

Política de Firma Electrónica de ANF AC



Fecha: 1 de septiembre de 2005

Versión: 1.0

OID: 1.3.6.1.4.1.18332.27.1

Este documento es propiedad de ANF Autoridad de Certificación.

Se autoriza su reproducción y difusión siempre que se reseñe:

- © Copyright ANF Autoridad de Certificación –
- Depósito Legal B.44.549-2005

PFE de ANF AC	Ref. Política de Firma Electrónica	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.27.1	Página 1 de 29

Política de Firma Electrónica de ANF AC

“PFE de ANF AC”

Versión 1.0 de fecha 1 de septiembre del 2005

Sumario

1. Introducción.

1.1 Presentación.

1.2 Identificación.

1.3 Datos de contacto.

1.3.1 Especificación del ente organizador.

1.3.2 Persona de contacto.

1.3.3 Determinación de la adecuación de esta Política de Firma Electrónica con la CPS de ANF AC.

1.4 Publicación.

1.5 Comunidad y ámbito de aplicación.

1.5.1 Autoridades de Certificación.

1.5.2 Autoridad de Registro.

1.5.3 Entidades finales.

1.5.4 Ámbito de aplicación.

2. Seguridad.

3. Firma Electrónica.

3.1 Firma electrónica de ANF AC.

3.1 Dispositivos de firma electrónica homologados por ANF AC.

3.1.a Difusión.

3.1.b Instalación

3.1.c Procedimiento

3.2 Dispositivos de verificación de firma electrónica

3.2.a Difusión

PFE de ANF AC	Ref. Política de Firma Electrónica	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.27.1	Página 2 de 29

-
- 3.2.b Instalación
 - 3.2.c Procedimiento
 - 3.2.d Informe de verificación
 - 3.2.e Informe de firma electrónica
 - 3.2.f Documento de firma electrónica interpretable
- 3.3 Ciclo de vida.

4. Sello digital de tiempo.

5. Servicio de consulta del estado de los certificados.

6. Obligaciones y Responsabilidades.

7. Responsabilidad Financiera.

8. Política de Confidencialidad

9. Interpretación y ejecución.

10. Publicación y repositorios.

PFE de ANF AC	Ref. Política de Firma Electrónica	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.27.1	Página 3 de 29

1. Introducción

1.1 Presentación.

El presente documento recoge la Política de Firma Electrónica de ANF AC. Esta Política especifica y complementa lo definido en la CPS de ANF AC.

Caso de que el lector no conozca los conceptos básicos de un sistema de Infraestructura de Clave Pública, certificados digitales y firma electrónica, 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 Política de Firma Electrónica, se ha inspirado en la norma ETSI TR 102 272 y ETSI TR 102 038, como guías de asistencia en la redacción de este tipo de documentos.

1.2 Identificación.

Nombre del documento	Política de Firma Electrónica de ANF AC
Versión	1.0
Autor	<i>Florencio Díaz Vilches</i>
Referencia de la política / OID	1.3.6.1.4.1.18332.27.1
Fecha de emisión	1 de septiembre de 2005
Fecha inicio de uso	1 de septiembre de 2005
Fecha fin de uso	-No aplicable-
Localización URL	https://www.anf.es/AC/documentos/
CPS relacionada	Declaración de Practicas de Certificación de ANF Autoridad de Certificación
Campo de aplicación	Ver punto 1.5.4

PFE de ANF AC	Ref. Política de Firma Electrónica	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.27.1	Página 4 de 29

El prefijo del OID de esta política de firma es 1.3.6.1.4.1.18332.27. el sufijo determina la versión de esta Política a la que hace referencia el *OID*. En el caso de este documento versión 1.0, el *OID* que lo identifica es 1.3.6.1.4.1.18332.27.1

Cualquier modificación que esta Autoridad de Certificación realice sobre este documento, conllevará un cambio de versión y del identificador de objeto (OID). El protocolo a seguir queda determinado en el apartado "*Procedimiento de Especificación de Cambios*" de la CPS con la que se relaciona.

