

SCTS-ENV

Swedish Customs Technical Specification

Kuvertspecifikation

Specifikation för kuvert och metadata

Version 1.0.2

Innehåll

1	Introduktion.....	3
2	Referenser.....	3
3	Dokumenthistorik	3
4	Kuvertets övergripande struktur	4
4.1	SOAP-nivån	4
4.2	XML Signatur-nivån	4
4.3	WCO Metadata-nivån	4
4.4	WCO Verksamhetsmeddelandenivån.....	5
5	Bindning till transportprotokollet	5
6	Introduktion till informationsmodellerna i denna specifikation.....	5
7	Informationsmodell för SOAP-kuvert.....	6
7.1	Fält för avsändarens och mottagarens adressuppgifter i kuvertet.....	6
7.2	Element i Envelope	7
7.3	Element i Envelope/Body	9
7.4	Partsidentiteter i SOAP-kuvertet	10
8	Informationsmodell för Tullverkets användning av XML Signature	11
8.1	Signering av dokument	11
8.2	Element i XML Signature.....	12
8.3	Mer information om signeringsprocessen.....	13
9	Informationsmodell för WCO Metadata.....	14
10	Parametersättning av kuvertet	15
11	XML-relaterade krav.....	16
12	Övriga krav.....	17
13	Användning av kuvertets scheman	17
14	Namespace och versioner	17
15	Kuvertexempel	18

1 Introduktion

Denna specifikation beskriver hur WCO-baserade XML-meddelanden signeras och förpackas. Specifikationen är avsedd att läsas av personer som bygger stöd för en elektronisk samverkan med Tullverket. Specifikationen beskriver inga specifika verksamhetsprocesser utan fokuserar på kuvertering av meddelanden vid den elektroniska överföringen. Kuvert är en obligatorisk komponent vid meddelandeutväxling av WCO-baserade XML-meddelanden med OFTP2 men kan även tillämpas med andra transportprotokoll.

Specifikationen beskriver inte transportprotokoll och tekniska svarsmeddelanden.

2 Referenser

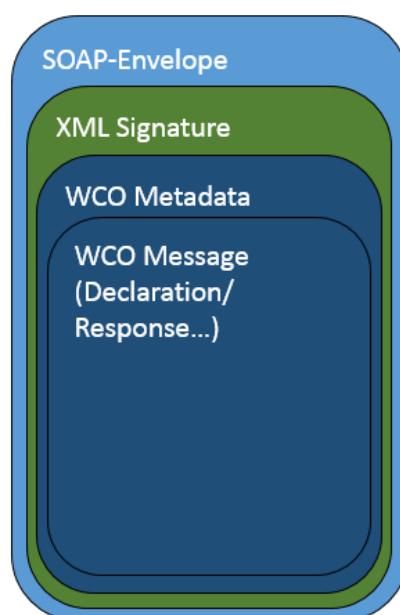
WCO Data model	http://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/pf_tools_datamodel.aspx
XML Schema	http://www.w3.org/XML/Schema
XPATH	http://www.w3.org/TR/xpath20/
SOAP Version 1.2	http://www.w3.org/TR/soap/
Web Services Addressing (WS-Addressing)	http://www.w3.org/TR/2006/REC-ws-addr-core-20060509/
XML Advanced Electronic Signatures (XAdES)	http://uri.etsi.org/01903/v1.4.1/
XML Signature Syntax and Processing Version 1.1	http://www.w3.org/TR/xmlsig-core/
Exclusive XML Canonicalization Version 1.0	http://www.w3.org/TR/xml-exc-c14n/

3 Dokumenthistorik

Version	Ändring	Datum
1.0	Första versionen	2016-05-13
1.0.1	Tillägg av XML-relaterade krav gällande whitespace.	2017-05-01
1.0.2	Tillägg av avsnitt 12, Övriga krav	2018-06-01

4 Kuvertets övergripande struktur

Tullverkets tekniska kuvert består av fyra nivåer där den fjärde nivån är det verksamhetsmeddelande som utväxlas mellan Tullverket och uppgiftslämnaren/uppgiftsmottagaren. Användning av WCO Metadata är obligatoriskt vid utväxling av verksamhetsmeddelande som bygger på WCO XML men det är även möjligt att andra XML-standarder kan kuverteras.



4.1 SOAP-nivån

Kuvertets översta nivå bygger på standarden SOAP version 1.2. Detta dokument samt tillhörande XML Scheman beskriver Tullverkets användning av standarden. Tullverket kompletterar standarden med egna element för adressinformation och dokumenttyper. Övriga element som används i kuvertet definieras i standarderna SOAP och WS-Addressing.

