Guía Rápida de aplicación de la política de firma electrónica de la AGE

Autor:	*Consejo Superior de Administración Electrónica*
Grupo de trabajo:	*MINETUR-MHAP*
Versión:	*v1.0*
Fecha:	23/01/2012
Fichero:	

ÍNDICE

1 INTRODUCCIÓN 3

2 ALCANCE DE LA POLÍTICA DE FIRMA 4

3 IDENTIFICACIÓN DE LA POLÍTICA DE FIRMA 5

4 FORMATOS ADMITIDOS DE FIRMA 6

5 REALIZACIÓN DE FIRMAS ELECTRÓNICAS - EPES 7

5.1 POLÍTICA DE FIRMA ELECTRÓNICA DE LA AGE 7
5.2 POLÍTICA DE FIRMA DE FACTURA ELECTRÓNICA (FACTURAE) 8

6 DETALLE DE LOS FORMATOS DE FIRMA ADMITIDOS POR LA POLÍTICA 9

7 DATOS A INCLUIR EN LA FIRMA POR EL FIRMANTE 10

8 INCLUSIÓN DE FORMATOS LONGEVOS 11

9 PERIODOS DE GRACIA PARA LA COMPROBACIÓN DEL ESTADO DE REVOCACIÓN DE UN CERTIFICADO. 13

10 ALGORITMOS CRIPTOGRÁFICOS A USAR 14

11 ANEXO 1: ESTRUCTURA DE LA FIRMA ELECTRÓNICA 15

11.1 FORMATO DE FIRMA ELECTRÓNICA AVANZADA BÁSICO XADES EPES 15
11.2 FORMATO DE FIRMA ELECTRÓNICA AVANZADA BÁSICO CADES EPES 17

12 ANEXO 2: FORMATO DE FICHEROS Y OBJETOS BINARIOS ADMITIDOS 18

12.1 CONSIDERACIONES GENERALES 18

1 Introducción

El artículo 24.1 del RD 1671/2009 indica que la política de firma electrónica y certificados en el ámbito de la Administración General del Estado y de sus organismos públicos está constituida por las directrices y normas técnicas aplicables a la utilización de certificados y firma electrónica dentro de su ámbito de aplicación.

Esta política representa el conjunto de criterios comunes de interoperabilidad asumidos por la Administración General del Estado (AGE) en relación con la generación y validación de firmas electrónicas basadas en certificados electrónicos y que afecta por tanto a las relaciones de la Administración con los ciudadanos y entre sus distintos órganos. El objetivo principal es facilitar el uso de firmas electrónicas seguras e interoperables entre los distintos departamentos y organismos de la AGE.

La política de firma electrónica se circunscribe a los certificados electrónicos previstos en la Ley 11/2007 expedidos para su empleo por la Administración General del Estado 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 RD 1671/2009.

2 Alcance de la política de firma

Una política de firma electrónica es un documento 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 debiera incluir el firmante en el proceso de generación de la firma, y la información que debiera comprobar el verificador en el proceso de validación de la misma.

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. 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).

Tal y como especifica la norma técnica de interoperabilidad de política de firma (Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados de la Administración. BOE 30/07/2011), en su sección II.5 Interacción con otras políticas.
“1. Cada organización valorará la necesidad y conveniencia de desarrollar una política propia frente a la posibilidad de utilizar una política marco existente.”

Por tanto, no es necesaria la definición de una política de firma para cada organización. Excepto para organismos que por sus características requieran un marco legal concreto de firma electrónica, no es recomendable crear políticas de firma particulares, ya que se corre el riesgo de incluir restricciones que den como resultado firmas electrónicas no interoperables con las políticas de otros organismos.

3 Identificación de la política de firma

Cada política tiene asignado un identificador único (OID/URI), que deberá ser conocido por las aplicaciones de los organismos con los que resulte necesario el intercambio de firmas, de forma que puedan reconocer la política de la firma origen. Así mismo, como indica la Norma Técnica de Interoperabilidad de Política de Firma Electrónica en su apartado II.5.3.d)
"*Para que otras aplicaciones puedan interpretar las reglas de una política particular correctamente, dicha política está disponible en formato XML (eXtensible Markup Language) y ASN.1 (Abstract Syntax Notation One).*"

De esta forma, la política de firma, además de en documento legible, deberá implementarse a su vez en un formato que pueda ser entendido por los sistemas encargados de la creación y validación de firma electrónica, para facilitar el procesado automático de la firma electrónica.

Las normas técnicas que especifican estas definiciones son:

- ETSI TR 102 038, v.1.1.1. Electronic Signatures and Infrastructures (SEI); XML format for signature policies.
- ETSI TR 102 272, v.1.1.1. Electronic Signatures and Infrastructures (SEI); ASN.1 format for signature policies.

