Política de firma electrónica basada en certificados emitidos por las jerarquías de ANF Autoridad de Certificación

Paseo de la Castellana,79 - 28046 - Madrid (España)
Teléfono: 902 902 172 (llamadas desde España)
Internacional (+34) 933 935 946
Fax: (+34) 933 031 611 · Web: www.anf.es

Nivel de Seguridad

Documento Público

Aviso Importante

Dirección: Paseo de la Castellana, 79 - 28046 - Madrid (España)

Teléfono: 902 902 172 (llamadas desde España) Internacional (+34) 933 935 946

Fax: (+34) 933 031 611 · Web: www.anf.es

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-)

La finalidad de esta política es reforzar la confianza en los actos firmados electrónicamente a través de determinadas condiciones para un contexto dado.

Cuando se firman datos, el firmante indica la aceptación de unas condiciones generales y unas condiciones particulares aplicables a la firma electrónica. Esta aceptación se realiza mediante la inclusión en la firma de un campo OID. Este identificador de objeto específica una determinada política de firma electrónica de forma unívoca.

Si el campo correspondiente a la normativa de firma electrónica está ausente y no se identifica ninguna normativa aplicable, entonces se debe 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).

Este documento detalla y complementa lo definido de forma genérica en la Declaración de Prácticas de Certificación de ANF AC OID 1.3.6.1.4.1.18332.1.9.1.1.

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.

1.1 Objeto del documento

Esta política representa el conjunto de criterios asumidos por ANF Autoridad de Certificación (en adelante, ANF AC) en relación a las transacciones que han sido firmadas electrónicamente empleando un certificado electrónico emitido por una de las jerarquías de ANF AC.

En conformidad con lo establecido en la ley 59/2003, de 19 de diciembre, de firma electrónica (en adelante, LFE) Art.18.b).2 este documento informa de los mecanismos que ANF AC pone a disposición de sus suscriptores para garantizar la fiabilidad de la firma electrónica de un documento a lo largo del tiempo.

1.2 Definición legal de la firma electrónica

La Ley 59/2003, de 19 de diciembre, de firma electrónica (en adelante, LFE), y el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, definen tres conceptos de firma:

- **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 /cualificada**:
  "Es 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, se infieren los siguientes requisitos:

- **Identidad:**
  Garantiza 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.

Los requerimientos y uso de certificados reconocidos, y la clasificación de los dispositivos que los contienen, queda detallada en la Declaración de Prácticas de Certificación y en las Políticas de Certificación de ANF AC.

1.3 Identificación del documento

Para el desarrollo de su contenido, se ha tenido en cuenta las siguientes especificaciones técnicas:

Nombre del documento	Política de firma electrónica
Versión	1.3
Estado de la política	APROBADO
Referencia del documento / OID	1.3.6.1.4.1.18332.27.1.1
Fecha de publicación	1 de junio de 2016
Fecha de expiración	No es aplicable
DPC relacionada	Declaración de Prácticas de Certificación (DPC) de ANF AC
Localización	https://www.anf.es/documentos

1.4 Referencias

Para el desarrollo de su contenido, se ha tenido en cuenta las siguientes especificaciones técnicas:

- ETSI TS 101 733, v.1.6.3, v1.7.4, v.1.8.1 y 2.2.1., Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES);
- ETSI TS 103 173, v.2.1.1., Electronic Signatures and Infrastructures (ESI); CAdES Baseline profile. Define un perfil de firmas CAdES (firmas avanzadas construidas sobre firmas CMS) convenientes para ser utilizadas en el ámbito de la Directiva Europea de Servicios, por las autoridades nacionales de los estados miembros de la UE;
- ETSI TS 119 124-(5 pts), v.1.1.1., Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability;
- ETSI TS 101 903, v.1.2.2, v.1.3.2, y 1.4.1., Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES);
- ETSI TS 103 171, v.2.1.1., Electronic Signatures and Infrastructures (ESI); XAdES Baseline profile. Define el perfil de firmas XAdES convenientes para ser utilizadas en el ámbito de la Directiva Europea de Servicios, por las autoridades nacionales de los estados miembros de la UE;
- ETSI TS 119 134-(5 pts), v.2.1.1., Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability;
- ETSI TS 103 174, v.2.1.1., Electronic Signatures and Infrastructures (ESI); ASiC Baseline profile. Define un perfil de contenedor ASiC (Associated Signatures Container: contenedor que engloba en un solo paquete un conjunto de documentos electrónicos y un conjunto de firmas electrónicas XAdES o CAdES sobre uno, varios o todos los documentos) convenientes para ser utilizadas en el ámbito de la Directiva Europea de Servicios, por las autoridades nacionales de los estados miembros de la UE;
- ETSI TS 102 778-3, v.1.2.1., Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview, Part 2: PAdES Basic;
- ETSI TS 103 172, v.2.1.1., Electronic Signatures and Infrastructures (ESI); XAdES Baseline profile. Define un perfil de firmas PAdES (firmas avanzadas para documentos PDF) convenientes para ser utilizadas en el ámbito de la Directiva Europea de Servicios, por las autoridades nacionales de los estados miembros de la UE;
- ETSI TS 119 144-(5 pts), v.2.1.1., Electronic Signatures and Infrastructures (ESI); PAdES digital signatures - Testing Conformance and Interoperability;
- 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; Part 1: Hash functions and asymmetric algorithms;
- ETSI TS 102 023, v.1.2.1 y v.1.2.2., Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities;
- ETSI TS 101 861 v.1.3.1., 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.
- ETSI TS 103 174, v.2.2.1., Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile
- ETSI TS 102 918, v.1.1.1., Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC)
- ETSI TS 101 862 *(Qualified Certificate Profile). Queda definida en las normas* EN 319 412-1, EN 319 412-5)
- ETSI TS 101 533, Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management