4.2 XML Signatur-nivån

Kuvertet tillåter tre typer av inkapslade objekt – BASE64-kodad fil/dokument, XML-dokument alternativt signerat XML-dokument. Då signatur används appliceras en extra nivå i kuvert-hierarkin.

4.3 WCO Metadata-nivån

WCO Metadata används för att ge tekniska upplysningar om det verksamhetsmeddelande som utväxlas. Exempelvis uppgifter om verksamhetsmeddelandets version och vilken specifik process det är avsett för.

4.4 WCO Verksamhetsmeddelandenivån

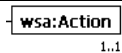
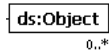
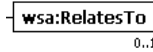



Innehåll och struktur på verksamhetsmeddelanden (såsom en importdeklaration) definieras i separata specifikationer. Vissa parametrar i kuvertet styrs dock av verksamhetsmeddelandets format. I respektive samverkansspecifikation finns ett avsnitt som parametersätter kuvertet för de uppgifter som är meddelandespecifika (såsom version och meddelandetyper).

5 Bindning till transportprotokollet

Tullverkets kuvert är inte bundet till något specifikt transportprotokoll.

6 Introduktion till informationsmodellerna i denna specifikation

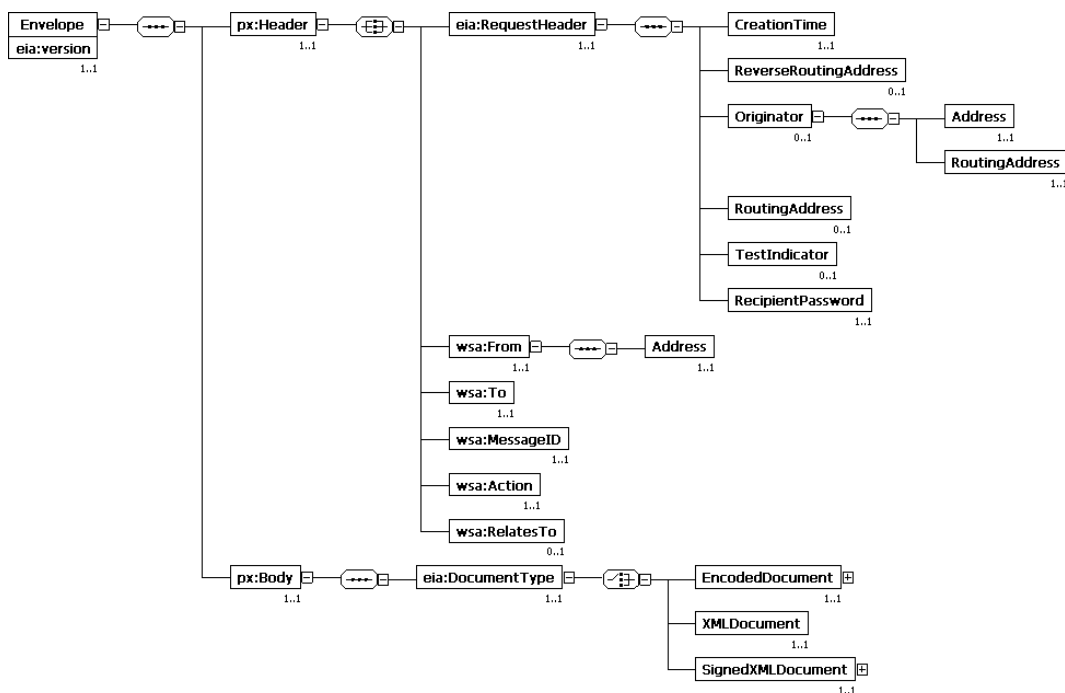
Diagrammen som illustrerar informationsmodellerna är en grafisk representation av XML-schemat och ska tolkas på följande sätt:

Exempel på notation	Förklaring
	Obligatoriskt element. Antalet tillåtna repetitioner anges under rutan. Elementet får anges minst 1 gång och maximalt 1 gång.
	Valfritt element som kan upprepas. Antalet tillåtna repetitioner anges under rutan. Elementet får anges minst 0 gånger och maximalt * (oändligt antal) gånger. I vissa fall visas istället max antal repetitioner såsom 1..99 vilket ska tolkas som minst 1 och max 99. Observera att det ibland kan förekomma regler som under vissa omständigheter gör att även valfria element (enligt schemat) blir obligatoriska (ur verksamhetssynpunkt).
	Valfritt element. Antalet tillåtna repetitioner anges under rutan. Elementet får anges minst 0 gånger och maximalt 1 gång. Observera att det ibland kan förekomma regler som under vissa omständigheter gör att även valfria element (enligt schemat) blir obligatoriska (ur verksamhetssynpunkt).
	Underliggande element kan anges i valfri ordningsföljd.
	Underliggande element måste anges i den ordningsföljd som specificeras i schemat.
	Endast ett av underliggande element får användas.

