



IT- og Telestyrelsen

Ministeriet for Videnskab
Teknologi og Udvikling

OIOUBL Guideline

UBL 2.0 Signature

OIOUBL Signatur

Version 1.1



Udgivelsen er beskyttet af Creative Commons license, Navngivning 2.5 

Kolofon

Kontakt:

IT- & Telestyrelsen

E-mail: oioubl@itst.dk

OIOUBL Version 2.01

April 2007

**Ministeriet for Videnskab, Teknologi og Udvikling
IT- og Telestyrelsen**

Datastandardiseringskontoret

Holsteinsgade 63

DK-2100 København Ø

Phone +45 3545 0000

Fax +45 3545 0010

<http://www.itst.dk>

itst@itst.dk

Ophavsrettigheder for denne udgivelse, jævnført Creative Common, Navngivning 2.5: 

Det er tilladt at:

- *fremstille bearbejdede værker ud fra dette dokument*
- *at fremstille eksemplarer og gøre dokumentet tilgængeligt for almenheden*
- *at benytte dokumentet i kommerciel henseende*

under betingelse af tydelig kildehenvisning til denne udgivelse fra IT- og Telestyrelsen.

Læs mere om rettighederne på <http://creativecommons.org/licenses/by/2.5/deed.da>.

Indholdsfortegnelse

1.Forord.....	4
1.1Formål med dokumentet	4
2.Relevante klassser i UBL.....	5
3.Beskrivelse.....	6
3.1Hvad er en UBL digital signatur?.....	6
3.2Angivelse af hvem, der har underskrevet.....	6
3.3Angivelse af Validator.....	7
3.4Angivelse af signatur.....	8
3.5 I hvilke dokumenter skal digital signatur anvendes?.....	9

1. Forord

Denne guideline er ét af en række dokumenter, der beskriver formålet med og anvendelsen af de forretningsdokumenter der udgør den danske lokalisering af UBL 2.0 kaldet OIOUBL.

Der er udarbejdet en guideline for hvert af forretningsdokumenterne, og derudover er der lavet generelle guidelines, der beskriver brugen af de elementer, der går på tværs af dokumenterne.

Målgruppen for dokumentet er teknikere eller forretningkyndige, som beskæftiger sig med at få e-handel til at fungere i praksis.

1.1 Formål med dokumentet

Formålet med dokumentet er at beskrive anvendelsen af signatur i OIOUBL.

2. Relevante klasser i UBL

Signatur kan anvendes på header niveau i alle UBL dokumenter. Det anvendes desuden i følgende klasser i UBL:

- Endorsement
- CertificateOfOriginApplication

Ingen af disse klasser anvendes i OIOUBL. Signaturer skal afløftes, hvis de indgår i dokumentet.

3. Beskrivelse

Dette kapitel beskriver UBL signatur og dens anvendelse i OIOUBL.

3.1 Hvad er en UBL digital signatur?

UBL Signatur beskriver de digitale underskrifter, der er påført et dokument. En signatur klasse skal ikke forveksles med en signatur, der er anvendt til at sikring af transporten, eller en XMLDSIG signatur. Man anvender signatur i sine dokumenter, når der er en forretningsmæssig årsag til det i forbindelse med behandlingen af dokumentet. En UBL signatur kan ikke garantere oprigtigheden af et dokument bedre end en håndskrevet underskrift på et papir-dokument. Det er ydre forhold, så som sikre netværksforbindelser og tillid til sine serviceydbydere, der i sidste ende skal give denne sikkerhed for oprigtighed. På samme måde som klassen Contract refererer til en kontrakt, der er indgået og vedrører et dokument, anvendes signatur til at referere til de underskrifter, der er påført dokumentet.

