Política de firma electrónica y sello electrónico

de

ANF Autoridad de Certificación

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

Web: www.anf.es

Índice

1 Introducción

ANF Autoridad de Certificación (ANF AC), es una entidad jurídica constituida al amparo de la Ley Orgánica 1/2002, de 22 de marzo. Inscrita en el Ministerio del Interior con el número nacional 171.443 y NIF G63287510.

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-)

Este documento es la política de firma electrónica de ANF AC. Esta política determina las condiciones generales y particulares aplicables a la firma electrónica para su creación validación y aumento.

ANF AC, administra este documento en conformidad con el Reglamento [UE] 910/2014 del Parlamento Europeo (eIDAS), y con la legislación nacional.

Esta política presenta una estructura normalizada de acuerdo con ETSI TS 119 172-1.

Esta Política de Firma Electrónica asume que el lector conoce los conceptos de PKI, certificados X-509 v3 firma electrónica y validación. En caso contrario se recomienda al lector que se forme en el conocimiento de los anteriores conceptos antes de hacer uso de los servicios a los que hace referencia este documento.

1.1 Descripción General

Respecto a la firma electrónica y el sello electrónico, avanzado o cualificado, de conformidad con el Reglamento eIDAS y con esta política, el resultado general de la aplicación de esta política no cambia, independientemente de si se trata de una firma / sello electrónico avanzado o cualificado, siempre que haya sido elaborado empleando un certificado cualificado de firma (QES), o un certificado cualificado de sello electrónico (QEseal).

Las funciones básicas de la firma electrónica *(definición, UIT-T X.509 | ISO / IEC 7488-2)* son:

- Identidad. Identifica al firmante de manera inequívoca.
- Integridad. Garantiza que el contenido del objeto datos firmado ha permanecido completo e inalterado, cualquier manipulación es detectada. *(UIT-T X.509 | ISO / IEC 9594-8)*
- No repudio. Asegura que el firmante no puede repudiar lo firmado.

La finalidad de esta política es garantizar el pleno consentimiento y libre voluntad del firmante, con ello se refuerza seguridad y eficacia jurídica de los actos firmados. Con ese objetivo, esta política establece determinados procedimientos, condiciones de generación y validación de firma.

Con carácter previo al acto de firma, el firmante debe de tener la posibilidad de comprobar los datos que va a firmar e, incluso, establecer unas condiciones generales y particulares aplicables a la firma electrónica. Esta política establece, entre otras medidas de seguridad, requisitos tipo WYSIWYS '*lo que ves es lo que firmas*' y contempla la inclusión, si es

voluntad del firmante, de una política de firma, uno o varios compromisos, menciones y salvedades en un campo firmado, dentro de la firma o implícitamente en el propio objeto de datos a firmar.

Si el campo correspondiente a la política de firma electrónica está ausente, y tampoco constan compromisos, menciones o salvedades, es decir, no se identifica ningún contexto aplicable a la firma, entonces se debe asumir que la firma ha sido generada sin ninguna restricción normativa, en consecuencia, 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 tanto, hará falta derivar el significado de la firma a partir del contexto, especialmente de la semántica del documento firmado.

1.2 Dominio comercial y aplicaciones

1.2.1 Alcance y límites de la política de firma electrónica

Está política se limita a la creación de firma electrónica / sello electrónico, aunque expresamente se establece la obligación del firmante y de los terceros que confían de validarla antes de depositar su confianza, así mismo se abordan determinados aspectos del aumento de firma *(conservación a largo plazo)*.

Este documento cubre los requerimientos y procedimientos para la elaboración de firmas electrónicas y sellos electrónicos que incluyen el sometimiento a esta política mediante la reseña del OID 1.3.6.1.4.1.18332.27.1.1.

Los requerimientos para el aumento de firmas, se detallan en la Política del servicio cualificado de conservación de firmas electrónicas cualificadas y del servicio cualificado de conservación de sellos electrónicos cualificados, OID 1.3.6.1.4.1.18332.61.

Los requerimientos para la validación de firmas, se detallan en la Política del servicio de validación cualificado de firmas electrónicas cualificadas y Sellos electrónicos cualificados, OID 1.3.6.1.4.1.18332.56.1.1

Estas políticas de creación, validación y conservación pueden ser aplicables a cualquier dominio de uso, p.ej. *B2B, B2C, Gov2B, Gov2C, legal/Justicia, financiero/Banca, medicina/Salud…etc*.

Las firmas electrónicas sometidas a esta política 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.

1.3 Identificación del documento

1.3.1 Nombre y versión del documento

Nombre del documento	Política de Firma Electrónica y Sello Electrónico

Versión	1.4
Estado de la política	APROBADO
Fecha de publicación	1 de diciembre de 2020
Fecha de aprobación	1 de diciembre de 2020
Publicada en	https://www.anf.es

La entrada en vigor de una nueva versión se produce en el momento de su publicación.

Versión	Cambios	Aprobación	Publicación
1.3	Correcciones técnicas	1/06/2016	1/06/2016
1.4	Correcciones técnicas	1/12/2020	1/12/2020

Revisión y aprobación		
Revisado por:	Departamento legal / Responsable de cumplimiento normativo	18 noviembre 2020
Aprobado por:	Junta Rectora de la PKI	18 noviembre 2020

1.3.2 Identificador del documento

Referencia del documento / OID	1.3.6.1.4.1.18332.27.1.1

No existen políticas subordinadas.

1.3.3 Reglas de conformidad

Esta política será revisada al menos una vez al año, y siempre que se produzcan cambios que asi lo requiera.

La versión de esta política solo será cambiada si se producen cambios sustanciales que afectan a su aplicabilidad.

1.3.4 Puntos de distribución

Esta política es publicada en la Web corporativa de ANF AC en versión de idioma español e inglés en las distintas versiones que han sido aprobadas, en caso de discrepancia, prevalece la versión de idioma español. Puede ser solicitada por correo electrónico o de forma presencial.

Web	http://www.anf.es
Correo electrónico	info@anf.es
Dirección	Paseo de la Castellana, 79 - Madrid – 28046 - España

Esta política está disponible en formato PDF *(firmado electrónicamente),* e impreso en papel.

1.4 Administración del documento

1.4.1 Organismo responsable de la administración del documento

El organismo encargado de revisar y aprobar en su caso esta política es la Junta Rectora de la PKI, maxima autoridad en la organización ANF AC.

Organismo	Junta Rectora de la PKI
Correo electrónico	juntapki@anf.es
Dirección	Paseo de la Castellana, 79 Localidad Madrid – 28046 - España
Teléfono contacto nacional	902 902 172 *(Llamadas desde España)*
Teléfono contacto Internac.	(+34) 933 935 946

1.4.2 Personas de contacto

Departamento Legal	Maricarmen Mateo	mcmateo@anf.es
Desarrollo de negocio	Alvaro Díaz	adiaz@anf.es
Tecnología y cumplimiento normativo	Pablo Díaz	pablo@anf.es
Delegado de protección de datos	Yohana Lema	yohana@anf.ac
Documentación y formación	Paula Jordan	paula.jordan@anf.es

1.4.3 Procedimiento de aprobación

La solicitud de revisión de la política de firma electrónica y sello electrónico la realiza la Dirección General de ANF AC a la Junta Rectora de la PKI. La solicitud expondrá las causas por las que se solicitan cambios o nuevas inclusiones de texto, e incluirá propuesta de nuevo texto.

La Junta Rectora de la PKI analiza la solicitud de revisión, valorando necesidad, adecuación y comprobando que los cambios estén en harmonía con la Declaración de Prácticas de Certificación (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1 de ANF AC y su adenda.

1.5 Definiciones y abreviaturas

1.5.1 Definiciones

Aceptación de la firma: verificación técnica a realizar sobre la propia firma o sobre los atributos de la firma.

Ancla de confianza: en sistemas criptográficos con estructura jerárquica, un ancla de confianza es una autoridad de certificación cuya confianza se asume y no es derivada. En la arquitectura X.509, un certificado raíz sería el ancla de confianza del que toda la cadena de confianza deriva.

Aplicación de firma/validación = suite de utilidades que permiten elaborar firmas electrónicas AdES y validación de firmas y sellos electrónicos (SVA)

Aplicación de validación de firmas: aplicación que valida una firma contra una política de validación de firmas, y que emite una indicación de estado (es decir, el estado de validación de la firma) y un informe de validación de la firma. La aplicación de validación de ANF AC está en conformidad con la ETSI TS 119 102-1.

Aumento de firma: proceso de incorporar determinada información a una firma con el objetivo de mantener la validez de esa firma a largo plazo.

> NOTA: El aumento de firmas es un proceso colateral a la validación de firmas, es decir, el proceso por el cual cierto material *(por ejemplo, sellos de tiempo, datos de validación e incluso material relacionado con archivos)* se incorpora a las firmas para hacerlos más resistentes al cambio o para aumentar su longevidad.

Cliente de validación de firmas: componente de software que implementa el protocolo de validación de firmas al usuario.

Dispositivo de creación de firma electrónica: un equipo o programa informático configurado que se utiliza para crear una firma electrónica.

Dispositivo cualificado de creación de firma electrónica: un dispositivo de cualificado (*QSCD*) que cumple los requisitos enumerados en el anexo II del Reglamento eiDAS.

Dispositivo cualificado de creación de sello electrónico: un dispositivo que cumple *mutatis mutandis* los requisitos enumerados en el anexo II del Reglamento eiDAS.

Dispositivo seguro de creación de firma electrónica: un dispositivo de seguro de firmas electrónicas (*SSCD*).

Estado de validación de la firma: una de las siguientes indicaciones: TOTAL-APROBADO, TOTAL-FALLO o INDETERMINADO.

Firma PDF en serie: el segundo (y subsiguientes) firmantes de un PDF no solo firman el documento sino también la firma del firmante anterior y cualquier modificación que también pueda haber tenido lugar *(por ejemplo, al completar formulario)*.

Informe de validación de firmas: informe completo de validación elaborado por la aplicación de validación de firmas. Permite inspeccionar los detalles de las valoraciones tomadas durante la validación e investigar las indicaciones de estado detalladas por la aplicación de validación. El informe elaborado por el servicio de validación de ANF AC cumple los requisitos establecidos por la ETSI TS 119102-1.y el informe se elabora conforme a la ETSI TS 119102-2

PoE de firma: la prueba de existencia de firma, es el objeto de datos de firma el cual es reseñado en el informe de validación.

Política de validación de firmas: conjunto de restricciones de validación de firmas que son procesadas por la aplicación de validación que determinan el resultado de la validación (APROBADO,FALLO o INDETERMINADO).

Prestador de servicios de validación cualificado: SVSP que proporciona un servicio de validación cualificado para sellos electrónicos cualificados y/o servicio de validación cualificado para firmas electrónicas cualificadas. A efectos de esta Política el prestador es ANF AC.

Prueba de existencia: evidencia que prueba que un objeto existió en una fecha / hora específica.

Reglamento eIDAS: Reglamento (UE) 910/2014, 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior. (eIDAS)

Reglas de aplicabilidad de firmas: conjunto de reglas, aplicables a una o más firmas electrónicas, que define los requisitos para determinar si una firma es adecuada para un negocio o un propósito legal en particular.

- El propietario de las reglas de aplicabilidad de la firma suele ser la parte que confía y estas reglas pueden ser compartidas por una comunidad. Las reglas de aplicabilidad de firmas pueden manejarse mediante una extensión del servicio proporcionado por el QSVSP que ofrecerá verificación de aplicabilidad.

Restricción de creación (firma): criterios utilizados al crear una firma digital.

Restricción de validación de firmas: criterios técnicos con los que se puede validar una firma electrónica. El servicio de validación de ANF AC sigue las especificaciones de la ETSI TS 119102-1

Ruta de certificación: lista ordenada de uno o más certificados de clave pública, comenzando con un certificado de CA raiz *(autofirmado)* y termina con el certificado de clave pública que se va a validar. Definido en ITU-T X.509 | ISO/IEC 9594-8.

Servicio de validación: sistema accesible a través de una red de comunicación, que valida una firma electrónica.

Servicio de validación cualificado para sellos electrónicos cualificados: según se especifica en el Reglamento (UE) nº 910/2014, articulo 40. A efectos de esta Política el servicio es el proporcionado por ANF AC.

Servicio de validación cualificado para firmas electrónicas cualificadas: según se especifica en el Reglamento (UE) nº 910/2014], articulo 33. A efectos de esta Política el servicio es el proporcionado por ANF AC.

Servidor de servicio de validación de firmas: equipamiento informático que implementa el protocolo de validación de firmas y procesa la validación de firma / sello electrónico.

Suscriptor: Corresponde al cliente, persona física o jurídica, que contrata el servicio de validación y somete a validación firmas y/o sellos electrónicos.

Tipo de compromiso (firma): indicación seleccionada por el firmante que establece la implicación exacta de una firma.

Usuario: Aplicación o ser humano que interactúa con un cliente de validación de firmas.

Validación de firma: proceso de verificación y confirmación de que una firma electrónica es válida.

Validación de firma: proceso de verificación y confirmación de que una firma digital es técnicamente válida.

Validación de la firma electrónica cualificada: según se especifica en el artículo 32 del Reglamento (UE) nº 910/2014.

Validación de sello electrónico cualificado: según se especifica en el artículo 40 del Reglamento (UE) nº 910/2014.

Verificación de aplicabilidad: parámetros de verificación para determinar si una firma se ajusta a las reglas de aplicabilidad de la firma se puede proporcionar como complemento del servicio de validación de firmas definido ETSI TS 119 441. Tiene un mayor alcance que la validación especificada en la citada ETSI TS-

Verificación de firma: proceso de verificación del valor criptográfico de una firma utilizando datos de verificación de firma.

Verificador: entidad que quiere validar o verificar una firma electrónica.

1.5.2 Abreviaturas

ANF AC:	ANF Autoridad de Certificación **.**
AV:	Autoridad de Validación.
AC / CA:	Autoridad de Certificación.
BSP:	Parámetros de alcance empresarial.
CRL:	Lista de certificados de revocación.
DA:	Aplicación de firma que incluye interface para usuario final.
DTBS:	Datos a firmar.
OCSP:	protocolo de comprobación del Estado de un certificado en línea.
OID:	Identificador de Objeto.
PCSC:	Prestador Cualificado de Servicios de Confianza.
PoE:	prueba de existencia.
QES:	Certificado cualificado de firma electrónica.
QEseal:	Certificado cualificado de sello electrónico.
QSCD:	Dispositivo cualificado de firma electrónica.
QSVS:	Servicio Cualificado de Validación de firmas / sellos.
QSVSP:	Prestador Cualificado de Servicios de Validación de firmas / sellos.
QTSP:	Prestador Cualificado de Servicios de Confianza.
LoA:	Nivel de garantía.

