ANEXO I
Política de Firma Electrónica y de Certificados de la Administración General del Estado

Aprobado por el Consejo Superior de Administración Electrónica,
en reunión de la Comisión Permanente de 30 de mayo de 2012

ÍNDICE

1 Consideraciones generales

La Ley 59/2003, de 19 de diciembre, de firma electrónica, define la firma electrónica distinguiendo los siguientes conceptos:

- **Firma electrónica:** *es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.*

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

- **Firma electrónica reconocida:** *es la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.*

Para que una firma electrónica pueda ser considerada firma electrónica avanzada en los términos de la Ley 59/2003 se infieren los siguientes requisitos:

- Identificación: que posibilita garantizar la identidad del firmante de manera única.

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

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

Cuando se firman datos, el firmante indica la aceptación de unas condiciones generales y unas condiciones particulares aplicables a aquella firma electrónica mediante la inclusión de un campo firmado, dentro de la firma, que específica una política explícita o implícita.

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

La finalidad de una política de firma es reforzar la confianza en las transacciones electrónicas a través de una serie de condiciones para un contexto dado, el cual puede ser una transacción determinada, un requisito jurídico o un rol que asuma la parte firmante, entre otros.

Este documento especifica las condiciones generales aplicables a la firma electrónica para su validación, en la relación electrónica de la Administración General del Estado (AGE) y sus organismos públicos vinculados o dependientes con los ciudadanos y entre los órganos y entidades de la AGE y sus organismos públicos vinculados o dependientes.

1.1 Objeto del documento

La política de firma electrónica y certificados de la AGE tiene por objeto establecer el conjunto de criterios comunes asumidos por dicha Administración y sus organismos públicos vinculados o dependientes, en relación con la autenticación y la firma electrónica, que afecta a las relaciones de esta Administración con los ciudadanos y entre sus distintos órganos, según lo previsto en el artículo 24.1 del Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

En general, una política de firma electrónica es un documento legal que contiene una serie de normas relativas a la firma electrónica, organizadas alrededor de los conceptos de generación y validación de firma, en un contexto particular (contractual, jurídico, legal,…), definiendo las reglas y obligaciones de todos los actores involucrados en dicho proceso. El objetivo de este proceso es determinar la validez de la firma electrónica para una transacción en particular, especificando la información que deberá incluir el firmante en el proceso de generación de la firma, y la información que deberá comprobar el verificador en el proceso de validación de la misma.

1.2 Ámbito de aplicación

Este documento se circunscribe a los certificados previstos en la Ley 11/2007 expedidos para su empleo por la AGE y los organismos públicos vinculados o dependientes de ésta y a los sistemas de firma electrónica basados en certificados recogidos en el artículo 10.1 y 10.2 del Real Decreto 1671/2009.

La política presenta una estructura normalizada del documento electrónico en relación con la creación y validación de firma electrónica, según los estándares técnicos europeos, para facilitar la interoperabilidad de estos documentos, describiendo el alcance y uso de la firma electrónica con la intención de cumplir las condiciones para una transacción concreta en el contexto de las relaciones con los ciudadanos y entre las Administraciones Públicas.

1.3 Referencias

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

- ETSI TS 101 733, v.1.6.3, v1.7.4 y v.1.8.1. Electronic Signatures and Infrastructures (SEI); CMS Advanced Electronic Signatures (CAdES).

- ETSI TS 101 903, v.1.2.2, v.1.3.2 y 1.4.1. Electronic Signatures and Infrastructures (SEI); XML Advanced Electronic Signatures (XAdES).

- ETSI TS 102 778, v 1.2.1. Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview, Part 2: PAdES Basic - Profile based on ISO 32000-1, Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles; Part 4: Long-term validation.

- ETSI TS 102 176-1 V2.0.0 Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms.

- ETSI TS 102 023, v.1.2.1 y v.1.2.2. Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.

- ETSI TS 101 861 V1.3.1 Time stamping profile.

- ETSI TR 102 038, v.1.1.1. Electronic Signatures and Infrastructures (SEI); XML format for signature policies.

- ETSI TR 102 041, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policies report.

- ETSI TR 102 045, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policy for extended business model.

- ETSI TR 102 272, v.1.1.1. Electronic Signatures and Infrastructures (SEI); ASN.1 format for signature policies.

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

- IETF RFC 3125, Electronic Signature Policies.

- IETF RFC 3161 actualizada por RFC 5816, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).

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

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

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

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

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

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

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

- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.

- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

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

- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

- Ley Orgánica 15/1999, de 13 de diciembre, de protección de los datos de carácter personal.

- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

- Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de propiedad intelectual.

- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.

- Descripción de los perfiles de certificados de la Ley 11/2007, de 22 de junio, que estarán asociados a esta política de firma: Perfiles de certificados en su última versión disponible

- Decisión de la Comisión Europea 130/ 2011, de 25 de febrero, que establece unos requisitos mínimos para el tratamiento transfronterizo de documentos firmados electrónicamente por las autoridades competentes bajo la Directiva 123/ 2006 relativa a los servicios en el mercado interior.

- Resolución de la Secretaria de Estado de Función Pública del 19 de julio de 2011 por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados de la Administración.

2 La política de firma electrónica

2.1 Alcance de la política de firma

Este documento propone una política de firma electrónica, que detalla las condiciones generales para la validación de la firma electrónica y una relación de formatos de objetos binarios y ficheros de referencia que deberán ser admitidos por todas las plataformas implicadas en las relaciones electrónicas de la Administración con los ciudadanos y con las Administraciones Públicas.

Esta política marco es de aplicación a toda la Administración General del Estado, y puede convivir junto con otras políticas particulares para una transacción determinada en un contexto concreto, siempre basadas en dicha política marco.

Para su identificación univoca, la política de firma dispondrá de un identificador único que podrá ser un OID en ASN.1 o una URI (URL o URN) en XML. Tanto el OID o la URI deberá incluirse obligatoriamente en la firma electrónica, empleando el campo correspondiente para identificar la política marco y la versión con las condiciones generales y específicas de aplicación para su validación, sin perjuicio de lo indicado posteriormente respecto a la posibilidad de acogerse a la modalidad de política implícita.