En el caso de la política de la AGE:

Nombre del documento	Política general de firma electrónica
Versión	1.8
Identificador de la Política (OID)[1]	OID 2.16.724.1.3.1.1.2.1.8
URL de definición de la política (PDF)	http://administracionelectronica.gob.es/es/ctt/politicafirma/politica_firma_AGE_v1_8.pdf
URL de definición de la política (XML)	http://administracionelectronica.gob.es/es/ctt/politicafirma/politica_firma_AGE_v1_8.xml
URL de definición de la política (ASN.1)	http://administracionelectronica.gob.es/es/ctt/politicafirma/politica_firma_AGE_v1_8.dat

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

4 Formatos admitidos de firma

Dentro de las distintas clases de los formatos XAdES y CAdES, los órganos y unidades administrativas de la Administración Pública deberán adecuar sus sistemas para la generación de la clase básica de al menos 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 dichos formatos (esto se puede hacer a través de la plataforma @firma que validará dichos formatos). Además deberán utilizar las versiones determinadas de los estándares que siguen los formatos y que se especifican en la política de firma.

Conviene aclarar que el concepto de versión del estándar que sigue el formato (por ejemplo XADES ETSI TS 101.902. v1.3.2) es diferente al de la clase del formato (BES, EPES, XL,…).
Sobre los algoritmos a usar para realizar las firmas electrónicas, la política recomienda ir migrando a algoritmos de huella o SHA2 y RSA 2048.

Se tendrá en consideración especial el formato PAdES (PDF Advanced Electronic Signatures), según especificación técnica ETSI TS 102 778-3, para su estudio y posible incorporación en futuras versiones de la política de firma, dada su especial relevancia como un formato de firma visible directamente por el ciudadano mediante herramientas estándar.

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

5 Realización de firmas electrónicas - EPES

Para realizar una firma electrónica acorde a una política de firma, es necesario indicarlo en la firma electrónica generada. Para ello, el OID o la URI deberá incluirse obligatoriamente en la firma electrónica, empleando el campo correspondiente, según cada formato, para identificar la política y la versión con las condiciones generales y específicas de aplicación para su validación.

El campo de una firma electrónica *SignaturePolicyIdentifier* identifica la política de firma sobre la que se basa el proceso de generación de firma electrónica.

A continuación se muestran los campos a completar para realizar firmas EPES en los diferentes formatos de firma reconocidos en la política de firma electrónica de la AGE y las de factura electrónica, formatos de firma soportados por la plataforma @firma.

5.1 Política de firma electrónica de la AGE

Formato	Atributo / Elemento	Valor
CAdES	sigPolicyId	2.16.724.1.3.1.1.2.1.8
	sigPolicyHash::hashAlgorithm	1.3.14.3.2.26
	sigPolicyHash::hashValue	7SxX3erFuH31TvAw9LZ70N7p1vA=
	sigPolicyQualifiers:: sigPolicyQualifierInfo:: sigPolicyQualifierId::SPuri	http://administracionelectronica.gob.es/es/ctt/politicafirma/politica_firma_AGE_v1_8.pdf
XAdES	SigPolicyId::Identifier	urn:oid:2.16.724.1.3.1.1.2.1.8
	SigPolicyId::Description	Política de firma electrónica para la Administración General del Estado
	SigPolicyHash::DigestMethod	http://www.w3.org/2000/09/xmldsig#sha1
	SigPolicyHash::DigestValue **XML**	V8lVVNGDCPen6VELRD1Ja8HARFk=
	SigPolicyHash::DigestValue **PDF**	VYICYpNOjso9g1mBiXDVxNORpKk=
	SigPolicyQualifiers:: SigPolicyQualifier::SPURI	http://administracionelectronica.gob.es/es/ctt/politicafirma/politica_firma_AGE_v1_8.pdf

En esta política de firma, en formato XAdES, existen dos valores de hash válidos:

- **XML:** este valor se corresponde con el hash en SHA-1 del elemento `SignaturePolicyInfo` del fichero XML de implementación de la política de firma correspondiente, tal y como se indica en el documento técnico TR 102 038 (*"TC Security – Electronic Signatures and Infrastructures (ESI); XML format for signature policies"*) referenciada en el punto 4.4.2 del estándar de XAdES ETSI TS 101 903, y que en el caso de la política de la AGE, dicho fichero se encuentra localizado en:

  http://administracionelectronica.gob.es/es/ctt/politicafirma/politica_firma_AGE_v1_8.xml

- **PDF:** este valor se corresponde con el hash en SHA-1 del documento PDF donde se especifica de forma legible la política de firma correspondiente. Hay que aclarar que este valor no es el aceptado por las normas técnicas de la ETSI mencionadas anteriormente (TR 102 038), pero se ha incluido como valor alternativo válido debido al uso extendido del mismo en algunas definiciones de políticas. Por tanto, no se recomienda su uso si bien @firma sí que valida firmas con política en la que se use el hash alternativo.

