marzo de 2004
Versión: 1.6
OID : 1.3.6.1.4.1.18332.1.6

Declaración de Prácticas de Certificación

Sumario

2.9 Seguridad de la adecuación de la CPS a las Políticas de Certificación.
2.10 Control de conformidad.
2.11 Plan de Contingencias y Seguridad de la Información.

3. Normas y Estándares.

3.1 ISO 7816.
3.2 PC-SC.
3.3 ISO/IEC X509 v.3.
3.4 Plug and Play.
3.5 Homologación de dispositivos por ANF AC.
3.6 Dispositivos seguros de creación de firma electrónica.
3.7 Dispositivo de verificación de firma.
3.8 Dispositivo de generación de datos de creación de firma.
3.9 Dispositivo de generación del contenedor TID.
3.10 Leyes y normas.

4. Certificados.

4.1 Contenedores homologados.
- 4.1.a Dispositivo de Generación del Contenedor TID.

4.2 Generación de datos de creación de firma.
- 4.2.a Difusión del dispositivo de generación de datos de creación de firma.
- 4.2.b Instalación del dispositivo y actualizaciones.
- 4.2.c Procedimiento de generación de los datos de creación de firma.
- 4.2.d El “certificado request”.

4.3 Modalidades de certificados.
4.4 Identificación y autentificación.
- 4.4.1 Tipos de nombres.
- 4.4.2 Pseudónimo.
- 4.4.3 Unicidad de nombres.
- 4.4.4 Identidad individual del usuario.
- 4.4.5 Identidad de los representados.
- 4.4.6 Nombre alternativo del sujeto
- 4.4.7 Procedimientos de resolución de disputas de nombres. Denominaciones comerciales y marcas.
- 4.4.8 Métodos de prueba de posesión de la clave privada.
- 4.4.9 Autentificación de la identidad de una persona jurídica.
- 4.4.10 Autentificación de la identidad de una persona física.
- 4.4.11 Autentificación de la identidad de los representantes.
- 4.4.12 Renovación rutinaria de un certificado.
- 4.4.13 Renovación de un certificado después de una revocación.
- 4.4.14 Renovación de un certificado suspendido.
- 4.4.15 Solicitud de revocación o suspensión

4.5 Solicitud, emisión y aceptación de Certificados.
- 4.5.1 Solicitud.
- 4.5.2 Emisión.
- 4.5.3 Aceptación.

4.6 Revocación de certificados.
- 4.6.1 Procedimiento.
- 4.6.2 Revocaciones.
- 4.6.3 Acreditaciones.

4.7 Caducidad y renovación.
4.8 Atributos.
4.9 Limitaciones de uso.
4.10 Condiciones de uso.
4.11 Tasas de activación, emisión y renovación.
4.12 Registro de certificados.
- 4.12.a Contenido.
- 4.12.b Accesibilidad.

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, 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 1.6, 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 ANF AC. Caso de que el lector no conozca los conceptos básicos de un sistema de PKI, 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	1.6
Autor	*Florencio Díaz Vilches*
Referencia del documento / OID	1.3.6.1.4.1.18332.1.6
Fecha de emisión	8 de marzo de 2004
Fecha de expiración	No es aplicable
Localización URL	https://www.anf.es/AC/documentos/

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

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

El prefijo del OID de esta CPS es 1.3.6.1.4.1.18332.**1.** el sufijo determina la versión de la CPS a la que hace referencia el OID. En el caso de este documento versión 6, el OID que lo identifica es 1.3.6.1.4.1.18332.1.6

El protocolo a seguir en el mantenimiento de este OID queda determinado en el apartado "12.4 *Procedimiento de Especificación de Cambios*" de este documento.

Este procedimiento se basa principalmente en las normas del "European Telecommunication Standards Institute" (ETSI): ETSI TS 102 042, ETSI TS 101 456, ETSI TS 102 023, ETSI TS 101 733, ETSI TS 101 861 y ETSI TS 101 862.

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.- 00 34 932 661 614
FAX.- 00 34 933 131 614
Dirección electrónica: ac@anf.es
Dirección web: https://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.- 00 34 932 661 614
FAX.- 00 34 933 131 614
Dirección electrónica: juntapki@anf.es

1.3.2 Persona de contacto

Para cualquier información relacionada con esta CPS:

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

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

Las modificaciones propuestas o las nuevas aportaciones a incluir sobre esta Declaración de Prácticas de Certificación, deben, previa a su aprobación, ser contrastadas con la CP's

que ANF AC tenga publicadas, a fin de asegurar que la Políticas de Certificación soportan estos cambios.

El procedimiento a seguir queda especificado en el apartado "*2.9 Seguridad de la adecuación de la CPS a las Políticas asociadas*".

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
Función Hash	Operación que se realiza aplicando un algoritmo de resumen a un conjunto de datos de cualquier tamaño, obteniendo un hash que tiene como propiedad el estar asociado unívocamente a los datos iniciales.
Hash	También llamado "resumen". Es el resultado que se obtiene tras aplicar una función hash.
PIN	Contraseña secreta que precisa el Contenedor para poder ser activado.
PKCS#7	"Crytographic Message Syntax Standard". Define una sintaxis para mensajes que incluyen procesos criptográficos, como firma electrónica y/o cifrado.
PKCS#10	"Certification Request Syntax Standard". Define la sintaxis de una petición de certificado.
PKCS#15	Es uno de los contenedores homologados de ANF AC. Sigue el estándar RSA http://www.rsasecurity.com/rsalabs/pkcs/pkcs-15/index.html
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.
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. 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.
Subject	Suscriptor o también llamado usuario del certificado. Es el titular de un certificado emitido por ANF AC.
Suscriptor	Titular de un certificado emitido por ANF AC.

Tarjeta TID	Tarjeta de Identificación Digital. TID™. Es un contenedor homologado TID.
Usuario	Titular de un certificado emitido por ANF AC.
X-500	Estándar desarrollado por la UIT define las recomendaciones del Directorio.
X-509	Estándar desarrollado por la UIT para las PKI y los certificados de atributos.

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	"Certificate Revocation List" . Lista de Revocación de Certificados en el ámbito de ANF AC de libre acceso.
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".
LOPD	Ley Orgánica de Protección de Datos 15/1999, de 13 de diciembre.
MD5	"Message Digest", versión 5. Algoritmo de resumen de mensajes (R.Rivest 1991).
NTP	"Network Time Protocol"
OID	"Digital Object Identifier" - Código Identificador del Objeto Digital
OCSP	"Online Certificate Status Protocol" – Protocolo informático que permite determinar la vigencia de un certificado electrónico.
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	Acrónimo de - "Rivest, Shamir y Adleman". Inventores del criptosistema de clave pública que permite la firma electrónica y el cifrado (1977).
SSCD	"Secure Signature –creation Device" Dispositivo Seguro de Creación de Firma.
SHA - 1	"Secure Hash Algorithm" (1994). Es el algoritmo seguro de resumen -hash-

SSL	“Secure Socket Layer”.
TID	Tarjeta de Identificación Digital.
UIT	Unión Internacional de Telecomunicaciones.
URL	Localizador de recursos uniforme “Uniform Resource Locator”
UTC	“Universal Time Coordinated”. Estándar oficial para contabilizar el tiempo actual
WWW	“Word Wide Web”.