2.2 Datos identificativos de la política

Se define el identificador de la política de firma de la AGE, con el OID 2.16.724.1.3.1.1.2.x.y, o el urn:oid: 2.16.724.1.3.1.1.2.x.y Se asignaran identificadores únicos (x.y) para distinguir las versiones sucesivas. También se asignaran identificadores a los distintos formatos de representación (formato legible de PDF, representación en sintaxis XML y representación en sintaxis ASN.1 siguiendo los estándares).

La presente política de firma y las políticas de firmas particulares de cada organismo basadas en esta política marco deberán estar disponibles en formato legible, de modo que puedan ser aplicadas en un contexto concreto para cumplir con los requerimientos de creación y validación de firma electrónica.

Las políticas particulares harán referencia al OID y la URL de la política marco de firma electrónica en la que se inscriben, con indicación expresa de la versión.

Para facilitar el procesado automático de la firma electrónica, la política de firma deberá implementarse a su vez en un formato que pueda ser interpretado y procesado automáticamente por los sistemas encargados de la creación y validación de la firma electrónica. Se recomienda que esté disponible al menos en formato “xml”, de acuerdo con el estándar **ETSI TR 102 038**, o en formato “ASN.1”, siguiendo el estándar **ETSI TR 102 272**.

2.3 Actores involucrados en la firma electrónica

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

- Firmante: persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.

- Verificador: entidad, ya sea persona física o legal, que valida o verifica una firma electrónica apoyándose en las condiciones exigidas por una política de firma concreta. Puede ser una entidad de validación de confianza o una tercera parte que esté interesada en la validez de una firma electrónica.

- Prestador de servicios de firma electrónica: la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.

- Emisor de la política de firma: entidad que se encarga de generar y gestionar el documento de política de firma, por el cual se deben regir el firmante y el verificador en los procesos de generación y validación de la firma electrónica.

2.4 Gestión de la política de firma

El mantenimiento, actualización y publicación electrónica del presente documento corresponderá a la Comisión Permanente del Consejo Superior de la Administración Electrónica (CP-CSAE) previo estudio del grupo de trabajo permanente constituido por la unidad competente en la normativa de firma electrónica del Ministerio de Industria, Energía y Turismo y la unidad competente en materia de política de firma del Ministerio de Hacienda y Administraciones Públicas. Los cambios a la política marco serán consensuados con las partes implicadas, así como el periodo de tiempo transitorio para la adaptación de las plataformas a la nueva política marco.

El Consejo Superior de la Administración Electrónica mantendrá, en los portales destinados a tal función (sede del Punto de acceso general de la Administración General del Estado, Portal del CTT), tanto la versión actualizada del presente documento como un repositorio con el historial de las versiones anteriores de la política de firma electrónica.

En el caso de actualización del presente documento, se identificará el lugar donde un validador puede encontrar las versiones anteriores para verificar una firma electrónica anterior a la política vigente.

En el momento de la firma se deberá incluir la referencia del identificador único de la versión del documento de política de firma electrónica sobre el que se ha basado su implementación, el cual determinará las condiciones que debe cumplir la firma electrónica en un momento determinado. El campo destinado para incluir esta referencia será, sólo para el formato AdES_EPES, la etiqueta *SignaturePolicyIdentifier,*

2.5 Archivado y custodia

Para garantizar la fiabilidad de una firma electrónica a lo largo del tiempo, esta deberá ser complementada con la información del estado del certificado asociado en el momento en que la misma se produjo y/o información no repudiable incorporando un sello de tiempo, así como los certificados que conforman la cadena de confianza.

Esto implica que si queremos tener una firma que pueda ser validada a lo largo del tiempo, la firma electrónica que se genera ha de incluir evidencias de su validez para que no pueda ser repudiada. Para este tipo de firmas deberá existir un servicio que mantenga dichas evidencias, y será necesario solicitar la actualización de las firmas antes de que las claves y el material criptográfico asociado sean vulnerables.

Las condiciones que se deberán dar para considerar una firma electrónica longeva son las siguientes:

1. En primer lugar, deberá verificarse la firma electrónica producida o verificada, validando la integridad de la firma, el cumplimiento de los estándares XAdES, CAdES o PAdES, y las referencias.

2. Deberá realizarse un proceso de completado de la firma electrónica, consistente en lo siguiente:

    a. Obtener las referencias a los certificados, así como almacenar los certificados del firmante.

    b. Obtener las referencias a las informaciones de estado de los certificados, como las listas de revocación de certificados (CRLs) o las respuestas OCSP, así como almacenarlas.

3. Al menos, deben sellarse las referencias a los certificados y a las informaciones de estado.

El almacenamiento de los certificados y las informaciones de estado podrá realizarse dentro del documento resultante de la firma electrónica o en un depósito específico:

- en caso de almacenar los certificados y las informaciones de estado dentro de la firma, se recomienda sellar también estas informaciones, siguiendo las modalidades de firmas AdES –X o -A.
- si los certificados y las informaciones de estado se almacenan en un depósito específico, se recomienda sellarlos de forma independiente.

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

- las plataformas de firma electrónica adoptadas en el ámbito de la AGE deberán disponer de mecanismos de resellado, para añadir, de forma periódica, un sello de fecha y hora de archivo con un algoritmo más resistente.

- la firma electrónica deberá almacenarse en un depósito seguro, garantizando la protección de la firma contra falsificaciones y asegurando la fecha exacta en que se guardó la firma electrónica (las operaciones de fechado se realizarán con marcas de fecha y hora, no siendo necesario su sellado criptográfico).

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

Para el archivado y gestión de documentos electrónicos se seguirán las recomendaciones de las guías técnicas de desarrollo del Esquema Nacional de Interoperabilidad (Real Decreto 4/2010, de 8 de enero).

2.6 Formatos admitidos de firma

El formato de los documentos electrónicos con firma electrónica avanzada, aplicada mediante los certificados electrónicos admitidos por las Administraciones Públicas y utilizados en el ámbito de las relaciones con o dentro de la Administración Pública, se deberá ajustar a las especificaciones de los estándares europeos relativos a los formatos de firma electrónica.