OBS - De värden som anges i XML-koden i detta dokument ska betraktas som exempel.

7 Informationsmodell för SOAP-kuvert

Nedan följer en beskrivning av de element som används. SOAP-kuvertet innehåller uppgifter som behövs för korrekt överföring, routing och spårning av meddelanden.



7.1 Fält för avsändarens och mottagarens adressuppgifter i kuvertet

Fält	Funktion
wsa:To	Obligatorisk primär partsidentifiering på mottagaren (organisationsnummer)
eia:RoutingAddress	Identifiering av mottagarens interna funktion/system som försändelsen ska styras till
wsa:From	Obligatorisk primär partsidentifiering på avsändaren (organisationsnummer)
eia:ReverseRoutingAddress	Identifiering av avsändarens interna funktion/system som svaret på denna försändelse ska styras till

7.2 Element i Envelope

Envelope/@version

```
<Envelope eia:version="1.0"> ... </Envelope>
```

I attributet version, placerat direkt i elementet Envelope, anges **versionsnumret** på denna specifikation enligt principen "major"."minor" (exempelvis 1.0). Om specifikationens versionsnummer har en tredje nivå (icke-funktionell ändring) ska denna inte anges.

Header/RequestHeader/CreationTime

```
<eia:CreationTime>2015-04-17T15:30:47Z</eia:CreationTime>
```

Datum och klockslag då kuvertet skapades. Datumet och klockslaget kan vara tidigare än översändningstidpunkten och ersätter inte eventuell tidstämpel som sätts av transportprotokollet. CreationTime ska sättas till UTC-tid (alltså svensk normaltid minus en timma respektive minus två timmar vid sommartid).

Header/RequestHeader/ReverseRoutingAddress

```
<eia:ReverseRoutingAddress>ABCD1234</eia:ReverseRoutingAddress>
```

En vidareadress används för styrning till intern funktion/system. **Avsändarens vidareadress** instruerar motparten vart svarsmeddelanden ska sändas. Uppgiften, avsändarens vidareadress, framgår av överenskommelse för elektronisk uppgiftslämning.

Motsvarar UNB S002.0008 i EDIFACT.

Header/RequestHeader/Originator

```
<eia:Originator>
  <eia:Address>urn:iso:6523:icd:0007:5544332211</eia:Address>
  <eia:RoutingAddress>ABCD1234</eia:RoutingAddress>
</eia:Originator>
```

Den **ursprungliga avsändarens** identifierare för adress och routingadress. Ursprunglig avsändare används endast om den skiljer sig från *Header/From*.

OBS – Originator används endast i undantagsfall och då specifik överenskommelse finns. Elementet används inte vid normal uppgiftsinlämning för import och exportdeklarationer.

Header/RequestHeader/RoutingAddress

```
<eia:RoutingAddress>CDEF1234</eia:RoutingAddress>
```

En vidareadress används av mottagaren för styrning till intern funktion/system. Uppgiften, **mottagarens vidareadress**, framgår av överenskommelse för elektronisk uppgiftslämning.

Motsvarar UNB S003.0014 i EDIFACT.

Header/RequestHeader/TestIndicator

```
<eia:TestIndicator>0</eia:TestIndicator>
```

Testindikator visar om försändelsen (kuvert och verksamhetsmeddelande) ska hanteras som ett testmeddelande av mottagaren. 0 innebär att försändelsen inte är test och 1 innebär att försändelsen är avsedd för test. Ytterligare värden kan förekomma och beskrivs i så fall i kodlistan för testindikator.

Om XML-elementet utelämnas betraktas försändelsens status som produktion (alltså värde 0).

Header/RequestHeader/RecipientPassword

```
<eia:RecipientPassword>tilldelat-lösenord</eia:RecipientPassword>
```

Lösenordet tilldelas i överenskommelsen för elektronisk uppgiftslämning.

Header/From

```
<wsa:From>
  <wsa:Address>urn:iso:6523:icd:0007:5544332211</wsa:Address>
</wsa:From>
```

Identitet på avsändaren av försändelsen. Identiteten ska avse uppgiftslämnaren eller Tullverket (beroende på vem som är avsändare) och inte eventuell tredjepartsoperatör som agerar meddelandeväxel.