1.5 Publicación.

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

La entidad con atribuciones para definir y aprobar sobre cualquier propuesta de modificación de esta CPS es la Junta Rectora de la PKI.

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

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 - Suscriptores

Son todas aquellas personas físicas o jurídicas que son titulares, o que constan como representantes de los titulares, de certificados digitales emitidos por esta autoridad 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 y en general el modelo de sistema PKI.

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 Seguridad.

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

- Los servicios de seguridad que se requiere que el sistema proporcione para satisfacer las necesidades de sus usuarios.
- Los servicios de seguridad que se requiere que el sistema proporcione para satisfacer las necesidades de ANF AC, en especial la protección de sus propias claves privadas, y código fuente del software empleado por los usuarios y la propia Autoridad de Certificación.
- Los servicios de seguridad requeridos para que el sistema atienda 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 considera tanto amenazas de tipo intencional e inteligente, como de tipo accidental.

2.1 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.

2.2 Seguridad de los equipos informáticos.

2.2.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.

2.2.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 reactivación de certificados
   e) Servicio de renovación de certificados

f) Servicio de recepción de certificados “Request”
g) Servicio de Sellos de Tiempo

En todos los casos, los datos son almacenados en un soporte magnético que se encuentra en lugar custodiado y de acceso restringido. Este soporte esta etiquetado con un identificador único, inventariado, precintado y firmado por el responsable de seguridad.
Transcurrido el plazo de retención previsto, los datos se destruirán salvo que fueran necesarios para otros fines previstos por la Ley. El proceso de destrucción de los datos seguirá el siguiente procedimiento:

a) Borrado de la información.
b) Escritura en disco.
c) Borrado de la información.
d) Formateo del dispositivo a bajo nivel.

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.

2.2.c Hardware.

2.2.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. 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, códigos fuente de software ...etc. Además de lo reseñado, ANF AC cuenta con equipos informáticos sin conexión a Internet ni a la propia Intranet, estos equipos se destinan a funciones especificas como: emisión de certificados y desarrollo de software.

Cada uno de los ordenadores empleados: servidores y estaciones de trabajo, son de uso exclusivo de ANF AC. 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 (tarjeta de identificación digital) administradoras del sistema.

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

2.2.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.

2.2.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. salvo los servidores de Internet y el ordenador encargado de la emisión de certificados, los cuales sincronizan su tiempo mediante un sistema GPS.

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.

2.2.e Copias de seguridad.

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

El personal encargado de su realización queda reseñado en el ANEXO II apartado 3.7

El protocolo de copias de seguridad establecido mantiene una copia diaria de los últimos 7 días, una copia individual de cada una de las últimas 4 semanas, y permanente de cada una de las copias semestrales que se han realizado. Cada dispositivo de copia empleado es identificado con un código único mediante etiqueta de seguridad firmada y sellada.

Las copias quedan depositadas en la Caja de Seguridad de una entidad bancaria. La copia antes de su deposito es cifrada, precintada, fechada y firmada por al menos dos empleados confiables (*Seguridad física de la Caja de Seguridad Bancaria detallada en el apartado 2.4.2*)

El almacenamiento a largo plazo de los registros se realiza en medios WORM ("escribir una vez leer muchas").

Copia del software de restauración de las copias de seguridad es integrado en cada uno de los soportes.

Trimestralmente se realizan pruebas de las copias de seguridad efectuadas, al objeto de asegurar que éstas se han realizado correctamente y que en el caso de tener que recurrir a ellas, la recuperación podrá llevarse a cabo. El procedimiento seguido es:

a) Las pruebas se realizan seleccionando tres de los dispositivos que contienen copias diarias, semanal y mensual, la copia semestral se verifica en el momento de su realización.
b) Para la comprobación del estado de las copias se realizan ficheros temporales, los cuales son borrados una vez finalizada la comprobación.
c) Son responsables de la verificación de las copias, el personal encargado de su realización, salvo la semestral que se realiza en presencia de dos responsables de ANF AC,

Se mantiene un inventario de los dispositivos de copia empleados por ANF AC y un diario de control de procesos.. Este inventario detalla el lugar donde es almacenado, el contenido y la fecha de la copia. Los empleados responsables del sistema de copias de seguridad se responsabilizan del cumplimiento del sistema firmando, manteniendo al día el diario de control de procesos y firmando cada operación realizada.

Se establece un periodo de vida de los soportes magnéticos de 24 meses, transcurrido ese periodo el soporte será desechado siguiendo el procedimiento establecido en el ANEXO II, apartado 3.8

El método de recuperación de datos queda especificado en el ANEXO II apartado 3.7

2.2.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, Políticas de Certificación y Anexos. 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.

2.2.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

2.2.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.

2.2.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.

2.2.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

2.2.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.

2.2.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.

2.2.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.

2.3 Seguridad del personal.

2.3.1 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.

2.3.2 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.

2.3.3 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 40h. 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.

2.3.4 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.

La operativa del procedimiento seguido queda documentada en el Anexo II de esta CPS, apartado 4.

2.3.5 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.

2.3.6 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.

2.3.7 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.

La operativa del procedimiento seguido queda documentada en el Anexo II de esta CPS, apartado 4.

2.4 Seguridad física.

ANF Autoridad de Certificación garantiza que cumple la normativa aplicable en todos los aspectos de seguridad física y las describe en el presente apartado.

Se han establecido diferentes perímetros de seguridad con barreras de seguridad y controles de entrada adecuados a las actividades que se desarrollan en cada uno de ellos. Todo ello con el fin de reducir el riesgo de accesos no autorizados o de daños a los recursos informáticos.

2.4.1 Centro de Datos

Los equipos informáticos que prestan servicio público (principal y espejos) se encuentran instalados en “data center” perteneciente a primeras compañías operadoras nacionales.

El edificio donde se encuentra instalada la infraestructura central de ANF AC es un recinto físicamente seguro, dotado de hasta seis niveles de seguridad para poder llegar a acceder a las máquinas y aplicaciones críticas.

Los sistemas están físicamente separados de otros sistemas existentes en el lugar, de forma que solo personal autorizado de ANF AC puede acceder a ellos, garantizando así la independencia de otros equipos y sistemas de terceros alojados en el lugar.

Entre las medidas de protección que poseen estas instalaciones, reseñar que:

- Las instalaciones cuentan con servicio de vigilancia de 24 horas y control por circuito de televisión cerrado permanente. Las cámaras no tienen posibilidad de efectuar visionado de las operaciones que se realizan en los servidores de ANF AC, a fin de evitar cualquier riesgo de visualización de los PIN de activación al ser introducidos u otros datos confidenciales.

- Situación alejada de sótanos para prevenir posibles inundaciones.

- La arquitectura y blindaje del edificio corresponden al diseño comúnmente empleado en establecimientos denominados “data center”.

- El edificio es un inmueble moderno, construido al efecto y de uso exclusivo del operador. Ubicado en zona empresarial de reconocido prestigio, de fácil y rápido acceso, en caso de necesidad, por parte de los servicios de Orden Público y Bomberos.

- El edificio se encuentra ubicado en zona de baja actividad sísmica y sin antecedentes de catástrofes naturales.

- El edificio se encuentra ubicado en zona de bajos niveles de delincuencia.