El Consejo Superior de la Administración Electrónica será la Entidad gestora encargada de publicar y actualizar la relación de las especificaciones relativas a los formatos admitidos por la presente política de firma.

Actualmente se consideran formatos admitidos:

- **formato XAdES (XML Advanced Electronic Signatures)**, según especificación técnica ETSI TS 101 903, versión 1.2.2 y versión 1.3.2. Asimismo, se admitirá la última versión 1.4.1 a partir del 31-12-2013. Para versiones posteriores del estándar se analizarán los cambios en la sintaxis y se aprobará la adaptación del perfil a la nueva versión del estándar a través de una adenda a esta política de firma[1].

- **formato CAdES (CMS Advanced Electronic Signatures),** según especificación técnica ETSI TS 101 733, versión 1.6.3 y versión 1.7. Asimismo, se admitirá la última versión 1.8.1 a partir del 31-12-2013. Para versiones posteriores del estándar se analizarán los cambios en la sintaxis y se aprobará la adaptación del perfil a la nueva versión del estándar a través de una adenda a esta política de firma.

- **formato PAdES (PDF Advanced Electronic Signatures),** según especificación técnica ETSI TS 102 778-3, versión 1.2.1 (se admitirán versiones posteriores siempre que no impliquen cambios significativos en la sintaxis de los tags usados en la presente política) y la ETSI TS 102 778-4 para el caso de firmas longevas en PADES (PAdES Long Term). En caso contrario se aprobará la adaptación del perfil a la nueva versión del estándar a través de una adenda a esta política de firma.

[1] A lo largo de este documento se utilizarán los prefijos ds: y xades: para hacer referencia a elementos definidos en los estándares XMLDSig y XAdES, respectivamente.

Este formato amplía las especificaciones del estándar de firma en PDF, añadiendo la información adicional de firma similar a la usada en las firmas CAdES o XADES. La parte 3 del estándar PAdES "PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles" recoge la estructura de las firmas PAdES cuando la firma incluida dentro del documento PDF es de tipo CAdES. Su utilización quedará en todo caso limitada a los documentos con formato PDF y que no van a ser tratados en procesos automatizados. Asimismo, se admitirá como formato de intercambio a partir de 31 de diciembre de 2013.

Se tendrá en cuenta la legislación Europea en relación a los formatos de firma admitidos en la Unión Europea, en especial aquellos definidos en los estándares europeos de firma electrónica y por tanto deberá ser actualizada según evolucionen dichas normas Europeas.

Dentro de las distintas clases de los formatos XAdES, CAdES y PAdES, los órganos y unidades administrativas de la Administración Pública deberán adecuar sus sistemas para la generación de, al menos, la clase básica de uno de estos formatos de firma electrónica, añadiendo información sobre la política de firma (clase EPES), y la verificación de las especificaciones de la clase básica de todos estos formatos.

La clase básica de firma electrónica para definir **una política de firma electrónica de interoperabilidad** es, según los estándares AdES, **la clase EPES.** A partir de este formato básico EPES es posible incluir suficiente información para validar la firma a largo plazo.

Si fuera necesario generar firmas con validación a largo plazo, se debería implementar un formato que incorporase propiedades adicionales, como información sobre revocación de certificados.

2.7 Creación de la firma electrónica

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

1. El usuario puede seleccionar un fichero, formulario u otro objeto binario para ser firmado (ver Anexo2 para saber los formatos de ficheros que deberán ser admitidos por las distintas plataformas). En el caso de firma de formulario, se le suele presentar al usuario el objeto binario a ser firmado, sin necesidad de selección previa.

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

    a. Si la firma electrónica puede ser validada para el formato del fichero específico que vaya a ser firmado, según la presente política o su política de firma particular correspondiente.
    b. Si los certificados han sido expedidos bajo una Declaración de Políticas de Certificación específica.
    c. Comprobación de la validez del certificado: si el certificado ha sido revocado, o suspendido, si entra dentro del periodo de validez del certificado, y la validación

de la cadena de certificación (incluidos la validación de todos los certificados en la cadena).

Si no se pueden realizar estas comprobaciones en el momento de la firma (por ejemplo para firmas en cliente sin acceso a servidor), en todo caso será necesario que los sistemas lo comprueben antes de aceptar el fichero, formulario u otro objeto binario firmado.

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

El servicio creará un fichero en formato XAdES,CAdES o PAdES para aquellos escenarios en los que sea conveniente.

Se recomienda que el fichero resultante tenga una extensión única de forma que los visores de documentos firmados puedan asociarse a esa extensión, haciendo más fácil al usuario el manejo de este tipo de ficheros. Esta extensión podría ser:

- ".xsig", si la firma implementada se ha realizado según el estándar XAdES
- ".csig", si la firma implementada se ha realizado según el estándar CAdES

En el caso de las firmas PAdES, al estar la firma incluida en un documento PDF, la extensión será aquella del formato PDF original.

2.8 Verificación de la firma electrónica

El verificador puede utilizar cualquier método para verificar la firma creada según la presente política. Las condiciones mínimas que se deberán producir para validar la firma serán las siguientes:

1. Garantía de que la firma es válida para el fichero específico que está firmado.

2. Validez de los certificados en el momento en que se produjo la firma, si los servicios de los prestadores facilitan los históricos de estado de los certificados, o en caso contrario, validez de los certificados en el momento de la validación: certificados no revocados, suspendidos, o que hayan expirado, y la validación de la cadena de certificación (incluida la validación de todos los certificados de la cadena). Esta información puede estar contenida en la propia firma en el caso de las firmas longevas.

3. Certificado expedido bajo una Declaración de Prácticas de Certificación específica.

4. Verificación, si existen y si así lo requiere la plataforma de relación electrónica o un servicio concreto de dicha plataforma, de los sellos de tiempo de los formatos implementados, incluyendo la verificación de los periodos de validez de los sellos.

