

---

## Open CDA 2008

---

### **Soveltamisopas CDA-asiakirjojen allekirjoittamiseen XML-allekirjoituksilla**

**Versio 1.11  
31.12.2009**



Asiakas: HL7 Finland ry  
Projekti: Open CDA 2007

Versio 2 (17)  
31.12.2009

Dokumentti: Soveltamisopas CDA-  
asiakirjojen allekirjoittamiseen XML-  
allekirjoituksilla

### Versiohistoria:

Versio:	Pvm:	Laatijat:	Muutokset:
1.00	4.12.2008	MH	
1.10	31.12.2009	MH	
1.11	1.11.2010	MH	ID-attribuutin kirjoitusasu tarkistettu ja yhdenmukaistettu

MH = Mikael Himanka



## Sisällysluettelo

<b>1.</b>	<b>JOHDANTO .....</b>	<b>4</b>
<b>2.</b>	<b>TAUSTAA.....</b>	<b>4</b>
2.1	XML ALLEKIRJOITUS .....	4
2.2	XML ALLEKIRJOITUKSEN HAASTEET.....	5
<b>3.</b>	<b>ALLEKIRJOITUS CDA ASIAKIRJOISSA .....</b>	<b>5</b>
3.1	DOKUMENTISSA KÄYTETYT MERKINNÄT.....	5
3.2	YLEISET PERIAATTEET.....	6
3.3	RAKENNE .....	6
3.4	CDA ASIAKIRJAN XML ALLEKIRJOITUKSEN VAATIMUKSET .....	7
3.5	KOHDISTAMINEN .....	7
3.6	MONIALLEKIRJOITUS.....	9
<b>4.</b>	<b>POTENTIAALISIA ONGELMAKOHTIA JA KEINOJA VÄLTÄÄ NE .....</b>	<b>10</b>
4.1	TYHIÄT MERKIT (WHITESPACE) .....	10
4.2	KOMMENTIT .....	11
4.3	NIMIÖIDEN KÄYTTÖ .....	11
4.4	MERKISTÖT .....	12
4.5	PAIKALLINEN VIITTAUS XPOINTERILLA .....	12
<b>5.</b>	<b>ESIMERKIT.....</b>	<b>12</b>
5.1	ALLEKIRJOITUS KOHDISTETTUNA PAIKALLISELLA VIITTAUKSELLA .....	12
5.2	ALLEKIRJOITUS KOHDISTETTUNA FILTER2 SUODATUKSELLA.....	14
5.3	MONIALLEKIRJOITUS.....	15



## 1. JOHDANTO

Tämä opas kuvaa XML allekirjoitusten käyttöä CDA asiakirjojen yhteydessä. Opas liittyy Open CDA 2008 Header 4.41 määrittymiseen ja Kelan määrittymiseen KanTa-palveluissa käytettävistä XML allekirjoituksista (2009-12-31).

Tämä opas on tarkoitettu avuksi CDA-asiakirjojen allekirjoituksia toteuttaville tahoille.

## 2. TAUSTAA

### 2.1 XML allekirjoitus

XML-allekirjoitus on XML-muotoinen tietorakenne jonka sisältämä sähköinen allekirjoitus kohdistuu XML-muotoiseen tietoon. XML-allekirjoitus on mahdollista liittää osaksi allekirjoitettua tietoa siten, että allekirjoituksen automaattinen tarkistaminen on mahdollista eri ympäristöissä.

XML -allekirjoitusstandardi määrittää joukon erilaisia menetelmiä joita voidaan käyttää allekirjoituksen muodostamisessa. Allekirjoituksen tarkistaminen edellyttää tukea samoille menetelmille joita on käytetty allekirjoituksen muodostamisessa.

