MINISTERIO DE ECONOMÍA Y HACIENDA
DIRECCIÓN GENERAL DEL PATRIMONIO DEL ESTADO

Documento de Guía de implementación de la Firma de documentos CODICE

Proyecto:

CODICE2

Versión: 1.1

Fecha: 30/07/2010

HOJA DE CONTROL DOCUMENTAL

CONTROL DE VERSIONES

Versión	Fecha	Realizado por	Descripción
1.0	22/06/2010	DGPE	Versión Inicial
1.1	30/07/2010	DGPE	Eliminada limitación de algoritmo de transformación en forma canónica. Ampliación del procedimiento para admitir más de un `<ds:Reference>` que referencie a todo el documento. Corrección de las erratas detectadas

INDICE

1 Introducción

1.1 Ámbito y objetivos del proyecto

El proyecto CODICE2 constituye una evolución de los modelos de documentos *CODICE* para que los nuevos modelos permitan afrontar el reto de implementar proyectos de licitación electrónica. La primera versión de los documentos *CODICE* ha permitido la creación de la Plataforma de Contratación del Estado y el intercambio de anuncios y notificaciones entre los distintos actores que participan en procesos de licitación electrónica. La nueva versión de *CODICE* debe permitir ir un paso más allá, estableciendo las bases para que se puedan desarrollar procesos de licitación electrónica como puede ser la admisión y exclusión de candidatos a un procedimiento o la evaluación de ofertas y adjudicación de las mismas.

1.2 Convenciones tipográficas

Los términos (siglas, palabras o expresiones) en cursiva están bien definidos en el Glosario al final de la presente memoria.

Los acrónimos entre corchetes (“[n]”) constituyen referencias bibliográficas. La relación de documentos, libros, direcciones Web, etc. que conforman la bibliografía aparece en el apartado Bibliografía, al final de esta memoria.

1.3 Alcance y contenido

El documento se estructura en dos secciones principales:

1.3.1 Conceptos básicos de la firma XML

Sección en la que se proporciona la explicación de los conceptos básicos de la firma sobre XMLs. Se explica sucintamente en que consiste la firma [XMLDSign] y [XAdES].

1.3.2 Firma en XML aplicada a los documentos CODICE

La aplicación de la firma sobre todos los componentes de *CODICE* se realizará de acuerdo con las indicaciones que se dan en esta sección. Mediante esta guía de implementación se pretende establecer un perfilado sobre *CODICE* que permita una forma única y estandarizada de realizar la firma digital.

1.3.3 Co-firmas, contrafirmas y sellos de tiempo en documentos CODICE

Se apuntarán las recomendaciones para el uso de co-firmas y contrafirmas de documentos *CODICE* y para la inclusión de sellos de tiempo única y exclusivamente en documentos firmados.

1.4 Audiencia objetivo

Analistas y diseñadores de componentes y documentos que necesiten depurar y/o extender tanto la librería de componentes como los documentos ensamblados.

Consultores tecnológicos, analistas, diseñadores y programadores que necesiten analizar, diseñar e implementar nuevos artefactos, sistemas de información y aplicaciones basados en los resultados del proyecto *CODICE*.

1.5 Espacios de nombres utilizados

La siguiente tabla recoge los espacios de nombres referenciados en esta guía de implementación.

Prefijo	Espacio de nombres
ds	http://www.w3.org/2000/09/xmldsig#

xades	http://uri.etsi.org/01903/v1.3.2#
cbc	urn:oasis:names:specification:ubl:schema:xsd:CommonBasicComponents-2
cac	urn:oasis:names:specification:ubl:schema:xsd:CommonAggregateComponents-2
ext	urn:oasis:names:specification:ubl:schema:xsd:CommonExtensionComponents-2
odsig	urn:oasis:names:tc:opendocument:xmlns:digitalsignature:1.0

2 Firma XML

2.1 Firma Digital

Método criptográfico utilizado en transmisión datos y documentos informáticos para demostrar su autenticidad. Para que esto sea así la firma digital debe proporcionar:

- Integridad: El documento o los datos firmados no han sido modificados, destruidos o perdidos desde que se firmaron
- Autenticación: La firma debe identificar al firmante haciendo que sea imposible suplantar o falsificar su identidad sin que este hecho sea detectado
- No repudio: Se puede probar la participación de las partes implicadas en la firma. El firmante no puede negar lo que firmó porque el receptor tiene pruebas de ello y viceversa –el documento firmado es imposible de modificar o falsificar una vez firmado-.
- Anterioridad: Con un *sello de tiempo* puede probarse que la firma se creó en un determinado momento.

2.2 Firma XML

La firma XML o *Digital Signature* es una recomendación del *World Wide Web Consortium* (*W3C*) que define una sintaxis XML para la firma digital. Puede utilizarse para firmar documentos de cualquier tipo pero está más orientada a documentos XML.