- IETF RFC 6960, X.509, Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.
- IETF RFC 3125, Electronic Signature Policies.
- IETF RFC 3161. actualizada por RFC 5816, Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP).
- 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 5652, Cryptographic Message Syntax (CMS).
- ITU-T Recommendation X.680 (1997), Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation.
- ISO 32000-1:2008, v.1.7., PDF (Portable Document Format).

Igualmente, se ha considerado como normativa básica aplicable:

- Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.
- 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.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
- 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.

2 Alcance de la política de firma

Este documento propone una política de firma electrónica que detalla las condiciones generales asociadas a las mismas.

Para su identificación univoca, la política de firma se identificará con un identificador único que será OID: **1.3.6.1.4.1.18332.27.1.1.** Esta deberá incluirse obligatoriamente en la firma electrónica, empleando el campo correspondiente para identificar la política marco y las condiciones generales y específicas de aplicación para su validación.

La presente política de firma está disponible en formato legible, de modo que puedan ser aplicadas en un contexto concreto para cumplir con los requerimientos de creación y validación de firma electrónica.

2.1 Comunidad de usuarios

Los operadores involucrados en el proceso de creación y validación de firma electrónica son:

- **Firmante:** es la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.
- **Tercero que confía:** persona física o jurídica receptora de la firma electrónica que previamente a confiar en ella, valida o verifica la firma electrónica apoyándose en las condiciones exigidas en este documento.
- **Emisor del certificado electrónico:** es la entidad de certificación que expide el certificado electrónico en el que se basa la creación de la firma electrónica.
- **Emisor de la política de firma:** es la entidad que se encarga de generar y gestionar el documento de política de firma, por el cual se deben regir el firmante y el tercero que confía en los procesos de generación y validación de firma electrónica.

2.2 Ámbito de aplicación

2.2.1 Usos Permitidos

La firma electrónica de ANF AC está destinada a ser utilizada 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, salvo en aquellas cuestiones en las que haya expresado una mención o salvedad, con los compromisos y condiciones que implícita o explícitamente se reseñan en los datos firmados.

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

2.2.2 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.

2.2.3 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.

2.3 Formatos de firma comunes

Los formatos de firma son especificaciones, comúnmente aprobadas como estándares reconocidos, que definen qué información debe o puede contener una firma electrónica y el cómo se estructura esa información.

A modo meramente enunciativo, no limitativo, se especifican:

- **Formato CAdES** (CMS AdvancedElectronicSignatures).
  Es la evolución del primer formato de firma estandarizado. Tiene la capacidad de firmar cualquier tipo de formato de fichero (.jpg, .avi, .doc, .exe, etc.). El resultado final es un fichero *.slc.
  El documento electrónico firmado pues quedar embebido en la propia firma: *Attached/implicit signature*: los dos elementos (documento y firma) se encuentran en el mismo fichero, y se firma todo el fichero
  Según especificación técnica ETSI TS 101 733.