1.3 Datos de contacto.

1.3.1 Especificación del ente organizador.

Esta Política de Firma Electrónica es propiedad de ANF AC

ANF Autoridad de Certificación:

Gran Vía de les Corts Catalanes, 996

08018 - Barcelona - España

Tfno.-+34 93 2 661614

FAX.-+34 93 3131 614

Dirección electrónica: ac@anf.es

Dirección web: <https://www.anf.es/>

Esta Política de Firma Electrónica esta administrada por la Junta Rectora de la PKI de ANF AC:

JRPKI de la ANF Autoridad de Certificación

Gran Vía de les Corts Catalanes, 996

08018 - Barcelona - España

Tfno.-+34 93 2 661614

FAX.-+34 93 3131 614

Dirección electrónica: juntapki@anf.es

PFE de ANF AC	Ref. Política de Firma Electrónica	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.27.1	Página 5 de 29

1.3.2 Persona de contacto

Para cualquier información relacionada con esta Política de Firma Electrónica:

Persona de contacto: F. Díaz

e-mail: fdiaz@anf.es

1.3.3 Determinación de la adecuación de esta Política de Firma Electrónica con la CPS de ANF AC.

Las modificaciones propuestas o las nuevas aportaciones a incluir sobre esta Política de Certificación, deberán, previa a su aprobación, ser contrastadas con la CPS de ANF AC, a fin de asegurar que la Declaración de Practicas de Certificación soporta estos cambios.

No se podrán realizar cambios que no sean soportados por la CPS relacionada. Deberá, en todo caso, contemplarse simultáneamente con actualizaciones de la CPS de ANF AC.

La Junta Rectora de la PKI de ANF AC es la entidad que determina la adecuación de esta Política de Certificación a la CPS de ANF AC con la que se relaciona.

1.4 Publicación.

Este documento puede obtenerse libremente en el Directorio <https://www.anf.es/AC/documentos/>, o en las oficinas centrales de ANF AC.

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

1.5 Comunidad y ámbito de aplicación.

PFE de ANF AC	Ref. Política de Firma Electrónica	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.27.1	Página 6 de 29

1.5.1 Autoridad de Certificación.

ANF Autoridad de Certificación es el único prestador de servicios de certificación de esta infraestructura de clave pública. Es la única titular y responsable de todos los servicios utilizados, los cuales administra y supervisa de forma directa. Tanto en lo que respecta a:

- la emisión de certificados,
- estampación de sellos digitales de tiempo,
- consultas de estado de vigencia de los certificados,
- servicio de firma electrónica, y
- servicio de verificación de firma electrónica.

Como en cuanto a la tecnología utilizada en el ámbito de esta PKI, la cual ha sido desarrollada en su integridad por los servicios técnicos de este PSC, habiendo utilizado en su elaboración componentes criptográficos de reconocido prestigio y de código fuente abierto. ANF AC cuenta con la capacidad para garantizar la seguridad e integridad de todos los componentes informáticos empleados y asume plenamente, su obligación de actualizarlos ante los nuevos requerimientos y mejoras que demande el mercado.

1.5.3 Entidades finales.

1.5.3.1 Usuarios

Todas aquellas personas físicas, o jurídicas, titulares de certificados electrónicos vigentes, emitidos por ANF AC y que emplean dispositivos de creación de firma electrónica de acuerdo con lo establecido en este documento.

1.5.3.2 Terceros de confianza

De forma general son todas aquellas personas físicas o jurídicas, entidades u organizaciones, Administraciones Públicas o Corporativas, que de forma voluntaria confían en las firmas electrónicas que están asociadas a un certificado electrónico vigente, emitido por ANF AC, que han sido generadas por un Dispositivo de Firma Electrónica homologado por ANF AC, y sobre las que se ha

PFE de ANF AC	Ref. Política de Firma Electrónica	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.27.1	Página 7 de 29

verificado su validez aplicando un Dispositivo de Verificación homologado por ANF AC.