5.2 Política de firma de factura electrónica (Facturae)

v3.0

Formato	Atributo / Elemento	Valor
XAdES	SigPolicyId::Identifier	http://www.facturae.es/politica%20de%20firma%20formato%20facturae/politica%20de%20firma%20formato%20facturae%20v3_0.pdf
	SigPolicyId::Description	Facturación electrónica con formato Facturae
	SigPolicyHash::DigestMethod	http://www.w3.org/2000/09/xmldsig#sha1
	SigPolicyHash::DigestValue XML	gVI+R5m6XW111fHWaeKEDnUoxtg=
	SigPolicyHash::DigestValue PDF	HQvPemjDslVpcNmaJPpbHzhdZ50=
	SigPolicyQualifiers:: SigPolicyQualifier::SPURI	http://www.facturae.es/politica%20de%20firma%20formato%20facturae/politica%20de%20firma%20formato%20facturae%20v3_0.pdf

v3.1

Formato	Atributo / Elemento	Valor
XAdES	SigPolicyId::Identifier	http://www.facturae.es/politica_de_firma_formato_factura e/politica_de_firma_formato_facturae_v3_1.pdf
	SigPolicyId::Description	Facturación electrónica con formato Facturae
	SigPolicyHash::DigestMethod	http://www.w3.org/2000/09/xmldsig#sha1
	SigPolicyHash::DigestValue XML	T76hEwl/oPYW7o0EdCXjEWki4as=
	SigPolicyHash::DigestValue PDF	Ohixl6upD6av8N7pEvDABhEL6hM=
	SigPolicyQualifiers:: SigPolicyQualifier::SPURI	http://www.facturae.es/politica_de_firma_formato_factura e/politica_de_firma_formato_facturae_v3_1.pdf

6 Detalle de los formatos de firma admitidos por la política

La política contempla los siguientes estándares europeos de firma electrónica avanzados en su versión básica que permite la implementación de una política de firma:

- **Formato XAdES** (XML Advanced Electronic Signatures), según especificación técnica ETSI TS 101 903, versión 1.2.2 y versión 1.3.2. En este tipo de firmas el fichero de firma es un XML. Los documentos pueden tener cualquier formato. La modalidad de firma que se ha seleccionado es 'Internally detached', donde genera un único fichero resultante que contiene el documento original, codificado en base64, y las firmas, encontrándose al mismo nivel XML lo firmado y la firma.

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

  Asimismo se admitirán las firmas XAdES enveloped. En el caso de **factura electrónica** se acuerda asumir el modo actualmente implementado, 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.

- **Formato CAdES** (CMS Advanced Electronic Signatures), según especificación técnica ETSI TS 101 733, versión 1.6.3 y versión 1.7.4. El fichero de firma es binario. Se adopta el tipo Signed Data con los datos incluidos (attached/implícito) para la estructura del documento, 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/explicita, que incluye el hash del documento original en la firma.

7 Datos a incluir en la firma por el firmante

En la firma deberá incluirse como mínimo y de manera obligatoria la siguiente información del firmante:

- **Fecha y hora de firma** (signingTime)
- **Certificado del firmante** (signingCertificate)
- **Política de firma** sobre la que se basa el proceso de generación de firma electrónica (SignaturePolicyIdentifier).
- **Formato del documento original** que es necesario para que el receptor conozca la forma de visualizar el documento (DataObjectFormat o Content Hints).

Datos opcionales:

- Lugar geográfico donde se ha realizado la firma del documento.
- Rol de la persona firmante en la firma electrónica.
- Acción del firmante sobre el documento firmado (lo aprueba, lo informa, lo recibe, lo certifica,...).
- Sello de tiempo sobre algunos o todos los objetos de la firma.

8 Inclusión de formatos longevos

La política indica que se debe usar al menos la clase básica de los formatos de firma electrónica XAdES o CAdES, añadiendo información sobre la política de firma (clase EPES).