XML -allekirjoitusstandardin mukaiseen sähköiseen allekirjoitukseen liittyviä parametreja ovat:

- *kanonikalisointimenetelmä*(canonicalization, c14n)
- *allekirjoitusmenetelmä*(signature)
- *viittaus allekirjoitettavaan tietoon* (reference URI)
- *tiedon muutokset ja suodatus* (transforms, filtering)
- *hajautusmenetelmä*(digest)

Kanonikalisoinnissa allekirjoitettava XML yhtenäistetään esitystavaltaan aina täsmälleen samaan muotoon. Allekirjoituksella osoitetaan tiedon muuttumattomuus ja liityntä allekirjoituksen muodostaneeseen tahoon. Viittauksella, muutoksilla ja suodatuksella osoitetaan allekirjoitettavasta asiakirjasta allekirjoitettavat kohdat ja voidaan muuntaa allekirjoitettavaa muotoa. Hajautuksella tarkoitetaan menetelmää, jolla allekirjoitettavasta kohdasta muodostetaan tiedon muuttumattomuuden osoittava tiiviste (hajautussumma).

XML allekirjoituksen rakenne on esitetty alla ("?" tarkoittaa nolla tai yksi, "+" tarkoittaa yksi tai useampi ja "\*" nolla tai useampi):



```
<ds:Signature Id?>
  <ds:SignedInfo>
    <ds:CanonicalizationMethod/>
    <ds:SignatureMethod/>
    (<ds:Reference URI? >
      (<ds:Transforms>)?
      <ds:DigestMethod>
      <ds:DigestValue>
    </ds:Reference>)+
  </ds:SignedInfo>
  <ds:SignatureValue>
  (<ds:KeyInfo>)?
  (<ds:Object Id?>)*
</ds:Signature>
```

## 2.2 XML allekirjoituksen haasteet

XML-allekirjoitus on kahden eri maailman kohtaamispiste. XML sekä sen päälle tehdyt määritykset, esimerkiksi CDA-dokumenttirakenne, ovat luonteeltaan *semanttisia*. Ne perustuvat merkityksiin ja niiden yksikäsitteiseen ilmaisemiseen. Sähköinen allekirjoitus taas perustuu bittijonoihin kohdistuviin algoritmisiin operaatioihin. XML-maailmassa operoidaan suhteellisen korkean tason abstraktioilla - merkityksillä ja kuinka niitä ilmaistaan - kun taas allekirjoitusmaailmassa toimitaan bittitasolla. Koska XML-standardit sallivat samojen merkitysten ilmaisemisen useilla eri tavoilla, syntyy tästä väistämättä ongelmia.

Näiden ongelmien ratkaisemiseksi on kehitetty XML-allekirjoitusstandardi, jota ylläpitää W3C (World Wide Web Consortium). Ongelman lähtökohtaisen hankaluuden ja kentällä olevien lukuisten toimijoiden takia kyseisestä standardista on muodostunut varsin mutkikas.

Keskeisimmät tulkintakohdat XML-allekirjoitustandardissa liittyvät suodatuksen ja kanonikalisointiin. Standardi tarjoaa lukuisia eri vaihtoehtoja päästä samaan lopputulokseen. Eri tilanteissa onkin usein perusteltua käyttää eri vaihtoehtoja.

Allekirjoituksiin liittyviä haasteita ja näistä selviytymiseen käytettävissä olevia menetelmiä käsitellään luvussa 4.

## 3. ALLEKIRJOITUS CDA ASIAKIRJOISSA

### 3.1 Dokumentissa käytetyt merkinnät

Sähköiseen allekirjoitukseen liittyvät osuudet CDA-dokumentissa ovat kolmen eri nimiavaruuden (namespace) alla. Lisäksi allekirjoituksiin liittyy rakenteita joiden tietotyyppi on määritelty XML Schemassa. Tässä määrittämisessä käytetään selvyuden vuoksi elementeistä ja attribuuteista etuliitteitä sen mukaan missä nimiavaruudessa ne ovat. Käytetyt etuliitteet ja näitä vastaavat nimiavaruudet ovat:

Taulukko 1

Etuliite (prefix)	Nimiavaruus (namespace)
hl7fi	urn:hl7finland



Etuliite (prefix)	Nimiavaruus (namespace)
ds	http://www.w3.org/2000/09/xmldsig#
cda	urn:hl7-org:v3
xs	http://www.w3.org/TR/2004/REC- xmldata-20041028/