3 Política de validación de firma electrónica

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

3.1 Identificación del documento

Nombre del documento	Política general de firma electrónica
Versión	1.9
Identificador de la Política (OID)[2]	OID 2.16.724.1.3.1.1.2.1.9
URI de referencia de la Política	En el Punto de acceso general de la Administración General del Estado. También disponible en: http://administracionelectronica.gob.es/es/ctt/politicafirma
Fecha de expedición	19 de noviembre de 2012
Ámbito de aplicación	Administración General del Estado

3.2 Periodo de validez

La presente Política de Firma Electrónica es válida desde la fecha de expedición del apartado anterior hasta la publicación de una nueva versión actualizada, pudiéndose facilitar un periodo de tiempo transitorio, en el cual convivan las dos versiones, que permita adecuar las diferentes plataformas de las administraciones públicas a las especificaciones de la nueva versión. Este periodo de tiempo transitorio deberá indicarse en la nueva versión, pasado el cual sólo será válida la versión actualizada.

3.3 Identificación del gestor del documento

Nombre del gestor de la política	CSAE - Ministerio de Hacienda y Administraciones Públicas
Dirección de contacto	Dirección postal: María de Molina, 50 Madrid 28071 ES

[2] Los dos últimos dígitos del identificador definirán las diferentes versiones de la política de firma.

3.4 Reglas comunes

Las reglas comunes para los actores involucrados en la firma electrónica, firmante y verificador, son un campo obligatorio que debe aparecer en cualquier política de firma. Permiten establecer responsabilidades respecto a la firma electrónica sobre la persona o entidad que crea la firma y la persona o entidad que la verifica, definiendo los requisitos mínimos que deben presentarse, debiendo estar firmados, si son requisitos para el firmante, o no firmados, si son requisitos para el verificador.

3.4.1 Reglas del firmante

El firmante se hará responsable de que el fichero que se quiere firmar no contiene contenido dinámico que pudiese modificar el resultado de la firma durante el tiempo. Si el fichero que se quiere firmar no ha sido creado por el firmante, deberá asegurarse que no existe contenido dinámico dentro del fichero, como pueden ser macros.

Formato XAdES

- La versión de XAdES contemplada en esta política, es la versión 1.3.2, siendo válidas implementaciones según la versión 1.2.2. teniéndose especial cuidado en indicar en todo momento la versión que se esté utilizando en tags en los que se hace referencia al número de versión.

En el ***anexo 1*** se detalla la estructura básica que debe tener una firma electrónica para poder ser considerada válida por el verificador.

- Para facilitar la interoperabilidad de los sistemas de información que manejan estos documentos firmados electrónicamente, en la generación de firmas XAdES **se propone** la siguiente estructura de fichero XML, en la cual se genera un único fichero resultante que contiene el documento original, codificado en base64[3], y las firmas, encontrándose al mismo nivel XML lo firmado y la firma, es decir el modo internally detached.

```
<documento>
  <documentoOriginal Id="original" encoding="base64" nombreFichero=nombreFichOriginal">
  ...
  </documentoOriginal>
  <ds:Signature>
        <ds:SignedInfo/>
              ...
              <ds:Reference URI="#original">
              </ds:Reference>
              ...
        </ds:SignedInfo>
  ...
  </ds:Signature>
</documento>
```

[3] Si el formato del documento original fuese un fichero que contenga sólo texto (fichero XML), no sería precisa su codificación en base64.

Asimismo, se admitirán las firmas XADES enveloped. En el caso de **factura electrónica** se acuerda asumir el modo actualmente implementado, mientras se evoluciona a un formato europeo, de acuerdo con el formato Facturae regulado en la Orden PRE/2971/2007; es decir, la firma se considera un campo más a añadir en el documento de factura.

- El firmante deberá proporcionar, como mínimo, la información contenida en las siguientes etiquetas dentro del campo ***SignedProperties*** (campo que contiene una serie de propiedades conjuntamente firmadas a la hora de la generación de la firma XMLDsig), las cuales son de **carácter obligatorio**:

  - *SigningTime*: indica la fecha y la hora. En el caso de firma en cliente sin acceder a servidor, será meramente indicativa (pues la fecha en el dispositivo cliente es fácilmente manipulable) y/o será utilizada con fines distintos a conocer la fecha y hora de firma. Las políticas particulares de firma electrónica **podrán determinar** características y restricciones **particulares** respecto a generación en cliente de las referencias temporales y sincronización del reloj.

  - *SigningCertificate*: contiene referencias a los certificados y algoritmos de seguridad utilizados para cada certificado. Este elemento deberá ser firmado con objeto de evitar la posibilidad de sustitución del certificado.

  - *SignaturePolicyIdentifier*: identifica la política de firma sobre la que se basa el proceso de generación de firma electrónica, y debe incluir los siguientes contenidos en los elementos en que se subdivide:

    - Una referencia explícita al presente documento de política de firma, o en su caso, al documento de política de firma particular de cada organismo, en el elemento *xades:SigPolicyId*. Para ello, aparecerá el OID que identifique la versión concreta de la política de firma o la URL de su localización.

      ```
      <xades:SigPolicyId>
          <xades:Identifier> ... </xades:Identifier>
      ```

    - La huella digital del documento de política de firma correspondiente y el algoritmo utilizado, en el elemento *<xades:SigPolicyHash>,* de manera que el verificador pueda comprobar, calculando a su vez este valor, que la firma está generada según la misma política de firma que se utilizara para su validación.

    - No obstante lo anterior, se admitirá que la firma incluya una referencia implícita a la política de firma siempre que la omisión del identificador de la política no induzca a confusión en cuanto a la política aplicable. En este caso, la política aplicable y su versión deberán poder deducirse a partir de otros campos de la firma como el del firmante y el de la fecha de la firma. Por razones de sencillez en la interoperabilidad, se recomienda que la política se indique siempre mediante una referencia explícita. En todo caso las políticas particulares de firma no podrán referenciarse de forma implícita.

  - La política de firma electrónica particular de cada ministerio, órgano, organismo o entidad pública estatal hará referencia a la URL u OID de la política marco de firma electrónica en la que se inscribe, con indicación expresa de la versión.

- *DataObjectFormat*: define el formato del documento original, y es necesario para que el receptor conozca la forma de visualizar el documento.