- **Formato XAdES** (XML AdvancedElectronicSignatures).
  Puede firmar cualquier tipo de fichero, aunque está especialmente indicado para ficheros *.xml. El resultado final es un fichero *.xml
  El documento electrónico firmado puede quedar incluido en la firma, la normas contempla las siguientes opciones:
  - *Attached*: aunque la firma y el documento se devuelven en un único fichero XML los dos se encuentran separados dentro del mismo y se firma únicamente la parte donde se encuentra el documento.
  - *Enveloped*: Si se ha firmado una parte del documento XML que la contiene, se llama una firma *envuelta (enveloped)*.
  - *Enveloping*: Si contiene los datos firmados dentro de sí mismo se llama una firma *envolvente (enveloping)*.

  Según especificación técnica ETSI TS 101 903.

- **Formato PAdES** (PDF AdvancedElectronicSignatures).
  Básicamente es una implementación del PKCS#7. Puede firmar ficheros PDF, aunque soporta datos XML. El resultado final es un fichero *.pdf.
  La firma se encuentra embebida en la propia estructura del documento, tal y como especifica el estándar ISO 32000-1:2008.
  Formato PAdES según especificación técnica ETSI TS 102 778-3.

- **Formato PDF Sign** (Firma interpretable de ANF AC).
  Puede firmar cualquier tipo de fichero. El resultado final es un fichero *.pdf en el que la firma es legible en base a una plantilla interpretable.
  El documento original es firmado en formato **CAdES** y la firma interpretable queda firmada en formato **PAdES,** todo ello integrado en un único documento de firma.

2.3.1 Vigencia de la firma electrónica

De acuerdo con los estándares internacionales, se debe establecer el término de **"**larga vigencia de la firma - XL**"**, siempre y cuando se atiendan los requerimientos que permitan **mantener su validez** y la capacidad de poder **verificarla a lo largo del tiempo**.

El proceso de verificación tiene como objetivo determinar:

- La integridad de los datos firmados asegurando que éstos no hayan sufrido ninguna modificación.
- La autenticidad de los certificados que han sido utilizados para firmar, y
- Comprobar que el estado del certificado con el que se firmó era vigente en el momento de la firma.

Una vez que el certificado caduca o es revocado, si la firma no incluye un Sello de Tiempo Electrónico la verificación de la firma será **negativa**, dado que no es posible determinar si el certificado, cuando se utilizó, era o no válido.

Para resolver este problema se debe de incluir en la firma electrónica información de la fecha de su creación (*Time Stamping*) y de la validez del certificado en ese instante (*respuesta OCSP firmada por la CA emisora del certificado empleado*). De este modo se consigue que la validez de la firma perdure más allá de la validez del certificado.

Todas las firmas creadas con dispositivos homologados por ANF AC, son firmas **AdES** (**Ad**vanced **E**lectrónic **S**ignature) **XL** (e**X**tendido **L**argo plazo = firmas de larga vigencia**)**.

Las normas ETSI de referencia, definen determinadas extensiones según los atributos que incorpora la firma electrónica, concretamente:

- **Firma Básica**
  - **AdES - BES**, es el formato básico para satisfacer los requisitos de la firma electrónica avanzada. Proporciona autenticación básica y protección de la integridad, no contempla el "no repudio" ni la validación a largo plazo.
  - **AdES – EPES**, es un AdES-BES al que se le incorpora información sobre la política de firma, como pudiera ser aquella información sobre el certificado empleado y la CA que lo emitió.
- **AdES T**, (T de TimeStamp). Es un AdES-EPES al que se le añade un sellado de tiempo con el fin de situar en el tiempo el instante en que se firma un documento. Se trata de una segunda firma realizada por ANF TSA CA (Time Stamp Authority).
- **AdES C**, (C de Cadena). Es un AdES-T al que se le añade referencias sobre los certificados y fuente de validación utilizada para confirmar la vigencia del certificado empleado. Esta modalidad es la base para una verificación longeva.
- **AdES X**, (X de eXtendida). Es un AdES-C al que se le añade información sobre la fecha y hora de los datos introducidos en la extensión C a las referencias creadas en el modelo AdES-C.
- **AdES XL**, (XL de eXtendido Largo plazo). Es un AdES-X al que se le añade los certificados (sólo clave pública) y las fuentes de validación que se usaron. A diferencia del -C, dónde sólo se incluía una referencia (un puntero), en este formato se añade una tercera firma (respuesta OCSP) realizada por ANF AC. Esto se utiliza para garantizar la validación muchos años después de la firma incluso en el caso que la CA que emitió el certificado, o la fuente de validación (OCSP

Responder o CRL), ya no esté disponible. Es decir, **garantiza la validación off-line a largo plazo**.