1.5.4 **Ámbito de aplicación.**

1.5.4.1 **Usos Permitidos**

Las firmas electrónicas generadas en el ámbito esta Política de Firma Electrónica, pueden utilizarse para autenticar todo tipo de documentos electrónicos, de acuerdo con las limitaciones de uso, declaración del emisor y restricciones derivadas de la Política de Certificación a la que esta sometido el certificado electrónico utilizado en su creación.

1.5.4.2 **Usos Restringidos**

El ámbito de aplicación de esta Política de Firma Electrónica, se circunscribe exclusivamente a firmas electrónicas que han sido generadas mediante un Dispositivo de Creación de Firma Electrónica homologado por ANF AC, empleando un certificado electrónico de entidad final vigente y emitido por ANF AC. Independientemente de lo citado, se excluye de la aplicación de esta Política de Certificación, aquellas firmas electrónicas asociadas a un certificado emitido bajo alguna de las siguientes jerarquías:

PSC subordinadas:

- ANF Basic CA
- ANF TSA CA
- ANF SSL CA
- ANF Encryption CA
- ANF OCSP Root Responder

Certificados de entidad final:

- ANF CRL Root Responder
- ANF OCSP Root Responder
- ANF CRL Clase 1 Responder
- AEAT.ANF.ES
- ANF OCSP Clase 1 Responder

PFE de ANF AC	Ref. Política de Firma Electrónica	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.27.1	Página 8 de 29

1.5.4.3 Usos Prohibidos

Todos aquellos no contemplados en los apartados “*Usos Permitidos*” y “*Usos Restringidos*” .

PFE de ANF AC	Ref. Política de Firma Electrónica	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.27.1	Página 9 de 29

2. Seguridad.

Se siguen los parámetros de Seguridad especificados en la Declaración de Prácticas de Certificación de ANF AC.

PFE de ANF AC	Ref. Política de Firma Electrónica	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.27.1	Página 10 de 29

3. Firma Electrónica.

La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante (LFE 59/2003, Tit. 1 Art. 3.1). A partir de este principio legal, la Ley de Firma Electrónica desarrolla un marco legal en el que se llega a equiparar jurídicamente la firma electrónica con la firma manuscrita (LFE 59/2003, Tit. 1 Art. 3.4) .

En este apartado se establece el alcance y el marco en el que se desarrolla la firma electrónica asociada a esta Política de Firma Electrónica.

3.1 Firma electrónica de ANF AC.

La firma electrónica de ANF AC se crea en un marco legal y contractual, en el cual se desea acreditar con fuerza probatoria y plena validez jurídica, que el firmante esta de acuerdo con los compromisos y condiciones que implícitamente o explícitamente se reseñan en los datos firmados.

Independientemente de lo anteriormente expresado, la validez de la firma electrónica esta condicionada a lo establecido en la Política de Certificación asociada al certificado electrónico utilizado, especialmente en cuanto a limitaciones, restricciones y usos prohibidos se refiere. Así como lo estipulado en la Declaración de Prácticas de Certificación, en especial, en cuanto a obligaciones y responsabilidades de los terceros de confianza.

3.2 Dispositivos de creación de firma electrónica homologados por ANF AC.

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

- *permiten identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere,*

PFE de ANF AC	Ref. Política de Firma Electrónica	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.27.1	Página 11 de 29

-
- que ha sido creada por medios que el firmante puede y debe de mantener bajo su exclusivo control y,
 - su validez es superior al periodo de vigencia del certificado al que se vincula.

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

Firma Electrónica Avanzada”

Una de las novedades que establece la actual Ley de Firma Electrónica 59/2003 respecto del Real Decreto-Ley 14/1999, es la denominación como firma electrónica reconocida. Esta firma electrónica 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*.