3.2 Angivelse af hvem, der har underskrevet

Man har mulighed for at referere til den ved hjælp af et ID på signaturen og en beskrivelse (f.eks. firmanavnet) af den part, der har underskrevet dokumentet. Dette er vist i eksemplet for neden.

```
<cac:Signature >
  <cbc:ID>Peter.Hansen@oioubl.dk</cbc:ID>
  <cac:SignatoryParty>
    <cac:PartyName>
      <cbc:Name>OIO fælleskøb A/S</cbc:Name>
    </cac:PartyName>
    <cac:Person>
      <cbc:FirstName>Peter</cbc:FirstName>
      <cbc:FamilyName>Hansen</cbc:FamilyName>
      <cbc:Title>Indkøbschef</cbc:Title>
    </cac:Person>
  </cac:SignatoryParty>
</cac:Signature>
```

En sådan signatur kan anvendes af modtageren i sit forretningsflow. Der er kan f.eks. være krav til at en leverandør skal have bestemte signaturer i en ordre for at han må behandle den, hvis den overstiger bestemte beløb, eller bestemte varegrupper. Leverandøren må så bero sig på, at kundens system sikrer, at signaturen stammer fra den korrekte person.

3.3 Angivelse af Validator

Hvis dokumentet kan komme til leverandøren ad flere kilder kan det være en idé at angive, hvilket system, der har valideret signaturen og hvornår det er sket. Dette gøres med ValidatorID og ValidationDate and ValidationTime

```
<cac:Signature >
  <cbc:ID>Peter.Hansen@oioubl.dk</cbc:ID>
  <cbc:ValidationDate>2006-09-13</cbc:ValidationDate>
  <cbc:ValidationTime>14:20:02</cbc:ValidationTime>
  <cbc:ValidatorID>DoorTrade.net/signout</cbc:ValidatorID>
  <cac:SignatoryParty>
    <cac:PartyName>
      <cbc:Name>OIO fælleskøb A/S</cbc:Name>
    </cac:PartyName>
    <cac:Person>
      <cbc:FirstName>Peter</cbc:FirstName>
      <cbc:FamilyName>Hansen</cbc:FamilyName>
      <cbc:Title>Indkøbschef</cbc:Title>
    </cac:Person>
  </cac:SignatoryParty>
</cac:Signature>
```

Med denne angivelse bør det være muligt at finde den originale signatur hos DoorTrade.net, hvis eventuelle uoverensstemmelser skulle optræde. Dette afhænger naturligvis af de serviceaftaler, der er indgået mellem kunden, leverandøren og udbyderen af signatur validator servicen.