SCA:	Aplicación de creación de firmas.
SD:	Documento del firmante.
SDO:	Objeto de datos firmado.
SSCD / **HSM**:	Módulo de Seguridad Criptográfica certificado Common Criteria ISO 15408 EAL 4+ o FIPS PUB 140-2 nivel 3.
SVA :	Aplicación de validación de firmas y sellos electrónicos.
SVP:	Protocolo de validación de firmas.
SVR:	Informe de validación de firmas.
SVS:	Servicio de validación de firmas.
SVSServ:	Servidor del servicio de validación de firma.
TA:	Ancla de confianza.
TSA:	Autoridad de Sellado de Tiempo.
TSP:	Prestador de Servicios de Confianza.
TSU:	Unidad de sellado de tiempo.
VPR:	Proceso de validación de firmas.
WYSIWYS:	'Lo que ves es lo que firmas'.
XMP:	eXtensible Metadata Platform.

2 Declaración de prácticas de seguridad de las aplicaciones

Las aplicaciones de firma de ANF AC, han sido diseñadas y desarrolladas de acuerdo con los requisitos establecidos en este documento:

- Safe Box ®. Aplicación con extensión shell de usuario final de firma electrónica y validación.
- Critical Access ®. Suite de aplicaciones de escritorio que incluye firma electrónica y validación.
- BlackBoxSign ®. Servidor de firma y validación.
- Sign to Sign ®. Workflow de firma y validación.
- Legal Snap Scan ®. Servicio de digitalización certificada.
- Servidor de firma a distancia para certificados centralizados.

Creación de firmas electrónicas / sellos electrónicos

Las aplicaciones de firma electrónica, creación de firma electrónica y dispositivos de creación de firma electrónica tienen que utilizar certificados cualificados de firma electrónica o sello electrónico vigentes, para crear firmas electrónicas avanzadas (AdES) o cualificadas (QAdES), en conformidad con el Reglamento eIDAS,

> Artículo 26. Avanzadas, deben de cumplir los requisitos siguientes:
>
> a) estar vinculada al firmante de manera única;
> b) permitir la identificación del firmante;
> c) haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, y
> d) estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.
>
> Artículo 3. Cualificadas:
>
> Una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas (QSCD -*Qualified Signature Creation Device*-) y que se basa en un certificado cualificado de firma electrónica.

De acuerdo con el contexto de firma, se tendrán en cuenta las siguientes restricciones:

- *ConstraintsOnCertificateMetadata:*
  Este conjunto de restricciones indica requisitos sobre certificados específicos. La semántica se define como sigue:
  - *LegalPersonSignerRequired*: El sujeto identificado en el certificado del firmante tiene que ser una persona jurídica, expresado como *boolean*.
  - *LegalPersonSignerAllowed*: El sujeto identificado en el certificado del firmante puede ser una persona jurídica, expresado como *boolean*.

Y, se asume el conjunto de restricciones ETSI TS 119 172-1 Anexo C, cuya semántica se aplica en el ámbito de la legislación UE, concretamente:

- *EUQualifiedCertificateRequired*: esta restricción indica que el certificado del firmante debe ser un certificado cualificado de firma electrónica / sello electrónico, según se define en la legislación de la UE aplicable; expresado como un *boolean*.
- *EUQualifiedCertificateSigRequired*: esta restricción indica que el certificado del firmante requiere que la firma se elabore en conformidad con las normas ETSI en la materia; expresado como un *boolean*.
- *EUQualifiedCertificateSealRequired*: esta restricción indica que el certificado del firmante debe ser un certificado cualificado de sello electrónico, según se define en la legislación de la UE aplicable; expresado como un *boolean*.
- *EUSSCDRequired*: esta restricción indica que la clave privada correspondiente a la clave pública del certificado del firmante, debe residir en un dispositivo seguro de creación de firmas; expresado como un *boolean*.
- *EUAdESigRequired*: esta restricción indica que la firma debe ser una firma electrónica avanzada tal como se define en la legislación de la UE aplicable; expresado como un *boolean*.
- *EUAdESealRequired*: esta restricción indica que la firma debe ser un sello electrónico avanzado como se define en las normas ETSI de referencia; expresado como un *boolean*.
- *EUQSigCDRequired*: esta restricción indica que la clave privada correspondiente a la clave pública del certificado del firmante, debe residir en un dispositivo cualificado de creación de firmas (*certificado como QSCD*); expresado como un *boolean*.
- EUQSealCDRequired: esta restricción indica que la clave privada correspondiente a la clave pública del certificado del firmante, debe residir en un dispositivo cualificado de creación de sellos (*certificado como QSealCD publicado en conformidad con el Art. 39 3) Reglamento eIDAS*); expresado como un *boolean*.

Los certificados pueden estar almacenados en un software criptográfico, o en un dispositivo QSCD físico, o en un servicio centralizado de firma a distancia, en cuyo caso debe de cumplir con los siguientes requisitos:

- caso de que el firmante haya confiado a un tercero los dispositivos cualificados de creación de firmas electrónicas, el tercero deberá ser un prestador cualificado de servicios de confianza de acuerdo con lo establecido en el Reglamento eIDAS Anexo II 3),
- el certificado empleado tiene que haber sido emitido con la calificación de cualificado, y haberse generado en un dispositivo cualificado de creación de firma electrónica, y
- el dispositivo tiene que emplear los procedimientos y mecanismos adecuados para garantizar que el firmante tiene el control exclusivo del uso de sus datos de creación de la firma electrónica, y que la utilización del dispositivo cumple los requisitos de la firma electrónica cualificada.

En cualquiera de los supuestos los dispositivos de creación de firma electrónica / sello electrónico deben emplear componentes cuya seguridad criptográfica se encuentra en conformidad con la ETSI TS 119 312.

Tal y como establece el Art. 29 del Reglamento eIDAS, se presumirá el cumplimiento de los requisitos para ser considerado dispositivo cualificado de creación de firma (QSCD), cuando exista una certificación expedida por organismo europeo *(Art. 30)*. Por tanto, el dispositivo de creación de firma para ser calificado como QSCD debe de constar en la lista de dispositivos cualificados que han sido notificados a la Comisión Europea por parte de los Estados miembros en virtud del artículo 31 del Reglamento (UE) 910/2014, publicada en,

https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds

Un dispositivo cualificado de creación de sello electrónico es aquel que cumple, mutatis mutandis, los requisitos indicados en el anexo II del Reglamento (UE) 910/2014.

Las aplicaciones de firma determinarán si la generación y la gestión de los datos de creación de firma correspondientes al certificado empleado para firmar es un dispositivo QSCD, verificando si en la extensión QcStatement, incluye el valor QSCD.

Conservación electrónica a largo plazo de firmas y sellos electrónicos

Con el fin de garantizar la conservación de firmas y sellos electrónicos a largo plazo, se recomienda utilizar un servicio cualificado de conservación electrónica a largo plazo con capacidad para aumentar la seguridad criptográfica.

Cualquiera de las partes puede delegar las responsabilidad de aumento de la firma, en el servicio cualificado de conservación de firma y sellos electrónicos cualificados de ANF AC OID 1.3.6.1.4.1.18332.61

Validación de la firma y sellos electrónicos

Para realizar la validación de la firma electrónica / sello electrónico, se debe de utilizar un servicio de validación cualificada de firmas y sellos electrónicos cualificados que esté registrado en la TSL de la UE.

Cualquiera de las partes puede delegar las responsabilidad de validación de firma, en el servicio cualificado de validación de firma y sellos electrónicos cualificados de ANF AC OID 1.3.6.1.4.1.18332.56.1.1.

2.1 Requisitos de control

2.1.1 Datos personales

Según lo definido en la Declaración de Prácticas de Certificación (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

2.1.2 Firmas electrónicas

Las aplicaciones de firma, aplicaciones de creación de firma, servicios de firma electrónica y, los implementadores de firmas electrónicas sometidas a esta política, tendrán en cuenta, siempre que sea posible, que las firmas satisfagan los requisitos legales que pueden ser exigibles según el tipo de negocio en el que intervienen. Para ello deben de asegurarse la calidad de las firmas controlando los siguientes elementos:

a) Dispositivos de firme empleados.
b) Certificados que han sido utilizados.
c) Calificación de los instrumentos a) y b).
d) Suite criptográfica de firma.
e) Longevidad deseada de las firmas electrónicas.
f) Características de protección deseadas (nivel de las firmas).
g) Calificación de los atributos obtenidos de terceros, en relación con el punto f).

h) Validación cualificada previo a depositar su confianza.

2.1.3 Continuidad del negocio

Según lo definido en la Declaración de Prácticas de Certificación (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

2.2 Seguridad de la información

2.2.1 Política de seguridad

Según lo definido en la Declaración de Prácticas de Certificación (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

2.2.2 Protección de la red

Según lo definido en la Declaración de Prácticas de Certificación (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

2.2.3 Protección de los sistemas de información

Según lo definido en la Declaración de Prácticas de Certificación (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

2.2.4 Integridad del software y de las aplicaciones

Según lo definido en la Declaración de Prácticas de Certificación (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

2.2.5 Seguridad de las trazas de auditoría

Según lo definido en la Declaración de Prácticas de Certificación (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

2.3 Requisitos de los procesos de creación y validación de firmas

2.3.1 Procesos y sistemas de creación de firmas

a) Gestión del tipo de contenido de datos. La aplicación de firma *(DA)* debe de incluir un control del tipo de objeto de datos a firmar, comprobando:
   i. adecuación del formato de firma seleccionado con el formato del documento a firmar, y
   ii. apercibir al firmante *(o impedir)* caso de que el formato del documento a firmar pueda incluir macros o enlaces que puedan mostrar al ojo humano objetos que en realidad no se firman.

b) Visor de atributos de firma.
   La firma mostrará al usuario los atributos que serán incluidos en la firma.

c) El sistema de creación de firma gestiona un proceso de control de tiempo y secuencia.

d) Incluye invocación explícita de firma.

e) Incluye selección de nivel de longevidad de la firma.

f) Incluye procedimiento de autenticación y control de acceso al sistema de firma.

g) Preparación del objeto de datos a firmar (DTBS).

El firmante selecciona el DTBS y la aplicación determina el formato, origen y garantiza la integridad, en el caso de que el firmante genere al hash del documento la aplicación registra que el hash ha sido elaborado por el firmante.

h) Representación DTBS.

El firmante debe tener la capacidad de poder acceder y visualizar el DTBS antes de elaborar la firma, en el caso de que el DTBS no sea accesible a ojo humano, *p.ej. un exe*, se apercibe al firmante.

i) Gestión de dispositivos de creación de firma.

De acuerdo con lo descrito en el apartado 2 de este documento.

j) Protección de la comunicación entre el dispositivo de creación de firma y el SCA.

La comunicación entre ambos sistemas tiene que estar protegida;

k) Seguridad de la suite criptográfica.

Los sistemas deben de emplear recursos criptográficos que estén en conformidad con la ETSI TS 119 312.

l) El proceso y los sistemas de creación de firma debe de tener la capacidad de adaptarse al uso de la comunidad. Para ello, pueden ofrecer la posibilidad de incluir:

- *compromisos*

  Que determinen el alcance de la firma y restricciones *(ver apartado 3.2.2)*.

- *Restricciones de la comunidad objetivo*

  Este conjunto de restricciones identifica la comunidad a la que cada documento y su (s) firma (s) está (n) dirigida e indica los requisitos en esa comunidad.

  P.ej. Estas reglas pueden establecer las condiciones en las que se puede confiar en una determinada firma, o incluir disposiciones relativas a la eficacia prevista de firmas, donde se requieren varias firmas.

m) Los dispositivos de creación de firma en caso de incluir operación de firma masiva, deben de incluir procesos y sistemas que garanticen los requerimientos de seguridad indicados en este apartado:

- *BulkSigningRelevance:*

  Esta restricción indica el requisito de referenciar datos firmados mediante mecanismos automatizados, en especial para firmas masivas. O bien, por el contrario, su prohibición. Los valores utilizados para expresar dichos requisitos son:

  - mandatedBulkSigning
  - prohibidoBulkSigning

- *ConstraintsOnTheNumberOfDOTBS*:

  Esta restricción indica el requisito de referenciar el número de objetos de datos que una firma puede firmar. La semántica para expresar un posible conjunto de valores se define de la siguiente manera

  minValue {<, ≤ , =} x {=, ≥, >} maxValue

2.3.2 Procesos y sistemas de validación de firmas,

Se debe de utilizar el proceso y sistema de validación de firmas y sellos electrónicos, definido en la Política de Validación de ANF AC OID 1.3.6.1.4.1.18332.56.1.1. que, entre otras cuestiones, garantice:

a) se aplican reglas de validación
b) el usuario dispone de un interface de validación;
c) se comprueba que el formato de firma es apropiado;
d) se verifica la vida útil de la firma;
e) se indica conformidad relativa a la entrada / salida de validación.

2.4 Requisitos de desarrollo y codificación

Se deben de disponer de una política que establezca requerimientos de desarrollo y codificación, en particular con:

1) Seguridad de los métodos de desarrollo del software,
   Según lo definido en la Declaración de Prácticas de Certificación (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1. y su adenda, en particular lo definido en la Política de Ciclo de Vida del Software y Hardware OID: 1.3.6.1.4.1.18332.57.1.1
2) Comprobación de cumplimiento normativo e interoperabilidad,
   Según lo definido en la Declaración de Prácticas de Certificación (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1. y su adenda.

2.5 Requerimientos generales

Se deben de disponer de medidas de control en relación con:

1) Interface de usuario,
   Según lo definido en la Declaración de Prácticas de Certificación (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1. y su adenda, en particular lo definido en la Política de Ciclo de Vida del Software y Hardware OID: 1.3.6.1.4.1.18332.57.1.1
2) Intervención con otros proveedores de servicios de confianza,
   Según lo definido en la Declaración de Prácticas de Certificación (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1. y su adenda.
3) Medidas generales de seguridad,
   Según lo definido en la Declaración de Prácticas de Certificación (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1. y su adenda.

3 Parámetros de alcance empresarial

Este apartado cubre las reglas o requisitos establecidos por esta política en función de los parámetros de alcance empresarial (BSP) que son:

- parámetros relacionados principalmente con la aplicación y / o el proceso comercial para los cuales la implementación de la (s) firma (s) son requeridos;
- parámetros influenciados principalmente por disposiciones legales asociadas a la aplicación y / o contexto empresarial;
- parámetros relacionados con los actores involucrados en la creación / validación de firmas; y
- otros parámetros de firma.

