

El presente documento contiene la sintaxis y las reglas de procesamiento que definen la firma electrónica del documento XML de la e-factura.

REFERENCIAS

[XMLDSig] XML Signature Syntax and Processing

[XADES] XML Advanced Electronic Signatures ETSI TS 101 903 v1.2.2

ETSI TS 102 023 "Policy requirements for time-stamping authorities"

NOTACIÓN

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.

INTRODUCCIÓN

El estándar XMLDSig recoge las reglas básicas de creación y procesamiento de firmas electrónicas de documentos XML. Dicho estándar se amplía con las especificaciones de XADES, donde se definen estructuras que permiten incorporar información adicional a firma que facilita su validación.

El cumplimiento de los estándares permite el reconocimiento de la firma por toda la comunidad electrónica, si bien su flexibilidad permite distintos grados de libertad que desde AEAT/CCI se precisa acotar para su aplicación a la factura electrónica.

SE definen dos formatos de firma electrónica:

- **Formato básico de firma electrónica avanzada** que contiene los elementos mínimos y necesarios para que la firma se considere firma electrónica avanzada acorde con la Ley 59/2003, de 19 de diciembre, de firma electrónica.
- **Formato de firma electrónica avanzada con información de validación** donde se incorporan propiedades de firma del estándar XADES al formato básico con objeto de proporcionar evidencias suficientes que garanticen la validez de la firma de la factura ante terceros.

También se incluyen, en el apartado 3, los requerimientos de archivado de firmas.

Por último, se indican los certificados electrónicos, las Autoridades de Sellado de Tiempo y los algoritmos que se admiten como válidos en concordancia con las presentes especificaciones.

1 FORMATO BÁSICO DE FIRMA ELECTRÓNICA AVANZADA

1.1 Objetivo

El formato básico de firma electrónica avanzada pretende proporcionar una estructura de firma que cumpliendo con la legislación vigente, incluya la mínima información.

1.2 Sintaxis

La estructura del formato básico de firma electrónica avanzada acorde con la presente política se adecua a las especificaciones definidas en XADES-EPES e incluye los campos que a continuación se detallan. Los campos señalados con * son opcionales.

```
<ds:Signature >
  <ds:SignedInfo/>
  <ds:SignatureValue/>
  <ds:KeyInfo>
    <ds:X509Data>
      <ds:X509Certificate/>
    </ds:X509Data>
  </ds:KeyInfo>
  <ds:Object>
    <xades:QualifyingProperties>
      <xades:SignedProperties>
        <xades:SignedSignatureProperties>
          <xades:SigningTime />
          <xades:SigningCertificate/> *
          <xades:SignaturePolicyIdentifier/>
          <xades:SignerRole/>
        </xades:SignedSignatureProperties>
      </xades:SignedProperties>
      <xades:UnSignedProperties/>
    </xades:QualifyingProperties>
  </ds:Object>
</ds:Signature>
```

1.3 Reglas de creación y validación de firma

- La firma se considera un campo más a añadir en el documento de factura y además debe aplicar a:
 - Todos los elementos de la factura
 - Los elementos de firma ubicados en el contenedor "SignedProperties"

- El certificado digital con el que se ha firmado incluido en el elemento **"KeyInfo"**

Para ello, el elemento ds:SignedInfo debe contener las siguientes referencias:

```
< ds: Reference URI="">
    <ds:TransformsAlgorithm
        ="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
</ ds: Reference >
```

```
<ds: Reference URI (#SignedProperties)
    type= http://uri.etsi.org/01903/v1.2.2#SignedProperties"/>
```

donde SignedPropertiesId es un atributo de tipo Id para identificar el elemento SignedProperties que contendrá los datos a firmar.

```
<ds: Reference URI (#KeyInfo)>
```

donde KeyInfoId es un atributo de tipo Id para identificar el elemento KeyInfo que contendrá el certificado firmante.