La Firma Electrónica Reconocida plantea dos nuevos e importantes requerimientos técnicos:

- 1.- Que el dispositivo utilizado cumpla con los requerimientos mínimos establecidos en la *LFE*, Art. 24.3.
- 2.- Y por lo tanto, que del producto resultante, es decir, la firma electrónica, se identifique, con seguridad, el dispositivo utilizado.

Los dispositivos de creación de firma electrónica homologados por ANF AC, generan firmas electrónicas que identifican con total certeza el dispositivo utilizado. La relación actualizada de dispositivos homologados por ANF AC, esta disponible en la URL:

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

ANF AC exclusivamente homologa dispositivos que cumplen con los requerimientos establecidos por la legislación vigente sobre **dispositivos seguros de creación de firma**, y en concreto:

LFE. 24.3. Un dispositivo seguro de creación de firma es un dispositivo de creación de firma que ofrece, al menos, las siguientes garantías:

PFE de ANF AC	Ref. Política de Firma Electrónica	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.27.1	Página 12 de 29

-
- a) *Que los datos utilizados para la generación de firma pueden producirse sólo una vez y asegura razonablemente su secreto.*
 - b) *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.*
 - c) *Que los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros.*
 - d) *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.*

Las firmas electrónicas creadas mediante dispositivos homologados por ANF AC, permiten identificar como mínimo:

- el certificado utilizado por el signatario y la entidad emisora, y sus identidades,
- el certificado empleado por el Servicio de Sellado Digital de Tiempo y la entidad emisora, y sus identidades,
- las limitaciones de uso del certificado del signatario,
- el dispositivo de firma empleado,
- la unidad emisora de sellos digitales de tiempo empleada,
- la fuente segura de tiempo sobre la que se sincroniza el servicio de sellado digital de tiempo,
- la unidad de servicio de OCSP consultada,
- la Política de Firma Electrónica a la que se someten la firma electrónica,
- los algoritmos criptográficos empleados para la creación de la firma electrónica,
- el formato en que se ha creado la firma y el formato de encapsulado,
- el nombre del documento y la extensión que identifica el tipo de formato del documento firmado,
- el código de transacción único de la firma electrónica vinculado al certificado empleado por el signatario.

y contienen como mínimo:

- el certificado del signatario,
- el documento original,
- la firma electrónica,

PFE de ANF AC	Ref. Política de Firma Electrónica	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.27.1	Página 13 de 29

-
- la referencia a esta política de firma
 - el sello digital de tiempo,
 - el resultado de la consulta OCSP, y
 - los links a las direcciones URL donde obtener mayor soporte documental e informativo de todos los elementos vinculados a la firma electrónica.

Los dispositivos de creación de firma electrónica homologados por ANF AC, garantizan un entorno de seguridad adecuado a las normas internacionales en esta materia, y a modo meramente enunciativo, no limitativo, cabe destacar:

- que el dispositivo de firma permite al usuario seleccionar el certificado electrónico que desea emplear,
- que el dispositivo de firma tiene la capacidad de firmar cualquier tipo de documento electrónico, independientemente de su formato o extensión del mismo.
- que el dispositivo permite al usuario consultar el documento y los atributos que serán incluidos en la firma antes de su creación,
- que se aplican medidas de seguridad para evitar la modificación o sustitución del documento seleccionado por el signatario, y que garantizan que los atributos de firma que fueron mostrados, son los mismos que se van a firmar,
- que las medidas de seguridad incorporadas en el dispositivo de firma, imposibilitan la creación de firmas electrónicas que incorporen en los atributos de firma cualquier tipo de código oculto, macro o código activo, y permite detectar cualquier modificación de los atributos firmados,
- que el dispositivo de firma crea una firma electrónica que garantiza la integridad y autenticidad de los atributos de firma,
- que el dispositivo de firma no altera los datos a firmar, manteniendo en todo momento la integridad de los mismos,
- que con el fin de garantizar la fiabilidad de la consulta del documento a firmar, se utiliza el mismo componente que emplea el firmante fuera del entorno del dispositivo de firma. El firmante tiene la posibilidad de abortar el proceso de firma en caso de disconformidad con los datos analizados,
- que, en caso de solicitar consulta y no exista componente para analizar los datos sobre los que se solicita la firma, el dispositivo de firma advierte al firmante del posible riesgo de firmar un contenido con potenciales datos falsos, y la responsabilidad que asume continuando con el proceso de creación de firma,