[XMLDSig] cumple los requerimientos de "Firma Electrónica Avanzada" -suponiendo que se han tomado todas las medidas de seguridad adecuadas para que así sea- expuestos en [99/93/EC]:

- Se identifica con un único firmante
- Identifica al firmante
- Se crea por medios que sólo el firmante puede conocer y mantener
- Se relaciona de tal manera con los datos que firma que un cambio en ellos es detectado

Por todo ello [XMLDSig] cumple los principios de integridad, autenticación y no repudio.

En [XMLDSig] se definen tres tipos de firmas:

- Enveloped: La firma está contenida dentro del documento que se firma
- Enveloping: La firma contiene al documento
- Detached: La firma está separada del documento firmado

Los mismos tipos de firmas están admitidos por [XAdES], que es otro estándar de firma XML que extiende y amplía a [XMLDSig] con la inclusión datos útiles para el proceso de validación –*sello de tiempo*, listas de revocación de certificados…- proporcionando así una mayor integridad a la firma haciendo que sea válida durante largos periodos de tiempo.

2.3 XMLDSig

[XMLDSig] es un estándar creado por la *W3C* que recoge las reglas básicas de creación y procesamiento de firmas electrónicas de documentos, principalmente en XML. Las firmas [XMLDSig] son firmas digitales creadas y pensadas para transacciones XML.

Puesto que una firma digital XML es un proceso matemático por el que los datos a firmar se transforman siguiendo una serie de reglas y cálculos basados en una clave y cuyos resultados son guardados en elementos XML y adjuntados o no a los datos primitivos del proceso, en el estándar [XMLDSig] encontramos:

- Definición de la estructura XML en la que almacenar la firma
- Definición del proceso de firma

- Definición del proceso de validación de firma
- Agrupación y aceptación de los algoritmos y procesos para la transformación en forma canónica de los datos firmados y de la firma
- Agrupación y aceptación de los algoritmos y procesos de transformación para la obtención de la firma

2.3.1 Entendiendo XMLDSig

En esta sección se recogen breves explicaciones del significado de los elementos XML más importantes que componen la firma [XMLDSig] y del papel que juegan en el proceso de firmado. El esquema de datos XML del estándar puede encontrarse en: http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/xmldsig-core-schema.xsd.

Como puede verse `<ds:Signature>` es un elemento simple que contiene información: lo que se está firmando, `<ds:SignedInfo>`; la propia firma, `<ds:SignatureValue>`; las claves utilizadas para firmar, `<ds:KeyInfo>`.

```
<element name="Signature" type="ds:SignatureType" />
<complexType name="SignatureType" mixed="false">
      <sequence>
            <element ref="ds:SignedInfo" />
            <element ref="ds:SignatureValue" />
            <element ref="ds:KeyInfo" minOccurs="0" />
            <element ref="ds:Object" minOccurs="0"
      maxOccurs="unbounded" />
      </sequence>
      <attribute name="Id" type="ID" use="optional" />
</complexType>
```

A continuación veremos sus atributos y elementos uno por uno:

El atributo `Id` es opcional pero es muy útil para identificar la firma dentro de un documento, sobre todo cuando se trabaja con firmas múltiples.

El elemento `<ds:SignatureValue>` contiene la firma codificada en Base64. La firma es el resultado de una serie de transformaciones sobre los datos binarios del elemento `<ds:SignedInfo>`. El elemento `<ds:SignatureValue>` contiene este valor binario de la firma codificado en Base64.

El elemento `<ds:SignedInfo>` puede dividirse en dos partes desde el punto de vista conceptual: información sobre el valor de la firma e información sobre los datos a firmar.

```
<element name="SignedInfo" type="ds:SignedInfoType" />
<complexType name="SignedInfoType" mixed="false">
      <sequence>
            <element ref="ds:CanonicalizationMethod" />
            <element ref="ds:SignatureMethod" />
            <element ref="ds:Reference" maxOccurs="unbounded" />
      </sequence>
      <attribute name="Id" type="ID" use="optional" />
</complexType>
```

`<ds:CanonicalizationMethod>` posee un atributo `Algorithm` que indica cómo se debe transformar a forma canónica el elemento `<ds:SignedInfo>` antes de realizar la firma.

Distintos XML pueden diferir en su forma de ser escritos y sin embargo significar lo mismo. Como la firma se realiza a nivel de bytes, aunque un documento signifique lo mismo y tenga la misma información que otro, ambos pueden tener firmas diferentes si no están escritos exactamente igual. Habrá que elegir entre una de todas las formas posibles de escribir un documento XML, la

forma canónica, y transformar los documentos a esta forma sin que su información y significado se vean alterados. A este proceso se le llama transformación en forma canónica. Habrá varias formas canónicas dependiendo del algoritmo que se utilice. Dos documentos están en la misma forma canónica si los algoritmos utilizados para su obtención son equivalentes.

<ds:SignatureMethod> especifica qué tipo de algoritmo de firma se utilizará para obtener la firma. La firma se realiza aplicando este algoritmo matemático sobre el elemento <ds:SignedInfo> que, puesto que contiene los valores hash de los distintos datos que se quieren firmar –como se verá a continuación-, será diferente en casa caso.

