XML Digital Signature inside UBL 2.0

Author: Oriol Bausà
Date: 22-3-07

Introduction

UBL 2.0 has an ABIE to define signatures in a document, but there are other standard initiatives in the electronic signature area that are being adopted or recommended by different organizations or bodies.

In Spain, as in other EU countries, the electronic signature is mandatory for documents like the electronic invoice, and it's recommended the use of XAdES or XMLDSIG signatures.

Object

This document goal is to propose a system to add enveloped or detached electronic signatures in the standard UBL 2.0 documents.

Method

In documents where a Signature ABIE exists, we should use it to identify the Signatory or other data, but mainly to specify the location of the electronic signature, either the enveloped one or the detached one.

We should use the Extensions UBL 2.0 component to add the XMLDSIG or XAdES electronic signature.

Sample instance of the Signature component to incorporate in a document to add an enveloped signature.

```
<cac:Signature>
      <cbc:ID>9831223</cbc:ID>
      <cac:SignatoryParty>
            <cac:PartyIdentification>
                  <cbc:ID schemeName="CIF">A823647774</cbc:ID>
            </cac:PartyIdentification>
            <cac:PartyName>
                  <cbc:Name>EMPRESA, S.A.</cbc:Name>
            </cac:PartyName>
      </cac:SignatoryParty>
      <cac:DigitalSignatureAttachment>
         <cac:ExternalReference>
            <cbc:URI>#12345</cbc:URI>
         </cac:ExternalReference>
```

```
      </cac:DigitalSignatureAttachment>
  </cac:Signature>
```

The document signature can be referenced in the DigitalSignatureAttachment as an ExternalReference in a local or remote URI. In the local URI case, we will use an Extension component to specify the signature

Invoice Signed sample

```
<?xml version="1.0" encoding="UTF-8"?>
<Invoice xmlns:qdt="urn:oasis:names:specification:ubl:schema:xsd:QualifiedDatatypes-2"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:ccts="urn:oasis:names:specification:ubl:schema:xsd:CoreComponentParameters-
2" xmlns:stat="urn:oasis:names:specification:ubl:schema:xsd:DocumentStatusCode-1.0"
xmlns:cbc="urn:oasis:names:specification:ubl:schema:xsd:CommonBasicComponents-2"
xmlns:cac="urn:oasis:names:specification:ubl:schema:xsd:CommonAggregateComponents-2"
xmlns:udt="urn:un:unece:uncefact:data:draft:UnqualifiedDataTypesSchemaModule:2"
xmlns="urn:oasis:names:specification:ubl:schema:xsd:Invoice-2">
    <ext:Extensions>
        <ext:Extension>
            <ext:Extensioncontent>
                <ds:Signature id="12345">
                    <ds:SignedInfo>
                        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315#WithComments"/>
                        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
                        <ds:Reference URI="">
                            <ds:Transforms>
                                <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                            </ds:Transforms>
                            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                            <ds:DigestValue>cDcuM3dlGWvKqR8kasR9itD3dZk</ds:DigestValue>
                        </ds:Reference>
                    </ds:SignedInfo>
                    <ds:SignatureValue>98s3df7G2fsd49sd3fsE74dsf2</ds:SignatureValue>
                    <ds:KeyInfo ID="DSA Public Key">
                        <ds:KeyValue>
                            <ds:DSAKeyValue> DSAKEY </ds:DSAKeyValue>
                        </ds:KeyValue>
                    </ds:KeyInfo>
                </ds:Signature>
            </ext:Extensioncontent>
        </ext:Extension>
    </ext:Extensions>
    <cbc:UBLVersionID>2.0</cbc:UBLVersionID>
    <cbc:CustomizationID>urn:oasis:names:specification:ubl:xpath:Invoice-2.0:sbs-1.0-draft</cbc:CustomizationID>
    <cbc:ProfileID>bpid:urn:oasis:names:draft:bpss:ubl-2-sbs-invoice-notification-draft</cbc:ProfileID>
    <cbc:ID>A00095678</cbc:ID>
    <cbc:CopyIndicator>false</cbc:CopyIndicator>
    <cbc:UUID>849FBBCE-E081-40B4-906C-94C5FF9D1AC3</cbc:UUID>
    <cbc:IssueDate>2005-06-21</cbc:IssueDate>
    <cbc:InvoiceTypeCode>SalesInvoice</cbc:InvoiceTypeCode>
    <cbc:Note>sample</cbc:Note>
    <cbc:TaxPointDate>2005-06-21</cbc:TaxPointDate>
    <cac:OrderReference>
        <cbc:ID>AEG012345</cbc:ID>
        <cbc:SalesOrderID>CON0095678</cbc:SalesOrderID>
        <cbc:UUID>6E09886B-DC6E-439F-82D1-7CCAC7F4E3B1</cbc:UUID>
        <cbc:IssueDate>2005-06-20</cbc:IssueDate>
    </cac:OrderReference>
    <cac:Signature>
        <cbc:ID>76868</cbc:ID>
        <cac:SignatoryParty>
            <cac:PartyName>
                <cbc:Name>Signatory</cbc:Name>
            </cac:PartyName>
```

```
            </cac:SignatoryParty>
            <cac:DigitalSignatureAttachment>
                <cac:ExternalReference>
                    <cbc:URI>#12345</cbc:URI>
                </cac:ExternalReference>
            </cac:DigitalSignatureAttachment>
        </cac:Signature>
        <cac:AccountingSupplierParty>
            <cbc:CustomerAssignedAccountID>CO001</cbc:CustomerAssignedAccountID>
            <cac:Party>
                <cac:PartyName>
                    <cbc:Name>Consortial</cbc:Name>

    .....

</Invoice>
```