PFE de ANF AC	Ref. Política de Firma Electrónica	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.27.1	Página 14 de 29

-
- que a fin de informar al firmante del riesgo que presupone firmar documentos que contienen código activo, el dispositivo de firma esta dotado de un sistema que permite identificar documentos electrónicos que pueden contener este tipo de código. El dispositivo en esos casos, le apercibe del riesgo y le recomienda la consulta del documento en un entorno que no permita la activación de un potencial código,
 - que el dispositivo de firma posibilita que el usuario puede consultar toda la información contenida en el certificado que va a utilizar,
 - que el dispositivo de firma antes de mostrar el certificado al usuario, o de utilizarlo, comprueba su integridad y autenticidad.
 - que se emplea un canal de comunicación seguro para acceder a los datos de creación de firma, y a los servidores remotos de certificación,
 - que los componentes informáticos empleados para la creación de la firma están firmados electrónicamente por ANF AC, a fin de garantizar la autenticidad e integridad de los mismos,
 - que el usuario del dispositivo de creación de firma dispone de mecanismos de uso sencillo para comprobar la integridad de los componentes del dispositivo, a fin de detectar cualquier posible corrupción, y en caso de haberse producido, proceder a su actualización automática.
 - la actualización de los componentes, se realiza automáticamente en un servidor integrado en la red servidores de ANF AC, identificado de forma segura y empleando comunicaciones protegidas SSL.,
 - los algoritmos de firma utilizados en cada momento por el dispositivo de firma, son los catalogados por ANF AC como autorizados. Se han incorporado medidas de seguridad que impiden el uso de un dispositivo de firma no actualizado al nivel de seguridad exigible por ANF AC,
 - que el proceso de creación de firma, solo puede ser activado utilizando certificados electrónicos vigentes, y que han sido emitidos por ANF AC,
 - que en el diseño de la interfaz de usuario, se han simplificado los procesos con el fin de imposibilitar cualquier tipo de confusión o error de uso,
 - que no es posible la activación de la firma de forma accidental, siendo preciso introducir la clave secreta de activación,
 - que el dispositivo de firma, facilita al usuario la capacidad de cambiar la clave secreta de activación del certificado, para ello es preciso activar el cambio mediante la

PFE de ANF AC	Ref. Política de Firma Electrónica	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.27.1	Página 15 de 29

-
- introducción de la clave vigente, e introducir dos veces la nueva clave a fin de confirmar que no se ha producido error alguno por parte de usuario,
- que el dispositivo de firma, incorpora medidas de seguridad que impiden el empleo de claves consideradas inseguras, exigiendo además longitudes mínimas de ocho dígitos,
 - que la clave introducida no es legible, queda custodiada durante su uso en un entorno seguro, y se destruye de forma segura tras concluir con su uso,
 - que el dispositivo de firma incorpora medidas de seguridad que imposibilitan los ataques de fuerza bruta, estableciendo un máximo de intentos de activación de los datos de creación de firma, superado el número de intentos por introducción de claves falsas, se procede al boqueo de los datos de generación de firma afectados,
 - que el dispositivo de firma comprueba, antes de acceder a los datos de creación de firma, el periodo de validez del certificado que se pretende utilizar, así como el estado de vigencia del certificado. En caso de caducidad o revocación, no permite finalizar el proceso de creación de firma.
 - que todo el contexto de creación de firma se realiza en un marco de seguridad inaccesible a terceros, siendo destruido de forma segura una vez que se ha generado la firma o por interrupción del proceso,
 - que el dispositivo de creación de firma electrónica y el servicio de sellado digital de tiempo incorporan, como medida de seguridad, un plazo de tiempo máximo para la elaboración, el cual en ningún caso es superior a diez segundos, Superado este intervalo de tiempo, el dispositivo de firma procede a la destrucción segura del contexto de firma, y el servidor remoto comunica una denegación de servicio,
 - que finalizado el proceso de firma, el dispositivo de firma procede automáticamente a verificar la firma electrónica creada. Caso de que el fichero de firma construido no quede validado por el verificador, se procede a la destrucción segura del mismo,
 - que el dispositivo de firma electrónica y los servicios de certificación de AN AC, incorporan un sistema de control que garantice la coherencia de los procesos de certificación solicitados, con la CPS y Políticas que conforman la PKI de ANF AC,
 - que en ningún momento los datos a firmar salen del contexto de seguridad y privacidad del firmante,
 - que en la comunicación establecida entre el dispositivo de creación de firma y los servicios de certificación de ANF AC, garantizan la integridad y confidencialidad de los datos intercambiados en el transaccional electrónico,