- Las etiquetas restantes que pueden agregarse en el campo SignedProperties serán consideradas de **carácter opcional**, sin perjuicio de su consideración obligatoria en políticas particulares, siempre basadas en la política marco:

  - *SignatureProductionPlace*: define el lugar geográfico donde se ha realizado la firma del documento.

    SignerRole: define el rol de la persona en la firma electrónica. Al menos uno de estos elementos ClaimedRoles o CertifiedRoles deben estar presentes en este campo.

  - En el caso de su utilización en una factura en formato Facturae**,** deberá contener uno de los siguientes valores en el campo *ClaimedRoles*:
    - "*supplier"* o "emisor": cuando la firma la realiza el emisor.
    - "*customer*" o "receptor": cuando la firma la realiza el receptor.
    - "*third party*" o "tercero": cuando la firma la realiza una persona o entidad distinta al emisor o al receptor.

  - *CommitmentTypeIndication*: define la acción del firmante sobre el documento firmado (lo aprueba, lo informa, lo recibe, lo certifica, ...).

  - *AllDataObjectsTimeStamp:* contiene un sello de tiempo, calculado antes de la generación de la firma, sobre todos los elementos contenidos en *ds:Reference*.

  - *IndividualDataObjectsTimeStamp:* contiene un sello de tiempo, calculado antes de la generación de la firma, sobre algunos de los elementos contenidos en *ds:Reference*.

- También se permitirá el uso de certificados de atributos para certificar el rol del firmante, en cuyo caso el elemento SignerRole incorporará un elemento CertifiedRoles, que contendrá la codificación en base-64 de uno o varios atributos de certificados del firmante.

- La etiqueta CounterSignature, refrendo de la firma electrónica y que se puede incluir en el campo *UnsignedProperties*, será considerada de **carácter opcional**. Las siguientes firmas, ya sean serie o paralelo, se añadirán según indica el estándar XAdES, según el documento ETSI TS 101 903 v1.3.2 (admitiéndose implementaciones según v1.2.2 y posteriores).

Formato CAdES

- La versión de CAdES empleada en esta política, es la versión 1.7.4, siendo válidas implementaciones según versión 1.6.3, teniéndose especial cuidado en indicar en todo

momento la versión que se esté utilizando en tags en los que se hace referencia al número de versión.

- El estándar CMS presenta distintas alternativas para la estructura del documento electrónico en relación con la firma electrónica. Se adopta el **tipo Signed Data** con los datos incluidos (attached) para la estructura del documento, especificado en los estándares CMS (IETF RCF 5652) y CAdES (ETSI TS 101 733), que mantiene el documento original y la firma en un mismo fichero.

- En el caso de que, debido al tamaño de los datos a firmar, no resulte técnicamente posible o aconsejable realizar las firmas con el formato anteriormente descrito, se generará la estructura de firma detached, que incluye el hash del documento original en la firma.

- Las siguientes etiquetas deberán ser firmadas y son de carácter obligatorio:

    - ***Content-type*****:** esta etiqueta especifica el tipo de contenido que debe ser firmado. Es una etiqueta obligatoria según el estándar CAdES.

    - ***Message-digest*****:** identifica el cifrado del contenido firmado *OCTET STRING* en *encapContentInfo*. Es una etiqueta obligatoria según el estándar CAdES.

    - ***ESS signing-certificate o ESS signing-certificate-v2*****:** es una etiqueta que permite el uso de SHA-1 (sólo para ESS signing-certificate) y la familia de algoritmos SHA-2 como algoritmo de seguridad. Es una etiqueta obligatoria según el estándar CAdES.

    - ***Signing-time*****:** indica la fecha y hora de la firma. En el caso de firma en cliente sin acceder a servidor, será meramente indicativa (pues la fecha en el dispositivo cliente es fácilmente manipulable) y/o será utilizada con fines distintos a conocer la fecha y hora de firma. Las políticas particulares de firma electrónica podrán determinar características y restricciones particulares respecto a generación en cliente de las referencias temporales y sincronización del reloj. Es una etiqueta de carácter obligatorio según está política de firma.

    - ***SignaturePolicyIdentifier*****:** es una etiqueta que indica la política de firma sobre la que se basará la generación de la firma electrónica. El documento deberá incorporar la referencia (OID) a la política de firma particular aplicada y la huella digital del documento de política de firma correspondiente y el algoritmo utilizado, en el elemento *SigPolicyHash,* de manera que el verificador pueda comprobar, calculando a su vez este valor, que la firma está generada según la misma política de firma que se utilizará para su validación.

    - ***Content-hints*****:** describe el formato del documento original, y su función es que el receptor discierna cómo debe visualizar el documento.

- Las siguientes etiquetas deberán ser firmadas y son de carácter opcional, sin perjuicio de que puedan ser considerados obligatorias en políticas particulares:

- ***Content-reference*:** puede ser utilizada como un modo de relacionar una contestación con el mensaje original al que se refiere.

- ***Content-identifier*:** esta etiqueta contiene un identificador que se puede utilizar en el atributo anterior.

- ***Commitment-type-indication*:** este etiqueta indica la acción del firmante sobre el documento firmado (lo aprueba, lo informa, lo recibe, lo certifica, ...).

- ***Signer-location*:** permite indicar el lugar geográfico donde se ha realizado la firma del documento. Al menos uno de estos elementos ClaimedRoles o CertifiedRoles deben estar presentes en esta etiqueta.

- ***Signer-attributes*:** indica el rol de la persona en la firma electrónica.

- ***Content-time-stamp*:** esta etiqueta permite un sello de tiempo, antes de la generación de la firma, sobre los datos que van a ser firmados, para incorporarla con la información firmada.

La etiqueta *CounterSignature*, refrendo de la firma electrónica, incluido en el campo de propiedades no firmadas, será considerada de **carácter opcional**. Las siguientes firmas se añadirán según indica el estándar CAdES, según el documento ETSI TS 101 733 v1.7.3 (admitiéndose implementaciones según v1.6.3 y posteriores).