- Ni el edificio, ni la zona en donde se encuentra, están considerados objetivos terroristas.

- Ausencia de ventanas al exterior del edificio.

- 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.

- Todo el cableado esta protegido contra daños o interceptación electromagnética o interceptación de la transmisión tanto de datos como de telefonía.

- Las mamparas que protegen las zonas centrales del núcleo son transparentes y cuentan con iluminación permanente, todo ello con el fin de posibilitar la observación desde cámaras de vigilancia o desde pasillos o incluso zona de oficinas administrativas, impidiendo así actividades ilícitas en el interior del bunker.

2.4.1.a Acceso físico

Perímetro de seguridad física

Además de las medidas reseñadas anteriormente, se han implementado sistemas de control de acceso personalizado, registrado el paso de las personas por cada zona. Así mismo se ha establecido que el personal visitante tiene que estar permanentemente tutelado por un responsable del data center.

Controles físicos de entrada

Se dispone de un exhaustivo sistema de control físico de personas a la entrada y a la salida que conforman diversos anillos de seguridad.

Se combinan diversos sistemas de seguridad, humanos y técnicos, en la realización de los controles físicos de entrada:

a) Acceso a la entrada identificándose mediante DNI ante el servicios de seguridad, registrando persona, hora de llegada, salida, autorización que ostenta y dotando de un numero de identificación personal.
b) Uso del número personal para su identificación ante los dispositivos de seguridad, comprobando autorización y registrando accesos.

Introducción o extracción de equipos

Se requiere autorización expresa para la realización de estas operaciones, llevando un inventario del material existente y de las entradas y salidas que se han producido.

Cada dispositivo cuenta con un identificador único, descripción, modelo y marca.

2.4.1.b Electricidad y Aire Acondicionado

Las salas donde se ubican los equipos que componen los sistemas de certificación de ANF AC, disponen de suministro de electricidad y aire acondicionado suficiente para crear un entorno operativo fiable. La instalación esta protegida contra caídas de corriente o cualquier anomalía en el suministro eléctrico mediante una línea auxiliar independiente de la fuente eléctrica principal.

Se han instalado mecanismos que mantienen controlados el calor y la humedad a niveles acordes con los equipos que se encuentran instalados en el lugar.

Aquellos sistemas que lo requieren, disponen de unidades de alimentación ininterrumpida y grupo electrógeno,

2.4.1.c Seguridad del cableado

El cableado se encuentra en falso suelo técnico y se encuentra protegidos por medios de detección ante incendio.

2.4.2 Caja de Seguridad Bancaria

ANF Autoridad de Certificación ha contratado en una entidad bancaria española una caja de seguridad en la que se depositan los dispositivos que quedan reseñados en este documento.

El acceso a la Caja de Seguridad esta restringido a los Directores Generales de ANF AC, los cuales tienen en su poder una de las llaves que permite la apertura de la Caja de Seguridad.

Entre las medidas de protección que poseen estas instalaciones bancarias, reseñar 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 “bunker bancario”.
- Las instalaciones se encuentran protegidas constantemente por personal perteneciente a empresa de seguridad autorizada por el correspondiente departamento del Ministerio del Interior.
- El personal al que la entidad bancaria tiene encomendada la administración de los accesos, confecciona un registro del día y hora de entrada y salida, identidad y firma de la persona que accede.
- El acceso al núcleo central se realiza superando distintos controles. El personal que accede se encuentra en todo momento acompañado por el personal responsable de la administración del “bunker bancario” y la operación de apertura de la caja bancaria se realiza mediante doble llave: una en poder del personal de ANF AC y otra en poder del personal de la entidad bancaria.
- Todas las instalaciones cuentan con sistemas de energía y aire acondicionado, que cumplen con las normas al efecto
- Todas las instalaciones cuentan con mecanismos de prevención y protección contra incendios. Dichos mecanismos cumplen con las normas industriales.

2.5 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.

2.5.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.

2.5.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.

2.5.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.

2.5.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).

2.5.e Caducidad.

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

2.6 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 cifrar automáticamente importantes volúmenes de ficheros y datos, a selección del usuario de ANF AC.

2.7 Seguridad criptográfica.

La infraestructura de clave pública PKI de ANF AC cuenta con un sistema de comunicaciones "Secure Sockets Layer" SSL de 128 bits, empleando algoritmo Sha1RSA.

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.

Los procedimientos técnicos y los algoritmos utilizados quedan ampliamente documentado y a disposición pública en el Anexo IX de esta CPS.

ANF AC, no almacena ni copia los datos de creación de firma de sus usuarios, ni tiene oportunidad para hacerlo, estos son generados de forma independiente por ellos mismos y sin intervención de terceros. Así mismo, ANF AC con el fin de facilitar un control completo a sus usuarios del software utilizado en el proceso anteriormente reseñado, pone a su disposición el código fuente del software criptográfico y de las aplicaciones que facilita para la generación de Claves, del contenedor de las mismas en el formato del token criptográfico bajo el erstándar PKCS#15 y del "Certificado Request" creado en formato estándar PKCS#10. Este material es entregado al usuario por la Autoridad de Registro en el momento de tramitar su petición de emisión de certificado digital. En los modelos de contenedores que son generados con la librería de Microsoft CryptoApi (*certificados que no tienen la capacidad de utilizar Dispositivos Seguros de Creación de Firma homologados por ANF AC, ver apartado "6.1 Dispositivo Seguro de Creación de Firma"*), el Dispositivo de Generación de Datos de Creación de Firma homologado por ANF AC se limita a hacer el uso indicado por ese fabricante. Esta librería criptográfica no tiene el código fuente abierto, el componente compilado viene intecorporado de forma estándar en todos los sistemas operativos Windows.

Dado que el software utilizado por los usuarios de ANF AC cuenta con mecanismos que garantizan la integridad y autenticidad de todos los elementos que conforman su plataforma de trabajo, aquellos usuarios que deseen trabajar con aplicativos cuyo código fuente ha sido previamente revisado por ellos, podrán requerir del departamento técnico de ANF AC que la compilación los dispositivos se realice sobre el código por ellos revisado y en su presencia. ANF AC no permite modificación alguna del código original, se reserva la propiedad intelectual del mismo, y aplicará las tasas correspondientes al servicio de ingeniería prestado.

El dispositivo de generación de datos de creación de firma confecciona, durante el proceso de creación del "certificado request", un informe de solicitud relativo a la petición de emisión del certificado digital, el cual es firmado electrónicamente con la clave privada generada en ese acto. El dispositivo tiene la capacidad de verificar automáticamente que el certificado emitido por ANF AC contiene la clave pública que corresponde a la clave privada que esta en posesión del titular, y que los datos reseñados son los especificados en la solicitud. Para ello, el dispositivo lee los datos contenidos en el certificado emitido por ANF AC, efectúa una verificación de la firma realizada sobre el informe de solicitud y de la correspondencia cierta de los datos relacionados entre el certificado y el informe.