- **AdES A**, (A de Archivo). Este formato incluye toda la información anterior pero incluye meta-información asociada a políticas de refirmado. Una política de refirmado establece un período de caducidad de la firma digital, y superado este tiempo, se procede a un refirmado. El escenario ideal para este formato de firma son aquellos documentos cuya validez sea muy elevada: 15, 20, 50 años, etc.

2.3.2 Atributos de los formatos de firma

La estructura básica completa de cada formato de firma esta publicada en http://www.anf.es.

La información especialmente relevante según formato de firma es:

2.3.2.1 Formato XAdES

La versión de XAdES. Se indicará en los tag el identificador de la versión de XAdES que se ha seguido para construir la firma.

Las siguientes etiquetas dentro del campo ***SignedProperties:***

- **SigningTime:** indica la fecha y la hora. Esta etiqueta tan solo es incluida si la firma cuenta con un Sello Digital de Tiempo.
- **SigningCertificate:** contiene referencias a los certificados y algoritmos de seguridad utilizados para cada certificado.
- **SignaturePolicyIdentifier:** identifica la política de firma sobre la que se basa el proceso de generación de firma electrónica.
- **DataObjectFormat:** define el formato del documento original.
- **SignatureProductionPlace**: define el lugar geográfico donde se ha realizado la firma del documento.
- **SignerRole:** define el rol de la persona en la firma electrónica. Al menos uno de estos elementos ClaimedRoles o CertifiedRoles deben estar presentes en este campo.
    - En el caso de su utilización en una factura en formato eFactura, deberá contener uno de los siguientes valores en el campo ClaimedRoles:
        - "supplier" o "emisor": cuando la firma la realiza el emisor.
        - "customer" o "receptor": cuando la firma la realiza el receptor.
        - "third party" o "tercero": cuando la firma la realiza una persona o entidad distinta al emisor o al receptor.
    - En el caso de utilizar certificados de atributos para certificar el rol del firmante el campo CertifiedRoles contendrá la codificación en base-64 de uno o varios atributos de certificados del firmante.
- **CommitmentTypeIndication:** define la acción del firmante sobre el documento firmado (lo aprueba, lo informa, lo recibe, lo certifica, ...)
- **AllDataObjectsTimeStamp:** contiene un sello de tiempo, calculado antes de la generación de la firma, sobre todos los elementos contenidos en *Reference*.
- **IndividualDataObjectsTimeStamp:** contiene un sello de tiempo, calculado antes de la generación de la firma, sobre algunos de los elementos contenidos en *Reference*.
- La etiqueta **CounterSignature:** refrendo de la firma electrónica y que se puede incluir en el campo *UnsignedProperties*. Las siguientes firmas, ya sean serie o paralelo, se añadirán según indica el estándar XAdES, según el documento ETSI TS 101 903 v1.4.2 (admitiéndose implementaciones según v1.2.2 y posteriores).

Propiedades no firmadas de la modalidad XAdES-C.

- **CompleteCertificateRefs** que contiene referencias a todos los certificados de la cadena de confianza necesaria para verificar la firma, excepto el certificado firmante.
- **CompleteRevocationRefs** que contiene referencias a las CRLs y/o respuestas OCSP usadas en la verificación de los certificados.

En el caso que se desee incorporar a la firma esta información de validación se recomienda utilizar el formato XAdES-X, que añade un sello de tiempo a la información anterior.

El formato XAdES-XL, además de la información incluida en XAdES-X contempla dos nuevas propiedades no firmadas.

- CertificateValues.
- RevocationValues.

Estas propiedades permite incluir, no sólo las referencias a la información de validación sino también la cadena de confianza completa y la CRL o respuesta OCSP obtenida en la validación.

2.3.2.2 Formato CAdES

Principales etiquetas que pueden ser incluidas en el documento de firma:

- **Content-type:** especifica el tipo de contenido que debe ser firmado. Es una etiqueta obligatoria según el estándar CAdES.
- **Message-digest:** identifica el cifrado del contenido *firmado OCTET STRING* en *encapContentInfo*. Es una etiqueta obligatoria según el estándar CAdES.
- **ESS signing-certificate** o **ESS signing-certificate-v2**: Permite el uso de SHA-1 (sólo para ESS signing-certificate) y la familia de algoritmos SHA-2 como algoritmo de seguridad. Es una etiqueta obligatoria según el estándar CAdES.
- **Signing-time:** indica la fecha y hora de la firma. Esta etiqueta tan solo es incluida si la firma cuenta con un Sello Digital de Tiempo.
- **SignaturePolicyIdentifier:** indica la política de firma sobre la que se basará la generación de la firma electrónica. El documento deberá incorporar la referencia (OID) a la política de firma particular aplicada y la huella digital del documento de política de firma correspondiente y el algoritmo utilizado, en el elemento *SigPolicyHash* digital del documento de política de firma correspondiente y el algoritmo utilizado, en el elemento *SigPolicyHash*, de manera que el verificador pueda comprobar, calculando a su vez este valor, que la firma está generada según la misma política de firma que se utilizará para su validación.
- **Content-hints:** describe el formato del documento original.
- **Content-reference:** puede ser utilizada como un modo de relacionar una contestación con el mensaje original al que se refiere.
- **Content-identifier**: contiene un identificador que se puede utilizar en el atributo anterior.
- **Commitment-type-indication:** indica la acción del firmante sobre el documento firmado (lo aprueba, lo informa, lo recibe, lo certifica...).
- **Signer-location:** permite indicar el lugar geográfico donde se ha realizado la firma del documento. Al menos uno de estos elementos *ClaimedRoles* o *CertifiedRoles* deben estar presentes en esta etiqueta.
- **Signer-attributes:** indica el rol de la persona en la firma electrónica.
- **Content-time-stamp:** permite un sello de tiempo, antes de la generación de la firma, sobre los datos que van a ser firmados, para incorporarla con la información firmada.
- **CounterSignature**, refrendo de la firma electrónica. Las siguientes firmas se añadirán según indica el estándar CAdES, según el documento ETSI TS 101 733 v2.2.1 (admitiéndose implementaciones según v1.6.3 y posteriores).

Dentro del formato de firma CAdES, el formato extendido CAdES-C incorpora dos atributos:

- **complete-certificate-references** que contiene referencias a todos los certificados de la cadena de confianza necesaria para verificar la firma.
- **complete-revocation-references** que contiene referencias a las CRLs y/o respuestas OCSP usadas en la verificación de la firma.

El formato CAdES-X Long además de la información incluida en CAdES-C, incluye dos nuevos atributos **certificate-values** y **revocation-values** que incluyen no sólo las referencias a la información de validación, sino también la cadena de confianza completa y la CRL o respuesta OCSP obtenida en la validación.

Se recomienda usar los siguientes formatos:

- En el caso que la validación se realice mediante consulta OCSP: a los formatos CAdES-X Long type 1 o CAdES-X Long type 2, que añaden un sellado de tiempo a la información incluida en una firma CAdES X Long.
- En este caso se incorporarán los atributos certificate-values y revocation-values puesto que la respuesta a una consulta OCSP no ocupa mucho espacio.
- En el caso que la validación no pueda realizarse mediante OCSP y se realice mediante consulta a una CRL: a los formatos CAdES-X type 1 o CAdES-X type 2, que incluyen un sellado de tiempo a la información incluida en una firma CAdES-C, es decir, a las referencias a las CRL consultada y los certificados de la cadena de confianza, no se recomienda incluir los atributos certificate-values y revocation-values ya que pueden ser muy voluminosos.

En el caso que se esté próximo a la caducidad del sello de tiempo añadido para construir la firma longeva, se puede transformar la firma CAdES-X Long type 1 o CAdES-X Long type 2, en una firma CAdES-A, añadiendo un sellado de tiempo de archivo a la firma antes

2.3.2.3 Formato PAdES

Principales etiquetas que pueden ser incluidas en el documento de firma:

- **Content-type:** especifica el tipo de contenido que debe ser firmado. Es obligatoria según el estándar PAdES.
- **Message-digest:** identifica el cifrado del contenido firmado OCTET STRING en encapContentInfo. Es obligatoria según el estándar PAdES.
- **ESS signing-certificate** o **ESS signing-certificate-v2** es una etiqueta que permite el uso de SHA-1 (sólo para *ESS signing-certificate*) y la familia de algoritmos SHA-2 como algoritmo de seguridad. Es una etiqueta obligatoria según el estándar PAdES.
- No se especificará el campo **Cert** del diccionario *Signature*.
- **Signature-policy-identifier:** identifica la política de firma sobre la que se basa el proceso de generación de firma electrónica. El documento deberá incorporar el OID de la política de firma particular aplicada.
- No se especificará el atributo **Content-hints**.
- No se especificará el atributo **SigningTime**. El tiempo de la firma debe indicarse en el campo M en diccionario Signature, un atributo específico del PDF.
- Commitment-type-indication: este etiqueta indica la acción del firmante sobre el documento firmado (lo aprueba, lo informa, lo recibe, lo certifica, etc.) Según el estándar PAdES deberá estar indicado en el campo Reason propio del PDF.
- **Signer-attributes:** indica el rol de la persona en la firma electrónica. Al menos uno de estos elementos ClaimedRoles o CertifiedRoles deben estar presentes en este campo.
- **Content-time-stamp:** permite un sello de tiempo, antes de la generación de la firma, sobre los datos que van a ser firmados, para incorporarla con la información firmada.
- Para el lugar de la firma se utilizará la entrada **Location** en el diccionario de firma, en lugar del elemento *signer-location* mencionado en el epígrafe de CAdES.