Formato PAdES

- La versión de PAdES empleada en esta política, es la versión 1.2.1, admitiéndose implementaciones posteriores, siempre que no impliquen cambios significativos en los tags empleados. En ese caso, será necesario actualizar el presente documento de Política de Firma electrónica.

- En la versión actual de la política de firma, solo se considera la posibilidad de utilizar algoritmos RSA para las firmas PAdES.

- *Es necesario incluir la siguiente extensión en el diccionario Catalog.*

  ```
  <</ESIC
  <</BaseVersion /1.7
    /ExtensionLevel 1
  >>
  >>
  ```

  En caso de incluir esta extensión, la firma se detectará como firma longeva (PAdES LTV) aunque no contenga los elementos de revocación.

- Las firmas PAdES se generarán con la estructura CAdES detached

- Los siguientes atributos deberán estar firmados y serán de carácter obligatorio:

- ***Content-type:*** especifica el tipo de contenido que debe ser firmado. Es obligatoria según el estándar PAdES.

- ***Message-digest:*** identifica el cifrado del contenido firmado OCTET STRING en encapContentInfo. Es obligatoria según el estándar PAdES.

- ***ESS signing-certificate o ESS signing-certificate-v2*** es una etiqueta que permite el uso de SHA-1 (sólo para ESS signing-certificate) y la familia de algoritmos SHA-2 como algoritmo de seguridad. Es una etiqueta obligatoria según el estándar PAdES.
- Nunca se debe especificar el campo Cert del diccionario Signature

- ***signature-policy-identifier:*** identifica la política de firma sobre la que se basa el proceso de generación de firma electrónica. El documento deberá incorporar el OID de la política de firma particular aplicada.

- No está permitido el atributo Content-hints

- Nunca se debe especificar el atributo SigningTime. El tiempo de la firma debe indicarse en el campo M en diccionario Signature, un atributo específico del PDF.

- Las siguientes etiquetas son de carácter opcional, sin perjuicio de que puedan ser considerados obligatorias en políticas particulares:

  - ***Commitment-type-indication*****:** este etiqueta indica la acción del firmante sobre el documento firmado (lo aprueba, lo informa, lo recibe, lo certifica, ...). Según el estándar PAdES debería estar indicado en el campo Reason propio del PDF.

  - ***Signer-attributes*****:** indica el rol de la persona en la firma electrónica. Al menos uno de estos elementos ClaimedRoles o CertifiedRoles deben estar presentes en este campo.

  - ***Content-time-stamp*****:** esta etiqueta permite un sello de tiempo, antes de la generación de la firma, sobre los datos que van a ser firmados, para incorporarla con la información firmada.

  - Para el lugar de la firma se utilizará la entrada ***Location*** en el diccionario de firma, en lugar del elemento signer-location mencionado en el epígrafe de CAdES.

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

3.4.2 Reglas del verificador

El formato básico de firma electrónica avanzada no contempla ninguna información de validación más allá del certificado firmante, que se incluye en la etiqueta Signing Certificate, y de la política de firma que se indique en la etiqueta Signature Policy.

Los atributos que podrá utilizar el verificador para comprobar que se cumplen los requisitos de la política de firma según la cual se ha generado la firma, independientemente del formato utilizado (XAdES, CAdES o PAdES), son las siguientes:

- *Signing Time*: sólo se utilizará en la verificación de las firmas electrónicas como indicación para comprobar el estado de los certificados en la fecha señalada, ya que únicamente se puede asegurar las referencias temporales mediante un sello de tiempo (especialmente en el caso de firmas en dispositivos cliente). Si se ha realizado el sellado de tiempo, el sello más antiguo dentro de la estructura de la firma se utilizará para determinar la fecha de la firma.

- *Signing Certificate*: se utilizará para comprobar y verificar el estado del certificado (y, en su caso, la cadena de certificación) en la fecha de la generación de la firma, en el caso que el certificado no estuviese caducado y se pueda acceder a los datos de verificación (CRL, OCSP, etc) o bien en el caso de que el PSC ofrezca un servicio de validación histórico del estado del certificado.

- *Signature Policy*: se deberá comprobar, que la política de firma que se ha utilizado para la generación de la firma se corresponde con la que se debe utilizar para un servicio en cuestión.

Si se han realizado varias firmas del mismo documento, se seguirá el mismo proceso de verificación que con la primera firma, comprobando la etiqueta *Counter Signature* en el campo de propiedades no firmadas, donde se informa de los refrendos de firma generados.

Será responsabilidad del encargado de la verificación de la firma definir sus procesos de validación y de archivado según los requisitos de la política de firma particular a la que se ajusta el servicio.

Existe un tiempo de espera, conocido como periodo de precaución o periodo de gracia, para comprobar el estado de revocación de un certificado. El verificador puede esperar este tiempo para validar la firma o realizarla en el mismo momento y revalidarla después. Esto se debe a que puede existir una pequeña demora desde que el firmante inicia la revocación de un certificado hasta que la información del estado de revocación del certificado se distribuye a los puntos de información correspondientes. Se recomienda que este periodo, desde el momento en que se realiza la firma o el sellado de tiempo sea, como mínimo, el tiempo máximo permitido para el refresco completo de las CRLs o el tiempo máximo de actualización del estado del certificado en el servicio OCSP. Estos tiempos podrán ser variables según el Prestador de Servicios de Certificación.

3.4.3 Reglas para los sellos de tiempo.

El sello de tiempo asegura que los datos, la firma del documento que va a ser sellado o la información del estado de los certificados incluidos en la firma electrónica, se generaron antes de una determinada fecha. El formato del sello de tiempo deberá cumplir las recomendaciones de IETF, RFC 5816, “Internet X.509 Public Key Infrastructure; Time-Stamp Protocol (TSP)”.

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

1. Datos sobre la identidad de la autoridad emisora (identidad jurídica, clave pública a utilizar en la verificación del sello, número de bits de la clave, el algoritmo de firma digital y la función hash utilizados).