Motsvarar UNB S002.0004 och 0007 i EDIFACT.

Header/To

```
<wsa:To>urn:iso:6523:icd:0007:5599887766</wsa:To>
```

Identitet på mottagaren av försändelsen. Identiteten ska avse uppgiftslämnaren eller Tullverket (beroende på vem som är mottagare) och inte eventuell tredjepartsoperatör som agerar meddelandeväxel.

Motsvarar UNB S003.0010 och 0007 i EDIFACT.

Header/MessageID

```
<wsa:MessageID>348c3340-51d2-11e3-8f96-0800200c9a33</wsa:MessageID>
```

En unik identitet på kuvertet, skapad av avsändaren. MessageID måste vara unik för varje kuvert som skapas. MessageID ska inte förväxlas med det bifogade verksamhetsmeddelandets eventuella ID-begrepp (såsom LRN). Det ska inte heller förväxlas med eventuellt ID-begrepp som skapas av transportprotokollet (exempelvis OFTP2). MessageID måste vara globalt unikt och följa UUID-format (exempelvis: 348c3340-51d2-11e3-8f96-0800200c9a33)

Motsvarar UNB 0020 i EDIFACT.

Header/Action

```
<wsa:Action>urn:tullverket:SE-CL0002:RESI-TLKV</wsa:Action>
```

Ett namn på den tjänst/funktion som är definierad för försändelsen (applikationsreferens). Används för att verifiera att meddelandets kuvert stämmer överens med vad som är godkänt för uppgiftlämnandet, att godkänd och korrekt meddelandetyper används samt att signatur är applicerad om det krävs. Slutligen används det för styrning till rätt internt system.

Action formateras på följande sätt:

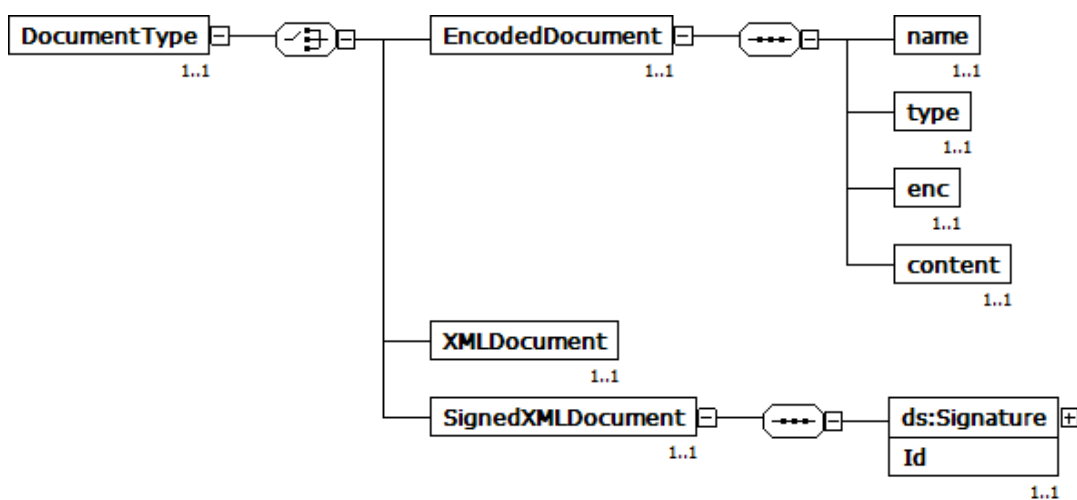
urn:tullverket:SE-CL0002:XYZ, där XYZ är applikationsreferensen och återfinns i samverkansspecifikationen för det aktuella verksamhetsmeddelandet. En sammanställning över samtliga applikationsreferenser finns i kodlistan SE-CL0002.

Motsvarar UNB 0026 i EDIFACT.

Header/RelatesTo

```
<wsa:RelatesTo>448c3340-51d2-11e3-8f96-0800200c9a33</wsa:RelatesTo>
```

Då ett svarsmeddelande av typen TechnicalLevel eller FunctionalLevel skickas (se specifikationen för svarsmeddelanden) används RelatesTo för att koppla samman detta kuvert med ursprungliga kuvertet. RelatesTo ska innehålla värdet från ursprungskuvertets MessageID-fältet.

7.3 Element i Envelope/Body**Body/DocumentType**

Tullverkets kuvert tillåter tre olika metoder att förpacka verksamhetsmeddelandet. Samverkansspecifikationen fastställer vilken metod som gäller för ett specifikt verksamhetsmeddelande.