Toda la información relativa al software criptográfico, código fuente de la librería criptográfica y documentación de procedimientos puede ser descargada en la URL.

https://www.anf.es/AC/documentos/software.htm

Con el fin de garantizar la integridad y autenticidad de estos ficheros, todos ellos se encuentran firmados electrónicamente. Para su verificación se puede descargar gratuitamente el dispositivo de verificación en la URL

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

Los procedimientos criptográficos utilizados por ANF AC han sido revisados por especialistas en la materia, y de forma periódica es revisada su calidad y su resistencia en lo que a seguridad se refiere. Las certificaciones acreditativas independientes son publicadas en la URL

https://www.anf.es/AC/documentos/Informes.htm

ANF AC facilita el código fuente de diversos componentes con el fin de que los usuarios puedan verificar su calidad y en caso de aprobación, tengan la capacidad de realizar una compilación que le permita trabajar con dispositivos de su completa confianza. ANF AC prohíbe cualquier modificación del código, y con el fin de evitar el empleo de estos dispositivos en caso de modificación, previa a su utilización, se verifica su huella digital. Por todo ello, la modificación intencionada o por ataque de terceros (virus o hackers) del componente compilado, da como resultado una denegación de servicio.

La apertura del código fuente no presupone renuncia alguna a los derechos de propiedad intelectual que ANF AC ostenta sobre el mismo.

2.8 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.

2.9 Seguridad de la adecuación de la CPS a las Políticas de Certificación.

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

2.10 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.

2.11 Plan de Contingencias y Seguridad de la Información.

ANF AC cuenta con un Plan de Contingencias y Seguridad de la Información que contempla:

- Política de Seguridad
- Análisis de Riesgos
- Plan de Contingencias

puede ser consultado en la URL:

https://www.anf.es/AC/documentos/anexo.htm

3. Normas y Estándares.

3.1 ISO 7816.

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

3.2 PC-SC.

Los lectores de SmartCard empleados por el software de usuario desarrollado por ANF AC cumple este estándar internacional.

3.3 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.

3.4 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) de Microsoft.

3.5 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 pone a su disposición una serie de dispositivos homologados por ANF AC. Los dispositivos que comprende este apartado son:

a) Dispositivo seguro de creación de firma
b) Dispositivo de verificación de firma.
c) Dispositivo de generación de datos de creación de firma
d) Dispositivo de generación del contenedor TID

Cualquier entidad podrá solicitar de ANF AC la homologación de los 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.

e) Los dispositivos de creación de firma deben cumplir la especificación técnica CEN-CWA 14169.

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 actualizaciones 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 a 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 figurarán publicados en la URL:

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

3.6 Dispositivos seguros de creación de firma electrónica.

En Anexo IV de esta CPS queda documentado técnicamente el procedimiento seguido por los dispositivos seguros de creación de firma homologados por ANF AC, y los algoritmos criptográficos que se emplean.

ANF AC exclusivamente homologa dispositivos de creación de firma electrónica que cumplen con los requerimientos establecidos en las normas técnicas publicadas a tales efectos en el «Diario Oficial de las Comunidades Europeas» publicadas el 15 de Julio de 2.003 (Decisión de la Comisión de 14 de julio de 2.003); así como lo estipulado en el Anexo III sobre Dispositivos Seguros de Creación de Firma de la Directiva 1999/93 del Parlamento Europeo y del Consejo de 13 de Diciembre de 1.999 por la que se establece un marco comunitario para la firma electrónica; y lo establecido en la Ley 59/2003 de 19 de Diciembre, de Firma Electrónica en el Titulo IV, Capítulo I Art. 24 punto 3 sobre dispositivos seguros de creación de firma. A modo meramente enunciativo se garantiza que los dispositivos homologados por ANF AC, 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.
7 Que el dispositivo previa a la utilización de los datos de creación de firma, establece conexión con el servidor de ANF AC a fin de comprobar el estado en que se encuentra el certificado del usuario. Denegando el servicio de firma si el certificado esta caducado o revocado.
8 Que el dispositivo para cada firma electrónica que procesa, requiere del Servicio de Sellos de Tiempo de ANF AC, que le sea generado un Sello de Tiempo único y exclusivo sobre la firma electrónica que ha creado.

AVISO IMPORTANTE: La actual Ley 59/2003 de 19 de Diciembre, de Firma Electrónica, en el Titulo IV, Capítulo II Art. 27 punto 3 sobre Certificación de dispositivos seguros de creación de firma electrónica, establece la posibilidad de obtener una certificación de estos dispositivos. No obstante a fecha de finalización del presente documento, España no cuenta aun con un Esquema de Certificación Nacional, ni entes de evaluación, ni de certificación. Esta situación imposibilita actualmente la posesión de esta certificación. No obstante la propia Ley de Firma Electrónica en el Artículo 28 punto 1 establece que

> "*Se presumirá que los productos de firma electrónica aludidos en la letra d) del apartado primero del artículo 20 y en el apartado tercero del artículo 24 son conformes con los requisitos previstos en dichos artículos si se ajustan a las normas técnicas correspondientes cuyos números de referencia hayan sido publicados en el «Diario Oficial de la Unión Europea».*"

3.7 Dispositivo de verificación de firma.

El dispositivo debe de estar homologado por ANF AC y es suministrado por esta AC de forma gratuita, a través de la URL:

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

siendo de libre distribución.

Este requerimiento no es aplicable a Agencia Tributaria AEAT ni a ninguna otra Administración Pública, las cuales podrán utilizar aquellos dispositivos de verificación que estimen más adecuados a sus requerimientos operacionales.

En Anexo IV de esta CPS queda documentado técnicamente el procedimiento seguido por el dispositivo de verificación de firma.

ANF AC garantiza que exclusivamente homologa dispositivos de verificación de firma que 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 Si la firma ha sido creada con un dispositivo seguro de creación de firma electrónica homologado por ANF AC, se verifica la integridad del Sello de Tiempo y la identidad de ANF AC como firmante del Sello de Tiempo.
5 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.

3.8 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. Así mismo, y con el fin de facilitar un control completo a sus usuarios del software utilizado en el proceso anteriormente reseñado, pone a su disposición el código fuente del software criptográfico y de determinadas aplicaciones de acuerdo con lo reseñado en el apartado “2.7 Seguridad Criptográfica”.

3.9 Dispositivo de generación del contenedor TID.

Los datos de creación de firma únicamente pueden ser almacenados en contenedores homologados por ANF AC. Esta Autoridad de Certificación ha homologado los publicados en la URL:

https://www.anf.es/AC/contenedores.htm

3.10 Leyes y normas.

Las siguientes leyes y normas han sido consideradas para la elaboración de este documento:

Directivas europeas

- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de Octubre de 1.995. Relativa a la Protección de Datos de las Personas Físicas.
- Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de Diciembre de 1.997. Relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.
- Directiva 99/93/CE del Parlamento Europeo y del Consejo, de 13 de Diciembre de 1.999. Por la que se establece un marco comunitario para la firma electrónica.

Leyes Españolas

- Real Decreto 994/1999, de 11 de Junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal.
- Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal.
- Ley 59/2003, de 19 de Diciembre de 2.003, de firma electrónica

4. Certificados.

ANF AC ha realizado todos los trámites necesarios para garantizar de forma fiable la veracidad de 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 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.

Los certificados emitidos por ANF AC respetan el formato definido por la UIT –T X-509, de fecha junio 1.997 o superiores (ISO/IEC 9594-8 de 1997) en la versión 3. Los certificados CRL siguen el formato UIT-T X-509, en su versión 2.