3.1 Relacionados con los procesos de la aplicación de firma

Las aplicaciones de firma de ANF AC, han sido diseñadas y desarrolladas de acuerdo con los requisitos establecidos en este documento:

- Safe Box ®. Aplicación con extensión shell de usuario final de firma electrónica y validación.
- Critical Access ®. Suite de aplicaciones de escritorio que incluye firma electrónica y validación.
- BlackBoxSign ®. Servidor de firma y validación.
- Sign to Sign ®. Workflow de firma y validación.
- Legal Snap Scan ®. Servicio de digitalización certificada.
- Servidor de firma a distancia para certificados centralizados.

Los tokens y almacenes de firma que se utilizan en el proceso de creación de una firma / sello electrónico aceptados por esta política son:

- Todo dispositivo calificado con certificación QSCD.
- Todo dispositivo HSM (certificado Common Criteria ISO 15408 nivel EAL 4+ o superior).
- Token USB Plug and Sign® de ANF AC.
- Software criptográfico en conformidad con el estándar PKCS#12.
- Store de certificados de Windows / Mozilla / Linux.

3.1.1 Flujo de trabajo *(secuenciación y tiempo)* de firmas

Esta política de firma aborda un conjunto de firmas.

3.1.2 Datos a firmar

Las aplicaciones de firma deben de tener la capacidad de gestionar los siguientes requerimientos:

- Conjunto de restricciones que establece que propiedades deben ser o no ser firmadas (*ContentRelatedConstraintsAsPartOfSignatureElements)*:

- *MandatedSignedQProperties-DataObjetFormat*
  Requiere un formato específico para el contenido que firma el firmante.
- *MandatedSignedQProperties-content-hints*
  Requerimientos específicos de información que es encapsulado en el objeto de datos, siendo el conjunto firmado. P.ej. *XMP para digitalización certificada de facturas*.
- *MandatedSignedQProperties-content-reference*
  Para requerir la incorporación de información, de forma tal que vincula la solicitud y respuesta del mensaje en un intercambio entre dos partes, u otras formas de enlaces. P.ej. *entrega certificada.*
- *MandatedSignedQProperties-content-identifier*
  Para requerir la presencia de un valor específico de un identificador que puede ser utilizado como atributo de calificación firmada "content-reference". P.ej. *QSCD en la firma de contratos de trabajo.*

- Esta restricción indica si todos los datos o solo una parte de ellos tiene que ser firmado (*DOTBSAsAWholeOrInParts*). Se define de la siguiente manera:
  - entero : todos los datos deben estar firmados;
  - partes : sólo se deben firmar determinadas partes de los datos. En este supuesto se debe utilizar información adicional para expresar qué partes tienen para ser firmadas.

3.1.3 Relación de los datos firmados y la firma

Aplicaciones de firma que obtienen el hash de los objetos de los datos a firmar e identifican todos los aspectos relevantes de los objetos de datos que se van a firmar. Estos aspectos incluyen:

1) La naturaleza y el formato de los datos que se van a firmar *(por ejemplo, binarios, datos estructurados, XML, documento PDF, documentos como Word u ODF, paquetes multimedia, imágenes, etc.)*. El formato de firma debe de ser el adecuado al formato del objeto de datos a firmar. Además, se deben de tener en cuenta otros aspectos cruciales, por ejemplo, es la amenaza de existencia de agentes de corrupción (*cualquier código que cambie la visualización del objeto de datos a firmar: una página PHP u un macro en un word*), o bien objetos de datos que son imposibles de visualizar, p.ej. *un ejecutable *.exe*
   En estos casos es conveniente apercibir al firmante del riesgo inherente que conllevan estos objetos.
2) Las aplicaciones de firma utilizarán por defecto el formato natural de firma según la sintaxis del objeto de datos. En concreto.
   a. Sintaxis XML, se utiliza formato XAdES.
   b. Sintaxis PDF, se utiliza formato PAdES.
   c. Objetos de datos binarios, se utiliza formato CAdES.

   No obstante, en determinadas circunstancias, podría ser justificado la selección de un formato de firma no considerado inicialmente como "la opción natural ".

3.1.3.1 Formato de firma y niveles a utilizar

Los formatos de firmas electrónicas / sellos electrónicos admitidos son:

- ETSI EN 319 132 "*XAdES Advanced Electronic Signature Profiles*".
- ETSI EN 319 122 "*CAdES Advanced Electronic Signature Profiles*".

- ETSI EN 319 142 "*PAdES Advanced Electronic Signature Profiles*".

Los niveles admitidos conforme al perfil base BASELINE son:

- XAdES - B – T - LT y LTA
- CAdES – B – T - LT y LTA
- PAdES – B – T - LT y LTA

3.1.3.1 Ubicación relativa de firmas y objetos de datos firmados

Se pueden distinguir tres ubicaciones relativas de firmas y objetos de datos firmados:

- Envolventes. La firma contiene el documento firmado,
  - En el caso de CAdES se denominan firmas *implícitas*, y
  - en XAdES son firmas *enveloping*.
- Envueltas. La firma incluida dentro del documento firmado, *enveloped*. Pueden ser PAdES o XAdES.

  Respecto a firmas CAdES, aunque se pueden incrustar dentro de objetos cuya estructura esté definida en ASN.1 (*siempre que esta estructura defina campos para incrustarlos*), o dentro de mensajes S/MIME, ni las especificaciones CMS ni CAdES definen un mecanismo para hacer referencia explícita a objetos de datos firmados que son externos a la firma.
- Separadas. La firma está separada del documento firmado.
  - En el caso de CAdES se denominan firmas *explícitas*, y
  - en XAdES son firmas *detached*.

Esta política sólo admite:

- XAdES. En cualquiera de las modalidades:
  - *enveloped*

    Las firmas XAdES se pueden incrustar en los documentos XML.
  - *Enveloping*

    XAdES también pueden envolver el objeto de datos firmado. Cuando este es un objeto binario, previamente se codifica a base64, y se encapsula dentro de un elemento *ds: Object* .
- CAdES. En la modalidad: *implícita*.

  Las firmas CAdES, ya que se basan en firmas CMS, pueden envolver el objeto de datos firmado, encapsulando en el campo *encapContentInfo 's eContent*.
- PAdES. En la modalidad: *enveloped*.

  Las firmas serán PAdES NoXML que, por su propia naturaleza centrada en el documento, están integradas dentro del documento PDF que firman.

3.1.3.2 Múltiples posiciones relativas simultáneas

En algunos escenarios de uso es necesario procesos de alta complejidad.

- *XAdES*: Debido al mecanismo de referencia heredado de XML Signature, una firma XAdES puede, al mismo tiempo, envolver uno de los objetos de datos que firma, y ser envuelto por otro objeto de datos que firma, y separarse de otro objeto de datos que firma.
- *PAdES-XML-EMB*: está modalidad de PAdES sí que puede estar al mismo tiempo, envueltas dentro de un documento firmado XML y separada de otro objeto de datos firmado.

3.1.3.3 Número de firmas y objetos de datos firmados

Opciones posibles:

a. *firmas paralelas* (*o independientes*) (*es decir, firmas aplicadas exactamente a los mismos datos*);
b. *firmas en serie* (*es decir, firmas aplicadas a diferentes datos y serializadas*). El objeto de datos puede ser un formulario que será cumplimentado previamente por cada firmante;
c. *contra-firmas* (*es decir, firmas aplicadas sucesivamente al conjunto de firmas anteriores, y opcionalmente a los mismos datos originales*); o
d. *Secuencial / jerárquica* (*es decir, el suscriptor del servicio establece un determinado orden de firma por el cual, el firmante 2 no puede firmar hasta que ha firmado el firmante 1*). En este escenario la firma puede ser en serie, contra-firma o combinación de ambos.
e. Unidad de acto (*es decir, varios firmantes en el mismo acto –momento en el tiempo- deben de firmar p.je. modalidad de autenticación dual*).

Múltiples firmas y objetos de datos. Formatos de firma admitidos: CAdES, XAdES y PAdES

i. *Documento firmado por una sola firma*: los tres formatos permiten esta situación.
ii. *Documento firmado por más de una firma*. Según formato se deben de tener en cuenta las siguientes consideraciones:

Contra-firmas

- Las firmas PAdES, CAdES y XAdES permiten la contra-firma. En todos los casos, las contra-firmas pueden ser a su vezFirmas PAdES, CAdES o XAdES respectivamente.

Firmas en serie y en paralelo

- PAdES
  - Firmas en serie. PAdES-NoXML firma cualquier otra firma PAdES-NoXML que ya esté presente en el documento cuando se crea: son siempre firmas en serie;
  - Firmas paralelas. PAdES-NoXML no permiten la generación de firmas paralelas;
  - Firmas PAdES XML permiten combinación de firmas en serie y en paralelo
- XAdES
  - Es capaz de gestionar cualquier número de firmas que firman un documento XML (*total o parcialmente*), con cualquier combinación de firmas en serie y en paralelo, y sin ninguna restricción sobre la ubicación relativa de las firmas y el objeto de datos firmado.
- CAdES
  - Firmas paralelas: pueden incorporar firmas como un atributo sin firmar, que permite una secuencia de contrafirmas en una de las firmas paralelas. Se debe de tener en cuenta que CAdES carece mecanismos para hacer referencia explícita a objetos de

datos firmados y, en consecuencia, las aplicaciones deben configurarse para gestionar adecuadamente cada combinación específica.

iii. Una firma requiere firmar más de un objeto de datos

- PAdES
  - PAdES-NoXML solo firman un contenedor PDF. Todo lo que hay dentro del contenedor PDF está firmado, pero nada más.
  - PAdES-XML al ser firmas XAdES, puede firmar más de un objeto de datos dentro del contenido XML del contenedor PDF.
  - PAdES-XML-EMB puede firmar objetos de datos que están fuera del contenedor PDF.
- CAdES
  - No pueden, por sí solas, firmar más de un objeto de datos.
- XAdES
  - Incorpora mecanismos nativos para firmar más de un objeto de datos.

3.1.3.4 Sellos de tiempo electrónico

ETSI EN 319102-1 denomina firmas con tiempo las que resultan de incorporar un token de sello de tiempo en la firma básica.

Las firmas PAdES, CAdES y XAdES proporcionan contenedores que permiten incluir dentro de una firma electrónica token de sello de tiempo. Modalidades posibles:

1) Incluir uno o más token (s) de sello de tiempo en los objetos de datos a firmar, antes de que la firma realmente se genere. Este procedimiento permite demostrar que ciertos objetos de datos se han generado antes de un determinado instante de tiempo.
2) Incluir dentro de una firma una marca de tiempo realizada por el firmante. Esta marca de tiempo no merece, en términos generales, la misma confianza que un sello de tiempo electrónico generado por un proveedor de servicios de sello de tiempo. Las aplicaciones de ANF AC, salvo Legal Snap Scan ® *(servicio digitalización de facturas en Metadatos XMP normativa fiscal en la materia)*, no permite la inclusión de marca de tiempo.
3) Incluir dentro de una firma electrónica uno o más tokens de sello de tiempo. Cada sello de tiempo prueba que la firma se generó antes de la hora indicada dentro del token de tiempo. Esta modalidad está fuertemente relacionada con la longevidad de las firmas electrónicas*.

Un token de sello de tiempo tiene un período de validez limitado, para proteger el propio token de sello de tiempo de firma puede ser necesario el uso de otro token de marca de tiempo que proteja al primero, lo que a su vez aumenta la longevidad de la firma *(ver punto 3.1.3.7 de este documento).*

* *La longevidad de una firma es el período de tiempo durante el cual se asegura la capacidad de reevaluar su validez técnica. De hecho, la primera medida dentro de los formatos de firma electrónica ETSI para permitir que la validez técnica de una firma pueda ser reevaluada durante un período de tiempo que va más allá del vencimiento o la revocación de cualquiera de los certificados dentro de la ruta de certificación del certificado del firmante, y más allá de la ruptura de cualquiera de los algoritmos (incluidos los algoritmos de resumen) utilizados para su generación, es la incorporación de un token de sello de tiempo en la firma antes de que ocurra cualquiera de los eventos antes mencionados.*

3.1.3.5 Incluir material de validación a largo plazo

ETSI EN 319102-1 denomina firmas con material de validación a largo plazo, aquellas resultantes de incorporar elementos de validación a firmas con sello de tiempo *(AdES Nivel LT).*

XAdES y CAdES nivel LT, especifican contenedores para referencias a datos de validación. Las firmas PAdES no incorporan este tipo de referencias, ya que este formato pretende ser un paquete autónomo en términos de validar una firma a largo plazo.

PAdES LT permite incorporar material de validación dentro del objeto PDF del diccionario DSS y opcionalmente dentro de los objetos del diccionario VRI (ETSI EN 319 142-2)

Los formatos ETSI permiten aumentar la firma incorporando las siguientes referencias:

- la secuencia de referencias al conjunto completo de certificados de CA utilizados para validar la firma digital hasta *(pero no incluyendo)* el certificado del firmante;
- la secuencia de referencias al conjunto completo de datos de revocación utilizados en la validación del firmante y certificados CA;
- las referencias al conjunto completo de certificados necesarios para verificar cualquier token de sello de tiempo incorporado en la firma en el momento en que se incorpora el atributo / propiedad sin firmar que encapsula estas referencias;
- las referencias al conjunto completo de datos de revocación necesarios para verificar cualquier token de sello de tiempo incorporado a la firma en el momento en que se incorpora el atributo / propiedad sin firmar que encapsula estas referencias;
- las referencias al conjunto completo de certificados utilizados para validar los certificados de atributo o afirmaciones firmadas, si está presente;
- las referencias al conjunto completo de datos de revocación utilizados en la validación de los certificados de atributo o afirmaciones firmadas, si está presente.

La mayoría de los sistemas PKI utilizan dos procedimientos para gestionar los datos de revocación: las CRL y las respuestas de servidores de estado de certificados en línea, obtenidos a través de protocolos diseñados para estos fines, como el protocolo OCSP.

Esta política de firma requiere que las respuestas OCSP deben de estar firmadas por la CA que emitió el certificado, y la verificación debe de tener un alcance completo de la ruta conforme a RFC 6960.

3.1.3.6 Incluir material para aumentar los datos de validación a largo plazo

Una firma electrónica requiere se pueda reevaluar durante un período de tiempo que va mucho más allá de su vencimiento o revocación e, incluso, de la falta de disponibilidad de los servicios de información de estado (CRL / OCSP). Además, la firma debe protegerse en caso de que se produzca una posible violación de algunos de los algoritmos criptográficos utilizados mediante algoritmos más fuertes.