Cada <ds:Reference> incluye el hash de un objeto de datos y las transformaciones aplicadas a ese objeto para producir dicho hash.

```
<element name="Reference" type="ds:ReferenceType" />
<complexType name="ReferenceType" mixed="false">
      <sequence>
            <element ref="ds:Transforms" minOccurs="0" />
            <element ref="ds:DigestMethod" />
            <element ref="ds:DigestValue" />
      </sequence>
      <attribute name="Id" type="ID" use="optional" />
      <attribute name="URI" type="anyURI" use="optional" />
      <attribute name="Type" type="anyURI" use="optional" />
</complexType>
```

El atributo URI identifica al objeto de datos que se va a firmar. Éste puede ser un objeto fuera del documento en el que está la firma o bien un objeto dentro del propio documento. Si su valor es cadena vacía identifica al documento completo que contiene la firma. Por supuesto puede haber varios <ds:Reference> permitiendo a una misma firma [XMLDSig] cubrir múltiples objetos.

<ds:DigestMethod> define la función hash utilizada y <ds:DigestValue> es el valor hash codificado en Base64.

<ds:Transforms> es opcional aunque es el elemento con más fuerza de <ds:Reference>. Si aparece, contendrá una lista de <ds:Transform> en la que cada uno de sus elementos indica un paso realizado en el procesamiento de cálculo del hash. Cada paso tiene como entrada la salida del anterior y puede incluir operaciones como transformación en forma canónica, codificación/decodificación, transformaciones XSL, validación de esquemas… La salida del último <ds:Transform> es la entrada de la función de cálculo del hash.

Al permitir que se puedan firmar distintas porciones de un documento, las modificaciones posteriores a la firma de las porciones no incluidas no afectarán en nada a la validación de la firma.

```
<element name="KeyInfo" type="ds:KeyInfoType" />
<complexType name="KeyInfoType" mixed="true">
      <choice maxOccurs="unbounded">
            <element ref="ds:KeyName" />
            <element ref="ds:KeyValue" />
            <element ref="ds:RetrievalMethod" />
            <element ref="ds:X509Data" />
            <element ref="ds:PGPData" />
            <element ref="ds:SPKIData" />
            <element ref="ds:MgmtData" />
            <any processContents="lax" namespace="##other"
            minOccurs="1" maxOccurs="1" />
            <!-- (1,1) elements from (0,unbounded) namespaces -->
      </choice>
      <attribute name="Id" type="ID" use="optional" />
</complexType>
```

<ds:KeyInfo> es una estructura opcional que identifica al firmante. Su contenido suele utilizarse en procesos de verificación de firmas, de ahí la importancia de que lo que se incluya en su interior sean los elementos de <ds:X509Data> o <ds:KeyValue> que contienen información del certificado firmante y de la clave pública del firmante respectivamente. La información que proporciona <ds:KeyInfo> en todos sus elementos debe corresponder al mismo certificado o clave.

En caso de no incluir la estructura <ds:KeyInfo>, la firma no podría considerarse como “Firma Electrónica Avanzada” puesto que el firmante no podría ser identificado.

<ds:Object> es también opcional y se utiliza para contener cualquier tipo de dato por lo general importante para la firma, como sellos de tiempo y, en el caso de una firma de tipo *enveloping*, para contener los datos que se firman.

```
<element name="Object" type="ds:ObjectType" />
<complexType name="ObjectType" mixed="true">
      <sequence minOccurs="0" maxOccurs="unbounded">
            <any namespace="##any" processContents="lax"
            minOccurs="1" maxOccurs="1" />
      </sequence>
      <attribute name="Id" type="ID" use="optional" />
      <attribute name="MimeType" type="string" use="optional" />
      <!--  add a grep facet  -->
      <attribute name="Encoding" type="anyURI" use="optional" />
</complexType>
```

Existen otros elementos opcionales que aparecen dentro de los elementos <ds:Object>: <ds:Manifest> y <ds:SignatureProperties> . El primero se utiliza para agrupar varios <ds:Reference>, mientras que el segundo es útil para añadir propiedades a la firma como un *sello de tiempo* o una lista de certificados.

2.4 XAdES

[XAdES] son las siglas de *XML Advanced Electronic Signatures*. Recoge un conjunto de extensiones a la recomendación [XMLDSig] propuesta por el *W3C*. Proporciona autenticación básica, protección de integridad y satisface requerimientos adicionales para firma electrónica avanzada. Un beneficio importante de [XAdES] es que los documentos firmados pueden seguir siendo válidos durante largos períodos de tiempo, incluso en el caso de que los algoritmos utilizados en el proceso de firma hayan sido rotos.