PFE de ANF AC	Ref. Política de Firma Electrónica	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.27.1	Página 16 de 29

Los contenedores homologados que contienen los datos de creación de firma, asociados a certificados que han sido emitidos por ANF AC con la calificación de reconocidos, cuentan con unas definiciones específicas que imposibilitan su uso en otros dispositivos de firma electrónica que no estén homologados por ANF AC. El certificado reconocido vinculado a este modelo de contenedor, especifica como restricción de uso:

“Limitado su uso a Dispositivos 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 directamente interoperables con los habituales sistemas comerciales de firma electrónica : –*Explorer, Netscape, Outlook, etc.*- En este supuesto, el certificado especifica como restricción de uso:

“No utilizable en Dispositivos de Creación de Firma homologados por ANF AC”.

La información correspondiente quedará recogida en el OID 1.3.6.1.4.1.18332.41

Los datos de creación de firma almacenados en un contenedor PKCS#15, y con uso restringido a “Limitado su uso a Dispositivos de Creación de Firma homologados por ANF AC”, **NO son exportables a otro tipo de formato.**

Para la elaboración de los dispositivos de creación de firma homologados, se han seguido las normas especificadas en URL:

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

3.2.a Difusión.

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

Todos los dispositivos cuentan con un sistema de actualización a nuevas versiones en línea. Las actualizaciones se realizan utilizando canales de comunicación seguros y verificando la autenticidad de componentes mediante tecnología de firma electrónica.

PFE de ANF AC	Ref. Política de Firma Electrónica	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.27.1	Página 17 de 29

3.2.b Instalación.

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

3.2.c Procedimiento.

Procedimiento seguido por los dispositivos homologados de creación de firma electrónica de ANF AC:

- 1) *Fase previa.*
 - Selección del fichero a firma.
 - Selección del certificado electrónico que se desea utilizar.
- 2) *Verificación.*
 - El signatario puede proceder a la comprobación del documento electrónico seleccionado y los atributos de firma que se incluirán.
 - El signatario puede proceder a la comprobación del certificado que ha seleccionado.
- 3) *Activación del proceso de firma.*
 - El signatario introduce su contraseña secreta de activación de los datos de creación de firma.
 - El dispositivo establece una comunicación segura con ANF AC, a fin de determinar el estado de vigencia del certificado electrónico que se pretende utilizar –OCSP-. En caso positivo, obtención de un número de transacción exclusivo.
- 4) *Proceso de creación de firma electrónica.*
 - Generación del hash.
 - Cifrado del hash utilizando los datos de creación de firma asociados al certificado del signatario.
 - Obtención de un Sello Digital de Tiempo que cumple lo establecido en la CPS de ANF TSA AC.
- 5) *Creación del fichero de firma electrónica.*
 - La firma queda generada en un fichero con formato CMS.
 - Se encapsula en formato S/MIME

PFE de ANF AC	Ref. Política de Firma Electrónica	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.27.1	Página 18 de 29

-
- La extensión otorgada al fichero es SLC

3.3 Dispositivo de verificación de firma.

Para verificar las firmas electrónicas emitidas por dispositivos de creación de firma homologados por ANF AC, se debe de utilizar un dispositivo de verificación de firma homologado por ANF AC.