ETSI EN 319102-1 para este nivel de firmas AdES LTA, requiere incorporar un token cualificado de sello de tiempo que cubre el contenido de la firma con datos de validación a largo plazo.

Las firmas CAdES, XAdES y PAdES proporcionan medios para proteger incluso firmas aumentadas y, en consecuencia, para aumentar su longevidad. Requisitos:

1) Incorporar cualquier material de validación faltante a la firma, incluido el material de validación del token de sello de tiempo previamente incorporado.
2) Proteger todo el material necesario para validar la firma *(incluidos los objetos de datos firmados, incluso si se separan de la firma y del material de validación)* generando un nuevo token de sello de tiempo utilizando un algoritmo de resumen más fuerte si es necesario. Este token de sello de tiempo en realidad proporciona una prueba de la existencia del sello de tiempo y al mismo tiempo protege su integridad.
3) Incorpora el nuevo token de sello de tiempo a la firma encapsulada en un contenedor adecuado.

Este tipo de tokens de sello de tiempo se conoce como tokens de sello de tiempo para la disponibilidad a largo plazo y la integridad de la validación material.

3.1.3.7 Indicación de compromiso/s asumido/s por el firmante

Las firmas CAdES, PAdES y XAdES proporcionan mecanismos para indicar el compromiso asumido por el firmante. Detalle de compromisos normalizados en el apartado 3.2.2 de este documento.

3.1.3.8 Proteger la indicación de la identidad del firmante

Todos los formatos de firma electrónica estandarizados por ETSI, a excepción de PAdES-CMS *, obligan a proteger tanto el certificado del firmante o el resumen del certificado del firmante con la propia firma.

La indicación de la identidad del firmante debe de quedar protegida.

* *ETSI EN 319142-2 [i.7], cláusula 4 para PAdES-CMS no exige la inclusión de ESS-signing-certificado o ESS-signing-certificate-v2*

3.1.3.9 Inclusión de roles y atributos del firmante

Las firmas CAdES, PAdES y XAdES proporcionan mecanismos para indicar el papel desempeñado por el firmante, lo que da derecho a incluir ciertos atributos.

En el ámbito de esta política, en caso de incluirse esta indicación contempla las siguientes opciones:

- una declaración "*certificada*", emitida por una autoridad de atributos (*por ejemplo, certificado de atributo: afirmación firmada por una autoridad de atributo que asume la veracidad de la información*) *;
- atributo incluido en el cuerpo del certificado cuya responsabilidad de veracidad es asumida por el emisor del certificado.
    - OID 2.5.4.12 Titulo (T) conforme [RFC 5280]

* *Los certificados de atributos no deben incluirse dentro PAdES-CMS firmas (ETSI EN 319 142-2,cláusula 4.2.1)*

3.1.3.10 Inclusión identificador de la Política de Firma

Las firmas CAdES, PAdES y XAdES proporcionan mecanismos para incorporar información explícita de la política de firma que regulan su generación y validación.

3.1.3.11 Inclusión de la indicación del formato de objeto de datos firmado

Las firmas digitales CAdES, XAdES y PAdES-XML-EMB proporcionan mecanismos para incorporar una indicación del formato del objeto de datos firmado como información firmada.

3.1.3.12 Aumento de firma –ciclo de vida-

Las firmas electrónicas pasan por etapas más complejas que la simple fase de generación y validación inicial. Es necesario que las firmas extiendan su longevidad más allá del periodo de vigencia de los certificados que han intervenido en su creación, y de la vida efectiva de los componentes criptográficos empleados.

El ciclo de vida de una firma electrónica hasta el momento que se descarta, comprende las siguientes etapas: *generación, validación y aumento de firma*.

Los formatos CAdES, XAdES y PAdES satisfacen este tipo de requisitos, permitiendo agregar datos adicionales a las firmas para sustentar sus ciclos de vida. El proceso de incorporar datos adicionales a una firma generada se llama aumento de firma.

Estos datos adicionales pueden ser datos de validación, es decir, datos necesarios para validar la firma *(por ejemplo, certificados CRL, respuestas OCSP, etc.),* y también pueden ser datos para aumentar la longevidad de las firmas *(por ejemplo, tokens de sello de tiempo tal y como se detalla en clausula 3.1.3.5 de este documento)*.

NOTA.- más información en el apartado 3.2.5.1 "Aumento de la longevidad y resistencia al cambio".

3.1.3.13 Incluir referencias a certificados

Tanto las firmas CAdES como XAdES definen contenedores para incluir referencias a:

1) certificados de CA dentro de la ruta de certificación del certificado del firmante;
2) certificados de autoridades de atributos y los certificados dentro de su ruta de certificación;
3) aserciones firmando certificados *(requerido cuando el firmante firma aserciones firmadas)* y los certificados dentro de sus rutas de certificación; y
4) certificados de tokens de sello de tiempo ya presentes en la firma en el momento de generar estos contenedores, y los certificados dentro de sus rutas de certificación.

Cada referencia contiene el valor de resumen calculado en el certificado referenciado utilizando un algoritmo de resumen específico y un identificador *(opcional)*. Las partes que confían pueden usar el valor de resumen para verificar que el certificado recuperado sea realmente el referenciado.

3.1.4 Objetivo

Está política de firma establece los siguientes requisitos:

1. La firma debe de estar en uno de los formatos establecidos en el apartado 3.1.3, firmas electrónicas avanzadas (AdES) o cualificadas (QAdES)

2. La firma se debe de haber creado empleando un certificado cualificado de firma (QES) o un certificado cualificado de sello electrónico (QEseal), que esté en conformidad con el Reglamento eIDAS.
3. Condición general: en la firma debe de constar esta política mediante la inclusión del OID 1.3.6.1.4.1.18332.27.1.1

   Descripción:

   El firmante realiza la firma con pleno consentimiento y libre voluntad, conoce y acepta que la firma está destinada a ser utilizada en un marco legal en el cual se desea acreditar con fuerza probatoria y plena eficacia jurídica que el firmante está de acuerdo con los datos firmados, salvo haber indicado compromiso/s, haber reseñado mención o salvedad que pueda limitar el alcance de los acuerdos 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 o requerimientos 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.
4. Condiciones particulares: el firmante puede indicar tipo de compromiso/s que determinan el alcance de la firma. El tipo indicado por el firmante se especifica mediante OID específico y queda incluido en la firma. Los compromisos admitidos por esta política están detallados en el apartado 3.2.2.
5. Menciones / salvedades: cuando es necesario, el firmante puede incluir un texto que queda incluido en la firma. Será necesario derivar el significado de la firma a partir del texto redactado por el firmante.

3.1.5 Asignación de responsabilidad para validación y aumento

Las partes que confían, previo a depositar su confianza en la firma / sello electrónico, deben de realizar proceso de validación utilizando un servicio cualificado de validación de firmas y sellos electrónicos registrado en la TSL de la UE.

- Partes que confían en la firma:
  - El firmante,
  - Los terceros que confían,
  - Procesos automáticos que corroboran / ratifican documentos firmados, o contrafirmar antes de contrafirmarlas como parte del flujo de datos, o publican documentos firmados.

Cualquiera de las partes puede delegar las responsabilidad de validación de firma, en el servicio cualificado de validación de firma y sellos electrónicos de ANF AC OID 1.3.6.1.4.1.18332.56.1.1.

La vigencia de la firma está asociada a la capacidad de validarla a lo largo del tiempo, para ello es necesario aplicar técnicas de aumento de seguridad criptográfica. El aumento de una firma electrónica es el proceso mediante el cual cierto material (*por ejemplo, marcas de tiempo, datos de validación, etc.*) se incorpora a las firmas para hacerlas más resistentes al cambio o para ampliar su longevidad (*re-sellado / re-timbrado*).

Para realizar un re-sellado adecuado se debe de utilizar componentes criptográficos aceptados por ETSI TS 119 312 y en conformidad con las normas de referencia ETSI en la materia (*relación de normas en apartado 3.1.3.1 de este documento*).

Cualquiera de las partes puede delegar las responsabilidad de aumento de firma en el servicio cualificado de conservación de firmas electrónicas y sellos electrónicos a largo plazo de ANF AC OID 1.3.6.1.4.1.18332.61.

3.2 Relacionados con los procesos de la aplicación de firma

3.2.1 Tipo legal de las firmas

De conformidad con el Reglamento (UE) nº 910/2014 [eIDAS], está política de firma abarca los siguientes tipos de firma:

- firma electrónica cualificada,
- firma electrónica avanzada respaldada por un certificado cualificado de firma,
- sello electrónico cualificado,
- sello electrónico avanzado respaldado por un certificado cualificado de sello electrónico.

Siempre que sea posible, el workflow de firma debe de tener en cuenta los requisitos legales que pueden ser requeridos según el tipo de acto (*p.ej. los contratos de trabajo, deben de ser formalizados con una firma electrónica cualificada*). Además, puede darse el caso que determinados actos jurídicos no pueden ser formalizados mediante firma electrónica (*p.ej. la firma de una escritura de compra-venta de un inmueble*)

Los escenarios de uso son innumerables, la realidad de mercado es que solo en determinados procesos la aplicación de firma puede determinar el tipo de acto que se va a formalizar, por ello, las partes que confían asumen la responsabilidad de comprobar que el tipo de firma es el adecuado e, incluso, si es posible la formalización mediante firma / sello electrónico.

ANF AC, pone a disposición de sus suscriptores un servicio de soporte legal gratuito:

- eMail. mcmateo@anf.es
- Tfno. 902 902 172

3.2.2 Compromiso asumido por el firmante

Siempre que sea posible, los implementadores deben de identificar y describir el propósito esperado de cada firma y, por lo tanto, el significado y la naturaleza precisa de la responsabilidad asumida por el firmante, es decir, el tipo de compromiso de cada firma electrónica según el escenario empresarial y el flujo de firmas. Además, los tipos de compromiso de firma pueden ser útiles para evitar posibles ambigüedades debido al hecho de que las firmas electrónicas pueden no proporcionar información contextual equivalente a la del mundo del papel, lo que genera incertidumbre sobre la intención del firmante.

La condición general correspondiente a esta política, queda recogido en el apartado “3.1.4 Objetivos”, con el OID 1.3.6.1.4.1.18332.27.1.1. Si se especifica una o varias de las siguientes condiciones particulares, y alguna de ellas entra en contradicción con la condición general, la condición particular prevalece sobre la condición general. Si el firmante ha escrito alguna mención o salvedad, y del texto redactado por el firmante se deduce alguna contradicción con la condición general o particular, la mención o salvedad prevalece sobre las anteriores.

Cada tipo de compromiso se expresa mediante un identificador único (OID o URI), puede incluir uno o varios.

Los compromisos particulares aceptados por esta política son:

- Compromisos publicados en ETSI 119 172-1 *(Anexo B)*
- Compromisos normalizados referenciados con OID propietario de ANF AC.

Compromisos particulares:

- OID 1.2.840.113549.1.9.16.6.1 - prueba de origen.
  Indica que el firmante reconoce haber creado, aprobado y enviado los datos firmados.
  El URI de este compromiso es http://uri.etsi.org/01903/v1.2.2#ProofOfOrigin .
- OID 1.2.840.113549.1.9.16.6.2 - como acuse de recibo.
  Indica que el firmante reconoce haber recibido el contenido de los datos firmados;
  El URI de este compromiso es http://uri.etsi.org/01903/v1.2.2#ProofOfReceipt .
- OID 1.2.840.113549.1.9.16.6.3 - prueba de entrega.
  Indica que el TSP que proporciona esa indicación ha entregado un dato firmado en un buzón accesible al destinatario de los datos firmados.
  El URI de este compromiso es http://uri.etsi.org/01903/v1.2.2#ProofOfDelivery .
- OID 1.2.840.113549.1.9.16.6.4 – prueba del remitente.
  Indica que la entidad que proporciona esa indicación ha enviado los datos firmados (pero no necesariamente lo creó).
  El URI de este compromiso es http://uri.etsi.org/01903/v1.2.2#ProofOfSender .
- OID 1.2.840.113549.1.9.16.6.5 - prueba de aprobación.
  Indica que el firmante ha aprobado el contenido de los datos firmados.
  El URI de este compromiso es http://uri.etsi.org/01903/v1.2.2#ProofOfApproval .
- OID 1.2.840.113549.1.9.16.6.6 - prueba de creación.
  Indica que el firmante ha creado los datos firmados (pero no necesariamente aprobados, ni enviados eso).
  El URI de este compromiso es http://uri.etsi.org/01903/v1.2.2#ProofOfCreation .

Compromisos propietarios:

- OID 1.3.6.1.4.1.18332.27.1.9 - Credencial en un control de acceso.
  La firma está destinada únicamente a fines de autenticación de entidades con el fin de dejar evidencia de la solicitud de acceso realizada por el firmante.
- OID 1.3.6.1.4.1.18332.27.1.12 - Autorización intermedia
  La firma está destinada únicamente como una aprobación intermedia como parte de un proceso de decisión;
- OID 1.3.6.1.4.1.18332.27.1.14 - Visto, marca de lectura.
  La firma está destinada únicamente para indicar haber revisado un documento;
- OID 1.3.6.1.4.1.18332.27.1.15 - Intervención en la digitalización certificada de un documento original.
  La firma está destinada únicamente a certificar que el firmante garantiza que el documento firmado es una copia certificada que se corresponde íntegramente con un original.;
- OID 1.3.6.1.4.1.18332.27.1.16 - Intervención como testigo.
  Indica que la firma está destinada únicamente a indicar haber sido testigo de la firma de otra persona en el mismo documento (datos firmados) la cual ha leído íntegramente el documento, y lo ha firmado como acreditación de su conformidad a los mismos.

El OID identifica de forma unívoca cada compromiso particular e, incluso, su descripción puede incluirse en la firma electrónica o implícitamente en la semántica del objeto de datos firmado. En caso de incluirse en la firma electrónica, deberá estar reseñado en el campo "*tipo de compromiso*" según se especifica en la norma ETSI EN de referencia.

Si el campo correspondiente a la política de firma electrónica está ausente, y tampoco constan compromisos, menciones o salvedades, es decir, no se identifica ningún contexto aplicable a la firma, entonces se debe asumir que la firma ha sido generada sin ninguna restricción normativa, en consecuencia, 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 tanto, hará falta derivar el significado de la firma a partir del contexto, especialmente de la semántica del documento firmado.