[XAdES] define cuatro formas o perfiles según el nivel de protección ofrecido:

- XAdES-BES (Basic Electronic Signature): Se construirá sobre un [XMLDSig] incorporando una serie de propiedades
- XAdES-EPES (Explicit Policy based Electronic Signature): Se construirá sobre un [XMLDSig] o un XAdES-BES incorporando una propiedad en la que se define la política particular de firma utilizada.
- XAdES-T (Timestamp): Se construye sobre una firma XAdES-BES o XAdES-EPES incorporando una propiedad que contiene un sello o marca de tiempo proporcionada por una *TSA* que certifica que la firma existe a partir de ese punto en el tiempo, protegiéndola contra el repudio
- XAdES-C (Complete): Se construye sobre una firma XAdES-T añadiendo referencias a certificados y listas de revocación utilizados durante la verificación y que serán útiles para poder seguir validando la firma en el futuro

Existen extensiones a XAdES-C que añaden más datos de validación. Con esta información adicional se hace posible que la firma sea válida incluso después de que los certificados y listas de revocación a las que se hace referencia en XAdES-C hayan dejado de ser accesibles y aunque los algoritmos de firma hayan caído en desuso.

Una firma [XAdES] es una firma [XMLDSig] con información adicional que garantiza la constitución de una "Firma Electrónica Avanzada" según la directiva [99/93/EC]. Se construye añadiendo elementos XML definidos en [XAdES] dentro de un `<ds:Object>` de [XMLDSig]. Estos nuevos elementos están recogidos bajo el mismo espacio de nombres, que difiere dependiendo de la versión utilizada. Las versiones más extendidas son XAdESv1.3.2 y XAdESv1.4.1 cuyos esquemas pueden encontrarse en http://uri.etsi.org/01903/v1.3.2/XAdES.xsd y http://uri.etsi.org/01903/v1.4.1/XAdESv141.xsd respectivamente.

```
<ds:Object>
      <xades:QualifyingProperties                Target="#signatureID"
      xmlns:xades="http://uri.etsi.org/01903/v1.3.2#" >
            <xades:SignedProperties id="SignedPropertiesId">
                  <xades:SignedSignatureProperties>
                        [...]
                  </xades:SignedSignatureProperties>
                  <xades:SignedDataObjectProperties>
                        [...]
                  </xades:SignedDataObjectProperties>
            </xades:SignedProperties>
            <xades:UnsignedProperties>
                  <xades:UnsignedSignatureProperties>
                        [...]
                  </xades:UnsignedSignatureProperties>
                  <UnsignedDataObjectProperties>
                        [...]
                  </UnsignedDataObjectProperties>
            </xades:UnsignedProperties>
      </xades:QualifyingProperties>
</ds:Object>
```

Se debe crear un nuevo elemento `<xades:QualifyingProperties>` e introducirlo dentro de `<ds:Object>`. Éste, posee un atributo obligatorio, `Target`, que se utiliza para hacer referencia a la firma XML a la que van asociadas las propiedades que contiene. `<xades:QualifyingProperties>` posee dos hijos:

- `<xades:SignedProperties>`: Propiedades adicionales que deben ser firmadas, como por ejemplo, la fecha de firma y el certificado firmante. Como puede verse posee un atributo `Id` que se utiliza para referenciar este elemento desde el `<ds:Reference>` de la firma. Contiene a su vez:

- <xades:SignedSignatureProperties>: Propiedades referentes a la firma
- <xades:SignedDataObjectProperties>: Propiedades referentes a los datos firmados

- <xades:UnsignedProperties>: Otras propiedades que no tienen por que ser firmadas, como referencias a certificados y listas de revocación, sellos de tiempo, etc.

A continuación se explican brevemente las principales características de las distintas extensiones [XAdES] para facilitar la comprensión de la política de firmado de documentos *CODICE* descrita en este documento.

2.4.1 XAdES-BES

XAdES-BES se construirá sobre un [XMLDSig] incorporando propiedades que se incluirán, algunas, entre los datos firmados (dentro del elemento <xades:SignedProperties>) y otras que no deben ser firmadas (dentro del elemento <xades:UnsignedProperties>).

El cálculo de la firma se realiza igual que en [XMLDSig] sobre los datos de negocio y sobre el nuevo conjunto de propiedades, <xades:SignedProperties>, cuando esté presente.

Esta forma extiende a [XMLDSig] haciendo obligatorio incluir o proteger el certificado firmante dentro de la firma utilizando una de las dos formas siguientes:

- Incorporándolo dentro de <xades:SigningCertificate> dentro de <xades:SignedSignatureProperties>
- Incorporándolo dentro de <ds:keyInfo> y firmando después el elemento

2.4.2 XAdES-EPES

XAdES-EPES extiende la definición de firma electrónica para acordar o identificar una determinada política para la firma (para necesidades particulares de negocio). Añade el elemento <xades:SignaturePolicyIdentifier> dentro de <xades:SignedSignatureProperties>. Este elemento puede contener referencias a documentos –o incluso el propio documento- en los que se recojan las pautas y reglas que componen la política de firma.

Esta política debe ser tenida en cuenta a la hora de verificar la firma electrónica.

