Política de Firma Electrónica

	Esta especificación ha sido preparada por ANF AC para liberar a terceras partes.	**NIVEL DE SEGURIDAD** DOCUMENTO PÚBLICO

Gran Via de les Corts Catalanes 996, Barcelona - España - CP 08018 - Tel 932 661 614 / Fax 933 031 611

ÍNDICE

1. Introducción

ANF Autoridad de Certificación, (en adelante ANF AC), es una entidad jurídica, constituida al amparo de la Ley Orgánica 1/2002 del 22 de marzo e inscrita en el Ministerio del Interior con el número nacional 171.443 y CIF G-63287510.

ANF AC 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-)*1.

El prefijo del OID de esta Política de Firma Electrónica es 1.3.6.1.4.1.18332.27., al cual se le añade una extensión de formato X.Y que recoge su versión. Además de asignar identificadores únicos para distinguir las versiones sucesivas, también se asignan identificadores a los distintos formatos de representación (p.ej. formato legible de PDF, representación en sintaxis XML y representación en sintaxis ASN.1 siguiendo los estándares…).

Cuando se firman datos, el firmante asume las condiciones generales y las condiciones particulares aplicables a esa firma electrónica incorporando un campo firmado, dentro de la firma, que específica el OID de esta Política de Firma Electrónica.

Si el campo correspondiente a la normativa de firma electrónica está ausente y no se identifica ninguna normativa aplicable, entonces se debe de asumir que la firma ha sido generada sin ninguna restricción normativa, y en consecuencia, que no se le ha asignado ningún significado concreto legal o contractual. Se trataría de una firma que no especifica de forma expresa ninguna semántica o significación concreta y, por lo tanto, hará falta derivar el significado de la firma a partir del contexto (y especialmente, de la semántica del documento firmado).

El presente documento es la Política de Firma Electrónica de ANF AC. Esta documentación contiene las directrices y normas técnicas a las que se someten las Firmas Electrónicas asociadas a esta política. Detalla las normas organizadas alrededor de los conceptos de generación, validación y su alcance como evidencia legal. Además especifica el conjunto de criterios comunes de interoperabilidad, definiendo las reglas y obligaciones de todos los actores involucrados en dicho proceso.

La política de firma electrónica detalla los formatos asumidos por esta PKI, y especifica lo que deberá incluir el firmante en el proceso de generación de la firma, así como la información que debe de comprobar el tercero que confía en el proceso de validación de la firma.

Este documento detalla y complementa lo definido de forma genérica en la Declaración de Prácticas de Certificación de ANF AC.

La presente Política de Firma Electrónica (en adelante, PFE) se ha estructurado conforme a lo dispuesto en normas técnicas de referencia internacional y en normas legales actualmente vigentes, se especifica detalle de todas las contempladas en el apartado Referencias de este documento.

Esta Política de Firma Electrónica asume que el lector conoce los conceptos de PKI, certificado y firma electrónica; en caso contrario se recomienda al lector que se forme en el conocimiento de los anteriores conceptos antes de continuar con la lectura del presente documento.

*[1] Información que puede ser consultada en: http://www.iana.org/assignments/enterprise-numbers

1.1. Descripción de las Firmas Electrónicas.

• **Firma electrónica general:** *"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."*

• **Firma electrónica avanzada:** "*Es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control."*

• **Firma electrónica reconocida:** Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma

Para que una firma electrónica pueda ser considerada firma electrónica avanzada, de la ley se infieren los siguientes requisitos:

• La identificación posibilita garantizar la identidad del firmante de manera única.

• Integridad: garantiza que el contenido de un mensaje de datos ha permanecido completo e inalterado, con independencia de los cambios que hubiera podido sufrir el medio que lo contiene como resultado del proceso de comunicación, archivo o presentación.

• No repudio: es la garantía de que no puedan ser negados los mensajes en una comunicación telemática.

1.2. Identificación del documento

Nombre del documento	Política de Firma Electrónica de ANF AC.
Versión	1.2
Estado de la política	APROBADO
Referencia del documento / OID	1.3.6.1.4.1.18332.27.1.1
Fecha de emisión	2 de diciembre de 2010
Fecha de expiración	No es aplicable
CPS relacionada	Declaración de Prácticas de Certificación (CPS) de ANF AC OID: 1.3.6.1.4.1. 18332.1.9 Disponible en https://www.anf.es/AC/documentos/
Localización	https://www.anf.es/AC/documentos/

1.3. Identificadores del Formato de Firma

Con el objeto de identificar los formatos de firma sometidos a esta PFE, ANF AC ha asignado los siguientes identificadores de objeto (OID).