Definiciones a utilizar en la inclusión de compromisos:

- **CommitmentTypesRequired:**
  Establece el conjunto de los valores requeridos para el compromiso expresado por el firmante y si esta expresión es requerida para ser parte de las propiedades de la firma. La semántica es:
  - **MandatedSignedQProperties-commitment-type-indication:** Esta restricción indica si la expresión del compromiso por el firmante debe ser parte de las propiedades calificadas firmadas; expresado como *boolean*.
  - **MandatedCommitmentTypeValues:** Esta restricción indica los posibles valores requeridos para el tipo de compromiso que va a expresar el firmante. La semántica se define de la siguiente manera:
    - **MatchingValuesIndicator:** forma en que se hacen coincidir los valores del tipo de compromiso en la firma, contra los posibles valores de compromiso requeridos. Puede tener los siguientes valores:
      - "todos" si se deben cumplir todos los valores;
      - "atLeastOne" si se debe cumplir al menos uno de los valores;
      - "ninguno" si no se cumplen todos los valores.
    - **CommitmentTypeValues**: una secuencia de compromiso no vacía que reseña identificadores de tipo (OID o URI), asociados a su descripción.

3.2.3 Nivel de seguridad de las evidencias cronológicas

Los implementadores deben diferenciar:

- Marca de tiempo
  Es la asignación por medios electrónicos de la fecha y hora a un documento. Puede ser generada por cualquier aplicación, sin cumplir ningún requisito legal o técnico. No ofrece seguridad jurídica.
  Solo puede ser empleada con fines técnicos y cuando una norma así lo requiera (*p.ej. servicio digitalización de facturas en Metadatos XMP*)
- Sello Cualificado de Tiempo Electrónico
  Ofrece eficacia jurídica. Está elaborado según estándares técnicos ETSI y en conformidad con el Reglamento eIDAS.

El sello cualificado de tiempo electrónico acredita la existencia de un objeto en un momento del tiempo, tiene presunción legal de certeza. Debe ser emitido por un Prestador Cualificado de Servicios de Confianza (PCSC), acreditado para la prestación de este servicio y registrado en la TSL de la UE.

Siempre que se requiera una evidencia de tiempo confiable se deben de utilizar un sello cualificado de tiempo electrónico, emitido por un PCSC registrado en la TSL de la UE como cualificado en la prestación del servicio de sellado de tiempo electrónico.

Las aplicaciones de firma deben de utilizar *(salvo regulación legal o fiscal aplicable)* sellos cualificados de tiempo electrónico. Para determinar la calificación de un sello electrónico, la aplicación de firma verificará que el sello está firmado por un PCSC que ha utilizado para firmar el sello de tiempo un certificado cualificado *(id-pe-qcStatements = "1.3.6.1.5.5.7.1.3"),* y que incluye el OID 0.4.0.19422.1.1 *(id-qcs-pkixQCSyntax-v2 - en conformidad con la norma ETSI EN 319 412-1)*. Al incluir este OID, el emisor afirma que el token de sello de tiempo se emite como un sello cualificado de tiempo electrónico según el Reglamento eIDAS (UE).

El sello cualificado de tiempo electrónico es un atributo requerido en firmas nivel T, LT y LTA.

Las definiciones de cómo tiene que ser la evidencias del tiempo son,

- *MandatedSignedQProperties-signing-time*
  Se requiere indicación de la hora y día en que se ha generado la firma.
- *MandatedSignedQProperties-content-time-stamp*
  Requiere un sello cualificado de tiempo electrónico sobre la totalidad de los datos firmados, como parte de las propiedades calificadas firmadas.
- *MandatedUnsignedQProperties-signature-time-stamp*
  Requiere un sello cualificado de tiempo electrónico en la firma.
- *MandatedUnsignedQProperties-archival-form*
  Requiere un sello de tiempo en el archivo.

Definiciones respecto al nivel de garantía requerido son,

- *LoAOnTimingEvidences*:
  Este conjunto de restricciones indica el nivel de garantía requerido (*LoA*) en la evidencia de tiempo. La semántica se define como sigue:
  - *LoA-on-signing-time*
    Esta restricción indica el LoA requerido en la firma del tiempo.
  - *LoA-on-content-time-stamp*
    Indica el LoA requerido en el contenido del sello de tiempo.
  - *LoA-on-signature-time-stamp*
    Indica el LoA requerido en la firma del sello de tiempo.
  - *LoA-on-archival-time-stamp*
    Indica el LoA requerido en el archivo del sello de tiempo.
  - *LoA-on-time-in-OCSP-response*
    Indica el LoA requerido en el tiempo expresado en la respuesta OCSP.
  - *LoA-on-time-in-CRL*
    Indica la LoA requerida en el tiempo expresado en la CRL

3.2.4 Formalidades de la firma

Una de las características más importantes de una firma es la forma en que se crea. A menudo denominada "*ceremonia de la firma*", es la forma en que se llama la atención del firmante sobre el significado del compromiso que está asumiendo mediante el acto de firmar. La calidad de la ceremonia de firma está directamente relacionada con el "*consentimiento y la voluntad*" del firmante.

Los implementadores deben identificar requisitos sobre cualquier tipo de evidencia relacionada con la libre voluntad o intención de firmar *(p.ej. según la importancia y trascendencia del acto, se podría utilizar 2FA para reforzar la evidencia)*. Es necesario que las aplicaciones de firma llamen la atención del firmante sobre la importancia del compromiso que se está asumiendo al aplicar sus datos de creación de firma. Todos estos requisitos se materializan disponiendo el firmante de una adecuada interfaz de firma.

Principales requisitos a contemplar:

1. En un entorno WYSIWYS, "*lo que ves es lo que firmas*". Definiciones que indican la medida requerida:
   - *WYSIWYSRequired*
     Indica el requisito de tener un "*lo que ves es lo que firmas*"; expresado como un *boolean*.
   - *WYSIWHBSRequired*
     Indica el requisito de tener un "*lo que ves es lo que ha sido firmado*"; expresado como un *boolean*.
   - *ProperAdviceAndInformationRequired*
     Indica si se requiere proporcionar al usuario *(firmante o verificador)* asesoramiento y la información adecuada sobre la creación de la firma, proceso de solicitud y sobre las consecuencias legales, así como una interfaz de usuario que garantiza, en la medida de lo posible, una firma legal válida con plenas garantías de consentimiento y voluntad; expresado como *boolean*.
   - *UserInterfaceDesignConstraints*
     Indica si es necesario diseñar la interfaz de usuario para cumplir los requisitos de garantía expresados en esta cláusula 3.2.4; expresado como *boolean*.
   - *CorrectValidationAndArchivalProcedures*
     Esta restricción indica si el SCA y el SVA deben mostrar a la parte que confía (*incluido el firmante*) los procedimientos correctos para la validación y el archivo de la firma y los datos de validación asociados; expresado como una tupla hecha de un *boolean* y un cadena de caracteres opcional.
2. Brindar a los usuarios asesoramiento, información y consejos adecuados sobre el proceso de firma de la aplicación:
   i) *asesoramiento e información adecuados sobre el proceso de solicitud de firma;*
   ii) *asesoramiento e información adecuados sobre las consecuencias legales;*
   iii) *una interfaz de usuario que permite atender los requisitos legales sobre la expresión de voluntad o intenciones del / los firmantes (compromisos de firma); y*
   iv) *diseñar la interfaz de usuario de manera que garantice un entorno de firma legal, incluso:*
      - *Implementación que permita y demuestra una clara expresión de la voluntad de firmar y la intención del usuario de estar obligado por la firma.*
      - *Implementación permitiendo y demostrando un consentimiento informado.*

- *Coherencia entre el uso de la creación de firma adecuada y los datos de verificación, firma dispositivo de creación, los datos a firmar y el alcance y el propósito esperado de la firma (o el acto de firma)*

3. Proporcionar a los usuarios un entorno de "*lo que ve es lo que firmas*". Para ello se verifica que el formato es un formato seguro o, en caso de ser un formato que permite macros o incluir objetos visibles al ojo humano pero que no van a ser firmados, se apercibe al firmante y no son mostrados. De igual forma si el objeto de datos no puede ser reproducido al sentido humano (vista u oído). Se recomienda al firmante revisar previamente el objeto de datos para confirmar que se trata del objeto de datos de interés.
4. A fin de evitar incertidumbre en el firmante o en los terceros que confían, la aplicación de firma y el informe de validación incluye una descripción explícita que evita posibles ambigüedades cuando las firmas no proporcionan información contextual equivalente a la del mundo del papel.
5. Se incluye información de ayuda sobre tipos de firma, niveles y modalidades.

La definición a utilizar es:

- *LoAOnLongevityAndResilience:-*
  Esta restricción indica el LoA requerido sobre la longevidad y resistencia de la evidencia proporcionada por la firma.

ANF AC, pone a disposición de todos los firmantes que se someten a esta política de firma, un servicio de soporte legal gratuito:

- eMail. mcmateo@anf.es
- Tfno. 902 902 172

Se pone a disposición de todas las partes que confían en la firma, servicio cualificado de validación de firmas y sellos electrónicos de ANF AC.

Las aplicaciones de creación de firma de ANF AC, se someten anualmente a auditoría de conformidad a fin de confirmar la adecuación de los perfiles de protección.

3.2.5 Longevidad y resistencia al cambio

El paso del tiempo tiene dos efectos diferentes sobre las firmas electrónicas:

- en primer lugar, los certificados utilizados pueden caducar, haber sido revocados o incluso, el servicio de validación del emisor dejar de estar disponible;
- en segundo lugar, los algoritmos criptográficos (*también incluidos los algoritmos de digestión – resumen hash-*), pueden debilitarse a medida que mejoran las técnicas de criptoanálisis y las capacidades informáticas.

La longevidad y resiliencia al cambio (*entendido como tal, la resistencia de las firmas al descubrimiento de debilidades de sus algoritmos*) están, en consecuencia, estrechamente relacionados entre sí.

La longevidad esperada y la resistencia al cambio de la firma de manera que sea verificable hasta un período de tiempo determinado, está íntimamente asociada al "*nivel*" de firma en que ha sido elaborada, además, teniendo en cuenta si sobre ella se ha aplicado un aumento de firma (*re-timbrado*).

- En el caso de firmas según formato Baseline nivel B que no cuentan con aumento de firma, el periodo de longevidad se reduce al tiempo de vigencia del certificado empleado *(caducidad o revocación)*, y estado de vigencia de seguridad de los componentes criptográficos. El periodo de validez puede llegar a ser inferior a un día.
- En el caso de firmas que incluyen sello cualificado de tiempo electrónico *(formato nivel T)* pero no cuenta con aumento de firma, el periodo de longevidad se extiende más allá del estado de vigencia del certificado pero se limita a la disponibilidad del servicio de OCSP o CRLs del emisor del certificado, y estado de vigencia de seguridad de los componentes criptográficos. El periodo de validez se puede considerar de medio plazo, dos años.
- En el caso de firmas que incluyen sello cualificado de tiempo electrónico y verificación de estado de vigencia del certificado *(formato nivel LT)* pero no cuenta con aumento de firma, el periodo de longevidad se extiende más allá del estado de vigencia del certificado aunque se haya perdido disponibilidad del servicio de OCSP o CRLs del emisor del certificado, pero queda limitado al estado de vigencia de seguridad de los componentes criptográficos. El periodo de validez se puede considerar de largo plazo, seis años.
- En el caso de firmas que incluyen sello cualificado de tiempo electrónico, verificación de estado de vigencia del certificado y se encuentran almacenadas en un servicio cualificado de conservación a largo plazo *(formato nivel LTA)*, el periodo de longevidad garantizado es de muy largo plazo, como mínimo 15 años.

Las partes que confían tienen que tener en cuenta la necesidad de longevidad y resiliencia que debe de ofrecer la firma de acuerdo con el alcance requerido según escenario de negocio.

3.2.5.1 Aumentar la longevidad y resistencia al cambio

Las firmas CAdES, XAdES y PAdES proporcionan medios para proteger firmas aumentadas y, en consecuencia, para aumentar su longevidad. Pasos necesarios para realizar el aumento:

1) Incorporar cualquier material de validación faltante a la firma, incluido el material de validación faltante de cualquier token de sello de tiempo previamente incorporado.
2) Proteger todo el material necesario para validar la firma *(incluidos los objetos de datos firmados, incluso si se separan de la firma y del material de validación)* generando un nuevo token de sello de tiempo utilizando un algoritmo de resumen más fuerte si es necesario. Este token de sello de tiempo en realidad proporciona una prueba de la existencia de todos los elementos y al mismo tiempo protege su integridad.
3) Incorporar el nuevo token de sello de tiempo a la firma encapsulada en un contenedor adecuado.

Este tipo de tokens de sello de tiempo se conoce como tokens de sello de tiempo para la disponibilidad a largo plazo y la integridad de la validación material. Como mínimo, estas firmas incorporarán todos los datos de validación necesarios para su validación y uno o más de estos tipo de tokens de sello de tiempo. En consecuencia, estas firmas requerirán al menos dos componentes específicos:

1) Contenedores para valores de datos de validación.
2) Contenedores para tokens de sello de tiempo de archivo.

Las especificaciones ETSI permiten combinaciones complejas de atributos / propiedades que se pueden proteger con sello de tiempo.

Las siguientes firmas CAdES, PAdES y XAdES incorporan este tipo de tokens de sello de tiempo:

- Firmas XAdES- LTA,
- Firmas CAdES- LTA,
- Firmas PAdES- LTA.

NOTA.- más información en apartado 3.1.3.13 "Aumento de firma –ciclo de vida-".

3.2.6 Archivo

El archivo está relacionado con la longevidad de las firmas, y las partes deben de tener en cuenta el alcance de seguridad requerido según escenario de negocio, y normativa legal, fiscal o sectorial que lo afecta.

La definición a utilizar es:

- *ArchivalConstraints*
  Esta restricción indica los requisitos con respecto al archivo de la firma y los datos de validación asociados.

Cualquiera de las partes puede delegar las responsabilidad de archivo de documentos y firmas en el servicio cualificado de conservación y almacenamiento de firmas electrónicas y sellos electrónicos a largo plazo de ANF AC OID 1.3.6.1.4.1.18332.61.

3.3 Actores involucrados en crear / aumentar / validar firmas

3.3.1 Identidad y atributos (roles) de los firmantes

Una firma no tiene valor si no se puede atribuir al firmante. Como regla general las aplicaciones de firma reseñadas en este documento emplean certificados cualificados en su creación, por tanto, la identidad del firmante se obtiene del certificado de firma / sello empleado para firmar, lo cual garantiza plena eficacia jurídica sobre la identidad del firmante.

El certificado cualificado empleado para la creación de firma, está sometido a los requisitos de identificación establecidos en la Declaración de Prácticas de Certificación del emisor del certificado, Política de Certificación a la que se somete el certificado, al Reglamento (UE) 910/2014 (eIDAS), legislación nacional y normas técnicas ETSI en la materia.