2.4.3 XAdES-T

El resto de firmas [XAdES] que se presentan a continuación incluyen datos útiles en el proceso de validación. Estos datos, al no ser firmados, pueden ser añadidos tanto por el firmante como por los verificadores según lo crean conveniente a lo largo del tiempo.

XAdES-T añade el elemento <xades:SignatureTimeStamp> a <xades:UnsignedSignatureProperties>.

Añade un sello o marca de tiempo proporcionada por una *TSA* para evitar el no repudio ante la posible caducidad o revocación del certificado firmante en el futuro.

2.4.4 XAdES-C

Añade a XAdES-T referencias al conjunto completo de autoridades de certificación (CAs) que han sido utilizadas para validar la firma electrónica así como referencias a los datos de revocación de los certificados.

Añade <xades:CompleteCertificateRefs> y <xades:CompleteRevocationsRefs> y opcionalmente <xades:AttributeCertificateRefs> y <xades:AtributeRevocationRefs>.

2.4.5 XAdES-X

Extended signatures with time forms. Extiende XAdES-C incluyendo sellos o marcas de tiempo

obtenidos cada vez que se modifica la información de <xades:CompleteCertificateRefs> y <xades:CompleteRevocationsRefs>.

2.4.6 XAdES-X-L

Extended long electronic signatures with time forms. Extiende XAdES-X incluyendo información completa –en lugar de las referencias- de los certificados y listas de revocación utilizadas en la firma.

2.4.7 XAdES-A

Archival electronic signatures. Incluye sellos de tiempo que se van renovando para garantizar la longevidad de las firmas incluso ante rotura de los algoritmos de firma.

3 Firma de documentos CODICE

El objetivo de esta sección es describir el procedimiento que debe seguirse para la firma de documentos *CODICE*. Se toma como referencia el documento [UBLforESig] donde se describe una metodología estándar de firma de documentos *UBL* 2.x basado en [XMLDSig] y [XAdES].

3.1 Características de la firma en CODICE

Las características del procedimiento propuesto son las siguientes:

- Se usará una firma XML enveloped aceptando las recomendaciones descritas en [UBLforESig]
- La firma se realizará sobre todo el documento *CODICE*
- La firma, conforme con [XMLDSig] o [XAdES] en cualquiera de sus formas, mantendrá su propio namespace –en ningún caso será modificado- y será insertada dentro del elemento `<ext:UBLExtension>` de forma que cumpla con los esquemas y sintaxis de *UBL* 2.x
- El elemento ASBIE de *UBL* `<cac:Signature>` no es un elemento obligatorio para documentos *CODICE*, estén o no firmados. Si aparece será un elemento más del documento y por tanto será firmado. Deberá llevar información que esté en consonancia con el firmante o los firmantes, actuando como un pie de firma. Este documento acepta todo lo que diga [UBLforESig] al respecto.
- El *sello de tiempo* de un documento *CODICE* únicamente se admitirá dentro de la firma XAdES-T -o de un perfil superior- realizada sobre el documento
- Se admitirán co-firmas y contrafirmas
- Como clave para firmar se admitirán únicamente claves de certificados X.509

3.2 Procedimiento de firma básica en CODICE

Los siguientes apartados marcan el guión a seguir para la correcta composición del documento *CODICE* firmado. Es importante recordar que antes de realizar el firmado del documento hay que componerlo correctamente, puesto que una vez firmado, si queremos que sea aceptado y que la firma sea verificada correctamente, no puede modificarse.

3.2.1 Uso de `ext:UBLExtension`

La firma digital será alojada dentro del elemento `<ext:UBLExtension>` como se propone en [UBLforESig]. Uno o más `<ext:UBLExtension>` están contenidos dentro de un elemento `<ext:UBLExtensions>` descendiente directo del elemento raíz del documento. Estos elementos están disponibles en *UBL* 2.x para la inclusión de datos no [UBL], como es nuestro caso.

Este elemento se construirá del siguiente modo:

- El elemento opcional `<cbc:ID>` de `<ext:UBLExtension>` se requiere como obligatorio y su valor será un identificador único en todo el documento
- El elemento `<ext:UBLExtension>` posee un elemento `<ext:UBLExtensionContent>` donde debe introducirse el elemento `<odsig:document-signatures>` definido en http://docs.oasis-open.org/office/v1.2/part3/cd01/OpenDocument-dsig-schema-v1.2-cd1.rng. Dentro de éste último es donde se incluyen las firmas [XMLDSig] o [XAdES] de todos los firmantes del documento. Por tanto, en el documento únicamente habrá un solo `<ext:UBLExtension>` para la inclusión de firmas
- Siempre que se use la firma [XAdES] y se implemente siguiendo las pautas marcadas en el documento [UBLforESig] se incorporará a `<ext:UBLExtension>` el elemento

<ext:ExtensionURI> con el valor de la URL que identifica el perfil de la firma implementado:

- http://docs.oasis-open.org/ubl/securitysc/cd-dsigp-1/xades-enveloped cuando se firma XAdES
- http://docs.oasis-open.org/ubl/securitysc/cd-dsigp-1/xmldsig-enveloped cuando se firma XMLDSig

En el Anexo I pueden verse ejemplos de cómo construir estas extensiones de UBL.