FIRMA ELECTRÓNICA	OID
Firma electrónica en formato XADES	1.3.6.1.4.1.18332.27.2.1
Firma electrónica en formato CADES	1.3.6.1.4.1.18332.27.3.1
Firma electrónica en formato PADES	1.3.6.1.4.1.18332.27.4.1
Firma electrónica en formato CMS	1.3.6.1.4.1.18332.27.5.1

1.4. Dispositivos de creación de firma electrónica homologados.

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,*
- *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 de ello se infiere que la firma electrónica debe de identificar 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*, está 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. Art.* 24.3. *Un dispositivo seguro de creación de firma es un dispositivo de creación de firma que ofrece, al menos, las siguientes garantías:*
>
> *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:

- el certificado del signatario, y restantes que componen la ruta de certificación,
- la firma electrónica,
- 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 apercibe 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,

- 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 introducción de la clave vigente, e introducir dos veces la nueva clave a fin de confirmar que no se ha producir 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, 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".

- La información correspondiente quedará recogida en la extensión propietaria OID 1.3.6.1.4.1.18332.41 del certificado electrónico utilizado.
- 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.

Estas firmas permiten garantizar los atributos de:

- Identidad del firmante.
- Integridad del documento y firma.
- No repudio del firmante.

Además incorporan elementos técnicos que garantizan:

- Verificación en origen.
- Larga vigencia de la firma electrónica.
- Legibilidad de la firma electrónica.

1.5. Comunidad de usuarios y ámbito de aplicación

1.5.1. Autoridades de Certificación

Esta PFE solo puede ser aplicada a firmas electrónicas que han sido generadas mediante el uso de certificados emitidos por ANF Autoridad de Certificación, y en las que se ha utilizado para su creación alguno de los dispositivos de firma homologados por ANF AC.

1.5.2. Emisor de la Política de Firma

ANF AC es el emisor de esta política de firma electrónica por la cual se deben de regir los usuarios finales en los procesos de generación y validación de una firma electrónica.

1.5.3. Usuarios Finales

Cabe distinguir los siguientes usuarios finales:

1.5.3.1. Firmante

Es la persona física que en nombre propio o en representación de tercera persona física o jurídica propietaria del certificado, genera la firma electrónica.

1.5.3.1.a. Obligaciones

Es obligación del firmante:

- El firmante se hará responsable de que el fichero que desea firmar no contiene contenido dinámico que pudiese modificar el resultado de la firma durante el tiempo. Si el fichero que se quiere firmar no ha sido creado por el firmante, deberá asegurarse que no existe contenido dinámico dentro del fichero, como pueden ser macros.
- Debe de evitar documentos que tengan enlaces a otros documentos externos, deben de ser autocontenidos. Se considerará como una excepción el caso de los esquemas de validación asociados a formatos XML.
- Debido al riesgo de introducción de código malicioso, se debe de tener especial precaución con documentos que contengan código ejecutable, como pueden ser macros. La documentación debe de estar libre de virus informáticos.
- Cuando el documento firmado no quede embebido en la firma, se debe de tener especial precaución en el procedimiento de almacenaje y custodia del

documento original, dado que algunos tipos de documentos se modifican por el mero hecho de consultarlos.

1.5.3.2. Terceros que confían en las firmas electrónicas

De forma general son todas aquellas personas físicas o jurídicas, entidades u organizaciones, Administraciones Públicas o Corporativas que de forma voluntaria desean confiar en las firmas electrónicas.

1.5.3.2.a. Obligaciones

Antes aceptar la firma:

- Los terceros que confían han de realizar las operaciones de clave pública de manera satisfactoria para confiar en la firma electrónica, utilizando para ellos los verificadores homologados por ANF AC.
- Así mismo asumen la responsabilidad de verificar las limitaciones de uso indicadas en el certificado, y su adecuación de acuerdo con lo establecido en la DPC y Políticas de Certificación asociadas al certificado utilizado, y
- se obligan a las condiciones de uso establecidas en este documento.