### 3.2 Yleiset periaatteet

CDA asiakirjojen allekirjoitukset perustuvat XML-allekirjoitusstandardiin siten että allekirjoituksen ympärille on toteutettu lisäksi lisätoiminnallisuutta CDA tason laajennuksina. Laajennuksina toteutetut toiminnot ovat allekirjoitusaika ja moniallekirjoitus. Allekirjoitusaika liittyy allekirjoituksen tapahtumahetkeen. Moniallekirjoitus toteuttaa laissa kuvatun toiminnallisuuden, jossa yksi allekirjoitus allekirjoittaa monta lääkemääräystä yhdellä kertaa<sup>1</sup>.

CDA asiakirjan sähköinen allekirjoitus kohdistuu **cda:structuredBody** -elementtiin ja koskee kaikkia sen lapsielementtejä ja näiden tietosisältöä. Allekirjoituksen muodostamisessa XML-rakenteen nimiavaruudet ja kommentit jätetään huomiotta.

### 3.3 Rakenne

Suomessa käytettävät CDA R2 dokumentin paikalliset laajennukset ovat CDA Headerin lopussa **hl7fi:localHeader** -elementin alla. Sähköiset allekirjoitukset ovat **hl7fi:localHeader/hl7fi:signatureCollection** -elementin alla.

**hl7fi:signatureCollection** -elementti sisältää nolla tai useampia **hl7fi:signature** -elementtejä. **hl7fi:signature** -elementti sisältää yhden allekirjoituksen tiedot. Kaikki eri tyyppiset allekirjoitukset sisältävät elementit **hl7fi:signatureDescription**, **hl7fi:signatureTimestamp** ja **ds:Signature**. Moniallekirjoitus sisältää lisäksi elementin **hl7fi:multipleDocumentSignature**.

CDA-allekirjoituksen rakenne ("?" tarkoittaa nolla tai yksi ja "\*" nolla tai useampi):

```
<hl7fi:signatureCollection>
  (<hl7fi:signature ID>
    <hl7fi:signatureDescription/>
    <hl7fi:signatureTimestamp ID/>
    (<hl7fi:multipleDocumentSignature ID>)?
    <ds:Signature/>
  </hl7fi:signature>)*
</hl7fi:signatureCollection>
```

(ds:Signature on XML -allekirjoituksen rakenteen mukainen)

**hl7fi:signatureDescription** -elementti kuvaa allekirjoituksen tyyppin. Tyyppin kuvaamiseen käytettävä koodisto on: "Sähköisen allekirjoituksen tyyppi" ja sen OID-tunnus on 1.2.246.537.5.40127.2006. Koodisto on Stakesin koodistopalvelimella muiden vastaavien CDA koodistojen tavoin.

Esimerkki **hl7fi:signatureDescription** -elementistä:

```
<hl7fi:signatureDescription code="1" codeSystem="1.2.246.537.5.40127.2006"
```

<sup>1</sup> Laki sähköisestä lääkemääräyksestä 2.2.2007/61, 7§ "Kaikki samaan potilaskäyntiin liittyvät lääkemääräykset voi allekirjoittaa yhdellä allekirjoitustoiminnolla."



```
codeSystemName="Sähköisen allekirjoituksen tyyppi"  
displayName="ammattihenkilön tekemä normaali allekirjoitus"/>
```

Esimerkki koodiston arvolistasta:

Koodisto: 1.2.246.777.5. 40127.2006 sähköisen allekirjoituksen tyyppi	
1	ammattihenkilön tekemä normaali allekirjoitus
2	ammattihenkilön tekemä moniallekirjoitus
3	järjestelmäallekirjoitus / perusjärjestelmä
4	järjestelmäallekirjoitus / KanTo
5	potilaan sähköinen allekirjoitus

(koodiston ajantasainen versio on jakelussa Stakesin koodistopalvelimella)

**hl7fi:signatureTimestamp** -elementti sisältää kellonajan sekunnin tarkkuudella. Elementti on tyyppiä **xs:dateTime**<sup>2</sup> ja sillä on pakollinen attribuutti **ID**. Kellonaikaa muodostettaessa tulee ottaa huomioon aikavyöhykkeen esittämistapa. Kellonajan muodostamiseen käytettävän ympäristön kellon on suositeltavaa olla synkronoitu keskitettyyn aikapalveluun.