Endast ett verksamhetsmeddelande kan inkluderas i kuvertet. Metoderna för kuvertering är:

1. BASE64-encodad fil (exempelvis PDF)

DocumentType/EncodedDocument

```
<eia:DocumentType>
  <eia:EncodedDocument>
    <eia:name>Delivery note</eia:name>
    <eia:type>PDF</eia:type>
    <eia:enc>BASE64</eia:enc>
    <eia:content>Q1p0dU1GUXhEUzhi</eia:content>
  </eia:EncodedDocument>
</eia:DocumentType>
```

2. XML-dokument (osignerat)

DocumentType/XMLDocument

```
<eia:DocumentType>
  <eia:XMLDocument>< Metadata>...</Metadata></eia:XMLDocument>
</eia:DocumentType>
```

3. Signerat XML-dokument

DocumentType/SignedXMLDocument

```
<eia:DocumentType>
  <eia:SignedXMLDocument>
    <Signature>...</Signature>
  </eia:SignedXMLDocument>
</eia:DocumentType>
```

Instruktioner för hur signaturen struktureras beskrivs i avsnittet "Signering av dokument"

7.4 Partsidentiteter i SOAP-kuvertet

Partsidentiteter formateras på följande sätt:

urn:iso:6523:icd:0007:XXXXXXXXXX där XXXXXXXXXXXX avser svenskt organisationsnummer. Värdet 0007 i prefixet kvalificerar/indikerar att IDt är ett svenskt organisationsnummer. Tillåten identitetstyp är

Kod	Betydelse
0007	Svenskt organisationsnummer

8 Informationsmodell för Tullverkets användning av XML Signature

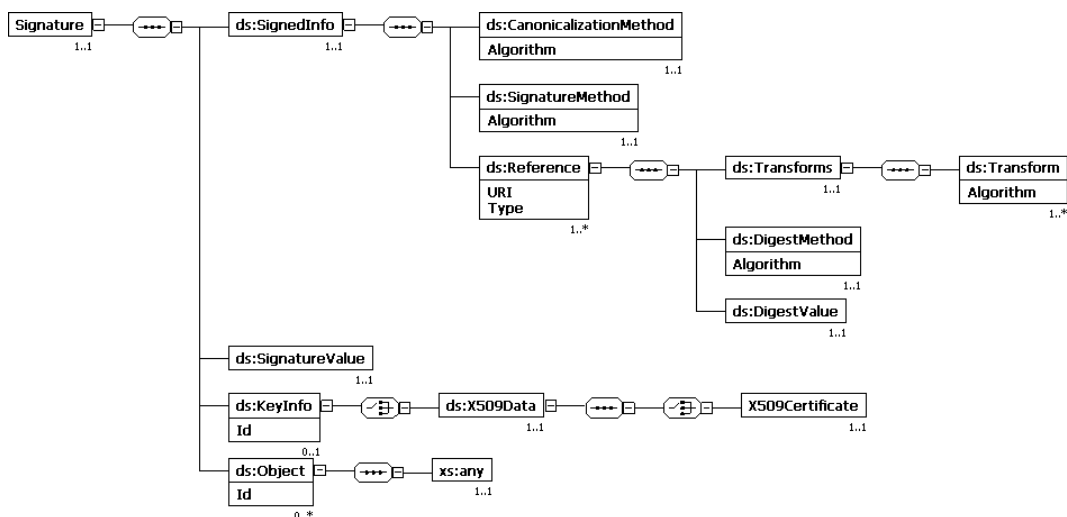
8.1 Signering av dokument

Signering av dokument ska göras i enlighet med W3C-standarden "XML Signature". Standarden beskriver både processen för att skapa en elektronisk signatur och hur den ska förpackas i XML-format. Standarden beskriver olika sätt att paketera signaturen och det signerade dokumentet. I Tullverkets kuvert används "Enveloping"-metoden vilket innebär att signatur-strukturen omsluter det signerade dokumentet.

Tullverket tillämpar XAdES som är en utökning till XML Signature för att komplettera med en tidsstämpel för signeringstidpunkten.

Vid kontroll av digitala signaturer måste den del av XML-meddelandet som signerats exakt överensstämma med den XML som användes vid signeringen. Detta innebär att varje tecken och dess inbördes ordning måste överensstämma mellan signering och kontroll för att signaturen ej ska betraktas som bruten.

Den kanoniska formen för det signerade dokumentet ska följa standarden "Exclusive XML Canonicalization" från W3C.