1.6. Ámbito de aplicación

1.6.1. Usos Permitidos

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 está de acuerdo con los compromisos y condiciones que implícitamente o explícitamente se reseñan en los datos firmados.

Las firmas electrónicas generadas en el ámbito esta Política de Firma Electrónica, pueden utilizarse para suscribir 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 está sometido el certificado electrónico utilizado en su creación.

1.6.2. 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 emitido por ANF AC y con el fin de crear la misma evidencia legal que si de una firma manuscrita se tratará.

1.6.3. Usos prohibidos

Está prohibida la creación de firmas electrónicas sometidas a esta Política de Firma Electrónica con el fin de realizar pruebas o test sin valor legal.

1.7. Política de Administración de ANF AC

1.7.1. Especificación de la Organización Administradora

Nombre	ANF Autoridad de Certificación
Dirección de email	fdiaz@anf.es
Dirección	Calle Orense, 85
	Madrid - 28020 - España
Número de teléfono	+34·902 902 172
Número de fax	+34·93 303 16 11

1.7.2. Persona de Contacto

Nombre	ANF Autoridad de Certificación
Dirección de email	fdiaz@anf.es
Dirección	Calle Orense, 85
	Madrid - 28020 - España
Número de teléfono	+34·902 902 172
Número de fax	+34·93 303 16 11

1.7.3. Competencia para determinar la adecuación de esta Política a la CPS de ANF AC

Las modificaciones propuestas o las nuevas aportaciones a incluir sobre esta Política, deben, previa a su aprobación por parte de la Junta Rectora de la PKI de ANF AC, ser contrastadas con las restantes Políticas de Certificación y DPC que ANF AC tenga publicadas, a fin de asegurar que las Políticas soportan estos cambios. Las modificaciones están recogidas en un documento de actualización de Políticas cuyo mantenimiento está garantizado por ANF AC y publicado en www.anf.es

Esta PFE detalla y completa lo estipulado en la "Declaración de Prácticas de Certificación" (DPC) de la PKI ANF AC, conteniendo las reglas a las que se sujeta, así como el ámbito de aplicación y las características técnicas de este tipo de firmas.

La presente Política de Firma Electrónica es válida desde la fecha de emisión hasta la publicación de una nueva versión. A fin de posibilitar la adecuación de los dispositivos de firma que se encuentran en explotación, se puede establecer un periodo de tiempo transitorio, en el cual convivan las dos versiones. Este periodo deberá indicarse en la nueva versión, pasado el cual sólo será válida la versión actualizada.

La pérdida de vigencia de un Política de Firma Electrónica, no afecta a las firmas que han sido emitidas con anterioridad a su sustitución, perdurando los efectos en

aquellas firmas que han sido emitidas, con sometimiento a esa determinada política, dentro del periodo de validez de la misma.

1.7.4. Referencias técnicas y legales

Para el desarrollo del contenido de esta PFE, se han tenido en cuenta:

Especificaciones técnicas:

- ETSI TS 101 733, v.1.8.3, v1.7.3 y v.1.8.1. Electronic Signatures and Infrastructures (SEI); CMS Advanced Electronic Signatures (CAdES).
- ETSI TS 101 903, v.1.4.2, v.1.3.2 y 1.4.1. Electronic Signatures and Infrastructures (SEI); XML Advanced Electronic Signatures (XAdES).
- ETSI TS 102 778, v 1.1.1. Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview, Part 2: PAdES Basic
- Profile based on ISO 32000-1, Part 3: PAdES Enhanced - PAdES-BES and PAdESEPES Profiles; Part 4: Long-term validation
- ETSI TS 102.176-1 V2.0.0 Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms
- ETSI TS 102 023 v1.2.2, v.1.2.1 y v.1.2.2. Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.
- ETSI TS 101 861 V1.3.1 Time stamping profile
- ETSI TR 102 038, v.1.1.1. Electronic Signatures and Infrastructures (SEI); XML format for signature policies.
- ETSI TR 102 041, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policies report.
- ETSI TR 102 045, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policy for extended business model.
- ETSI TR 102 272, v.1.1.1. Electronic Signatures and Infrastructures (SEI); ASN.1 format for signature policies.

- IETF RFC 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.

- IETF RFC 3125, Electronic Signature Policies.