4.1 Contenedores homologados.

Son propietarios de estos contenedores, 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 Políticas de Certificación asociadas a los certificados emitidos por ANF AC determinan el contenedor que debe usarse en cada tipo de Certificado .

4.1.a Dispositivo de Generación del Contenedor TID.

ANF AC facilita este dispositivo, el cual tiene la capacidad de generar el contenedor que almacena los datos de creación de firma. 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 se realizará el proceso de solicitud, identificación y autenticación por parte de la AR.

La distribución esta restringida a las Autoridades de Registro.

4.2 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 (*Características técnicas del proceso seguido por el dispositivo en ANEXO IV*). Así mismo, y con el fin de facilitar un control completo a sus usuarios del software utilizado en el proceso anteriormente reseñado, pone a su disposición el código fuente del software criptográfico y de determinadas aplicaciones de acuerdo con lo reseñado en el apartado “2.7 Seguridad Criptográfica”.

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

4.2.a Difusión del dispositivo de generación de datos de creación de firma.

ANF AC pone a disposición gratuita de sus usuarios el dispositivo de generación de datos de creación de firma electrónica. Este dispositivo esta grabado en un soporte óptico, el cual esta gráficamente estampado con los distintivos de esta Autoridad de Certificación.

La distribución esta restringida a las Autoridades de Registro Reconocidas, las cuales tras efectuar el correspondiente proceso de identificación y autentificación, hacen entrega del dispositivo facilitando al usuario un localizador que permite determinar el expediente de identificación realizado, “localizador AR”. No obstante, cuando el proceso de identificación y autentificación se ha llevado a cabo ante Autoridades de Registro Colaboradoras, ANF AC será la encargada de hacer entrega del dispositivo enviándolo por correo certificado.

La distribución de las actualizaciones de este software esta igualmente restringida a las Autoridades de Registro.

4.2.b Instalación del dispositivo.

El usuario de ANF AC debe de proceder a la instalación del dispositivo siguiendo sus instrucciones técnicas. Las actualizaciones están firmadas electrónicamente por ANF AC y previamente a su instalación el usuario debe de comprobar los componentes mediante el dispositivo de verificación de firma electrónica homologado.

4.2.c Procedimiento de generación de datos de creación de firma.

Una vez instalado el dispositivo de generación de datos de creación de firma, el usuario esta en disposición de cumplimentar el cuestionario que le permitirá posteriormente generar su “certificado request” en formato PKCS#10 y generar los datos de creación de firma que estarán contenidos en un token criptográfico en formato PKCS#15. Además de los datos personales deberá facilitar el localizador de identificación que le facilitó la AR.

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. Este PIN debe de tener una longitud mínima de 8 dígitos alfanuméricos, y puede denegar un PIN propuesto por considerarlo inseguro; el sistema cuenta con una biblioteca de claves no autorizadas.

El dispositivo tiene la capacidad de generar automáticamente el par de claves necesarias para poder procesar con garantía técnica firmas electrónicas avanzadas, el usuario no requiere de conocimientos específicos para su utilización y lo debe de realizar sin la intervención de terceros. ANF AC no almacena ni copia los datos de creación de firma de

sus usuarios, ni tiene oportunidad para hacerlo. (*Características técnicas del proceso seguido por el dispositivo en ANEXO IV, otras especificaciones en el apartado "2.7 Seguridad Criptográfica" de este documento*)

Los datos de generación de firma son introducidos automáticamente en uno de los contenedores homologados TID autorizado por la Política de Certificación asociada a ese certificado. Simultáneamente el dispositivo crea un "certificado request" en el cual constan los datos personales por él reseñados, localizador AR, además de un número de identificación único y exclusivo para ese certificado (certificado de petición – request).

4.2.d El "certificado request".

a) Queda construido en formato PKCS#10.
b) Contiene además del identificador único, localizador AR y los datos del usuario, la clave pública.
c) El fichero es firmado por el usuario con la clave privada integrada en el contenedor homologado TID.
d) El "certificado request" es cifrado y queda listo para su envío a ANF AC.
e) Todo el proceso es realizado de forma automática, sin posibilidad de manipulación por parte del usuario ni de terceros, salvo la elección del PIN para la activación del proceso.

Para posibilitar la emisión del certificado, el usuario debe remitir el "certificado request" utilizando el mismo dispositivo de generación de datos de creación de firma que empleo para su generación. Este programa utiliza un canal de comunicación "Secure Sockets Layer" SSL para su comunicación con el servidor de ANF AC.

Mayor detalle de los procedimiento seguido y documentación relacionada en apartado "2.7 Seguridad Criptográfica" y en el Anexo IV, de este documento.

4.3 Modalidades de certificados.

ANF AC emite los siguientes tipos de Certificados de Usuarios:

- Certificados ANF Clase 1 CA

a) Clase 2 de Persona física

b) Clase 2 de Persona jurídica

Estos certificados están asociados al emisor :

O : ANF Autoridad de Certificación
CN : ANF Server CA
OU : ANF Clase 1 CA

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.

La representación debe estar acreditada documentalmente mediante instrumento legal suficiente. Este documento quedará referenciado en el OID 1.3.6.1.4.1.18332.14 del certificado emitido.

4.4.6 Nombre alternativo del sujeto.

Los datos del campo **Subject** de los certificados emitidos por ANF AC tienen la siguiente estructura:

	PERSONAS FÍSICAS	**PERSONAS JURÍDICAS**
Country	ES	ES
CommonName	Identidad del titular del Certificado	Razón Social
Surname	Apellidos (como constan en el DNI)	Apellidos del responsable (como constan en el DNI)
GivenName	Nombre de pila (como consta en el DNI)	Nombre propio del responsable (como consta en el DNI)
SerialNumber	NIF del titular	NIF del titular del certificado (persona jurídica)
1.3.6.1.4.1.18838.1.1		NIF del responsable

Como norma general, los certificados emitidos por esta autoridad de certificación pueden integrar otras extensiones en el campo **Subject**, extensiones que en ningún caso son vinculantes para la Agencia Estatal de Administración Tributaria “”AEAT” u otras Administraciones Públicas. Las características de estas extensiones quedan especificadas en el apartado correspondiente de cada una de las Políticas de Certificación a las que se vinculan los certificados emitidos.

La inclusión de estos datos siempre será por imperativo legal, o a requerimiento de los titulares y contando con su expresa autorización. Como ya ha quedado expresado, esta información no representarán para Agencia Tributaria AEAT u otras Administraciones Públicas, vinculación o reconocimiento alguno.

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, es 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 suspensión de certificados.

4.4.15 Solicitud de revocación o suspensión

El método de identificación y autentificación para solicitar una revocación se establece en cada una de las modalidades contempladas en el apartado "4.5.1 Procedimiento de revocación de certificados".

Esta autoridad de certificación no permite la suspensión de certificados.