Los procesos de firma deben de tener en cuenta que en algunos escenarios de uso los atributos que posee o el papel desempeñado por un firmante, son al menos tan importantes como su identidad. P.ej. *el documento debe de ser firmado por determinada persona (un contrato), o puede ser sellado por una de las aplicaciones informáticas de uno de los departamentos de una organización (una garantía), o debe ser firmado por un médico (receta electrónica), o asociado a una determinada autoridad jerárquica (Director Comercial)*

Los implementadores deben de tener en cuenta no solo los valores contenidos en el certificado, también tienen que tener en cuenta otros requisitos, haciendo constar el conjunto de atributos, autoridades y responsabilidades que están asociados con cada firmante, sus derechos de acceso o autoridad para firmar en nombre de la organización que pretende

representar, etc. La inclusión de atributos o roles, implica que se debe de disponer de una acreditación certificada que garantice legalmente tal mención, P.ej.

- prueba de que un empleado o representante está autorizado a realizar transacciones sobre un valor específico;
- prueba de autorización de delegación para firmar, etc.

La definición a utilizar es:

- *MandatedSignedQProperties-signer-attributes:*
  Esta restricción indica si el firmante debe de tener una calificación. El atributo es obligatorio y las restricciones asociadas a los atributos necesarias. Esto se puede expresar como una tupla hecha de un booleano asociado con una secuencia de identificadores que expresan restricciones sobre los atributos requeridos del firmante. Dichas restricciones sobre los atributos o roles del firmante pueden cubrir:
  - qué roles / atributos son obligatorios;
  - identificación de los roles / atributos que necesitan ser certificados o estar presente dentro de afirmaciones firmadas;
  - restricciones sobre el tipo de roles / atributos; y
  - restricciones sobre los valores de roles / atributos.

Cuando sea necesario, esta restricción puede usarse para expresar si es requerido un atributo y los requisitos asociados.

3.3.2 Nivel de seguridad requerido para la autenticación del firmante

Se requiere que los certificados *(firma electrónica o sello electrónico)*, estén emitidos como cualificados por un Prestador Cualificado de Servicios de Confianza acreditado e inscrito en la Lista de Confianza de la UE.

Los implementadores deben identificar cuál es el nivel de garantía requerido para la autenticación del firmante en cada firma que se generará dentro del proceso empresarial, es decir, cuáles son las expectativas en términos de confianza que requiere el escenario de uso. *P.ej. si se requiere 2FA, o si hay medidas restrictivas en cuanto a la hora o terminal informático, etc.*

La definición a utilizar es:

- *NameConstraints:*
  Estas restricciones indican requisitos sobre los nombres distinguidos para certificados emitidos *(p. ej., al firmante, CA, respondedores OCSP, emisores de CRL,Unidades de Sellado de Tiempo)* como se define en IETF RFC 5280

3.3.3 Dispositivos de creación de firmas

De acuerdo con lo establecido en el Reglamente eIDAS, un «dispositivo de creación de firma electrónica», es un equipo o programa informático que se utiliza para crear una firma electrónica. Los dispositivos de creación de firma reconocidos por esta política son:

- Todas las aplicaciones y plataformas de ANF AC reseñadas en este documento. Concretamente:
  - Safe Box®.
  - Critical Access ®.

- BlackBoxSign®.
- Legal Snap Scan ®.
- Sign to Sign®.
- Servidor de firma a distancia para certificados centralizados.

Tokens y almacenes de firma que se utilizan en el proceso de creación de una firma / sello electrónico reconocidos por esta política:

- Todo dispositivo calificado con certificación QSCD.
- Todo dispositivo HSM *(certificado Common Criteria ISO 15408 nivel EAL 4+ o superior).*
- Token USB Plug and Sign ® de ANF AC.
- Token en software criptográfico con middleware ANF AC y en conforme al estándar PKCS#12.
- Store de certificados de Windows / Mozilla / Linux.

3.4 Otros parámetros de negocio

3.4.1 Otra información que se asociará a la firma

No se prevé requisitos en esta materia.

3.4.2 Componentes criptográficos

Tienen que cumplir lo establecido en la ETSI TS 119 312 "*Cryptographic Suites*"

Los implementadores conocerán y seguirán las orientaciones de la ETSI TR 119 300 "*Guidance on the use of standards for cryptographic suites*".

La definición a utilizar es:

- *NameConstraints:*
  Estas restricciones indican requisitos sobre los nombres distinguidos para certificados emitidos,
  p. ej.: al firmante, CA, respondedores OCSP, emisores de CRL, Unidades de Sellado de Tiempo como se define en IETF RFC 5280
- *X509CertificateValidationConstraints*
  Este conjunto de restricciones indica los requisitos para realizar el proceso de validación de la ruta de certificación conforme IETF RFC 5280. Estas restricciones pueden ser diferentes para diferentes tipos de certificados *(por ejemplo, certificados emitidos al firmante, a las CA, a respondedores OCSP, emisores de CRL, unidades de sellado de tiempo)*. La semántica es como sigue:
- *SetOfTrustAnchors*

Esta restricción indica un conjunto de jerarquías de confianza aceptables *(TA)* como una restricción para el proceso validación. Tales *TA* deben proporcionarse en forma de certificados autofirmados *(certificado raíz) (cláusula 6.1.1 de IETF RFC 5280)* y un tiempo hasta que estas jerarquías de confianza se consideraron fiables.

P.ej.: El conjunto de TA se puede proporcionar bajo la forma de:

- Puntos de confianza especificados en las políticas de validación de firmas;
- Conjuntos de CA confiables, por ejemplo, representados por sus certificados raíz almacenados en el entorno *(como el store de Windows o Mozilla)*;
- listas de estado del servicio de confianza;
- Listas de confianza UE como se define en eIDAS.

- *CertificationPath*

  Esta restricción indica una ruta de certificación requerida para ser utilizada por la SVA para la validación de la firma. La ruta del certificado tiene una longitud 'n' desde el ancla de confianza *(TA)* hacia abajo al certificado utilizado para validar un objeto firmado *(por ejemplo, el certificado con sello de tiempo)*. Esta restricción puede incluir el camino a considerar o indicar la necesidad de considerar la ruta proporcionada en la firma, si la hubiera.

  - *user-initial-policy-set:* esta restricción es como se describe en IETF RFC 5280 cláusula 6.1.1 punto (c).
  - *initial-policy-mapping-inhibit:* esta restricción es como se describe en IETF RFC 5280 cláusula 6.1.1 punto (e).
  - *initial-explicit-policy:* esta restricción es como se describe en IETF RFC 5280 cláusula 6.1.1 punto (f).
  - *initial-any-policy-inhibit:* esta restricción es como se describe en IETF RFC 5280 cláusula 6.1.1 punto (g).
  - *initial-permitted-subtrees:* esta restricción es como se describe en IETF RFC 5280 cláusula 6.1.1 punto (h).
  - *initial-excluded-subtrees:* esta restricción es como se describe en IETF RFC 5280 cláusula 6.1.1 punto (i).
  - *path-length-constraints:* indica restricciones sobre el número de certificados de CA en una ruta de certificación. Esto puede necesitar definir valores iniciales o manejar tal restricción de manera diferente *(por ejemplo, ignórela)*.
  - policy-constraints: esta restricción indica requisitos para las políticas de certificación a las que se hace referencia en los certificados. Esto puede necesitar definir valores iniciales para esto o manejar la restricción de manera diferente *(por ejemplo, ignórelo)*. Esto también debería permitir la capacidad de requerir una extensión de política de certificación de entidad final.

3.4.3 Entorno tecnológico

Las aplicaciones de firma electrónica identificadas en esta política son funcionales en sistemas operativos Windows a partir versión 7 y Linux, no son funcionales en Mac OS de Apple.

En el caso de aplicaciones móviles, son funcionales en sistemas operativos Android e iOS. Los implementadores deben identificar claramente qué tipo (s) de documento (s) y qué firmas dentro de ellos serán gestionadas. Según escenario de uso puede requerir servicios específicos para apoyar estas tareas y, en consecuencia, utilizar conjuntos específicos de estándares.

3.4.3.1 Selección de estándares

Los formatos de firmas electrónicas / sellos electrónicos admitidos estarán en conformidad con la estructura normalizada por,

- ETSI EN 319 132-1 y ETSI EN 319 132-2
  "*XAdES Advanced Electronic Signature Profiles*".
- ETSI EN 319 122-1 y ETSI EN 319 122-2
  "*CAdES Advanced Electronic Signature Profiles*".
- ETSI EN 319 142-1 y ETSI EN 319 142-2
  "*PAdES Advanced Electronic Signature Profiles*".

Procedimiento,

- ETSI TS 119 172-1
  "Part 1: *Building blocks and table of contents for human readable signature policy documents*"
- ETSI TS 119 101
  "*Policy and security requirements for applications for signature creation and signature validation*"
- ETSI EN 319 102-1
  "*Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation*"
- ETSI TR 119 001
  "*The framework for standardization of signatures; Definitions and abbreviations*"

Sellos de tiempo,

- ETSI EN 319 422-1
  "*Time-stamping protocol and time-stamp token profiles*"

Respuestas OCSP,

- RFC 6960
  "*Online Certificate Status Protocol - OCSP*"

Certificados X509 v.3,

- RFC 5280
  "*Online Certificate Status Protocol - OCSP*"
- ETSI EN 319 401
  "*General Policy Requirements for Trust Service Providers*"
- ETSI EN 319 412-5
  "*Part 5: QCStatements*"

Suites Criptográfi Procedimiento,

- ETSI TS 119 312
  "*Cryptographic Suites*"
- ETSI TR 119 300
  "*Guidance on the use of standards for cryptographic suites*"

Lista de servicios de confianza (TSL)

- ETSI TS 119 612 *"Trusted Lists"*

4 Mecanismos técnicos e implementación de estándares

4.1 Relacionados con los procesos de la aplicación de firma

Tabla 1: Resumen de declaración de política de firma

Autoridad de política de firma: ANF Autoridad de Certificación NIF G63287510 **Política de Firma:** Política de Firma Electrónica y Sello Electrónico OID 1.3.6.1.4.1.18332.27.1.1 **Identificador de la (s) firma (s) en el flujo de trabajo:** Firmas AdES / QAdES			
BSP	**Título BSP**	**Resumen declaración negocio**	**Contraparte declaración técnica**
(a)	Flujo de trabajo *(secuenciación y tiempo)* de firmas	1. Safe Box®. 2. Critical Access ®. 3. BlackBoxSign®. 4. Sign to Sign®. 5. Servidor de firma a distancia	1. Aplicación con extensión shell de usuario final de firma electrónica y validación. 2. Suite de aplicaciones de escritorio que incluye firma electrónica y validación. 3. Servidor de firma y validación. 4. Workflow de firma y validación. 5. Para certificados centralizados. En todos los casos: • Se requiere el uso de certificado cualificado vigente expedido por PCSC inscrito en la TSL UE. • la responsabilidad de obtener el hash del objeto de datos es de la aplicación de firma de ANF AC.
(b)	Datos a firmar *(DTBS)*	1. Safe Box®. 2. Critical Access ®. 3. BlackBoxSign®. 4. Sign to Sign®. 5. Servidor de firma a distancia	1. Aplicación para entorno Windows, incluye Shell Extensión. Desarrollada en Java, utiliza CriptoAPI B & , interopera con middlware de ANF AC, y plataformas de firma a distancia, credenciales y certificados centralizados. 2. Aplicación escritorio Windows. Desarrollada en Java, utiliza CriptoAPI B & , interopera con middlware de ANF AC, y plataformas de firma a distancia, credenciales y certificados centralizados. 3. Plataforma híbrida: *Cloud (docker / S3 bucker) y CPD Java, Phyton, C++, PHP (framework Laravel).* 4. Plataforma en Cloud desarrollada en PHP (framework Laravel), interopera con BlackBoxSign®. 5. Plataforma híbrida: *Cloud (docker / S3 bucker) y CPD Java, Phyton, C++, PHP (framework Laravel).*
(c)	Relación entre DTBS y firma/s	Formatos de firma/sello aceptados AdES / QAdES en conformidad con: 1. ETSI EN 319 132 2. ETSI EN 319 122 3. ETSI EN 319 142	Niveles admitidos conforme al perfil base BASELINE: 1. XAdES - B – T - LT y LTA 2. CAdES – B – T - LT y LTA 3. PAdES – B – T - LT y LTA Modalidades de firma admitidas: 1. XAdES: enveloped o enveloping.

			2. CAdES: implícita. 3. PAdES: enveloped.
(d)	Comunidad objetivo	No se restringe la comunidad de firmantes ni terceros que confían. **Condiciones generales**: La firma está destinada a ser utilizada en un marco legal y contractual. 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. **Condiciones particulares**: Se definen compromisos bajo los cuales se confía en una determinada firma o incluir, cuando es necesario, disposiciones relativas a la eficacia prevista de las firmas.	En todos los supuestos las condición general y las condiciones particulares se identifican de forma unívoca mediante OID y se realiza descripción de alcance y uso.
(e)	Asignación de responsabilidad para la validación y el aumento de firmas	Partes que confían en la firma: - El firmante, - terceros que confían, - procesos automáticos que corroboran / ratifican documentos firmados, o contrafirmar antes de contrafirmarlas como parte del flujo de datos, o publican documentos firmados. Previo a depositar su confianza, se requiere validación de las firmas / sellos electrónicos.	Para realizar la validación, se debe de utilizar el servicio cualificado de validación de firma y sellos electrónicos de ANF AC.
(f)	Tipo legal de firma	En conformidad con el Reglamento (UE) nº 910/2014 [eIDAS]	• firma electrónica cualificada, • firma electrónica avanzada respaldada por un certificado cualificado de firma, • sello electrónico cualificado, • sello electrónico avanzado respaldado por un certificado cualificado de sello electrónico.
(g)	Compromiso asumido por el firmante	Cada tipo de compromiso y la propia política de firma, se expresa como un identificador único (OID o URI)	La Política de Firma se hace constar con el OID 1.3.6.1.4.1.18332.27.1.1, y se reconocen compromisos definidos por ETSI TS 119 172-1 ANEXO B y compromisos propietarios definidos en este documento.