Los estándares CAdES (ETSI TS 101 733) y XAdES (ETSI TS 101 903) contemplan la posibilidad de incorporar a las firmas electrónicas información adicional para garantizar la validez de una firma a largo plazo o su conservación en el tiempo una vez que haya vencido el periodo de validez del certificado. Por ello, cada organismo puede extender la firma a partir de la clase EPES a un formato longevo (AdES –T, -C, -X, -XL, -A) tal y como se detalla a continuación:

1. Sello de tiempo del momento de la firma

- Formato de firma con ello de tiempo EPES –T: Se añade un sello de tiempo (TimeStamp) avalado por una TSA reconocida por el MITyC, con el fin de situar en el tiempo el instante en que se firma un documento.

- 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/revocación del certificado del firmante.

2. Formatos longevos (con información de validación)

   En el caso de que se deseen generar firmas longevas, se recomienda incluir la información de validación y añadirle un sello de tiempo a dicha información (formatos EPES–A). 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 (CRL) que aumenta de forma desproporcionada el tamaño de la firma, opcionalmente, en lugar de generar firmas de tipo EPES-A como se ha indicado anteriormente, se pueden incluir referencias a dicha información y un sello de tiempo (formatos EPES-X).

La necesidad de utilizar firmas longevas, o el hecho de utilizar un formato longevo u otro dependerá del procedimiento administrativo concreto, de sus requisitos de trazabilidad acorde con el ENS (requisito 5.7.5), y de la necesidad de custodia de las firmas durante periodos prolongados de tiempo.

Para determinar la necesidad de usar sellos de tiempo, se puede consultar la guía al respecto:

http://www.mpt.gob.es/dms/es/publicaciones/centro_de_publicaciones_de_la_sgt/Otras_Publicaciones/parrafo/guia_sello_tiempo/Guia_uso_sello_tiempo-INTERNET.pdf

El detalle de la información incluida en los formatos longevos es:

- Formato de firma con información de validación EPES –C: La firma añade un conjunto de referencias a los certificados de la cadena de certificación y su estado (CRL u OCSP).
- Formato de firma extendida EPES –X: Añade sellos de tiempo a las referencias introducidas por AdES –C.
- Formato de firma longeva EPES –XL: Añade los propios certificados y la información de revocación completa para permitir la verificación en el futuro incluso si las fuentes originales no estuvieran ya disponibles.
- Formato de firma de archivo EPES –A: Incluye toda la información necesaria para su verificación en la propia firma y permite la fiabilidad de dicha información mediante sellos de tiempo a lo largo del tiempo. Añade sellos de tiempo a las evidencias introducidas por AdES –XL. El proceso de resellado deberá repetirse antes de que caduque el sello de tiempo.

El sellado de tiempo y la información de validación pueden ser añadidos por el emisor, el receptor o un tercero y se deben incluir como propiedades no firmadas**.**

Conviene señalar que la firma longeva no es el único mecanismo para preservar una firma a lo largo del tiempo. 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.

También es posible conservar la validez de las firmas electrónicas mediante la utilización de sistemas de archivo especializados en la custodia. La utilización de dichos sistemas está fuera del alcance de este documento.

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

9 Periodos de gracia para la comprobación del estado de revocación de un certificado.

Para las operaciones de firma, existe un periodo de tiempo de espera, conocido como periodo de precaución o periodo de gracia, para comprobar el estado de revocación de un certificado. Por ello, toda la información de revocación en formatos AdES se recomienda incluirla después de trascurrido el periodo de precaución o periodo de gracia.

Este periodo como mínimo debe ser 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 la Declaración de Prácticas de Certificación del Prestador de Servicios de Certificación.

En la página web de @firma (http://administracionelectronica.gob.es/es/ctt/afirma) para usuarios registrados de las AAPP, hay una estimación de los periodos de gracia de los PSC que están incorporados en @firma.

10 Algoritmos criptográficos a usar

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 y CAdES, 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 pudieran adoptarse en el Esquema Nacional de Seguridad, desarrollado a partir del artículo 42 de la Ley 11/2007.

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.

Se podrán utilizar cualquiera de los siguientes algoritmos para la firma electrónica: RSA/SHA1 (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).