4.5 Solicitud, emisión y aceptación de los Certificados.

4.5.1 Solicitud.

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

4.5.2 Emisión.

Periódicamente y de acuerdo con las necesidades de servicio, dos responsables de ANF AC se personan en las instalaciones donde se encuentra el ordenador que contiene las Claves Privadas de ANF AC y que permite la creación de certificados de usuario (*ver CPS apartado Protección de Claves Privadas*). Procedimiento:

a) Se recoge el dispositivo de almacenamiento externo que permitirá traspasar los "dictámenes aceptados" y los "certificados request" al ordenador de emisión.
    a. Este dispositivo se encuentra depositado en las mismas instalaciones donde se ubican los equipos informáticos que se van a utilizar.
    b. El dispositivo esta embalado y con precinto de seguridad firmado.
b) En presencia de ambos responsables se verifica el estado del embalaje y del precinto que lo protege.
    a. Se procede a la apertura del embalaje quitando el precinto de seguridad.
    b. Los responsables verifican el número de serie del dispositivo con relación al anotado en el diario de control.
    c. Se realiza conexión al servidor que contienen los dictámenes favorables. El servidor reconoce automáticamente esta unidad como una unidad de almacenamiento externo, no es precisa la parada y arranque del equipo.
c) Se ejecuta el programa de traspaso. Este programa requiere para su activación la identificación de al menos uno de los responsables mediante el empleo de su SmartCard de seguridad.
    a. Activado el programa, se realiza automáticamente un proceso de verificación de las firmas estampadas en los dictámenes, de la integridad de los "certificados request" y de la coherencia de los datos recogidos en los dictámenes respecto a los contenidos en los certificados. El programa realiza un acta del día en la que se detalla la existencia o no existencia de dictámenes favorables, así como los rechazados y posibles incidencias de integridad o coherencia.
    b. El aplicativo requiere la firma del acta como requerimiento previo para copiar los ficheros al dispositivo externo. El responsable firma electrónicamente el acta, previa verificación del sistema del estado de su certificado. En caso de conformidad de firma, el programa lleva a cabo el traspaso de datos, incluyendo copia del acta firmada.

c. Finalizado el traspaso, el programa verifica la correcta copia de la información y traspasa los ficheros copiados al repositorio general del servidor, incluyendo el acta firmada.

d) Finalizado este proceso, la unidad es desconectada y conectada al ordenador destinado a la emisión de los certificados de usuario.
   a. Conexión al ordenador del dispositivo de almacenamiento externo.
   b. Anotación en el diario de control de la hora en la que se produce el encendido del ordenador. (firmado por los dos responsables).
   c. Encendido del ordenador y proceso de activación empleando para ello las SmartCard de seguridad que identifican a los responsables ante el sistema.
   d. Activación de las SmartCard mediante la introducción de los PIN correspondientes.
   e. Verificación por parte de los responsables, el registro de LOG de arranque, activación, desactivación del equipo, comprobando la coherencia con las anotaciones existentes en el diario.
   f. Caso de conformidad acceso al sistema y activación del programa de creación de certificados.
   g. Comprobación del código de referencia de la última acta emitida por el programa, con la anotación realizada en el diario de control.
   h. Caso de conformidad, los responsables en primer lugar requieren del sistema un proceso de sincronización horaria.
   i. Seguidamente el programa genera en primer lugar un acta que mantiene un número correlativo de referencia mediante el sistema de +1 al inmediatamente anterior generado, y en la que se detalla, como en el caso del servidor anterior, los procesos que se van a realizar: *relación de los dictámenes favorables y "certificados request" que va a procesar, verificación de la integridad de los ficheros y firmas estampadas en los dictámenes y en el acta firmada anteriormente por uno de los responsables, coherencia como unicidad de nombres y de identificadores de certificados en relación con los que ha emitido hasta la fecha*.
      Relaciona finalmente los certificados que va ha crear, solicitando la firma de ambos responsables.
   j. Procesado correctamente actas y certificados, el sistema procede al borrado de todos los datos contenidos en la unidad de almacenamiento externo, mediante el sistema de borrado, grabación y borrado. Finalmente descarga todos los certificados creados y el acta emitida.
   k. Se procede a la desactivación del sistema y apagado del ordenador. Tomando nota de la hora en que todo ello se produce y siendo anotado por los responsables en el diario de control.

e) El dispositivo de almacenamiento externo es nuevamente conectado al servidor de ANF AC. Se procede:
   a. Activación del programa de publicación mediante la SmartCard de uno de los responsables presentes y activación mediante PIN secreto.
   b. El programa verifica la coherencia e integridad de los ficheros que va a descargar, así como de las firmas estampadas en ellos. Concretamente:
      i. Estado de los certificados de firma empleados por los responsables para firmar las actas.
      ii. Verificación de los certificados creados, comprobando mediante la clave pública de ANF AC la validez de los mismos, así como la integridad de los ficheros.
      iii. Verificación del Acta emitida y coherencia de los ficheros en ella recogidos en relación a los almacenados en el dispositivo.

c. En caso de conformidad de todo ello, el programa procede a la descarga de la información de la unidad de almacenamiento: certificados y acta de creación.
d. Finalizado el proceso, los datos son borrados bajo el sistema de: borrado, escritura, borrado y formateo de unidad.

f) Finalizado este proceso, los responsables de ANF AC proceden a:
a. Extracción de la unidad de almacenamiento del servidor.
b. Firma en el diario de control de conclusión de la operación de emisión de creación de certificados.
c. Embalaje y precintado de seguridad de la unidad de almacenamiento externo.

Cualquier incidencia en los procesos especificados en este apartado, es considerada como una incidencia grave, y se procederá de acuerdo con lo reseñado en el apartado "*En caso de que los recursos, el software y/o los datos informáticos estén gravemente dañados*" de la CPS de ANF AC.

4.5.3 Aceptación.

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

4.6 Revocación de certificados.

4.6.1 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 :

https://www.anf.es/AR/

La persona física titular del certificado deberá acreditar su identidad mediante Documento Nacional de Identidad, pasaporte u otros medios admitidos en Derecho. En cualquier caso deberá presentar documentos originales.
En el caso de certificados expedidos a personas jurídicas, el solicitante deberá acreditar su identidad como queda reseñado en el anterior supuesto de "personas físicas" y además, deberá acreditar su facultad como representante legal , mediante poder notarial original o documento legal suficiente.

- **Telemáticamente:**
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.

- **Llamada telefónica:**
Mediante llamada telefónica a la Oficina de Atención al Cliente

902 902 172

formulando la correspondiente solicitud y atendiendo a los requerimientos de identificación que se le formulen: como mínimo facilitando el logín y contraseña vinculados al certificado en cuestión, o mediante el sistema “preguntas y respuestas” reseñado en el “apartado 4.12.d.3 b)”.

- **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.

- **Mediante correo electrónico:**
  Enviando un correo firmado electrónicamente. La firma deberá estar vinculada a un certificado emitido por ANF AC, o por alguna otra entidad de certificación oficialmente acreditada.

4.6.2 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 revocación, o simultáneamente a que se produzca la misma. Este correo esta firmado electrónicamente.

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.

4.6.3 Acreditaciones.

Independientemente del procedimiento seguido para efectuar la revocación 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 revocación en que se encuentra su certificado. Esta acreditación estará fechada y será firmada por ANF AC.

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, caso de determinar importe límite de firma, este se considerará que esta expresado en la moneda reseñada en el OID 1.3.6.1.4.1.18332.88.

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.

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

Ninguno de los atributos reseñados en los certificados emitidos por esta Autoridad de Certificación son vinculantes para la Agencia Tributaria, ni para ninguna otra Administración Pública.

4.9 Limitaciones de uso.

Las especificadas en la Política de Certificación correspondientes al certificado emitido.