3.2.2 *Uso de* `cac:Signature`

Ya se ha comentado que este elemento de [UBL], y por tanto de *CODICE*, no es obligatorio para completar el proceso de firma que aquí se describe. Si se utiliza se acepta lo descrito en [UBLforESig] acerca de este elemento. Aquí se recogen las consideraciones más importantes del mencionado documento sobre este elemento:

- Habrá un único elemento <cac:Signature> en todo el documento independientemente del número de firmantes
- El elemento <cac:Signature>/<cbc:SignatureMethod> no es obligatorio pero si aparece debe identificar el perfil de firma utilizado siempre y cuando se cumpla con lo descrito en [UBLforESig] para dicho perfil. En nuestro caso únicamente aceptamos firmas enveloped por tanto su valor será:
  - http://docs.oasis-open.org/ubl/securitysc/cd-dsigp-1/xades-enveloped En firmas XAdES
  - http://docs.oasis-open.org/ubl/securitysc/cd-dsigp-1/xmldsig-enveloped en firmas XMLDSig
- <cac:Signature>/<cbc:ID> estará presente y será fijado a UBLDSIG
- El elemento <cac:Signature>/<cac:SignatoryParty>/<cac:PartyIdentification> también será obligatorio y deberá contener un elemento <cbc:ID> con el valor SignatureDefined

Puede hacerse uso de otros elementos dentro de <cac:Signature> pero su definición no entra dentro del alcance de este documento.

En el Anexo II puede verse un ejemplo de cómo incluir este elemento dentro del documento.

3.2.3 *Preparación y realización de la firma*

La firma, como ya se ha comentado, se realizará sobre el documento completo y podrá llevarse a cabo con un componente propio o externo de firma de documentos XML. En cualquier caso la firma satisfará como mínimo los requerimientos de “Firma Electrónica Avanzada” comentados en apartados anteriores. Se podrá utilizar [XMLDSig] o [XAdES].

Se utilizará para firmar la clave privada de un certificado digital X509 válido no caducado.

3.2.3.1 *Firma básica XMLDSig*

Se firma todo el documento incluido el elemento <odsig:document-signatures>. En esta implementación no podrán añadirse nuevos datos al documento después de firmar, ni siquiera extensiones en el formato acordado, puesto que la validación fallaría.

Las consideraciones a tener en cuenta a la hora de realizar una correcta implementación son las siguientes:

- Algoritmo de transformación en forma canónica del elemento <ds:SignedInfo>. Valor del atributo Algorithm del elemento <ds:CanonicalizationMethod>.
- Algoritmo de firma. Valor del atributo Algorithm del elemento

<ds:SignatureMethod>: Cualquier algoritmo de firma que use certificados X509

- Al menos un <ds:Reference> que haga referencia a todo el documento *CODICE* mediante la inclusión de una transformación <ds:Transform> (pueden incluirse transformaciones adicionales) con una de las siguientes expresiones XPath. Con todas se consigue evitar que la propia firma sea firmada:
    - No evita que el resto de firmas existentes en el documento sean firmadas: http://www.w3.org/2000/09/xmldsig#enveloped-signature
    - Evita que el resto de firmas existentes en el documento sean firmadas:

```
<ds:XPath                                                    xmlns:odsig=”
urn:oasis:names:tc:opendocument:xmlns:digitalsignature:1.0”>
      not(ancestor-or-self::odsig:document-signatures)
</ds:XPath>
```

    - Evita que el resto de firmas existentes en el documento sean firmadas:

```
<ds:XPath>not(ancestor-or-self::ds:Signature)</ds:XPath>
```

    - Evita que el resto de firmas existentes en el documento sean firmadas, ya que si recordamos solo se permite un elemento <odsig:document-signatures> en el mismo documento:

```
<ds:XPath>
      count(ancestor-or-self::odsig:document-signatures |
      here()/ancestor::odsig:document-signatures[1]) >
      count(ancestor-or-self::odsig:document-signatures)
</ds:XPath>
```

- En la firma aparecerá el elemento <ds:KeyInfo> y contendrá obligatoriamente el certificado X509 firmante: <ds:X509Data>/<ds:X509Certificate> con el contenido público del certificado.