ANF AC tan solo homologa dispositivos que cuentan con la capacidad de verificar automáticamente si:

- La firma digital fue creada por la clave privada vinculada a la clave pública perteneciente al certificado del usuario.
- Estado del certificado y capacidad de firma: atributos e importe límite de firma.
- Que el documento, no ha sido alterado desde que se creó la firma digital.
- Identidad del usuario y de la AC que emite el certificado. Garantiza con su firma electrónica y sello de tiempo, que la transacción se realizó empleando un certificado vigente.

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.

3.3.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/dispositivos/>

Las actualizaciones de este software están firmadas electrónicamente y son gratuitas.

3.3.b Instalación.

PFE de ANF AC	Ref. Política de Firma Electrónica	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.27.1	Página 19 de 29

El usuario debe de proceder a la instalación del dispositivo siguiendo las instrucciones técnicas.

3.3.c Procedimiento.

Procedimiento seguido por los dispositivos homologados de verificación de firma electrónica de ANF AC:

- 1) *Fase previa.*
Selección del fichero firmado.
- 2) *Verificación.*
Se procede a las siguientes comprobación:
 - Coherencia de la firma electrónica con la Política de Firma Electrónica y Declaración de Prácticas de la Autoridad de Sellos de Tiempo.
 - Verificación de la firma electrónica y sello digital de tiempo.
- 3) *Emisión del informe de verificación.*
Se emite informe detallado del protocolo de verificación seguido y resultado obtenido.
- 4) *Creación de un documento de firma electrónica interpretable (opcional)*
Se trata de una representación gráfica, visualmente legible, de la firma electrónica en formato html. Incluye dentro del código, los datos íntegros del fichero original de firma electrónica, lo cual permite posteriores procesos de verificación utilizando este documento.
- 6) *Creación de un Informe de firma electrónica (opcional)*
Se trata de una representación gráfica, visualmente legible, de la firma electrónica en formato html. No incluye los datos del fichero de firma electrónica.

3.3.d Informe de verificación.

Este documento no se encuentra firmado electrónicamente, ni incluye la integridad de los datos de firma electrónica. Solo debe de confiarse en él si se ha obtenido por aplicación directa del Dispositivo de verificación sobre el fichero original de firma electrónica, o sobre el Documento de Firma Electrónica interpretable. No es

PFE de ANF AC	Ref. Política de Firma Electrónica	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.27.1	Página 20 de 29

recomendable confiar en documentos almacenados no autenticados. Almacene de forma segura: documento original de firma electrónica y dispositivo homologado de verificación.

3.3.e Informe de firma electrónica.

Este documento no se encuentra firmado electrónicamente. Solo debe confiarse en él si se ha obtenido por aplicación directa del Dispositivo de verificación sobre el fichero original de firma electrónica, o sobre el Documento de Firma Electrónica interpretable. No es recomendable confiar en documentos almacenados no autenticados. Almacene de forma segura: documento original de firma electrónica y dispositivo homologado de verificación.

3.3.f Documento de firma electrónica interpretable.

Este documento no se encuentra firmado electrónicamente, aunque incluye la integridad de los datos de firma electrónica. Solo debe confiarse en él si se ha obtenido por aplicación directa del Dispositivo de verificación sobre el fichero original de firma electrónica, o tras comprobar su autenticidad por aplicación del dispositivo de verificación sobre este documento.

Asimismo, el destinatario del documento o fichero electrónico firmado, puede requerir que el proceso de verificación sea realizado por el propio PSC, en cuyo caso, ANF AC emitirá un Acta de verificación firmada electrónicamente por el PSC, la cual 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.