3.4 Angivelse af signatur

Det kan også lade sig gøre, at referere eller vedhæfte den signatur, der er anvendt i dokumentet. Hvis man gør det, bør man også angive det dokument, underskriveren har set, da han underskrev dokumentet. Dette er nemlig sjældent det samme som det fremsendte dokument. Oftest er det en html eller billede-repræsentation (f.eks. jpg eller Tiff) af xml-dokumentet. Dette er vist i nedestående eksempel:

```
<cac:Signature>
  <cbc:ID schemeID="CVR">16356709</cbc:ID>
  <cbc:ValidationDate>2006-09-13</cbc:ValidationDate>
  <cbc:ValidationTime>15:20:02</cbc:ValidationTime>
  <cbc:ValidatorID>DoorTrade.net/signout</cbc:ValidatorID>
  <cbc:CanonicalizationMethod>http://www.w3.org/TR/2001/REC-xml-c14n-20010315
</cbc:CanonicalizationMethod>
  <cbc:SignatureMethod>http://www.w3.org/2000/09/xmldsig#dsa-sha1</cbc:SignatureMethod>
  cac:SignatoryParty>
    <cac:PartyIdentification>
      <cbc:ID schemeID="DK:CVR">DK16356709</cbc:ID>
    </cac:PartyIdentification>
    <cac:PartyName>
      <cbc:Name>Tavleleverandøren</cbc:Name>
    </cac:PartyName>
    <cac:PartyLegalEntity>
      <cbc:RegistrationName>Tavleleverandøren</cbc:RegistrationName>
      <cbc:CompanyID schemeID="CVR">DK16356706</cbc:CompanyID>
    </cac:PartyLegalEntity>
    <cac:Contact>
      <cbc:Name>Hugo Jensen</cbc:Name>
      <cbc:Telephone>15812337</cbc:Telephone>
      <cbc:ElectronicMail>Hugo@tavl.dk</cbc:ElectronicMail>
    </cac:Contact>
  </cac:SignatoryParty>
  <cac:DigitalSignatureAttachment>
    cbc:EmbeddedDocumentBinaryObject mimeType="text/xml">
CA8U21nbnmF0dXJlIHhtbG5zPSJodHRwOi8vd3d3LnczLm9yZy8yMDAwLzA5L3htbGRzaWcwiIj4NCiAgICA8U21nbnmVksW5mbz4N
CiAgICAgIDxYW5vbmljYWxpemF0aW9uTWV0aG9kIEFsZ29yaXR0bT0iaHR0cDovL3d3dy53My5vcmcvVFImMjAwMS9SRUMteG1
sLWMxNG4tMjAwMTAzMjU1IC8+DQogICAgICA8U21nbnmF0dXJlTWV0aG9kIEFsZ29yaXR0bT0iaHR0cDovL3d3dy53My5vcmcvMj
AwMC8wOS94bWxkc2lnI3JzYS1zaGEeIiAvPg0KICAgICAgPFJlZmVzZW5jZSBVUkk9IiI+DQogICAgICAgIDxUcmFuc2ZvcmlzP
g0KICAgICAgICAgIDxUcmFuc2ZvcmlzPj0KICAgICAgPC9UcmFuc2ZvcmlzPj0KICAgICAgICA8RGlnczN0TWV0aG9kIEFsZ29yaXR0bT0
iaHR0cDovL3d3dy53My5vcmcvMjAwMC8wOS94bWxkc2lnI3NoYTEiIC8+DQogICAgICAgIDxUcmFuc2ZvcmlzPj0KICAgICAgIDxUcmFuc2ZvcmlzPj0K
poOXJFbFVpeEpwMDJpUzdnN1E9PC9EaWdlc3RwYXN1ZT4NCiAgICAgIDxUcmFuc2ZvcmlzPj0KICAgICAgIDxUcmFuc2ZvcmlzPj0K
A0KICA8L1NpZ25hdHVyZT4=
    </cbc:EmbeddedDocumentBinaryObject>
  </cac:DigitalSignatureAttachment>
  <cac:OriginalDocumentReference>
    <cbc:ID>A00095678</cbc:ID>
    <cbc:CopyIndicator>>false</cbc:CopyIndicator>
    <cac:Attachment>
      <cac:ExternalReference>
        <cbc:URI>archieive.DoorTrade.net/signature/16356709/6E09886B-DC6E-43EE-
82D1-7CCAC7F4E3B1.jpg</cbc:URI>
        <cbc:DocumentHash>UxNQUFPLMnHHJU1tQ1p0dU1GUXhEUzOIUbhGHJ
        </cbc:DocumentHash>
        <cbc:ExpiryDate>2011-08-13</cbc:ExpiryDate>
      </cac:ExternalReference>
    </cac:OriginalDocumentReference>
  </cac:Signature>
```

I eksemplet er det XMLDSIG signaturen (Se <http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/Overview.html>) vedlagt som mimeattachement (Base64 encoded xml), mens det originale dokument er linket til via en URI. Man kan anvende CanonicalizationMethod og SignatorMethod til at kontrollere signatoren op imod det oprindelige dokument.

Hvis der er aftale om en sikker transformeringsmetode, som alle parter har tillid til, kan det originale dokument i stedet repræsenteres ved en liste af de stier (XPath) fra dokument, som har

dannet kilde til det, underskriveren har set. Se nærmere om dette i OIOUBL_GUIDE_DOKUMENTREF (Ref. G21).

3.5 I hvilke dokumenter skal digital signatur anvendes?

De konkrete krav til anvendelse af digital signatur aftales bilateralt. Et eksempel kan være, at kunden køber ind ved hjælp af en indkøbsløsning og derfor ikke selv har direkte kontrol over , hvem der køber hvad ind. I disse tilfælde vil det være ordren, der påføres digital signatur.