Illustrationen ovan beskriver den delmängd av XML-signature som används av Tullverket. Elementen och attributen som beskrivs här är de som är signifikanta/nödvändiga för Tullverkets hantering. Om standardprogramvaror skapar ytterligare element eller attribut utöver det som beskrivs här måste de tas bort.

8.2 Element i XML Signature

Signature/SignedInfo/CanonicalizationMethod

```
<xsig:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
```

Attributet Algorithm i Elementet CanonicalizationMethod indikerar kanoniseringsmetoden som använts för formatering av SignedInfo-element och dess underelement.

Signature/SignedInfo/SignatureMethod

```
<xsig:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
```

Attributet Algorithm i Elementet SignatureMethod indikerar vilken algoritm som använts för att generera signaturen.

Signature/KeyInfo/X509Data

```
<xsig:KeyInfo Id="Keyinfo-Id">
  <xsig:X509Data>
    <xsig:X509Certificate>MIICdDeGg ..... AwIBAIQ9sN9xKY=</xsig:X509Certificate>
  </xsig:X509Data>
</xsig:KeyInfo>
```

Det BASE64-kodade signeringscertifikatet som används för signering av meddelandet läggs i elementet KeyInfo/X509Data/X509Certificate. Exemplet ovan är nedkortat.

Signature/SignedInfo/Reference (för det signerade verksamhetsmeddelandet)

```
<xsig:Reference Type="http://www.w3.org/2000/09/xmldsig#Object" URI="#signature1">
  <xsig:Transforms>
    <xsig:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
  </xsig:Transforms>
  <xsig:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
  <xsig:DigestValue>ljE7AC1c5kzITeggUMjJrQrIW9s=</xsig:DigestValue>
</xsig:Reference>
```

Reference-elementen innehåller en referens till det signerade objektet samt identifiering av den kanoniseringsmetod som använts för verksamhetsmeddelandet. Det innehåller också verksamhetsmeddelandets digest-värde (hash-värdet) samt algoritmen som använts för att beräkna den. Digest-värdet ska vara BASE64-kodat.

Signature/SignedInfo/Reference (för SignedProperties enligt XAdES)

```
<xsig:Reference Type="http://uri.etsi.org/01903#SignedProperties"
URI="#SignedPropertiesId">
  <xsig:Transforms>
    <xsig:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
  </xsig:Transforms>
  <xsig:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
  <xsig:DigestValue>cmbssiUG07eZmloZBTc1rs7TRUIqU=</xsig:DigestValue>
</xsig:Reference>
```

På motsvarande sätt som referensen för verksamhetsmeddelandet så ingår även en tidsstämpel för signeringstidpunkten. Användning av ska följa standarden XAdES. Strukturen på uppgifterna beskrivs nedan under Signature/Object.

Signature/SignedInfo/Reference (för KeyInfo)

```
<xsig:Reference Type="http://www.w3.org/2000/09/xmlsig#KeyInfo" URI="#Keyinfo-Id">
  <xsig:Transforms>
    <xsig:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
  </xsig:Transforms>
  <xsig:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
  <xsig:DigestValue>7jyokXEpSe3Y69+H0...2WtUz2faEWnf24=</xsig:DigestValue>
</xsig:Reference>
```

Referens till certifikatet som används för signering läggs i en SignedInfo/Reference på samma sätt som för tidsstämpeln och verksamhetsmeddelandet.

Signature/SignatureValue

```
<xsig:SignatureValue>Wv+J/.....aFCG7SqvFwrH35vQQ==</xsig:SignatureValue>
```

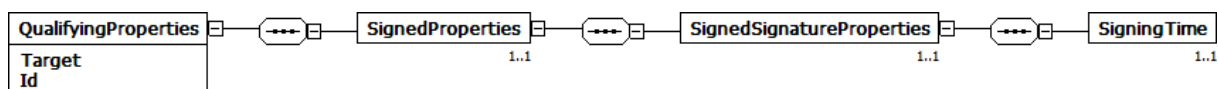
SignatureValue innehåller det faktiska värdet av den digitala signaturen, BASE64-kodat.

Signature/Object (placering av verksamhetsmeddelandet)

```
<xsig:Object Id="signature1">
  <MetaData>.....</MetaData>
</xsig:Object>
```

Verksamhetsmeddelandet (elementet MetaData i exemplet ovan) placeras i Object-elementet. Id-attributet används som pekare i SignedInfo/Reference och kopplar därmed en specifik signatur till detta objekt.