PFE de ANF AC	Ref. Política de Firma Electrónica	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.27.1	Página 21 de 29

3.4 Ciclo de vida.

El ciclo de vida de una firma emitida con un dispositivo homologado por ANF AC es de larga duración. Se establece un periodo de validez mínimo de quince años, siempre y cuando:

- 1/ Los algoritmos criptográficos utilizados en la emisión de los certificados y en la generación de la firma electrónica sigan siendo considerados internacionalmente como seguros.
- 2/ La longitud de la clave empleada en la emisión de los certificados y en la generación de la firma electrónica siga siendo considerada internacionalmente como segura.
- 3/ La firma electrónica incorpore un Sello de Tiempo emitido por ANF TSA AC.

ANF AC realiza un seguimiento constante de las novedades que se producen en el campo de la criptografía. Se mantiene un informe actualizado del estado de vigencia de los algoritmos y longitud de clave que utiliza, de acceso público en la URL

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

Asimismo mantiene una página sobre aquellas incidencias que han podido afectar a sistemas PKI o a dispositivos que pueden ser de uso común. URL

<http://www.anf.es/incidencias/>

ANF AC ante cualquier sospecha de futura debilidad de los componentes criptográficos procede de acuerdo con lo establecido en el apartado "Seguridad Criptográfica". En caso de confirmación de riesgo, se procede de acuerdo con lo establecido en el Plan de Contingencias –Criptográfica-.

Caso de producirse un cambio de algoritmo o ampliación de la longitud de clave, los usuarios y terceros de confianza, disponen de un servicio especial de re-timbrado que permita mantener la vigencia de las firmas hasta ese momento producidas. En caso de uso se aplicarán las tasas publicadas en cada momento.

ANF AC comunicará personalmente a los usuarios, mediante correo electrónico, cualquier novedad al respecto, y al público en general a través de su servicio Web. |

PFE de ANF AC	Ref. Política de Firma Electrónica	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.27.1	Página 22 de 29

4 Sello digital de tiempo.

En todos los posibles aspectos, según lo especificado en la Declaración de Prácticas de Certificación de ANF TSA AC.

PFE de ANF AC	Ref. Política de Firma Electrónica	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.27.1	Página 23 de 29

5. Servicio de consulta del estado de los certificados.

El procedimiento de consulta del estado de vigencia de los certificados utilizados para la creación de firmas electrónicas sometidas a esta Política de Firma Electrónica, es OCSP.

En todos los posibles aspectos relativos al servicio de consulta OCSP, según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

PFE de ANF AC	Ref. Política de Firma Electrónica	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.27.1	Página 24 de 29

6. Obligaciones y Responsabilidades.

En todos los posibles aspectos, según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

PFE de ANF AC	Ref. Política de Firma Electrónica	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.27.1	Página 25 de 29

7. Responsabilidad Financiera.

En todos los posibles aspectos, según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

PFE de ANF AC	Ref. Política de Firma Electrónica	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.27.1	Página 26 de 29

8. Política de Confidencialidad.

En todos los posibles aspectos, según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

PFE de ANF AC	Ref. Política de Firma Electrónica	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.27.1	Página 27 de 29

9. Interpretación y ejecución.

En todos los posibles aspectos, según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

PFE de ANF AC	Ref. Política de Firma Electrónica	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.27.1	Página 28 de 29

10. Publicación y repositorios.

En todos los posibles aspectos, según lo especificado en la Declaración de Prácticas de Certificación de ANF AC.

Esta Política de Firma Electrónica es pública y puede obtenerse libremente en la URL <https://www.anf.es/AC/documentos/>, o en las oficinas de ANF AC.

PFE de ANF AC	Ref. Política de Firma Electrónica	Versión: 1.0
	OID: 1.3.6.1.4.1.18332.27.1	Página 29 de 29