(h)	Nivel de seguridad sobre las evidencias cronológicas	Según lo definido en las normas ETSI en esta materia	1. Comprobación de estado (OCSP). Vigencia del certificado. 2. Comprobación calificación y adecuación del tipo certificado. 3. Generación hash del objeto de datos, path, nombre y formato. 4. Solicitud al firmante de los datos de activación de firma. 5. Elaboración de firma. 6. Construcción de la firma. Según nivel obtención de respuesta OCSP, y/o TimeStamping.
(i)	Formalidades de la firma	Ayuda y medidas de seguridad adecuadas al proceso de firma.	1. Entorno WYSIWYS (What You See Is What You Get). 2. El firmante dispone: i) asesoramiento e información sobre el proceso de la solicitud firma; ii) asesoramiento e información sobre las consecuencias legales; y iii) una interfaz de usuario que permite atender los requisitos legales sobre la expresión de voluntad o intenciones del / los firmantes
(j)	Longevidad y resiliencia al cambio	La longevidad esperada y la resistencia al cambio de la firma de manera que sea verificable hasta un período de tiempo determinado.	• Formato Baseline nivel B. El periodo de validez puede llegar a ser inferior a un día. • Formato Baseline nivel T. El periodo de validez puede llegar hasta 2 años. • Formato Baseline nivel LT. El periodo de validez se puede considerar de largo plazo, seis años. • Formato Baseline nivel LTA. El periodo de validez se puede considerar de muy largo plazo, mínimo 15 años.
(k)	Archivo	Para garantizar el archivo de los documentos firmados se requiere utilizar un servicio cualificado de conservación y almacenamiento de firmas y sellos electrónicos a largo plazo.	Requisitos recogidos en la Política de conservación de firmas y sellos electrónicos de ANF AC, OID 1.3.6.1.4.1.18332.61
(l)	Identidad de los firmantes	Se requiere el uso de certificados de identidad cualificados, emitidos por un Prestador Cualificado de Servicios de Confianza acreditado para la emisión de dichos certificados, e inscrito en la Lista de Confianza de la UE.	Sometido a los requisitos de identificación establecidos en la Declaración de Practicas de Certificación y Política de Certificación a la que se somete el certificado. Debe de incluir la información requerida por el Reglamento eIDAS, legislación nacional y normas técnicas ETSI en la materia.

(m)	Nivel de seguridad requerido para la autenticación del firmante	Se requiere que los certificados sean certificados cualificados, emitidos por un Prestador Cualificado de Servicios de Confianza acreditado para la emisión de dichos certificados, e inscrito en la Lista de Confianza de la UE.	En conformidad con el Reglamento eIDAS, y legislación nacional.
(n)	Dispositivos de creación de firmas	Se admiten todos los dispositivos QSCD-HSM y los reseñados en apartado 3.3.3	Aplicaciones y plataformas de ANF AC: • Safe Box®. • Critical Access ®. • BlackBoxSign®. • Sign to Sign®. • Servidor de firma a distancia Tokens: • Dispositivos QSCD. • Dispositivos HSM . • Token USB Plug and Sign con middleware de ANF AC. • Token en software criptográfico PKCS#12 con middleware ANF AC. • Store de certificados de Windows / Mozilla / Linux.
(o)	Otra información que se asociará con la firma	No se prevé requisitos en esta materia.	No se prevé requisitos en esta materia.
(p)	Suites criptográficas	ETSI TS 119 312	ETSI TS 119 312
(q)	Entorno tecnológico	sistemas operativos Windows versión 7 o superior, y Linux,	No son funcionales en SO Apple
Declaraciones de prácticas de aplicación de creación / validación de firmas		Política de Validación OID 1.3.6.1.4.1.18332.56.1.1.	Política de Validación OID 1.3.6.1.4.1.18332.56.1.1.
Resumen de los formatos de firma seleccionados según apartado 3.1.3.1, que incluye detalles sobre el formato de los datos firmados, la ubicación relativa de la firma y los datos firmados (es decir, envueltos, envolventes, implícitos), los atributos específicos de la firma y el nivel esperado del formato de firma seleccionado:			

4.2 Restricciones de entrada y salida -creación, aumento y validación-

4.2.1 Restricciones de entrada - generar, aumentar y validar -

Tabla 2

Autoridad de política de firma: ANF Autoridad de Certificación NIF G63287510 **Política de Firma:** Política de Firma Electrónica y Sello Electrónico OID 1.3.6.1.4.1.18332.27.1.1 **Identificador de la (s) firma (s) en el flujo de trabajo:** Firmas AdES /QAdES							
BSP	**BSP título**	**Resumen declaración negocio**	**Contraparte declaración técnica**	**Restricción (es)**	**Valor de restricción en la creación de la firma (SCA o DA)**	**Valor de restricción en el aumento de firmas (SCA, SVA o DA)**	**Valor de restricción en la validación de la firma (SVA o DA)**
(a)	Workflow (sequencing & timing) ver Tabla 1	ver Tabla 1	ver Tabla 1	**(a)1. OrderInSequence:** El workflow contempla multiples posibilidades de secuencia de firma y multiples firmantes.	AdES / QAdES Ver apartado 3.1.1	Política OID 1.3.6.1.4.1.18332.61	Política OID 1.3.6.1.4.1.18332.56.1.1
				(a) 2. SequencingNature: Características de la firma relación con la secuenciación: **(a) 2.1 Mandated-independent:** Las firmas independientes se definen como firmas aplicadas exactamente a los mismos datos. Sta restricción indica que la firma tiene que ser necesariamente independiente. **(a)2.2 Mandated-serial:** Las firmas en serie se definen como firmas aplicadas a diferentes datos y serializadas. Esta restricción indica que la firma está obligada a ser en seríe. **(a)2.3 MandatedUnsignedQProperties-counter-signature:** Las contrafirmas se definen como firmas aplicadas sucesivamente al conjunto de firmas anteriores y, opcionalmente, a los mismos datos originales. Esta restricción indica que la propiedad calificada sin firmar debe estar presente en la firma.	Ver apartado 3.1.1.1		

BSP	BSP título	Resumen declaración negocio	Contraparte declaración técnica	Restricción (es)	Valor de restricción en la creación de la firma (SCA o DA)	Valor de restricción en el aumento de firmas (SCA, SVA o DA)	Valor de restricción en la validación de la firma (SVA o DA)
				(a) 3. Relevancia del tiempo: **(a) 3.1 TimingRelevanceOnSequencing:** Esta restricción indica la relevancia requerida en la sincronización con respecto a la secuencia de la firmas. La semántica se define de la siguiente manera: - [no] antes de una fecha determinada, - [no] después de una fecha determinada, - [no] antes de un cierto período de tiempo, - exactamente en una determinada cantidad de tiempo, - [no] después de un cierto período de tiempo. **(a)3.2 TimingRelevanceOnEvidence:** Define como tiene que ser la evidencias del tiempo. Concretamente: • **(a)3.2.1 MandatedSignedQProperties-signing-time** Requiere indicación de la hora y dia en que se ha generado la firma. Sello cualificado de tiempo electrónico. • **(a)3.2.2 MandatedSignedQProperties-content-time-stamp** Requiere un sello cualificado de tiempo electrónico sobre la totalidad de los datos firmados, como parte de las propiedades calificadas firmadas. • **(a)3.2.3 MandatedUnsignedQProperties-signature-time-stamp** Requiere un sello cualificado de tiempo electrónico en la firma. • **(a)3.2.4 MandatedUnsignedQProperties-archival-form** Requiere un sello de tiempo en el archivo.	Ver apartado 3.1.1.1 Ver apartado 3.2.3		
				(a)4. MassSigningAcceptable (yes/no): Está restricción indica si se acepta la firma masiva con respecto al tipo de firma. Expresado en boolean.	Ver apartado 3.1.1.1		

BSP	BSP título	Resumen declaración negocio	Contraparte declaración técnica	Restricción (es)	Valor de restricción en la creación de la firma (SCA o DA)	Valor de restricción en el aumento de firmas (SCA, SVA o DA)	Valor de restricción en la validación de la firma (SVA o DA)
(b)	DTBS			**(b)1. ConstraintOnDTBS:** Esta restricción indica requisitos sobre el tipo de datos que debe firmar el firmante	Ver apartado 3.1.1.1		
				(b)2. ContentRelatedConstraintsAsPartOfSignatureElements: Conjunto de restricciones que establece que propiedades deben ser o no ser firmadas: **(b)2.1 MandatedSignedQProperties-DataObjetFormat** Requiere un formato específico para el contenido que firma el firmante. **(b)2.2 MandatedSignedQProperties-content-hints** Requerimientos específicos de información que es encapsulado en el objeto de datos, siendo el conjunto firmado. **(b)2.3 MandatedSignedQProperties-content-reference** Para requerir la incorporación de información, de forma tal que vincula la solicitud y respuesta de mensaje en un intercambio entre dos partes, u otras formas de enlaces. **(b)2.4 MandatedSignedQProperties-content-identifier** Para requerir la presencia de un valor específico de un identificador que puede sr utilizado como atributo de calificación firmada “content-reference”.	Ver apartado 3.1.2		
				(b)3. DOTBSAsAWholeOrInParts: Esta restricción indica si todos los datos o solo una parte de ellos tiene que ser firmado. Se define de la siguiente manera: - entero : todos los datos deben estar firmados; - partes : solo se deben firmar determinadas partes de los datos. En este supuso se debe utilizar información adicional para expresar qué partes tienen para ser firmadas. .	Ver apartado 3.1.2		

BSP	BSP título	Resumen declaración negocio	Contraparte declaración técnica	Restricción (es)	Valor de restricción en la creación de la firma (SCA o DA)	Valor de restricción en el aumento de firmas (SCA, SVA o DA)	Valor de restricción en la validación de la firma (SVA o DA)
(c)	Relación Entre DTBS y firma			**(c)1. BulkSigningRelevance:** Esta restricción indica el requisito de referenciar datos firmados mediante mecanismos automatizados, en especial para firmas masivas. O bien, por el contrario a su prohibición. Los valores utilizados para expresar dichos requisitos son: **(c)1.1 mandatedBulkSigning** **(c) 1.2 prohibidoBulkSigning.**	Ver apartado 2.3.1 m)		
				(c)2. ConstraintsOnTheNumberOfDOTBS: Este requisito indica el número de objetos de datos que una firma puede firmar. La semántica para expresar un posible conjunto de valores se define de la siguiente manera minValue {<, ≤ , =} x {=, ≥, >} maxValue	Ver apartado 2.3.1 m)		
				(c) 3. SignatureRelativePosition: Este requisito indica la posición relativa de la firma y los datos firmados. Para expresar dichos requisitos se definen como sigue: • implícita; • enveloped; • enveloping	Ver apartado 3.1.3.1		
				(c)4. MandatedSignatureFormat: El formato de firma obligatorio determina el formato y nivel de firma requeridos.	Ver apartado 3.1.3		
(d)	Dirigido a la comunidad			**(d)1. TargetedCommunityConstraints:** Este conjunto de restricciones identifica la comunidad a la que cada documento y su (s) firma (s) está (n) dirigida e indica los requisitos en esa comunidad. EJEMPLO: Estas reglas, por ejemplo, pueden establecer las condiciones en las que se puede confiar en una determinada firma, o incluir disposiciones relativas a la eficacia prevista de firmas, donde se requieren varias firmas.	Ver apartado 2.3.1		

BSP	BSP título	Resumen declaración negocio	Contrapart e declaración técnica	Restricción (es)	Valor de restricción en la creación de la firma (SCA o DA)	Valor de restricción en el aumento de firmas (SCA, SVA o DA)	Valor de restricción en la validación de la firma (SVA o DA)
(e)	Asignación de responsabilidad para validación y aumento			**(e)1. ValidationRequiredBeforeAugmenting:** Esta restricción indica si se requiere validación antes de aumentar una firma a un nivel superior, expresado como boolean.		Política OID 1.3.6.1.4.1.18332.61	
				(e)2. AugmentToLevel: Esta restricción indica el nivel del formato de firma que debe alcanzarse después de haber aumentado una firma.		Política OID 1.3.6.1.4.1.18332.61	
(f)	Legal type			**(f)1. ConstraintsOnCertificateMetadata:** Este conjunto de restricciones indica requisitos sobre certificados específicos. Semántica se define como sigue:: **(f)1.1. LegalPersonSignerRequired:** El sujeto identificado en el certificado del firmante tiene que ser una persona jurídica, expresado como boolean. **(f)1.2. LegalPersonSignerAllowed:** El sujeto identificado en el certificado del firmante puede ser una persona jurídica, expresado como boolean. Se asumen el conjunto de restricciones del Anexo C ETSI TS 119 172-1, cuya semántica se aplica al contexto de la legislación UE.	Ver apartado 2		

(g)	Commitment type			**(g)1. CommitmentTypesRequired:** Establece el conjunto de los valores requeridos para el compromiso expresado por el firmante y si esta expresión es requerida para ser parte de las propiedades de la firma. La semántica es:: **(g)1.1. MandatedSignedQProperties-commitment-type-indication:** Esta restricción indica si la expresión del compromiso por el firmante debe ser parte de las propiedades calificadas firmadas; expresado como *boolean*. **(g)1.2. MandatedCommitmentTypeValues:** Esta restricción indica los posibles valores requeridos para el tipo de compromiso que se va a expresar por el firmante. La semántica se define de la siguiente manera: • **MatchingValuesIndicator:** forma en que se hacen coincidir los valores del tipo de compromiso en la firma, contra los posibles valores de compromiso requeridos. Puede tener los siguientes valores: – "todos" si se deben cumplir todos los valores; – "atLeastOne" si se debe cumplir al menos uno de los valores; – "ninguno" si no se cumplen todos los valores. • **CommitmentTypeValues**: una secuencia de compromiso no vacía que reseña identificadores de tipo (OID o URI), asociados a su descripción.	Ver apartado 3.2.2		

(h)	Nivel de seguridad sincronización de evidencias			**(h)1. LoAOnTimingEvidences:** Este conjunto de restricciones indica el nivel de garantía requerido (LoA) en la evidencia de timpo. La semántica se define como sigue: **(h)1.1. LoA-on-signing-time:** Esta restricción indica el LoA requerido en la firma del tiempo. **(h)1.2. LoA-on-content-time-stamp:** indica el LoA requerido en el contenido del sello de tiempo. **(h)1.3. LoA-on-signature-time-stamp:** indica el LoA requerido en la firma del sello de tiempo. **(h)1.4. LoA-on-archival-time-stamp:** indica el LoA requerido en el archivo del sello de tiempo. **(h)1.5. LoA-on-time-in-OCSP-response:** indica el LoA requerido en el tiempo expresado en la respuesta OCSP. **(h)1.6. LoA-on-time-in-CRL:** indica la LoA requerida en el tiempo expresado en la CRL.	Ver apartado 3.2.3		
(i)	Formalities of signing			**(i)1. WYSIWYSRequired:** Indica el requisito de tener un "lo que ves es lo que usted firma "; expresado como un boolean.	Ver apartado 3.2.4		