Signature/Object (placering av tidsstämpel)



```
<QualifyingProperties xmlns="http://uri.etsi.org/01903/v1.3.2#" Target="#xmlsig-Signature">
  <SignedProperties Id="SignedPropertiesId">
    <SignedSignatureProperties>
      <SigningTime>2015-04-05T09:11:24.268Z</SigningTime>
    </SignedSignatureProperties>
  </SignedProperties>
</QualifyingProperties>
```

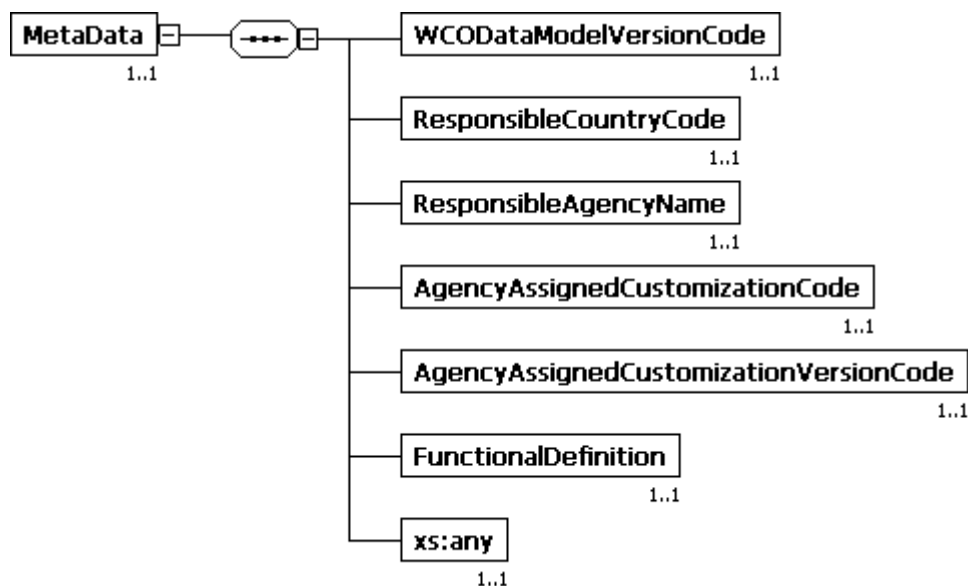
Signeringstidpunkten läggs, på samma sätt som för verksamhetsmeddelandets, i ett Object-element. Datum och klockslaget ska anges i UTC-tid.

8.3 Mer information om signeringsprocessen

Information om signeringsprocessen finns att läsa i dokumentet "Riktlinjer och anvisningar avseende säkerhet vid informationsutbyte via EDI" på Tullverket.se.

9 Informationsmodell för WCO Metadata

WCO Metadata innehåller uppgifter som beskriver verksamhetsmeddelandet såsom version och vem som utfärdat den specifikation som följs (Tullverket).



WCODataModelVersionCode

```
<WCODataModelVersionCode>3.5-SE</WCODataModelVersionCode>
```

Versionsnamn på den semantiska datamodellen som används som bas för verksamhetsmeddelandet.

ResponsibleCountryCode

```
<ResponsibleCountryCode>SE</ResponsibleCountryCode>
```

Landskoden avser den organisationen som tagit fram specifikationen för verksamhetsmeddelandet.

ResponsibleAgencyName

```
<ResponsibleAgencyName>Swedish Customs</ResponsibleAgencyName>
```

Namn på den organisationen som tagit fram specifikationen för verksamhetsmeddelandet

AgencyAssignedCustomizationCode

```
<AgencyAssignedCustomizationCode>CWHOP</AgencyAssignedCustomizationCode>
```

Identifiering av den samverkansspecifikation för informationsutbytet som använts.

AgencyAssignedCustomizationVersionCode

```
<AgencyAssignedCustomizationVersionCode>1</AgencyAssignedCustomizationVersionCode>
```

Versionen på den samverkansspecifikation som använts.

FunctionalDefinition

```
<FunctionalDefinition>CWDS</FunctionalDefinition>
```

Verksamhetsmeddelandets namn.

10 Parametersättning av kuvertet

Värden för vissa element som beskrivits ovan är beroende av process och typ av verksamhetsmeddelande. Dessa värden finns samlade i samverkansspecifikationen för det aktuella verksamhetsmeddelandet. Uppgifter som är relaterade till den elektroniska signaturen definieras i Tullverkets riktlinjer kring säkerhet vid informationsutbyte (mer om detta finns att läsa på Tullverket.se). Partsspecifika uppgifter (såsom lösenord och partsidentitet) definieras i överenskommelsen för elektronisk uppgiftslämning.