- Es necesario utilizar el elemento **ds:KeyInfo**, conteniendo, al menos, el certificado firmante codificado en base64. Además dicha información precisa ser firmada con objeto de evitar la posibilidad de sustitución del certificado.
- El elemento **xades:SignerRole** deberá contener uno y sólo uno de los siguientes atributos en el campo **ClaimedRoles**:
 - **"emisor"**: cuando la firma de la factura la realiza el emisor.
 - **"receptor"**: cuando la firma de la factura la realiza el receptor.
 - **"tercero"**: cuando la firma la realiza una persona o entidad distinta al emisor o al receptor de la factura.
- Los certificados y algoritmos criptográficos admitidos para la generación de la firma se incluyen en los apartados 4 y 6 de la presente política.
- El elemento **xades:SignaturePolicyIdentifier** debe incluir los siguientes contenidos en los elementos en que se subdivide:
 - una referencia explícita al presente documento de política de firma, elemento xades:SigPolicyId
 - la huella digital de este documento y el algoritmo utilizado , elemento xades:SigPolicyHash
 - referencia mundial única de la empresa que custodia esta política, CCI, otorgada por IANA (24491), elemento xades:SigPolicyQualifiers
- A continuación se detalla un ejemplo de la codificación requerida para el grupo QualifyingProperties:

```
<ds:Object>
```

```
<xades:QualifyingProperties xmlns:xades="http://uri.etsi.org/01903/v1.2.2#"
Target="#Signature">
  <xades:SignedProperties Id="SignedProperties">
    <xades:SignedSignatureProperties>
      <xades:SigningTime>2006-10-19T13:14:20+02:00</xades:SigningTime>
      <xades:SignaturePolicyIdentifier>
        <xades:SignaturePolicyId>
          <xades:SigPolicyId>
            <xades:Identifier>http://www.asociacioncci.es/docs/AEAT/2005/v1.2/especific
afirma.pdf</xades:Identifier>
            <xades:Description>Especificaciones de firma electrónica e-Factura
v1.2</xades:Description>
          </xades:SigPolicyId>
          <xades:SigPolicyHash>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>xmfh8D/Ec/hHeE1IB4zPd61zHIY=</ds:DigestValue>
          </xades:SigPolicyHash>
          <xades:SigPolicyQualifiers>
            <xades:SigPolicyQualifier>
              <xades:SPURI> urn:oid:1.3.6.1.4.1.24491</xades:SPURI>
            </xades:SigPolicyQualifier>
          </xades:SigPolicyQualifiers>
        </xades:SignaturePolicyId>
      </xades:SignaturePolicyIdentifier>
    </xades:SignedSignatureProperties>
  </xades:SignedProperties>
</xades:QualifyingProperties>
</ds:Object>
```

- El formato básico de firma electrónica avanzada no incluye ninguna información de validación más allá del certificado firmante, que está incluido en el campo **ds:KeyInfo**.
Será menester del encargado de la validación de la firma definir sus procesos de validación y si procede, archivado.
El formato de firma electrónica con evidencias ante terceros que se define en el siguiente apartado propone un método para incluir información de validación en el documento de factura.

2 FORMATO DE FIRMA ELECTRÓNICA AVANZADA CON INFORMACIÓN DE VALIDACIÓN

2.1 Objetivo

El formato incorpora al formato básico información adicional a la firma necesaria para su validación como por ejemplo, sellado de tiempo, o evidencia de que la firma existía antes de un determinado momento en el tiempo, información sobre la cadena de certificación y el estado de revocación de los mismos.

La inclusión de esta información a la firma proporciona evidencias ante terceros o potenciales arbitrajes.