- El atributo **Counter-Signature**, refrendo de la firma electrónica, no está permitida en este tipo de firmas. Las siguientes firmas se añadirán según indica el estándar PAdES, según el documento ETSI TS 102 778-3 y parte 4, versión 1.1.2.

2.4 Almacenamiento del documento original firmado

En todos los formatos de firma, el documento de firma puede estar separado o unido al documento original firmado.

- Cuando el documento original se incluye en la firma:
  - En el caso de CAdES estas firmas se denominan firmas implícitas.
    - Se adopta el tipo Signed Data. Para la estructura del documento original firmado, según lo especificado en los estándares CMS (IETF RCF 5652) y CAdES (ETSI TS 101 733), que mantiene el documento original y la firma en un mismo fichero.

    Los formatos PAdES y PDF Sign siguen el modelo CAdES.
  - En el caso de firmas XAdES, la norma establece diferentes modalidades:
    - envolventes (enveloping). Incluye el documento original en la firma. En este modelo la estructura XML de firma es la única en el documento de firma, y esta contiene internamente el documento original firmado. En este caso, los datos firmados se encuentran en el nodo "Object", y si los datos no son XML, no es posible insertarlos directamente dentro de una estructura XML, por lo que se codifican previamente en Base64.
    - envueltas (enveloped). Un contenido XML auto-contiene su propia firma digital, insertándola en un nodo propio interno, por lo que, al contrario que en los formatos anteriores, no es posible firmar contenido que no sea XML.
- Cuando el documento original no es incluido en la firma:
  - En el caso CAdES estas firmas se llaman firmas explícitas. La firma y el documento firmado son ficheros diferentes.

    Los formatos PAdES y PDF Sign siguen el modelo CAdES.
  - En el caso de firmas XAdES estas firmas son modalidad "dettached".

2.5 Creación de la firma electrónica

Los dispositivos de creación de firma electrónica homologados por ANF AC comprueban la validez del certificado antes de permitir su uso. Si el resultado es que el certificado no está vigente, el proceso de firma se interrumpe.

Los dispositivos de firma electrónica homologados por ANF AC cumplen los requerimientos establecidos en el Art. 24 de la Ley 59/2003, de 19 de diciembre, de firma electrónica (en adelante, LFE), concretamente:

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. *Un dispositivo de creación de firma es un programa o sistema informático que sirve para aplicar los datos de creación de firma.*
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.*

La relación de dispositivos homologados, sus especificaciones técnicas y calificación se encuentran publicados en http://www.anf.es

ANF AC es un prestador cualificado de servicios de confianza, que emite certificados electrónicos reconocidos. La creación de una firma electrónica reconocida /cualificada requiere:

- Haber sido creada con un certificado reconocido / cualificado, y
- Haber empleado un dispositivo seguro / cualificado de creación de firma.

2.6 Verificación de la firma electrónica

Para verificar la firma electrónica se debe utilizar un dispositivo de verificación de firma electrónica homologado por ANF AC.

Los dispositivos de verificación de firma electrónica homologados por ANF AC cumplen los requerimientos establecidos en el Art. 25 de la ley 59/2003, de 19 de diciembre, de firma electrónica (en adelante, LFE), concretamente:

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 garantizarán, siempre que sea técnicamente posible, que el proceso de verificación de una firma electrónica satisfaga, al menos, los siguientes requisitos:*

a) *Que los datos utilizados para verificar la firma correspondan a los datos mostrados a la persona que verifica la firma.*

b) *Que la firma se verifique de forma fiable y el resultado de esa verificación se presente correctamente.*

c) *Que la persona que verifica la firma electrónica pueda, en caso necesario, establecer de forma fiable el contenido de los datos firmados y detectar si han sido modificados.*

d) *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.*

e) *Que se verifiquen de forma fiable la autenticidad y la validez del certificado electrónico correspondiente.*

f) *Que pueda detectarse cualquier cambio relativo a su seguridad.*

4. *Asimismo, los datos referentes a la verificación de la firma, tales como el momento en que ésta se produce o una constatación de la validez del certificado electrónico en ese momento, podrán ser almacenados por la persona que verifica la firma electrónica o por terceros de confianza.*