  Es obligatorio incluir el certificado firmante para poder conocer la clave pública para la verificación de la misma y para tener información completa de la identidad del firmante. El resto de elementos que pueden incluirse dentro de <ds:KeyInfo> podrán ir informados aunque su contenido será tratado como información adicional y no relevante

- Pueden añadirse datos en <ds:Object> pero no porque los requiera la implementación de documentos *CODICE* que aquí se describe. Serán tratados por tanto como información adicional y no relevante

La estructura de la firma básica [XMLDSig] será la que aparece en el siguiente cuadro. Los elementos y atributos que preceden al signo ‘?’ son opcionales en esta implementación.

```
<ds:Signature Id?>
      <ds:SignedInfo>
            <ds:CanonicalizationMethod/>
            <ds:SignatureMethod/>
            <ds:Reference URI=””>
                  <ds:Transforms></ds:Transforms>
                  <ds:DigestMethod></ds:DigestMethod>
                   <ds:DigestValue></ds:DigestValue>
            </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue></ds:SignatureValue>
      <ds:KeyInfo>
            <ds:X509Data>
                  <ds:X509Certificate></ds:X509Certificate >
            </ds:X509Data>
            (<!-- Resto de componentes de ds:KeyInfo -->)?
      </ds:KeyInfo>
      (<ds:Object></ds:Object>)?
</ds:Signature>
```

3.2.3.2 Firma básica XAdES

Se utilizará XAdESv1.3.2 sin restricción en cuanto al perfil de firma [XAdES] utilizado. Cualquier versión posterior a ésta será válida mientras no implique cambios significativos en la sintaxis definida en este documento.

Al tratarse [XAdES] de una extensión de [XMLDSig] las consideraciones a tener en cuenta a la hora de realizar una correcta implementación son las mismas que las descritas más arriba para la firma básica [XMLDSig]

El uso de [XAdES] permite la inclusión de datos después del firmado dentro de la propia firma.

3.2.4 Inserción de la firma en el documento CODICE

Una vez realizada, la firma debe insertarse dentro del `<ext:UBLExtension>/<ext:UBLExtensions>/<ext:UBLExtensionContent>/<odsig:document-signatures>` del documento

3.2.5 Validación de la firma

La validación se realizará secuencialmente en dos pasos:

1. Verificación de que la estructura del documento *CODICE* cumple con los requerimientos descritos en [UBLforESig] complementados con los propios de esta guía de implementación y que aquí se describen:
   a. Las firmas digitales son de tipo *XML enveloped* y están incluidas en las extensiones de [UBL] dentro de `<odsig:document-signatures>`
   b. El valor del elemento `<cbc:ID>` de `<ext:UBLExtension>` es único en el documento
   c. Las transformaciones indicadas en la firma digital cumplen con las formas y algoritmos aquí presentadas
2. Validación estándar de firmas XML descrita en [XMLDSig]:
   a. Verificación de los valores de los hash de los datos que se firman y que se encuentran en `ds:Signature/ds:SignedInfo/ds:Reference[]`
   b. Verificación del valor del valor de la firma que se encuentra en `ds:Signature/ds:SignatureValue`

   Para ampliar el proceso de validación de firmas de documentos *CODICE* y conocer cómo debe realizarse la implementación puede consultarse [XMLDSig] y [XAdES] donde se explica

cómo validar cualquier firma de cualquiera de estos dos tipos.

Existen un gran número de APIs y herramientas *off-line* y *on-line*, como [VALIDe], que nos pueden ayudar en la tarea de validación

3.3 Procedimiento de co-firmas en CODICE

Las co-firmas son las llamadas firmas en paralelo en las que todas firman los mismos datos pero no las firmas de los demás. Por tanto hay que excluir del proceso de firma los datos correspondientes a las firmas de los demás firmantes en el momento de realizarla.

Se utilizarán firmas básicas [XMLDSig] y [XAdES] para realizar cada una de las firmas de los co-firmantes. Hay que considerar lo siguiente:

- Es necesario excluir del proceso de firma todas las firmas ya generadas para que el proceso de validación no falle. Por tanto será obligatorio el uso de una de las transformaciones XPath siguientes:

```
<ds:XPath>not(ancestor-or-self::ds:Signature)</ds:XPath>
```

o

```
<ds:XPath                                                    xmlns:odsig=”
urn:oasis:names:tc:opendocument:xmlns:digitalsignature:1.0”>
      not(ancestor-or-self::odsig:document-signatures)
</ds:XPath>
```

o

```
<ds:XPath>
      count(ancestor-or-self::odsig:document-signatures |
      here()/ancestor::odsig:document-signatures[1]) >
      count(ancestor-or-self::odsig:document-signatures)
</ds:XPath>
```

- No puede añadirse información adicional al documento después de haber firmado

3.4 Procedimiento de contrafirmas en CODICE

Contrafirmas o firmas secuenciales son aquellas en las que se firma el valor de de una firma anterior.

Únicamente se admitirán contrafirmas [XAdES]. La firma primitiva debe seguir el formato [XAdES] en cualquiera de sus formas para posteriormente ser contrafirmada siguiendo el mismo estándar y utilizando las recomendaciones escritas en [XAdES] sobre este tema.

3.5 Sellos de tiempo en documentos CODICE

Los sellos de tiempo no son un elemento exclusivo de firmas de documentos, pero se ha considerado oportuno hacer referencia a ellos en esta guía de implementación porque cualquier documento *CODICE* que quiera entregarse con *sello de tiempo* tiene que ir, obligatoriamente, firmado por la entidad competente en formato XAdES-T incluyéndose dicho sello en la firma siguiendo las especificaciones de la recomendación [XAdES].