				(i)2. WYSIWHBSRequired: Indica el requisito de tener un "lo que ves es lo que ha sido firmado"; expresado como un boolean.	Ver apartado 3.2.4		
				(i)3. ProperAdviceAndInformationRequired: Indica si se requiere proporcionar al usuario (firmante o verificador) asesoramiento y la información adecuada sobre la creación de la firma, proceso de solicitud y sobre las consecuencias legales, así como una interfaz de usuario que garantiza, en la medida de lo posible, una firma legal válida con plenas garantías de consentimiento y voluntad; expresado como boolean.	Ver apartado 3.2.4		
				(i)4. UserInterfaceDesignConstraints: Indica si es necesario diseñar la interfaz de usuario para cumplir los requisitos de garantía expresados en la cláusula 3.2.4; expresado como boolean.	Ver apartado 3.2.4		

BSP	BSP título	Resumen declaración negocio	Contraparte declaración técnica	Restricción(es)	Valor de restricción en la creación de la firma (SCA o DA)	Valor de restricción en el aumento de firmas (SCA, SVA o DA)	Valor de restricción en la validación de la firma (SVA o DA)
				(i)5. CorrectValidationAndArchivalProcedures: Esta restricción indica si el SCA y el SVA deben mostrar a la parte que confía (*incluido el firmante*) los procedimientos correctos para la validación y el archivo de la firma y los datos de validación asociados; expresado como una tupla hecha de un boolean y un cadena de caracteres opcional.	Ver apartado 3.2.4		
(j)	Longevidad y resilencia			**(j)1. LoAOnLongevityAndResilience:** Esta restricción indica el LoA requerido sobre la longevidad y resistencia que la evidencia proporcionada por la firma.	Ver apartado 3.2.5		
(k)	Archivo			**(k)1. ArchivalConstraints:** Esta restricción indica los requisitos con respecto al archivo de lafirma y los datos de validación asociados.	Ver apartado 3.2.6		
(l)	Identidad y atributos de rol del firmante			**(l)1. ConstraintsOnCertificateMetadata-LegalPersonSignerRequired:** El sujeto identificado en el certificado del firmante tiene que ser una persona jurídica, expresado como boolean.	Ver apartado 2		

				(I)2. ConstraintsOnCertificateMetadata-LegalPersonSignerAllowed: El sujeto identificado en el certificado del firmante puede ser una persona jurídica, expresado como boolean.	Ver apartado 2		
				(I) 3. MandatedSignedQProperties-signer-attributes: Esta restricción indica si el firmante debe de tener una calificación. El atributo es obligatorio y las restricciones asociadas a los atributos necesarias. Esto se puede expresar como una tupla hecha de un booleano asociado con una secuencia de identificadores que expresan restricciones sobre los atributos requeridos del firmante. Dichas restricciones sobre los atributos o roles del firmante pueden cubrir: • qué roles / atributos son obligatorios; • identificación de los roles / atributos que necesitan ser certificados o estar presente dentro de afirmaciones firmadas; • restricciones sobre el tipo de roles / atributos; y • restricciones sobre los valores de roles / atributos. Cuando sea necesario esta restricción puede usarse para expresar si es requerido un atributo y los requisitos asociados.	Ver apartado 3.3.1		
				(I) 4. NameConstraints: Estas restricciones indican requisitos sobre los nombres distinguidos para certificados emitidos (*p. ej., al firmante, CA, respondedores OCSP, emisores de CRL,Unidades de Sellado de Tiempo*) como se define en IETF RFC 5280.	Ver apartado 3.3.2		

BSP	BSP título	Resumen declaración negocio	Contraparte declaración técnica	Restricción(es)	Valor de restricción en la creación de la firma (SCA o DA)	Valor de restricción en el aumento de firmas (SCA, SVA o DA)	Valor de restricción en la validación de la firma (SVA o DA)
(m)	LoA sobre autenticación de firmante			**1. X509CertificateValidationConstraints:** este conjunto de restricciones indica los requisitos para realizar el proceso de validación de la ruta de certificación conforme IETF RFC 5280. Estas restricciones pueden ser diferentes para diferentes tipos de certificados (por ejemplo, certificados emitidos al firmante, a las CA, a respondedores OCSP, emisores de CRL, unidades de sellado de tiempo). La semántica es como sigue: • **(m)1.1. SetOfTrustAnchors:** esta restricción indica un conjunto de jerarquías de confianza aceptables (TA) como una restricción para el proceso validación. Tales TA deben proporcionarse en forma de certificados autofirmados (certificado raíz) (cláusula	Ver apartado 3.3.2		

				6.1.1 de IETF RFC 5280) y un tiempo hasta que estas jerarquías de confianza se consideraron fiables. P.ej.: El conjunto de TA se puede proporcionar bajo la forma de: - Puntos de confianza especificados en las políticas de validación de firmas; - Conjuntos de CA confiables, por ejemplo, representados por sus certificados raíz almacenados en el entorno (como el store de Windows o Mozilla); - listas de estado del servicio de confianza; - Listas de confianza UE como se define en eIDAS. • **(m)1.2. CertificationPath:** esta restricción indica una ruta certificación requerida para ser utilizada por la SVA para la validación de la firma. La ruta del certificado tiene una longitud 'n' desde el ancla de confianza (TA) hacia abajo al certificado utilizado para validar un objeto firmado (por ejemplo, el certificado con sello de tiempo). Esta restricción puede incluir el camino a considerar o indicar la necesidad de considerar la ruta proporcionada en la firma, si la hubiera. • **(m)1.3. user-initial-policy-set:** esta restricción es como se describe en IETF RFC 5280 cláusula 6.1.1 punto (c). • **(m)1.4. initial-policy-mapping-inhibit:** esta restricción es como se describe en IETF RFC 5280 cláusula 6.1.1 punto (e). • **(m)1.5. initial-explicit-policy:** esta restricción es como se describe en IETF RFC 5280 cláusula 6.1.1 punto (f). • **(m)1.6. initial-any-policy-inhibit:** esta restricción es como se describe en IETF RFC 5280 cláusula 6.1.1 punto (g). • **(m)1.7. initial-permitted-subtrees:** esta restricción es como se describe en IETF RFC 5280 cláusula 6.1.1 punto (h). • **(m)1.8. initial-excluded-subtrees:** esta restricción es como se describe en IETF RFC 5280 cláusula 6.1.1 punto (i). • **(m)1.9. path-length-constraints:** indica restricciones sobre el número de certificados de CA en una ruta de certificación. Esto puede necesitar definir valores iniciales o manejar tal restricción de manera diferente (por ejemplo, ignórela).			

BSP	BSP título	Resumen declaración negocio	Contraparte declaración técnica	Restricción(es)	Valor de restricción en la creación de la firma (SCA o DA)	Valor de restricción en el aumento de firmas (SCA, SVA o DA)	Valor de restricción en la validación de la firma (SVA o DA)
				• **(m)1.10. policy-constraints:** esta restricción indica requisitos para las políticas de certificación a las que se hace referencia en los certificados. Esto puede necesitar definir valores iniciales para esto o manejar la restricción de manera diferente (*por ejemplo, ignórelo*) . Esto también debería permitir la capacidad de requerir una extensión de política de certificación de entidad final.	Ver apartado 3.3.2		

				(m) **2. RevocationConstraints:** Este conjunto de restricciones indica los requisitos aplicables al verificar el estado de validez del certificado y de los certificados que forman la ruta de certificación. Estas restricciones pueden ser diferentes para diferentes tipos de certificado (*por ejemplo, certificados emitidos al firmante, a las CA, a OCSP respondedores, emisores de CRL, unidades de sellado de tiempo*). La semántica es como sigue • **(m)2.1. RevocationCheckingConstraints: i**ndica los requisitos para verificar la revocación del certificado. Tallas restricciones pueden especificar si la verificación de revocación es necesaria o no y si se deben utilizar respuestas OCSP o CRL. Semántica para un posible conjunto de valores es la siguiente manera: – **clrCheck:** Se realizarán comprobaciones contra las CRL actuales (o Listas de revocación de autoridad); – **ocspCheck:** El estado de revocación se comprobará mediante OCSP IETF RFC 6960; – **bothCheck:** Se llevarán a cabo controles OCSP y CRL; – **eitherCheck:** Se realizarán controles OCSP o CRL; – **noCheck:** No se requiere verificación. • **(m)2.2. RevocationFreshnessConstraints:** Esta restricción indica los requisitos de tiempo en la información de revocación. Las restricciones pueden indicar la diferencia máxima aceptada entre la fecha de emisión de la información sobre el estado de revocación de un certificado y el momento de la validación, o requerir que la SVA solo acepta información de revocación emitida un cierto tiempo después de la se ha creado la firma. • **(m)2.3. RevocationInfoOnExpiredCerts:** esta restricción exige que el certificado del firmante sea emitido por una autoridad de certificación que mantiene los avisos de revocación certificados incluso después de que hayan expirado.	Ver apartado 3.3.2		

BSP	BSP título	Resumen declaración negocio	Contraparte declaración técnica	Restricción(es)	Valor de restricción en la creación de la firma (SCA o DA)	Valor de restricción en el aumento de firmas (SCA, SVA o DA)	Valor de restricción en la validación de la firma (SVA o DA)
				(m)3. LoAOnTSPPractices: Esta restricción indica la LoA requerida sobre las prácticas implementadas por el TSP que ha emitido los certificados, es decir, los certificados presentes en la ruta del certificado del firmante y, opcionalmente, los presentes en todos o algunas de las otras cadenas de certificados validadas.			
(n)	Signature Creation Devices			**(n)1. LoAOnSCD:** Esta restricción indica la LoA requerida en el dispositivo de creación de firmas en que reside en la clave privada, es decir, los certificados presentes en la ruta del certificado del certificado del firmante y, opcionalmente, aquellos certificados presentes en todas o algunas de las otras cadenas de certificados validados.	Ver apartado 3.3.2		
(o)	Other information to be associated with signatures			**(o)1. MandatedSignedQProperties-signer-location:** Esta restricción indica que la ubicación del firmante debe expresarse como una propiedad calificada firmada y además puede expresar restricciones sobre el valor.	Ver apartado 3.3.2		
				(o)2. MandatedUnsignedQProperties-signature-policy-extension: Esta restricción indica que la extensión de la política de firmas es necesaria como propiedad calificada no firmada y, además, puede expresar restricciones sobre los valores.	Ver apartado 3.3.2		
				(o)3. MandatedUnsignedQProperties-signature-policy-inclusion-in-archival-form: Esta restricción indica el requisito de incluir la política de firmas como parte de la propiedad calificada sin firmar correspondiente.	Ver apartado 3.3.2		
(p)	Cryptographic suites			**(p)1. CryptographicSuitesConstraints:** Esta restricción indica requisitos sobre algoritmos y parámetros utilizados al crear firmas o al validar objetos firmados o aumento (*por ejemplo, firma, certificados, CRL,Respuestas OCSP, marcas de tiempo*).	Ver apartado 3.3.2		
(q)	Technological environment			**(q)1. TechnologicalEnvironmentConstraints:** Esta restricción indica los requisitos del entorno tecnológico en el que se procesan las firmas	Ver apartado 3.3.2		

Tabla A.3

(p)1. Restricciones criptográficas				
Tipo de firma	**Identificador de algoritmo**	**Mínimo tamaño de clave de firma**	**Longitud mínima de valor hash**	**Fecha de caducidad**
Firma a validar	Sha256RSA	2048-bit	256-bit	Máximo 5 años
Certificado de firmante	Sha256RSA	2048-bit	256-bit	Máximo 5 años
Certificado CA en una cadena válida	Sha256RSA	2048-bit	256-bit	Máximo 5 años
Time-Stamp Token	Sha256RSA	2048-bit	256-bit	Máximo 5 años
OCSP response	Sha256RSA	2048-bit	256-bit	Máximo 5 años
CRLs	Sha256RSA	2048-bit	256-bit	Máximo 5 años

4.2.2 Restricciones de salida que se utilizarán al validar firmas

Según lo establecido en la Política de Validación de ANF AC OID 1.3.6.1.4.1.18332.56.1.1.

4.2.3 Restricciones de salida que se utilizarán para aumentar firmas

Según lo establecido en la Política del Servicio cualificado de conservación de firmas electrónicas cualificadas y del Servicio cualificado de conservación de sellos electrónicos cualificados de ANF AC OID 1.3.6.1.4.1.18332.61.

5 Otros asuntos comerciales y legales

5.1 Consentimiento para aceptar firmas

No se requiere consentimiento expreso para aceptar firmas electrónicas.

5.2 Condición para confiar en las firmas electrónicas

Previo a confiar en una firma electrónica / sello electrónico, se requiere someterla a un sistema cualificado de validación que esté en conformidad con eIDAS y reconocido en la TSL de la UE.

5.3 Tarifas aplicables

Las tarifas de los servicios de confianza de ANF AC están publicadas en la web corporativa

Https://www.anf.es

5.4 Responsabilidad financiera

Según lo definido en la Declaración de Prácticas de Certificación (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

5.5 Confidencialidad de la información

Según lo definido en la Declaración de Prácticas de Certificación (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

5.6 Privacidad de la información personal

Según lo definido en la Declaración de Prácticas de Certificación (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

5.7 Derechos de propiedad intelectual

Según lo definido en la Declaración de Prácticas de Certificación (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

5.8 Representaciones y garantías

Según lo definido en la Declaración de Prácticas de Certificación (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

5.9 Renuncias de garantías

Según lo definido en la Declaración de Prácticas de Certificación (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

5.10 Limitaciones de responsabilidad

Según lo definido en la Declaración de Prácticas de Certificación (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

5.11 Indemnizaciones

Según lo definido en la Declaración de Prácticas de Certificación (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

5.12 Plazo y terminación

Según lo definido en la Declaración de Prácticas de Certificación (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

5.13 Avisos y comunicaciones individuales con los participantes

Según lo definido en la Declaración de Prácticas de Certificación (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

5.14 Enmiendas

Según lo definido en la Declaración de Prácticas de Certificación (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

5.15 Procedimientos de resolución de disputas

Según lo definido en la Declaración de Prácticas de Certificación (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

5.16 Ley aplicable

Según lo definido en la Declaración de Prácticas de Certificación (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

5.17 Cumplimiento de la ley aplicable

Según lo definido en la Declaración de Prácticas de Certificación (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

6 Auditoría de cumplimiento y otras evaluaciones

6.1 Auditorías de cumplimiento –alcance y periodicidad-

Según lo definido en la Declaración de Prácticas de Certificación (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.