- IETF RFC 3161, En Agosto de 2001 se publicó el estándar RFC 3161 "Internet X.509 Public Key Infrastructure Time Stamp Protocols" (actualizado en algunos aspectos por la RFC 5816 que permite el uso de ESSCertIDv2, tal como se define en el RFC 5035).

- IETF RFC 5280, RFC 4325 y RFC 4630, Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile.

- IETF RFC 5652, RFC 4853 y RFC 3852, Cryptographic Message Syntax (CMS).

- ITU-T Recommendation X.680 (1997): "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

- IETF RFC 3126 "Electronic Signature Formats for long term electronic signatures.

Igualmente, se ha considerado como normativa básica aplicable a la materia:

- Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica (Diario Oficial n° L 013 de 19/01/2000. pág. 0012-0020).

- Ley 59/2003, de 19 de diciembre, de firma electrónica.

- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

- Ley 56/ 2007 o Ley para el Impulso de la Sociedad de la Información

- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la

  Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos

- Real Decreto 3/2010 , de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica

- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Ley Orgánica 15/1999, de 13 de diciembre, de protección de los datos de carácter personal.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la ley de propiedad intelectual.

Esta PFE ha tenido en consideración y se ha inspirado en lo definido en el *Esquema nacional de identificación y firma electrónica de las Administraciones Públicas, Política de Firma Electrónica v1.8* OID 2.16.724.1.3.1.1.2.1.8; en conformidad con el Real Decreto 4/2010 del Gobierno de España; y la guía de Perfiles de Certificados Electrónicos v.1.7.6 publicada por el Consejo Superior de Administración Electrónica.

1.7.5. Procedimiento de Publicación

ANF AC publica la presente Política de Firma Electrónica, Políticas de Certificación y CPS en el repositorio público accesible a todos los ciudadanos en www.anf.es

Para facilitar el procesado automático de la firma electrónica, esta PFE esta implementada a su vez en formato "xml" según ETSI TR 102 038 v1.1.1. y en formato "ASN.1" según ETSI TR 102 272, v.1.1.1., a fin de que pueda ser interpretada por los sistemas encargados de la creación y validación de firma electrónica.

2. Creación de una firma

Las plataformas que presten el servicio de creación de firma electrónica deberán cumplir las siguientes características:

1. El usuario puede seleccionar un fichero, formulario u otro objeto binario para ser firmado. En el caso de firma de formulario, se le suele presentar al usuario el objeto binario a ser firmado, sin necesidad de selección previa.

2. El servicio de firma electrónica ejecutará una serie de verificaciones:

a. Si la firma electrónica puede ser validada para el formato del fichero específico que vaya a ser firmado, según la presente política de firma.

b. Si los certificados han sido expedidos bajo una determinada Política de Certificación de ANF AC.

c. Comprobación de la validez del certificado: si el certificado ha sido revocado, si se encuentra dentro del periodo de validez, y la validación de la ruta de certificación (incluidos la validación de todos los certificados en la cadena).

d. Si el dispositivo de firma y sus módulos criptográficos están debidamente identificados y homologados por ANF AC, y su estado es de vigencia.

e. Si la plantilla de construcción de firma electrónica legible esta integra y vigente.

Cuando una de estas verificaciones es errónea, el proceso de firma se interrumpirá.

2.1. Formatos admitidos de firma electrónica.

Actualmente se consideran formatos admitidos:

- Formato XAdES (XML Advanced Electronic Signatures), según especificaciónténica ETSI TS 101 903, versión 1.4.2 y versión 1.3.2.

- Formato CAdES (CMS Advanced Electronic Signatures), según especificación técnica ETSI TS 101 733, versión 1.8.3 y versión 1.7.4.
- Formato PAdES (PDF Advanced Electronic Signatures), según especificación técnica ETSI TS 102 778-3, versión 1.2.1.
- Formato CMS (CMS Cryptographic Message Syntax), según especificación técnica IETF RCF 5652.

Para versiones posteriores de los estándares se analizarán los cambios en la sintaxis y se aprobará la adaptación del perfil a la nueva versión del estándar

Se tendrá en cuenta la legislación Europea en relación a los formatos de firma admitidos en la Unión Europea, en especial aquellos definidos en los estándares europeos de firma electrónica.