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.

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, son conservadas y accesibles al menos por un periodo mínimo de **quince años**.

El Registro de Certificados se localiza en la siguiente URL :

https://www.anf.es/AC/Certificados/Registro.asp

4.12.a Contenido.

a) Documental:

Documentación original relativa al proceso de identificación y autenticación que acredita la identidad de los usuarios de ANF AC.

Documentación o informes realizados por el Departamento Jurídico de ANF AC o por la Autoridad de Registro.

En general, escritos y documentos relacionados con los usuarios de ANF AC y sus certificados.

b) Informatizado:

World Wide Web, acceso a base de datos**:** Identificador del certificado, fecha de emisión, fecha de caducidad, fecha de renovación, fecha de activación, revocación (fecha y causa), atributos, importe límite de firma electrónica, estado (activado, caducado, revocado), 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.

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, revocación.

c) 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 tiene la posibilidad de configurar el proceso 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, estado (activado, caducado, revocado), 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.

Público en general, vía World Wide Web. Mediante el Identificador del certificado, se podrá determinar el estado de activación o revocación del certificado, e incluso obtener una copia del mismo.

Otras procedimientos de acceso, 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.

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).

Login: Este debe de ser único para cada usuario o propietario. El sistema verifica si el login propuesto ya ha sido seleccionado por otra persona, en cuyo caso ANF AC rechaza la propuesta y requiere una nueva propuesta.

Contraseña: El sistema mantiene una biblioteca de contraseñas de habitual uso en ataques informáticos, catalogado como claves inseguras e impidiendo su utilización en el entorno de esta entidad de certificación. La contraseña tiene que tener un mínimo de 8 dígitos alfanuméricos.

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. En ningún caso puede modificar datos que afecten a la propia integridad o coherencia de los reseñados en el certificado.

Si está desactivado, podrá utilizar estas claves para acceder al Registro de Certificados con la única posibilidad de revocar 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 revocar su certificado siempre que lo deseen.

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

1) La firma digital corresponde al documento al que se la vincula.
Y haga constar:
a) integridad cierta del 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 es fechado y firmado por ANF AC. El soporte en el que se emite el informe es electrónico.

Esta labor realizada por la AC es con cargo al solicitante.

4.12.f Mantenimiento de los datos.

ANF AC mantiene 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 publica 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 deben de comprobar el estado de validez del certificado de ANF AC empleando los dispositivos de verificación homologados por ANF AC.

4.13 Difusión Certificados de Usuarios.

ANF AC facilitará copia de los Certificados de forma telemática. Los interesados deberán acceder a la Web de ANF AC, URL: https://www.anf.es/ , teniendo conocimiento del identificador del certificado en cuestión.

4.14 Cifrado de Datos.

El uso de Certificados de Cifrado de ANF AC se realizará bajo la exclusiva responsabilidad del usuario.

Se hace constar que algunos países prohíben o condicionan su uso, el suscriptor del certificado esta obligado a informarse en cada caso y adecuar su empleo a la legislación correspondiente.

4.15 Certificados de ANF AC.

4.15.a Proceso de Generación de las Claves y emisión de los certificados de ANF AC.

El proceso seguido para la Generación de las Claves y emisión de los certificados de ANF AC queda reseñado en el Acta levantada de la Ceremonia efectuada. Puede ser descargada de la URL :

https://www.anf.es/AC/repositorio/ActaAC.zip

4.15.b 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, al igual que el ordenador que lo contiene, el cual esta protegido 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.

El ordenador se encuentra ubicado en instalaciones de alta seguridad que cumplen las especificaciones reseñadas en el apartado "*2.4 Seguridad física*".

Otras características relevantes:

a) El ordenador no esta conectado a Internet, ni a una Intranet. Y solamente en presencia física de dos responsables de ANF AC se encuentra arrancado, durante el resto del tiempo el ordenador permanece apagado.
b) El ordenador gestiona un registro en el que consta el momento en que es arrancado, activación del sistema, desactivación del sistema.
c) El ordenador al ser encendido procede a efectuar una sincronización horaria mediante sistema GPS.
d) El ordenador se encuentra precintado con etiquetas de seguridad. Las laborares de mantenimiento se realizan en presencia de al menos dos responsables de ANF AC.
e) El ordenador se encuentra en las mismas instalaciones donde se ubica el servidor de ANF AC que recoge los dictámenes de emisión (*ver en CP apartado correspondiente*) .
f) ANF AC lleva un diario en el que se registra el acceso al equipo, cada anotación es firmada por dos responsables de la AC. Además en el diario:
    a. Se anota los números de referencia de las actas emitidas por el dispositivo de emisión de certificados.
    b. Se anota el número de serie del dispositivo de almacenamiento externo utilizado para efectuar los traspasos.

4.15.c Copia de seguridad de las claves.

ANF AC con el fin de garantizar la continuidad del sistema ante cualquier posibilidad de siniestro, cuenta con una copia de las Claves Privadas de la entidad y de las SmartCard que permiten su activación en Caja de Seguridad bancaria.

4.15.d 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.e Difusión.

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

https://www.anf.es/AC/repositorio/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 Número de versión.

El formato de las CRL's es el especificado en la versión 2 (v2) UTI-T X.509.

4.16.b.2 CRL y extensiones.

La presente CPS y sus Políticas de Certificación soportan y utilizan CRLs conformes al estándar UTI-T – X.509

5 Autoridad de Registro.

Para llevar a cabo la Prestación del Servicio de Certificación, ANF AC podrá realizarla de forma autónoma o utilizando 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.

- Las Autoridades de Registro son las encargadas de distribuir el dispositivo de generación de datos de creación de firma.

- 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 analizan toda la documentación aportada por el solicitante, la compulsan con las copia que se incluyan en el formulario de petición (numerándolas y visándolas una a una), efectúan una estimación de la capacidad del solicitante para ostentar el certificado solicitado, la adecuación de la clase de certificado solicitado a las características del solicitante, determinan la suficiencia y validez de las acreditaciones que acompaña a la solicitud y rechazan en caso de duda su tramitación. En general aceptar o denegar la tramitación de solicitudes de certificados.

- 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".

- Todos los tramites realizados por las Autoridades de Registro son firmados electrónicamente por los operadores que los realizan, asumiendo así su plena responsabilidad en el proceso.

- Las AR llevan un registro diario de las tramitaciones realizadas. Este registro sigue un orden cronológico y cada tramitación cuenta con un localizador numérico correlativo. En caso de aceptación del tramite de petición, la AR facilitará ese código de identificación del tramite agregando su propio identificador como Autoridad de Registro reconocida. Ambos código son el denominado "Localizador AR".

- 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.

- 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.

- 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 revocar el certificado, aunque todo ello se haya realizado de forma voluntaria por el propio titular.

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 Firma Electrónica Reconocida

Los dispositivos de creación de firma electrónica homologados por ANF AC, generan firmas electrónicas que cumplen con los siguientes requerimientos:

a) Que permiten identificar al firmante y detectar cualquier cambio ulterior de los datos firmados,
b) Que está vinculada al firmante de manera única y a los datos a que se refiere,
c) 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"

No obstante, una de las novedades que establece la actual Ley de Firma Electrónica respecto del Real Decreto-Ley 14/1999, es la denominación como firma electrónica reconocida de la firma electrónica que se equipara funcionalmente a la firma manuscrita. Se establece que no basta con la firma electrónica avanzada para la equiparación con la firma manuscrita; es preciso que la firma electrónica avanzada esté basada en un certificado reconocido y haya sido creada por un dispositivo seguro de creación.