La relación de dispositivos homologados, sus especificaciones técnicas y calificación se encuentran publicados en http://www.anf.es

2.7 Elementos criptográficos

Para los entornos de seguridad genérica de acuerdo con las especificaciones técnicas ETSI TS 102 176-1 sobre "Electronic Signatures and Infraestructures (ESI); Algorithms and parameters for secure electronic signature". Además se tendrá en cuenta los criterios que, al respecto, se hayan adoptado en el Esquema Nacional de Seguridad, desarrollado a partir del artículo 42 de la Ley 11/2007, por el Real Decreto 3/2010, de 6 de noviembre.

Se permite utilizar cualquiera de los siguientes algoritmos:

- Hash (Digestión), SHA-2withRSA (SHA224withRSA, SHA256withRSA, SHA384withRSA, SHA512withRSA)
- Cifrado, RSA

Para los entornos de alta seguridad, se tendrá en cuenta el criterio del Centro Criptológico Nacional, CCN, siendo de aplicación las recomendaciones revisadas de la CCN-STIC 405. Asimismo, se deberá atender a la recomendación CCN-STIC 807 ("Criptografía de Empleo en el ENS"), según lo establecido en el Esquema Nacional de Seguridad.

De forma general se puede utilizar cualquiera de los siguientes algoritmos para la firma electrónica:

- RSA/SHA224, RSA/SHA256, RSA/SHA384 y RSA/SHA512 recomendado para archivado de documentos electrónicos (very long term signatures).

Las longitudes de clave serán como mínimo de 2048 bits.

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 http://www.anf.es

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.

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.

2.8 Firmantes

Se contemplan las siguientes opciones:

- **Firmas simples**. Documentos de firma de un solo firmante.
- **Firma en línea**. Es la firma múltiple en la que todos los firmantes están al mismo nivel y en la que no importa el orden en el que se firma.
- **Contra-firma o firma en cascada**. Firma múltiple en la que el orden en el que se firma es importante. Cada firma debe refrendar o certificar la firma del firmante anterior.

3 Política de validación de firma electrónica

En este apartado se especifican las condiciones que se deberán considerar por parte del firmante, en el proceso de generación de firma electrónica, y por parte del tercero de confianza, en el proceso de validación de la firma.

3.1 Periodo de validez

La presente Política de Firma Electrónica es válida desde la fecha de expedición hasta la publicación de una nueva versión actualizada.

3.2 Reglas comunes

Estas reglas permiten establecer responsabilidades respecto a la firma electrónica sobre la persona o entidad que crea la firma electrónica, y la persona o entidad que la verifica, definiendo los requisitos mínimos que deben presentarse.

3.2.1 Reglas del firmante

Todo dispositivo de firma electrónica homologado por ANF AC, da al firmante la posibilidad de consultar el documento electrónico antes de procesar la aceptación del mismo, incluso le otorga la capacidad de reseñar menciones o salvedades que ampliarán o delimitarán lo expresado en el propio documento a firmar.

El firmante asume la responsabilidad de comprobar si el documento electrónico contiene contenido dinámico. Si el fichero que se quiere firmar no ha sido creado por el firmante, éste deberá comprobar su contenido previamente a introducir los datos de activación de firma (PIN), asumiendo que al firmarlo expresa además de su aceptación, el reconocimiento tácito de haberlo revisado previamente.

Salvo que el firmante tenga contratado a ANF AC el Servicio de Conservación de firmas electrónicas, es responsabilidad del firmante la conservación y custodia de la firma electrónica.

3.2.2 Reglas del tercero que confía

El tercero que confía es responsable de verificar la firma electrónica antes de proceder a su aceptación. Para realizar la correspondiente validación deberá utilizar un dispositivo de verificación homologado por ANF AC.

Además el tercero que confía, mediante sus propios recursos, comprobará la adecuación del tipo de certificado electrónico empleado por el firmante, así como las limitaciones de uso reseñadas en el "key usage", "Extended Key Usage", y las que puedan estar reseñadas en otras extensiones del propio certificado.

El tercero que confía, aceptando la firma electrónica, realiza una aceptación tácita de las limitaciones de responsabilidad que ANF AC acepta asumir según queda especificado en el cuerpo del propio certificado, y en su correspondiente Política de Certificación.

Salvo que el firmante tenga contratado a ANF AC el Servicio de Conservación de firmas electrónicas, es responsabilidad del firmante la conservación y custodia de la firma electrónica.