2.2. Reglas de uso de los algoritmos y longitudes de clave.

ANF AC mantiene información pública sobre el estado de vigencia de los algoritmos y longitudes de clave de firma autorizada en:

http://www.anf.es/anf/certificacion/servicios-avanzados/200.1.116.html

El servicio de vigilancia criptográfica de ANF AC, toma entre otras referencias y guías de seguridad las especificaciones técnicas ETSI TS 102 176-1 sobre "Electronic Signatures and Infraestructures (ESI); Algorithms and parameters for secure electronic signature". Y los criterios adoptados en el Esquema Nacional de Seguridad desarrollado a partir del artículo 42 de la Ley 11/2007.

Los titulares de certificados emitidos por ANF AC, deben de emplear dispositivos que utilicen componentes criptográficos clasificados como seguros.

En el supuesto de que un algoritmo o clave pierda su clasificación de seguro y pase a situación de riesgo, los terceros que confían deberán re-timbrar las firmas con el fin de asegurar su estado de vigencia.

2.3. Servicio se estampación de sellado digital de tiempo de ANF AC.

El servicio de TimeStgamping de ANF AC ECUADOR cumple las especificaciones técnicas ETSI TS 102 023 v1.2.2, "Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities". Y asegura que los datos originales del documento que va a ser sellado, se generaron antes de una determinada fecha. El formato del sello de tiempo cumple las recomendaciones de IETF RFC 5816, "Internet X.509 Public Key Infrastructure; Time-Stamp Protocol (TSP)" que actualiza RFC 5816 (actualiza RFC 3161).

Los elementos básicos que componen un sello digital de tiempo de ANF AC son:

1. Datos sobre la identidad de la autoridad emisora (identidad jurídica, clave pública a utilizar en la verificación del sello, número de bits de la clave, el algoritmo de firma digital y la función hash utilizados).
2. Tipo de solicitud cursada (valor hash y datos de referencia).
3. Parámetros del secuenciador (valores hash "anterior", "actual" y "siguiente").
4. Fecha y hora UTC.
5. Firma digital de todo lo anterior con la clave pública y esquema de firma digital especificados.

El sellado de tiempo se realiza siempre antes de la caducidad del certificado del firmante.

2.4. Servicio de validación en origen OCSP

Desde el momento en que se realiza la firma y se estampa el sellado digital de tiempo es, como mínimo, el tiempo máximo de actualización del estado del certificado en el servicio OCSP.

Los dispositivos de firma electrónica homologados por ANF AC, validan el estado del certificado con posterioridad al momento de generar la firma electrónica, y posterior al momento de estampación de sello digital de tiempo. Las respuestas OCSP están fechadas y firmadas por ANF AC.

En cuanto al periodo de precaución o periodo de gracia, cabe señalar que no se fija periodo alguno, considerando que la respuesta OCSP corresponde al estado real del certificado, en el momento fijado en dicha información de estado.

2.5. Archivo y custodia

ANF AC, salvo contrato específico en el que se asuma este servicio, no almacena, y por lo tanto no asume la responsabilidad de custodiar los documentos de firma generados por sus suscriptores.

Los firmantes y los terceros que confían, para garantizar la fiabilidad de una firma electrónica a lo largo del tiempo, deberán asegurarse que la firma incorpora la información del estado del certificado asociado en el momento en que la misma se produjo, e información no repudiable incorporando un sello de tiempo, así como los certificados que conforman la cadena de confianza.

Para el archivado y gestión de documentos electrónicos se recomienda seguir las guías técnicas de desarrollo del Esquema Nacional de Interoperabilidad (RD 4/2010).

Para proteger las firmas electrónicas frente a la posible obsolescencia de los algoritmos y poder seguir asegurando sus características a lo largo del tiempo de validez, se deberá seguir uno de los siguientes procesos, de acuerdo con las especificaciones técnicas para firmas electrónicas según tipo:

- las plataformas de almacenamiento y custodia de firmas electrónicas deberán disponer de mecanismos de re-timbrado, para añadir, de forma periódica, un sello de fecha y hora de archivo con un algoritmo más resistente.
- la firma electrónica deberá almacenarse en un depósito seguro, garantizando la protección de la firma contra falsificaciones y asegurando la fecha exacta en que se guardó la firma electrónica.

Es necesario que con posterioridad las firmas puedan renovarse (refirmado o countersignature) y actualizar los elementos de confianza (sellos de tiempo), garantizando la fiabilidad de la firma electrónica.