Esimerkkejä **hl7fi:signatureTimestamp** -elementistä:

```
<hl7fi:signatureTimestamp ID="TSid001">2008-11-21T12:18:06Z</hl7fi:signatureTimestamp>  
<hl7fi:signatureTimestamp ID="TSid002">2008-11-21T12:18:07+02:00:00</hl7fi:signatureTimestamp>
```

**hl7fi:multipleDocumentSignature** -elementti sisältää viittaukset moniallekirjoituksen kohteena oleviin CDA-asiakirjoihin joista jokaiseen liitetään kopio samasta moniallekirjoituksesta. Elementillä on attribuutti **ID**. Kukin viittaus on oma **hl7fi:Ref** elementtinsä jonka **OID**-attribuutti on kohteena olevan CDA-asiakirjan OID ja **hash**-attribuutissa kyseisen asiakirjan **/cda:ClinicalDocument/ cda:component/ cda:structuredBody** elementistä laskettu tiiviste. Tiivisteen laskemisessa käytetään samoja kanonikalisointi- ja hajautusalgoritmeja kuin moniallekirjoitusrakenteeseen kohdistuvassa allekirjoituksessa.

Esimerkki **hl7fi:multipleDocumentSignature** -elementistä:

```
<hl7fi:multipleDocumentSignature ID="MDSid001">  
  <hl7fi:Ref OID="1.2.246.10.98765432.93.2007.16" hash="bFEFUCL6NjvIw4tlwCTAvfYsWLM="/>  
  <hl7fi:Ref OID="1.2.246.10.98765432.93.2007.2" hash="MZlz+sdPtKCORLFvyxf6IAInXt0="/>  
  <hl7fi:Ref OID="1.2.246.10.98765432.93.2007.3" hash="B9/F5tBlS5o/xOGQmkQ4MjEXYxU="/>  
</hl7fi:multipleDocumentSignature>
```

### 3.4 CDA asiakirjan XML allekirjoituksen vaatimukset

CDA R2 asiakirjojen sähköisiä allekirjoituksia koskevat vaatimukset esitetään ja ylläpidetään Kelan CDA R2 -asiakirjojen sähköisen allekirjoituksen määrittämis-dokumentissa.

### 3.5 Kohdistaminen

CDA asiakirjan XML allekirjoituksessa on kaksi reference -elementtiä joista toinen kohdistuu aikaleimaan (**hl7fi:signatureTimestamp** -elementti). Toinen **ds:reference** -elementti kohdistuu

<sup>2</sup> XML Schema Part 2: Datatypes Second Edition. W3C Recommendation 28 October 2004,  
<http://www.w3.org/TR/xmlschema-2/#dateTime>



moniallekirjoituksessa hl7fi:multipleDocumentSignature -elementtiin ja muissa allekirjoituksissa **cda:structuredBody**-elementtiin (**/cda:ClinicalDocument/cda:component/cda:structuredBody**).

Kohdistaminen voi tapahtua joko pelkällä **URI**-attribuutilla tai **URI**-attribuutin ja Filter-suodatuksen yhdistelmällä.

**URI**-attribuutin avulla viittaaminen tapahtuu XPointer-standardin<sup>3</sup> mukaisesti. XML-allekirjoitusstandardin mukaisissa ympäristöissä tuettuja XPointereita ovat ainakin dokumentin juureen viittaava tyhjä arvo (**URI=""**) ja dokumentin sisäinen viittaus elementin **ID**-atribuuttiin (**URI="#arvo"**). XPointer kohdistuu tiettyyn elementtiin ja kaikkiin sen alasolmuihin.

Kansainvälisessä CDA-standardissa **cda:structuredBody**-elementillä ei ole **ID**-attribuuttia. Suomen HL7-yhdistyksen viralliseen CDA R2 -skeemaan on lisätty **ID**-attribuutti (tyyppiä **xs:id**).