2. Tipo de solicitud cursada (si es un valor hash o un documento, cuál es su valor y datos de referencia).

3. Parámetros del secuenciador (valores hash "anterior", "actual" y "siguiente").

4. Fecha y hora UTC.

5. Firma digital de todo lo anterior con la clave pública y esquema de firma digital especificados.

El sellado de tiempo puede ser añadido por el emisor, el receptor o un tercero y se debe incluir como propiedad no firmada en el campo **Signature Time Stamp.**

El sellado de tiempo debe realizarse en un momento próximo a la fecha incluida en el campo ***Signing Time*** y, en cualquier caso, siempre antes de la caducidad del certificado del firmante.

La presente política admite sellos de tiempo expedidos por prestadores de servicios de sellado de tiempo que cumplan las especificaciones técnicas ETSI TS 102 023, “Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities”.

3.4.4 Reglas de confianza para firmas longevas

Los estándares CAdES (ETSI TS 101 733), XAdES (ETSI TS 101 903) y PAdES (ETSI TS 102 778-4) contemplan la posibilidad de incorporar a las firmas electrónicas información adicional para garantizar la validez de una firma a largo plazo, una vez vencido el periodo de validez del certificado. Esta información puede ser incluida tanto por el firmante como por el verificador, y se recomienda hacerlo después de trascurrido el periodo de precaución o periodo de gracia. Existen dos tipos de datos a incluir como información adicional de validación:

- la información del estado del certificado en el momento en que se produce la validación de la firma o una referencia a los mismos.

- certificados que conforman la cadena de confianza.

En el caso de que se deseen generar firmas longevas, se recomienda incluir la información de validación anterior, y añadirle un sello de tiempo. En estos tipos de firma la validez de la firma resultante viene determinada por la duración del sello de tiempo que se añade a la firma longeva.

En el caso que se desee incorporar a la firma la información de validación, se recomienda usar validación mediante OCSP, ya que mediante este método las propiedades o atributos a incluir son de menor tamaño**.**

Si la consulta al estado de validación de la firma se realiza mediante un método que resulta en una información muy voluminosa que aumenta de forma desproporcionada el tamaño de la firma, opcionalmente, en lugar de la información de validación indicada anteriormente, se pueden incluir en la firma longeva referencias a dicha información,

Formato XAdES

Dentro del formato de firma XAdES, el formato extendido XAdES-C incorpora estas entre otras propiedades no firmadas:

- **CompleteCertificateRefs** que contiene referencias a todos los certificados de la cadena de confianza necesaria para verificar la firma, excepto el certificado firmante.

- **CompleteRevocationRefs** que contiene referencias a las CRLs y/o respuestas OCSP usadas en la verificación de los certificados.

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

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

- **CertificateValues,**
- **RevocationValues**

Estas propiedades incluyen, no solo las referencias a la información de validación sino también la cadena de confianza completa y la CRL o respuesta OCSP obtenida en la validación. Para los atributos CertificateValues y Revocation-Values se recomienda hacer la validación por OCSP ya que estos valores pueden ser muy voluminosos en caso de realizar la validación mediante CRL.

En el caso que se desee incorporar a la firma esta información de validación, se recomienda usar el formato **XADES-A**, que añade un sello de tiempo a la información anterior.

Formato CAdES

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

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

El formato CAdES-X Long además de la información incluida en CAdES-C, incluye dos nuevos atributos **certificate-values** y **revocation-values** que incluyen, no solo las referencias a la información de validación sino también la cadena de confianza completa y la CRL o respuesta OCSP obtenida en la validación. Para los atributos CertificateValues y Revocation-Values en las firmas longevas se recomienda hacer la validación por OCSP ya que estos valores pueden ser muy voluminosos en caso de realizar la validación mediante CRL.

Se recomienda usar los siguientes formatos.

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

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

Formato PAdES

Con el fin de permitir el upgrade de firmas a LTV es necesario incluir la siguiente extensión en el diccionario Catalog:

```
<</ESIC

<</BaseVersion /1.7
  /ExtensionLevel 1
>>
>>
```

La validación de firmas LTV implicaría la verificación de esta extensión y la existencia de los atributos requeridos (sellos de tiempo, respuestas OCSP o CRLs y certificados).

Se recomienda usar validación mediante OCSP, ya que el tamaño de la información de validación a añadir será menor.

Se recomienda añadir un sello de tiempo que incluya dicha información de validación, ya que la validez de la firma resultante viene determinada por la duración del sello de tiempo que se añade a la firma longeva.

3.5 Reglas de confianza de certificados de atributos

Esta política de firma no fija ninguna regla específica respecto a los certificados de atributos.

Las políticas de firma particulares de cada organismo o entidad dentro de la Administración Pública, basadas en la presente política marco, podrán fijar reglas específicas para cada uno de los servicios que prestan, siendo necesario cumplir sus requisitos para que la firma sea válida en ese contexto.

3.6 Reglas de uso de algoritmos

Para los entornos de seguridad genérica se tomará la referencia a la URN en la que se publican las funciones de hash y los algoritmos de firma utilizados por las especificaciones XAdES, CAdES y PAdES, como formatos de firma adoptados, de acuerdo con las especificaciones técnicas ETSI TS 102 176-1 sobre “Electronic Signatures and Infraestructures (ESI); Algorithms and parameters for secure electronic signature”. Todo ello sin perjuicio de los criterios que, al respecto, se hayan adoptado en el Esquema Nacional de Seguridad, desarrollado a partir del artículo 42 de la Ley 11/2007, por el Real Decreto 3/2010, de 6 de noviembre.

La presente política admite como válidos los algoritmos de generación de hash, codificación en base64, firma, normalización y transformación definidos en los estándares XMLDSig y CMS.

Para los entornos de alta seguridad, de acuerdo con el criterio del Centro Criptológico Nacional, CCN, serán de aplicación las recomendaciones revisadas de la CCN-STIC 405. Asimismo, para garantizar el cumplimiento del Esquema Nacional de Seguridad, se deberá atender a la recomendación CCN-STIC 807 (“Criptografía de Empleo en el ENS”).

Se podrán utilizar cualquiera de los siguientes algoritmos para la firma electrónica: RSA/SHA 1 (formato que se recomienda reemplazar en el medio plazo por algoritmos más robustos), RSA/SHA256 y RSA/SHA512 que es recomendado para archivado de documentos electrónicos (very long term signatures).