3.2.3 Reglas para los sellos de tiempo

El sello de tiempo asegura que los datos originales firmados se generaron antes de una determinada fecha, y determinan el instante en el que el firmante utilizó su certificado para elaborar la firma electrónica.

Los dispositivos de firma electrónica homologados por ANF AC, obtienen estampación de Sello de Tiempo Electrónico de las Unidades de Sellado de Tiempo (TSU). El formato del sello de tiempo electrónico emitido por los TSU de ANF AC cumplen las recomendaciones de IETF, RFC 5816, "Internet X.509 Public Key Infrastructure; Time-StampProtocol (TSP)", estando firmados electrónicamente por certificados electrónicos de ANF AC TSA.

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

1. Datos sobre la identidad de la autoridad emisora (ANF AC TSA).
2. Parámetros del secuenciador (valores hash "anterior", "actual" y "siguiente").
3. Número de transacción univoco.
4. Fecha y hora UTC.
5. La Unidad de Sellado de Tiempo (TSU) firma el TImeStamping con un certificado emitido por ANF TSA CA.

ANF AC dispone de un servicio de sellado de fecha y hora, conforme con la ETSI TS 102 023, según las especificaciones definidas en la DPC OID 1.3.6.1.4.1.18332.5.1 de ANF Autoridad de Sellado de Tiempo.

3.2.4 Reglas respuestas OCSP

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

Los Respondedores OCSP de ANF AC cumplen la norma de referencia IETC RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP. Las respuestas OCSP están fechadas y firmadas con certificados emitios por ANF AC.

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.

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.

3.2.5 Reglas de confianza para firmas longevas

Los estándares CAdES (ETSI TS 101 733), XAdES (ETSI TS 101 903) y PAdES (ETSI TS 101 733) contemplan la posibilidad de incorporar a las firmas electrónicas información adicional para garantizar la validez de una firma a largo plazo, una vez vencido el periodo de validez del certificado. El método para obtener firmas longevas es el descrito en las modalidades AdES XL y AdES A.

4 Conservación de las firmas electrónicas

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 tienen que ser conscientes que el proceso de verificación de una firma debe poder repetirse años después de su generación y con el paso del tiempo, los soportes magnéticos u ópticos pueden degradarse, y sin olvidar que la tecnología avanza inexorablemente: los componentes criptográficos: *claves y algoritmos que hoy son seguros, en un futuro se pueden considerar obsoletos, o incluso el formato de ficheros ha cambiado y no podremos acceder a la información sino hemos guardado las aplicaciones necesarias*.

Por todo ello, no es suficiente obtener una firma electrónica que reúna los requisitos para ser clasificada como firma electrónicas de larga vigencia, este documento debe de conservarse de forma adecuada, tanto desde el punto de vista de seguridad física almacenándolo en lugar seguro, sino que además se debe de tener en cuenta las características intrínsecas de este instrumento.

Seguridad técnica

La adecuada conservación de las firmas electrónicas de larga vigencia, requiere determinar en cada momento el estado de seguridad criptográfica de los componentes empleados en su creación y, caso de entrar en riesgo, se debe de realizar un re-timbrado de las firmas antes de que las claves y el material criptográfico asociado sean vulnerables.

En el caso de Firmas AdES, se recomienda seguir el formato AdES A.

El servicio de Conservación de firmas electrónicas de ANF AC, incluye un servicio de Re-Timbrado. Mediante este servicio de re-sellado se vuelven a sellar sellos previamente emitidos en cualquiera de sus modalidades. Los sellos son generados en formato binario siguiendo el estándar RFC 3161 "*Internet X.509 Public Key Infrastructure Time Stamp Protocols*", estándar definido por la Internet Engineering Task Force (IETF) para el protocolo Time Stamp.

Para el archivado y gestión de documentos electrónicos, el servicio de Conservación de firmas electrónicas sigue las recomendaciones de las guías técnicas de desarrollo del Esquema Nacional de Interoperabilidad así como lo indicado en el estándar de ETSI TS 101 533.

5 Gestión de la política de firma

Esta PFE detalla y completa lo estipulado en la "Declaración de Prácticas de Certificación" (DPC) de la PKI ANF AC.

El mantenimiento, actualización y publicación electrónica del presente documento corresponderá a la Junta Rectora de la PKI de ANF AC.

La presente Política de Firma Electrónica es válida desde la fecha de emisión hasta la publicación de una nueva versión.

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.

5.1 Procedimiento de Publicación

ANF AC publica la presente Política de Firma Electrónica en sus repositorios http://www.anf.es