4 Anexo I

Si se firma siguiendo las recomendaciones de [UBLforESig]

```
<ext:UBLExtensions
xmlns:ext="urn:oasis:names:specification:ubl:schema:xsd:CommonExtensi
onComponents-2">
      [...]
      <ext:UBLExtension>
            <cbc:ID>0000000001001</cbc:ID>
            <ext:ExtensionURI>http://docs.oasis-
      open.org/ubl/securitysc/cd-dsigp-1/xmldsig-enveloped
            </ext:ExtensionURI>
            <ext:ExtensionContent
      xmlns:ext="urn:oasis:names:specification:ubl:schema:xsd:CommonE
      xtensionComponents-2">
                  <odsig:document-signatures
            xmlns:odsig="urn:oasis:names:tc:opendocument:xmlns:digita
            lsignature:1.0">
                        <ds:Signature
                  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
                  Id="signature-f1a5-9b1d-972b-d591">
                        [...]
                        </ds:Signature>
                  </odsig:document-signatures>
            </ext:ExtensionContent>
      </ext:UBLExtension>
      [...]
</ext:UBLExtensions>
```

En caso contrario

```
<ext:UBLExtensions
xmlns:ext="urn:oasis:names:specification:ubl:schema:xsd:CommonExtensi
onComponents-2">
      [...]
      <ext:UBLExtension>
            <cbc:ID>0000000001001</cbc:ID>
            <ext:ExtensionContent
      xmlns:ext="urn:oasis:names:specification:ubl:schema:xsd:CommonE
      xtensionComponents-2">
                  <odsig:document-signatures
            xmlns:odsig="urn:oasis:names:tc:opendocument:xmlns:digita
            lsignature:1.0">
                        <ds:Signature
            xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
            Id="signature-f1a5-9b1d-972b-d591">
                        [...]
                        </ds:Signature>
                  </odsig:document-signatures>
            </ext:ExtensionContent>
      </ext:UBLExtension>
      [...]
</ext:UBLExtensions>
```

5 Anexo II

Ejemplo de inclusión del elemento <cac:Signature> de CODICE

```
<cac:Signature>
      <cbc:ID>000000000</cbc:ID>
      [...]
      <cbc:SignatureMethod>http://docs.oasis-
open.org/ubl/securitysc/cd-dsigp-1/xmldsig-enveloped
      </cbc:SignatureMethod>
      [...]
</cac:Signature>
```

6 Glosario

CODICE: Componentes y Documentos Interoperables para la Contratación Electrónica. Arquitectura de componentes y documentos electrónicos estándar para el desarrollo de aplicaciones de contratación pública electrónica Española de conformidad con los procedimientos y prescripciones de la Directiva 2004/18 y de la normativa española en materia de contratación pública, así como con los estándares y recomendaciones internacionales aplicables a la identificación, denominación, definición y construcción de dichos componentes.

TSA: Time-Stamping Authority. Avala, aportando confiabilidad, que un conjunto de datos fue formado antes de un determinado instante de tiempo.

CA: Certificate Autority. Entidad de confianza responsable de emitir y revocar los certificados digitales utilizados en la firma electrónica.

Digital Signature: Método criptográfico utilizado en transmisión datos y documentos informáticos para demostrar su autenticidad.

Sello de tiempo o **Timestamping**: Valor que contiene una indicación de fecha y tiempo dada por una autoridad confiable que avala que un conjunto de datos existían antes de este punto en el tiempo.

UBL: *Universal Business Language*.

W3C*: World Wide Web Consortium*. Consorcio internacional que produce recomendaciones para la World Wide Web.

7 Bibliografía

[XMLDSig] D. Eastlake et al., *XML-Signature Syntax and Processing (Second Edition)*, http://www.w3.org/TR/2008/REC-xmldsig-core-20080610, W3C Recommendation, June 2008.

[99/93/EC] *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML, Official Journal L 013 , 19/01/2000 P. 0012 – 0020

[XAdES] *XML Advanced Electronic Signatures (XAdES),* http://webapp.etsi.org/WorkProgram/Report_WorkItem.asp?WKI_ID=28064, ETSI TS 101 903 ver. 1.4.1, June 2009.

[UBLforESig] Andrea Caccia, Roberto Cisternino, Oriol Bausà Peris, Julián Inza, *UBL Electronic Signature Profile Version 1.0*, OASIS Committee Draft 06 - 25 May 2010

[UBL] *Universal Business Language v2.0*, http://docs.oasis-open.org/ubl/os-UBL-2.0/, OASIS Standard, 12 December 2006.

[XPointer] S. DeRose, E. Maler, R. Daniel Jr., *XPointer xpointer() Scheme*, http://www.w3.org/TR/xptr-xpointer/, W3C Working Draft 19 December 2002.

[VALIDe] *Servicio de Validación de Firmas y Certificados Online* http://www.ctt.map.es/web/proyectos/valide, Ministerio de Administraciones Públicas