2.2 Sintaxis

La estructura del formato de firma electrónica avanzada con evidencias ante terceros se adecua a las especificaciones definidas en el formato básico y en el estándar XADES-C e incluye los campos que a continuación se detallan, reseñándose en negrita la nueva información incorporada. Los campos señalados con * son opcionales.

```
<ds:Signature >
  <ds:SignedInfo/>
  <ds:SignatureValue/>
  <ds:KeyInfo>
    <ds:X509Data>
      <ds:X509Certificate/>
    </ds:X509Data>
  </ds:KeyInfo>
  <ds:Object>
    <xades:QualifyingProperties>
      <xades:SignedProperties>
        <xades:SignedSignatureProperties>
          <xades:SigningTime />
          <xades:SigningCertificate/> *
          <xades:SignaturePolicyIdentifier/>
          <xades:SignerRole/>
        </xades:SignedSignatureProperties>
      </xades:SignedProperties>
      <xades:UnSignedProperties>
        <xades: UnSignedSignatureProperties>
          <xades: SignatureTimeStamp />
          <xades: CompleteCertificationRefs/>
          <xades: CompleteRevocationRefs/>*
          <xades: RevocationValues/>*
        </xades: UnSignedSignatureProperties>
      </xades:UnSignedProperties>
    </xades:QualifyingProperties>
  </ds:Object>
```

</ds:Signature>

2.3 Reglas de creación y validación de firma

- El sellado de tiempo y la información de validación puede ser añadida por el emisor, el receptor o un tercero y debe ser incluida como propiedades no firmadas del campo **ds:Signature**.
- El sellado de tiempo debe realizarse en un momento próximo a la fecha incluida en el elemento **xades:SigningTime**. Como recomendación antes de los tres días siguientes y, en cualquier caso, siempre antes de la caducidad del certificado del firmante.
- Con objeto de garantizar que la información sobre el estado de revocación del certificado firmante se ha propagado convenientemente a los puntos de información correspondientes, la validación de la firma debe realizarse transcurridas al menos 24 horas desde la fecha en la que se realiza el sellado de tiempo, que es el momento en el que se aporta garantías de la existencia de la firma.
- Se requiere informar de la cadena de confianza completa del certificado del firmante, si bien sólo se precisa referencia a los certificados y no su valor completo. Para ello, se utilizará el elemento **xades:CompleteCertificationRefs**.
- Una tarea imprescindible para validar una firma electrónica es conocer el estado del certificado firmante. Obviamente, si el certificado está revocado la firma no puede admitirse como válida. La presente política admite dos métodos de obtención de información de revocación: consultas online OCSP y consultas a listas de certificados revocados o CRLs.

El formato de firma electrónica con información de validación, deberá incluir:

- O bien respuesta OCSP (convenientemente fechada y firmada) sobre el estado del certificado firmante. Dicha información deberá incluirse en el elemento **xades:RevocationValues**.
- O alternativamente, referencia al valor y la ubicación de las CRLs consultadas para conocer el estado del certificado firmante. Dicha información deberá incluirse en el elemento **xades:CompleteRevocationRefs**.
- Los certificados y algoritmos criptográficos admitidos para la generación de la firma se incluyen en los apartados 4 y 6 de la presente política.

3 ARCHIVADO

El archivado de firmas conforme a la presente política consiste en almacenar el documento firmado según la definición del formato de firma electrónica avanzada con información de validación.

Si como método de verificación del estado del certificado firmante, se utilizó consultas a CRLs, será necesario almacenar la CRL consultada, que además, deberá incluir fecha y firma del responsable de su expedición.

Opcionalmente, se podrá almacenar información sobre el estado de los certificados de las Autoridades de Certificación pertenecientes a la cadena de confianza del certificado firmante.

4 CERTIFICADOS ELECTRÓNICOS

Se consideran válidos para ejecutar la firma conforme a la presente política, todos aquellos certificados que cumplan con lo indicado en los apartados a) ó c) del artículo 18 del Reglamento por el que se regulan las obligaciones de facturación y que está recogido en el R. D. 1496/2003 de 28 de Noviembre.

5 AUTORIDADES DE SELLADO DE TIEMPO

La presente política admite sellos de tiempo expedidos por aquellas Autoridades de Sellado de Tiempo que cumplan con la norma ETSI TS 102 023 "Policy requirements for time-stamping authorities"

6 ALGORITMOS

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