3. Verificación de la firma electrónica

Los terceros que confían, antes de aceptar las firmas electrónicas sometidas a esta Política de Firma Electrónica, deben proceder a su verificación. Para ello se tienen que utilizar verificadores homologados por ANF AC. Estos verificadores garantizan como mínimo:

1. que la firma es válida para el fichero específico que está firmado;
2. validez de los certificados en el momento en que se produjo la firma, mediante comprobación de la respuesta OCSP que contienen, la cual ha debido verificar todos los certificados que componen la ruta de certificación;
3. comprobación de los Sellos Digitales de Tiempo;
4. estado de vigencia de los componentes criptográficos utilizados y dispositivo de firma empleado;
5. los datos utilizados para verificar la firma corresponden a los datos mostrados al verificador;
6. la firma se verifica de forma fiable y el resultado de esa verificación figura correctamente;
7. el verificador puede, en caso necesario, establecer de forma fiable el contenido de los datos firmados;
8. se verifican de forma fiable la autenticidad y la validez del certificado exigido al verificarse la firma;
9. figuran correctamente el resultado de la verificación y la identidad del firmante;
10. consta claramente la utilización de un seudónimo; y
11. puede detectarse cualquier cambio pertinente relativo a la seguridad.

Además el tercero que confía, mediante sus propios recursos, comprobará la adecuación del certificado de firma al objeto de firma electrónica al que se ha aplicado, sus limitaciones de uso, y plena aceptación de las limitaciones a la responsabilidad que ANF AC acepta asumir según queda especificado en el cuerpo del propio certificado, y en su correspondiente Política de Certificación.

Si se han realizado varias firmas del mismo documento, se seguirá el mismo proceso de verificación que con la primera firma.

3.1. Difusión de verificadores.

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/

4. Firmas Electrónicas de Larga Vigencia.

El proceso de comprobación de una firma electrónica debe poder realizarse incluso años después de su generación.

Debido a que el certificado electrónico tiene una vigencia limitada, en la mayoría de los casos 2 años y puede llegar a ser mucho menor si se ha producido su revocación, la firma debe de contener los elementos necesarios que permitan determinar su fecha de creación.

ANF AC ECUADOR atiende estos requerimientos en conformidad con la norma RFC 3126 "Electronic Signature Formats for long term electronic signatures":

La Firma electrónica emitida por dispositivos homologados por ANF AC, incorpora un sello digital de tiempo. La fecha de la firma electrónica está avalada por un ANF AC TSA, con ello se puede establecer con total exactitud y garantía si la firma electrónica se generó antes de una posible revocación del certificado. No obstante, el TimeStamping por sí solo no es evidencia suficiente y es preciso incorporar información completa de validación. Es decir, la firma generada en el ámbito de esta Política incorpora un conjunto de referencias a los certificados de la cadena de certificación y su estado (OCSP verificación en origen) como base para la verificación longeva, y como en el caso del TimeStamping, la respuesta OCSP está intervenida por ANF AC en calidad de Autoridad de Validación.

La clase básica para definir una política de firma electrónica de interoperabilidad es, según los estándares AdES, la clase EPES. ANF AC ECUADOR adopta los estándares ETSI (European Telecommunications Standards Institute) para los formatos CADES, XADES y PADES.

A partir de este formato básico EPES es posible incluir suficiente información para validar la firma a largo plazo, incorporando para ello información del estado del certificado firmado por la entidad emisora, y TimeStamping.

ANF AC dispone de un servicio de sellado de fecha y hora, según determina la ETSI TS 102 023, conforme a DPC OID 1.3.6.1.4.1.18332.5.1 de ANF Autoridad de Sellado de Tiempo, y un servicio de validación bajo protocolo OCSP según determina el estándar RFC 2560.

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 Digital de Tiempo expedido y firmado por ANF AC.

4/ La firma electrónica incorpore una respuesta OCSP expedida y firmada por ANF AC.

5/ En caso de que los algoritmos y longitud de claves hayan entrado en situación de riesgo, y antes de ser clasificados como inseguros, se haya procedido a un re-timbrado de la firma utilizando componentes criptográficos clasificados seguros.

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.

5. Obligaciones y Responsabilidades.

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

6. Controles de seguridad técnica

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

7. Responsabilidad Financiera.

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

8. Interpretación y ejecución.

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