Filter -suodatuksen avulla XPointerin tekemää kohdistusta on mahdollista rajata yksityiskohtaisesti. Yleisesti tuettuja Filter -suodatuksia on kaksi erilaista; XML Path Language Version 1.0 (XPath) ja XML-Signature XPath Filter 2.0 (Filter2). Suodatkset ovat kuvailuvoimaltaan vastaavia, mutta Filter2 toteutukset ovat useimmissa ympäristöissä tehokkaampia kuin XPath toteutukset.

Seuraavassa on esimerkit kolmesta mahdollisesta kohdistustavasta:

- Kohdistus pelkällä reference-elementillä XML ID -attribuuttiin

```
<ds:Reference URI="#TSid001">...</ds:Reference>
<ds:Reference URI="#MDSid001">...</ds:Reference>
```
- Kohdistus juureen ja allekirjoitettavan tiedon suodattaminen XPath-suodatuksella

```
<ds:Reference URI="">
  <ds:Transforms>
    <ds:Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116">
      <ds:XPath>ancestor-or-self::*[local-name()='signatureTimestamp']</ds:XPath>
    </ds:Transform>
  </ds:Transforms>...
</ds:Reference>
<ds:Reference URI="">
  <ds:Transforms>
    <ds:Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116">
      <ds:XPath>ancestor-or-self::*[local-name()='structuredBody']</ds:XPath>
    </ds:Transform>
  </ds:Transforms>...
</ds:Reference>
```
- Kohdistus juureen ja allekirjoitettavan tiedon suodattaminen Filter2-suodatuksella käyttäen elementin nimeä tunnisteena

```
<ds:Reference URI="">
  <ds:Transforms>
    <ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
      <dsig-xpath:XPath
        xmlns:dsig-xpath="http://www.w3.org/2002/06/xmldsig-filter2"
        Filter="intersect">//*[local-name()='signatureTimestamp']</dsig-xpath:XPath>
      </ds:Transform>
    </ds:Transforms>...
</ds:Reference>
```

<sup>3</sup> XML Pointer Language (XPointer) Version 1.0, W3C Candidate Recommendation 11 September 2001, <http://www.w3.org/TR/2001/CR-xptr-20010911/>





```
</ds:Reference>
<ds:Reference URI="">
<ds:Transforms>
  <ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
    <dsig-xpath:XPath
      xmlns:dsig-xpath="http://www.w3.org/2002/06/xmldsig-filter2"
      Filter="intersect">//*[local-name()='structuredBody']</dsig-xpath:XPath>
    </ds:Transform>
  </ds:Transforms>...
</ds:Reference>
```

- Kohdistus juureen ja allekirjoitettavan tiedon suodattaminen Filter2-suodatuksella käyttäen **ID**-attribuutin arvoa tunnisteena

```
<ds:Reference URI="">
<ds:Transforms>
  <ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
    <dsig-xpath:XPath
      xmlns:dsig-xpath="http://www.w3.org/2002/06/xmldsig-filter2"
      Filter="intersect">//*[@ID='TSid001']</dsig-xpath:XPath>
    </ds:Transform>
  </ds:Transforms>...
</ds:Reference>
<ds:Reference URI="">
<ds:Transforms>
  <ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
    <dsig-xpath:XPath
      xmlns:dsig-xpath="http://www.w3.org/2002/06/xmldsig-filter2"
      Filter="intersect">//*[@ID='MDSid001']</dsig-xpath:XPath>
    </ds:Transform>
  </ds:Transforms>...
</ds:Reference>
```

### 3.6 Moniallekirjoitus

Moniallekirjoituksen muodostamisessa ja tarkistamisessa on yksi lisäkerros välissä verrattuna tavalliseen allekirjoitukseen.