De aktuella elementen är:

Beskrivning	Värde definieras i	Nivå	Element
Applikationsreferens	Samverkansspecifikation	SOAP	Envelope/Header/Action
Versionsnamn på WCO datamodell	Samverkansspecifikation	Metadata	WCODataModelVersionCode
Landkod för ansvarig utgivare	Samverkansspecifikation	Metadata	ResponsibleCountryCode
Namn på ansvarig utgivare	Samverkansspecifikation	Metadata	ResponsibleAgencyName
Kod för samverkansspecifikation	Samverkansspecifikation	Metadata	AgencyAssignedCustomizationCode
Version på samverkansspecifikation	Samverkansspecifikation	Metadata	AgencyAssignedCustomizationVersionCode
Meddelandenamn	Samverkansspecifikation	Metadata	FunctionalDefinition
Metod för checksummeberäkning	Riktlinjer kring säkerhet	Signatur	DigestMethod/@Algorithmt
Metod för beräkning av elektronisk signatur	Riktlinjer kring säkerhet	Signatur	SignatureMethod/@Algorithmt

Kanoniseringsmetod	Riktlinjer kring säkerhet	Signatur	CanonicalizationMethod/@Algoritm
Avsändare	Överenskommelse för elektronisk uppgiftslämning	SOAP	wsa:From
Mottagare	Överenskommelse för elektronisk uppgiftslämning	SOAP	wsa:To
Avsändarens vidareadress	Överenskommelse för elektronisk uppgiftslämning	SOAP	eia:RequestHeader/ReverseRoutingAddress
Ursprunglig avsändare	Överenskommelse för elektronisk uppgiftslämning	SOAP	eia:RequestHeader/Originator
Mottagarens vidareadress	Överenskommelse för elektronisk uppgiftslämning	SOAP	eia:RequestHeader/RoutingAddress
Lösenord	Överenskommelse för elektronisk uppgiftslämning	SOAP	eia:RequestHeader/RecipientPassword

11 XML-relaterade krav

1. UTF-8 ska användas som encoding på samtliga nivåer
2. Elementen i tns:Header kan anges i valfri ordningsföljd
3. Elementen i eia:RequestHeader måste anges i den ordningsföljd som XML-schemat beskriver
4. Relevanta namespace för respektive nivå bör deklarerars på det element som bildar roten för nivån (alltså Envelope/Signature/Metadata/Verksamhetsmeddelande)
5. Vid routing av meddelanden är det viktigt att inget förändras i XML-strukturen då signeringen förutsätter oförändrat innehåll (se upp med programvaror som döper om namespace-prefix)
6. XML-element som inte innehåller ett värde eller andra element/attribut ska utelämnas.
7. XML-element som innehåller ett värde ska inte inledas eller avslutas med whitespace (tab, radbrytning eller mellanslag)

12 Övriga krav

Av tekniska skäl är storleken på en överföring begränsad till 5 MB. För att skicka överföringar över 1 MB krävs komprimering på transportprotokollsnivå.

13 Användning av kuvertets scheman

Kuvertets XML-scheman består av flera olika delar med olika syften. De olika delarna är sammansatta utifrån standarder från olika organisationer (W3C, WCO och Tullverket). För att förenkla implementationen har Tullverket skapat anpassade scheman där funktionalitet som inte används i vissa fall är borttagen.

Nedan listas de scheman som används för validering. Respektive schema har i sin tur importerade schemamoduler (separata filer). Samtliga filer måste finnas tillgänglig för att validering ska fungera.

1. soap-envelope.xsd - Validerar kuvertets huvud inklusive signatur
2. XAdES.xsd - Validerar tidstämpel
3. DocumentMetaData_1p0.xsd - validerar verksamhetsmeddelandets metadata.

14 Namespace och versioner

Rotelement/ startelement	Relevanta Namespace	Prefix som används som exempel i denna specifikation
Envelope	http://www.w3.org/2003/05/soap-envelope http://tullverket.se/ei/addressing-1 http://www.w3.org/2005/08/addressing	px eia wsa
Signature	http://www.w3.org/2000/09/xmldsig#	xsig
QualifyingProperties (för tidsstämpeln)	http://uri.etsi.org/01903/v1.3.2#	[inget, default]
MetaData	urn:se:customs:datamodel:WCO:DocumentMetadata:1	[inget, default]
Verksamhets- meddelande	Se relevant meddelandespecifikation	-

15 Kuvertexempel

Ett kuvertexempel som visar hur man använder SignedXMLDocument finns i bilaga ENV-Envelope-UseCase1.xml