11 Anexo 1: Estructura de la firma electrónica

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

11.1 Formato de firma electrónica avanzada básico XAdES EPES

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

Una firma XAdES-EPES incorpora un elemento firmado incluido dentro de las SignedSignatureProperties llamado **SignaturePolicyIdentifier**. Por tanto, que el elemento sea un subelemento de las propiedades firmadas significa que la información es firmada y aceptada por el firmante. A continuación se define la definición del elemento según el esquema XSD:

```
<xsd:element name="SignaturePolicyIdentifier" type="SignaturePolicyIdentifierType"/>

<xsd:complexType name="SignaturePolicyIdentifierType">
	<xsd:choice>
		<xsd:element name="SignaturePolicyId" type="SignaturePolicyIdType"/>
		<xsd:element name="SignaturePolicyImplied"/>
	</xsd:choice>
</xsd:complexType>

<xsd:complexType name="SignaturePolicyIdType">
	<xsd:sequence>
		<xsd:element name="SigPolicyId" type="ObjectIdentifierType"/>
		<xsd:element ref="ds:Transforms" minOccurs="0"/>
		<xsd:element name="SigPolicyHash" type="DigestAlgAndValueType"/>
		<xsd:element name="SigPolicyQualifiers"      type="SigPolicyQualifiersListType"
		 minOccurs="0"/>
	</xsd:sequence>
</xsd:complexType>

<xsd:complexType name="ObjectIdentifierType">
	<xsd:sequence>
		<xsd:element name="Identifier" type="IdentifierType"/>
		<xsd:element name="Description" type="xsd:string" minOccurs="0"/>
		<xsd:element name="DocumentationReferences" type="DocumentationReferencesType"
		 minOccurs="0"/>
	</xsd:sequence>
</xsd:complexType>

<xsd:complexType name="DigestAlgAndValueType">
	<xsd:sequence>
		<xsd:element ref="ds:DigestMethod"/>
		<xsd:element ref="ds:DigestValue"/>
	</xsd:sequence>
</xsd:complexType>

<xsd:complexType name="SigPolicyQualifiersListType">
	<xsd:sequence>
		<xsd:element name="SigPolicyQualifier" type="AnyType" maxOccurs="unbounded"/>
	</xsd:sequence>
</xsd:complexType>

<xsd:element name="SPURI" type="xsd:anyURI"/>

<xsd:element name="SPUserNotice" type="SPUserNoticeType"/>

<xsd:complexType name="SPUserNoticeType">
	<xsd:sequence>
		<xsd:element name="NoticeRef" type="NoticeReferenceType" minOccurs="0"/>
		<xsd:element name="ExplicitText" type="xsd:string" minOccurs="0"/>
	</xsd:sequence>
</xsd:complexType>

<xsd:complexType name="NoticeReferenceType">
	<xsd:sequence>
		<xsd:element name="Organization" type="xsd:string"/>
		<xsd:element name="NoticeNumbers" type="IntegerListType"/>
	</xsd:sequence>
</xsd:complexType>

<xsd:complexType name="IntegerListType">
	<xsd:sequence>
		<xsd:element name="int" type="xsd:integer" minOccurs="0"
		 maxOccurs="unbounded"/>
	</xsd:sequence>
</xsd:complexType>
```

11.2 Formato de firma electrónica avanzada básico CAdES EPES

Una firma CAdES-EPES incorpora un atributo firmado obligatorio llamado **signaturepolicy-identifier** (1.2.840.113549.1.9.16.2.15), cuyo valor se corresponderá con el OID de la política de firma del Organismo en cuestión. Por tanto, que sea un atributo firmado significa que la información es firmada y aceptada por el firmante. A continuación se define la estructura ASN.1 de dicho atributo:

```
SignaturePolicyIdentifier ::=CHOICE {
        signaturePolicyId SignaturePolicyId,
        signaturePolicyImplied SignaturePolicyImplied -- not used
}

SignaturePolicyId ::= SEQUENCE {
        sigPolicyId SigPolicyId,
        sigPolicyHash SigPolicyHash,
        sigPolicyQualifiers SEQUENCE SIZE (1..MAX) OF SigPolicyQualifierInfo OPTIONAL
}

SigPolicyQualifierInfo ::= SEQUENCE {
        sigPolicyQualifierId SigPolicyQualifierId,
        sigQualifier ANY DEFINED BY sigPolicyQualifierId
}

SigPolicyQualifierId ::= SPuri (1.2.840.113549.1.9.16.5.1)

SPuri ::= IA5String

SigPolicyQualifierId ::= SPUserNotice (1.2.840.113549.1.9.16.5.2)

SPUserNotice ::= SEQUENCE {
        noticeRef NoticeReference OPTIONAL,
        explicitText DisplayText OPTIONAL
}

NoticeReference ::= SEQUENCE {
        organization DisplayText,
        noticeNumbers SEQUENCE OF INTEGER
}

DisplayText ::= CHOICE {
        visibleString VisibleString (SIZE (1..200)),
        bmpString BMPString (SIZE (1..200)),
        utf8String UTF8String (SIZE (1..200))
}

SignaturePolicyImplied ::= NULL
```

12 Anexo 2: Formato de ficheros y objetos binarios admitidos

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 RD 4/2010.

12.1 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.