3.7 Reglas específicas de compromisos

Esta política de firma no fija ninguna regla respecto a compromisos específicos.

Las políticas de firma particulares de cada organismo o entidad dentro de la AGE, basadas en la presente política marco, podrán fijar reglas específicas para cada uno de los servicios que prestan, siendo necesario cumplir sus requisitos para que la firma sea válida en ese contexto.

4 Anexo 1: Estructura de la firma electrónica

Este anexo incluye la estructura básica que se deberá seguir para la generación de una firma electrónica:

4.1 Formato de firma electrónica avanzada básico XAdES EPES[4]

```
<ds:Signature ID ? >
   <ds:SignedInfo>
      <ds:CanonicalizationMethod/>
      <ds:SignatureMethod/>
      (<ds:Reference URI ? >
         (<ds:Transforms/>) ?
         <ds:DigestMethod/>
         <ds:DigestValue/>
       </ds:Reference>) +
   </ds:SignedInfo>
   <ds:SignatureValue/>
   (<ds:KeyInfo>) ?
   <ds:Object>
      <QualifyingProperties>
         <SignedProperties>
            <SignedSignatureProperties>
               SigningTime
               SigningCertificate
               SignaturePolicyIdentifier
               (SignatureProductionPlace) ?
               (SignerRole) ?
            </SignedSignatureProperties>
            <SignedDataObjectProperties>
               DataObjectFormat +
               (CommitmentTypeIndication) *
               (AllDataObjectsTimeStamp) *
```

Los símbolos “+”, “?” y “*” significan:

+ significa una o más ocurrencias
? significa cero o una ocurrencia
* significa cero o más ocurrencias

```
                (IndividualDataObjectsTimeStamp) *
            </SignedDataObjectProperties>
        </SignedProperties>
        <UnsignedProperties>
            <UnsignedSignatureProperties>
                (CounterSignature) *
            </UnsignedSignatureProperties>
            <UnSignedDataObjectProperties>
            </UnSignedDataObjectProperties>
        </UnsignedProperties>
    </QualifyingProperties>
  </ds:Object>
</ds:Signature>
```

4.2 Formato de firma electrónica avanzada básico CAdES EPES

```
DEFINITIONS EXPLICIT TAGS ::=

BEGIN

IMPORTS

-- RFC 3852   Cryptographic Message Syntax (CMS)
     ContentInfo, ContentType, id-data, id-signedData, SignedData,
     EncapsulatedContentInfo, SignerInfo, SignedAttributes,
     id-contentType, id-messageDigest, MessageDigest, id-signingTime, SigningTime,
FROM CryptographicMessageSyntax2004   { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-
9(9) smime(16) modules(0) cms-2004(24) }-- RFC 2634   Enhanced Security Services for S/MIME
     id-aa-signingCertificate, SigningCertificate,  IssuerSerial,
     id-aa-contentReference, ContentReference, id-aa-contentIdentifier, ContentIdentifier
     id-aa-contentHint, ContentHints
     FROM ExtendedSecurityServices   { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9)
          smime(16) modules(0) ess(2) }

-- RFC 5035   Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility
     id-aa-signingCertificatev2
     FROM ExtendedSecurityServices-2006   { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9
          (9) smime(16) modules(0) id-mod-ess-2006(30) }

-- ETSI TS 101 733   V1.7.3 (2007-01)    CMS Advanced Electronic Signatures (CAdES).
     id-aa-ets-sigPolicyId, SignaturePolicy, SignaturePolicyId,
     id-aa-ets-commitmentType, CommitmentTypeIndication, CommitmentTypeId,
     id-aa-ets-signerLocation, SignerLocation,
     id-aa-ets-signerAttr, SignerAttribute,
     id-aa-ets-contentTimestamp, ContentTimestamp
     FROM    ETS-ElectronicSignatureFormats-ExplicitSyntax97       {   iso(1)   member-body(2)   us(840)
          rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-mod(0) eSignature-explicit97(29) }
;
...

END
```

5 Anexo 2: Formato de ficheros y objetos binarios admitidos

Este marco de condiciones generales sobre los formatos de fichero de referencia a admitir por las plataformas de relación electrónica de la AGE con los ciudadanos y con las Administraciones Públicas pretende establecer unas consideraciones generales así como la relación de formatos de fichero y objetos binarios que deberán ser admitidos por todas las plataformas para facilitar su interoperabilidad. No obstante lo anterior, estas plataformas podrán admitir otros formatos de acuerdo con las necesidades específicas que en cada caso se planteen.

La relación completa de las condiciones generales en materia de formatos de fichero se establecerá por el marco normativo de desarrollo del Esquema Nacional de Interoperabilidad tal y como estable la Disposición adicional primera del Real Decreto 4/2010, de 8 de enero.

5.1 Consideraciones generales

- Los formatos de los documentos electrónicos admitidos no deberían obligar a disponer de licencias para visualizarlos o imprimirlos en diferentes sistemas operativos. Se deberían evitar en la medida de lo posible los formatos propietarios, porque no es posible asegurar la supervivencia de la empresa. En este sentido, la adhesión a los estándares internacionales es un requisito para la disponibilidad a largo plazo de un documento electrónico.

- Sería deseable disponer de la posibilidad de comprobar automáticamente el formato y su versión antes de admitirlo en el sistema, es decir, sólo se deberían admitir ficheros cuyo formato pudiera ser comprobado por una máquina antes de su aceptación por el Registro electrónico.

- Sólo se deberían admitir formatos estables que gozaran de la aceptación general y tuvieran una expectativa de vida larga. La evolución de los formatos debería mantener compatibilidad con los formatos anteriores.

- Habría que evitar documentos que tuvieran enlaces a otros documentos externos ya que debieran ser autocontenidos. Se considerará como una excepción el caso de los esquemas de validación asociados a formatos XML.

- Debido al riesgo de introducción de código malicioso, se deberá tener especial precaución con aquellos que contengan código ejecutable, como pueden ser macros. La documentación que se presente deberá estar libre de virus informáticos.