6.1 Dispositivos seguros de creación de firma electrónica.

Para procesar una "firma electrónica reconocida" con dispositivos seguros de creación homologados por ANF AC, solo pueden emplearse datos de creación de firma que están vinculados a certificados que específicamente permiten su empleo.

Tal y como se ha indicado en el anterior apartado, la actual legislación, siguiendo las pautas impuestas por la Directiva 1999/93/CE, establece diferentes efectos de seguridad jurídica según el instrumento de creación de firma que se haya utilizado. A entender de esta entidad prestadora de servicios de certificación, dado que los certificados que emite siempre se expiden bajo la consideración de "certificados reconocidos", es necesario que los usuarios de esta PKI y los terceros de confianza puedan determinar fácilmente, con total seguridad y certeza, si la firma electrónica vinculada se ha obtenido empleando un dispositivo seguro de creación homologado por ANF AC o no. Lógicamente si el dispositivo empleado no ha sido revisado por ANF AC, ésta no ha podido verificar el grado de fiabilidad o efectividad del mismo.

Para ello, ANF AC ha definido unos requerimientos técnicos sobre los contenedores homologados PKCS#15 que imposibilitan su uso por dispositivos de firma electrónica que no estén homologados por ANF AC. En este supuesto, el certificado se especifica, como restricción de uso:

"Limitado su uso a Dispositivos Seguros de Creación de Firma homologados por ANF AC".

Por el contrario, cuando los datos de creación de firma están en otra modalidad de contenedor, suelen ser interoperables con los habituales sistemas comerciales de firma electrónica – Explorer, Netscape, Outllok, etc.- pero en ningún caso con los dispositivos seguros de creación de firma homologados por ANF AC. En este supuesto, el certificado se especifica, como restricción de uso:

"No utilizable en Dispositivos Seguros de Creación de Firma homologados por ANF AC".

Los datos de creación de firma almacenados en un contenedor PKCS#15 no son exportables a otro tipo de contenedor.

6.1.a Difusión.

ANF AC pone a disposición gratuita de sus usuarios los dispositivos seguros de creación de firma electrónica a través de las Autoridades de Registro Reconocidas. No obstante, cuando el proceso de identificación y autentificación se ha llevado a cabo ante Autoridades de Registro Colaboradoras, ANF AC será la encargada de hacer entrega del dispositivo enviándolo por correo certificado.

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

https://www.anf.es/AC/repositorio/software.htm

6.1.b Instalación.

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

6.1.c Procedimiento de firma.

El usuario debe de contar con el PIN de activación correspondiente para que el sistema pueda generar la firma.

En Anexo IV consta detalle del procedimiento técnico seguido en la creación de firma.

6.2 Dispositivo de verificación de firma.

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

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.
b) Estado del certificado y capacidad de firma: atributos e importe límite de firma.
c) Que el documento, no ha sido alterado 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 el estado del certificado, valorar la adecuación del tipo de certificado vinculado a la firma electrónica, así como los atributos y las posibles limitaciones de uso.

6.2.a Difusión.

ANF AC pone a disposición pública y gratuita el dispositivo de verificación de firma, puede ser descargado de la URL:

https://www.anf.es/AC/repositorio/verificador.zip

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

https://www.anf.es/AC/repositorio/software.htm

6.2.b Instalación.

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

6.2.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.**

   Los dispositivos homologados por ANF AC siguen el procedimiento técnico reseñado en el Anexo IV .

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:

- Información del estado en el que se encuentra en ese momento el certificado asociado a las firmas electrónicas verificadas. Fecha de revocación en su caso.

7 Obligaciones y Responsabilidades.

7.1 ANF AC.

7.1.1 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.

7.1.2 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 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.

7.1.3 Limitaciones de las responsabilidades.

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

7.1.4 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.

7.1.5 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.

7.1.6 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 a la Junta Rectora de la PKI acerca de los daños producidos.

7.1.7 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.

7.1.8 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.

7.1.9 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 .

7.1.10 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..

7.2 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.
- Se compromete, tras recibir su certificado, a comprobar urgentemente la correspondencia del mismo con la petición formulada. Para ello, empleará la opción de comprobación de certificados que incluye el dispositivo de generación de datos de creación de firma. Caso de que la comprobación resulte negativa, comunicará el hecho de forma inmediata a ANF AC.
- 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 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.

7.3 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..

- Agencia Tributaria "AEAT" gestionará la verificación del estado de los certificados de los usuarios de esta Autoridad de Certificación, mediante la utilización del correspondiente servicio Web que a tal efecto ha implantado ANF AC. Servicio que utiliza el protocolo SOAP de acuerdo con las especificaciones técnicas relacionadas con la O.M. HAC/1181/2003

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

7.4 Autoridad de Registro.

7.4.1 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.

- En caso de representantes de Personas Jurídicas, se comprobará la suficiencia legal de los documentos acreditativos de los representantes, estos deberán ser originales y tratarse de documentos públicos que acrediten de forma fehaciente las facultades del firmante para actuar en nombre de la entidad a la que represente y, en caso de ser de obligatoria inscripción en registro público, se verificará que los mismos cuentan con la correspondiente acreditación, anotando en el formulario de solicitud los datos regístrales.

- 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.

- Se prestará la máxima atención a que el solicitante lo es por su voluntad y no actúa bajo presión, consultándole de forma expresa y requiriendo, en caso de duda, entrevista individual. Si la duda persiste la AR deberá denegar el tramite de la solicitud.

- 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, 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.

7.4.2 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.

8 Responsabilidad Financiera.

8.1 Indemnización a las partes confiantes.

ANF AC de acuerdo con lo establecido en la Ley de Firma Electrónica, ha suscrito 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.

Los datos relativos a la póliza contratada constan publicados en la URL:

https://www.anf.es/AC/seguro/

8.2 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.

8.3 Procesos administrativos.

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

9 Política de Confidencialidad.

9.1 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.*

9.2 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”.

9.3 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.

9.4 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.

9.5 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.

10 Oficina de Atención al Cliente.

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

10.1 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.

10.2 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.

10.3 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:

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

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

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

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

11 Interpretación y Ejecución.

11.1 Ley aplicable.

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

11.2 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.

11.3 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

11.4 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.

11.5 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.

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

11.6 Procedimientos de resolución de disputas.

11.6.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.

11.6.b Procedimiento judicial.

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

12 Publicación y repositorios.

12.1 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 https://www.anf.es/AC/documentos/.

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

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

El certificado emitidos por ANF AC son públicos y se encuentran disponible en el sitio Web de la autoridad de certificación https://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 revocados por ANF AC es pública y se encuentra disponible en el sitio Web de la autoridad de certificación https://www.anf.es . Su consulta sobre base de datos esta regulada en este documento, al igual que la obtención de una copia en formato CRL v2 del repositorio.

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

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

12.2 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.

12.3 Controles de acceso.

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

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

12.4 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.

12.5 Procedimiento de Publicación y Notificación.

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

12.6 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.

13 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.
a) 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).