Moniallekirjoituksen muodostaminen tapahtuu seuraavasti:

1. Muodostetaan uusi **hl7fi:signature** -elementti jonka sisältö on seuraava:
  - **hl7fi:signatureDescription** -elementti on moniallekirjoituksen mukainen:

```
<hl7fi:signatureDescription code="2"
  codeSystem="1.2.246.537.5.40127.2006"
  codeSystemName="Sähköisen allekirjoituksen tyyppi"
  displayName="ammattihenkilön tekemä moniallekirjoitus"/>
```
  - **hl7fi:signatureTimestamp** -elementti on samanlainen kaikissa eri allekirjoituksissa.
  - **hl7fi:multipleDocumentSignature** -elementti (tarkempi kuvaus alla)
  - **ds:Signature** -elementti sisältää sähköisen allekirjoituksen joka kohdistuu **hl7fi:signatureTimestamp** -elementtiin.
2. **hl7fi:multipleDocumentSignature** -elementti sisältää kutakin allekirjoitettavaa CDA R2 asiakirjaa kohden **hl7fi:Ref** -elementin seuraavasti:



- **OID** -attribuutin arvona on CDA R2 asiakirjan tunniste (**cda:ClinicalDocument/id** -elementin **root** ja **extension** -attribuuttien mukainen arvo)
- **hash** -attribuutin arvona on CDA R2 asiakirjan allekirjoitettavasta sisällöstä muodostettu tiiviste. Tiiviste muodostetaan asiakirjan **cda:structuredBody** -elementin sisällöstä käyttäen samoja menetelmiä ja parametreja kuin samoilla parametreilla kuin moniallekirjoitusrakenteeseen itseensä kohdistuvassa XML -allekirjoituksessa. Poikkeuksena kohdistamiseen liittyvät parametrit eli **URI** attribuutti ja Xpath sekä Filter2 -suodattimet jotka tulee korvata **cda:structuredBody**-elementtiin kohdistuvilla arvoilla.

```
<hl7fi:multipleDocumentSignature ID="MDSid001">  
  <hl7fi:Ref OID="1.2.246.10.98765432.93.2007.16" hash="bFEFUCL6Njvlw4tlwCTAvfYsWLM="/>  
  <hl7fi:Ref OID="1.2.246.10.98765432.93.2007.2" hash="MZlz+sdPtKCORLFvyxf6IAInXt0="/>  
  <hl7fi:Ref OID="1.2.246.10.98765432.93.2007.3" hash="B9/F5tBIs5o/xOGQmkQ4MjEXYxU="/>  
</hl7fi:multipleDocumentSignature>
```

3. Moniallekirjoitusrakenne allekirjoitetaan XML allekirjoituksella ja muodostetaan.
4. Kuhunkin moniallekirjoitettuun asiakirjaan liitetään sama **hl7fi:signature** -elementti

Moniallekirjoituksen tarkistaminen tapahtuu seuraavasti:

1. Tarkistetaan moniallekirjoitusrakenteen sähköinen allekirjoitus XML-allekirjoitusstandardin toteuttavalla validaattorilla
2. Tarkistetaan moniallekirjoitusrakenteen ja moniallekirjoitetun asiakirjan välinen liitos

Moniallekirjoituksen muodostamisen vaiheessa 1. ja tarkistamisen vaiheessa 2. tarvittava **cda:structuredBody** -elementin tiivisteen laskeminen edellyttää XML-allekirjoituksen mukaista toiminnallisuutta. Käytännön toteutuksissa voidaan hyödyntää XML -allekirjoitustoteutusta esimerkiksi siten, että asiakirja allekirjoitetaan palvelinvarmenteella mutta tätä allekirjoitusta ei tallenneta vaan pelkästään sen sisältämä tiiviste tallennetaan moniallekirjoitusrakennetta varten.

#### 4. POTENTIAALISIA ONGELMAKOHTIA JA KEINOJA VÄLTTÄÄ NE

##### 4.1 Tyhjät merkit (whitespace)

Erilaiset XML-työkalut käsittelevät tyhjiä merkkejä eri tavoin, jonka seurauksena allekirjoitusten eheys saattaa rikkoutua. Erityisesti rivinvaihdot ovat ongelmallisia eivätkä eri sovellukset käsittele niitä yhdenmukaisesti<sup>4</sup>.

Tyhjien merkkien yhtenäistäminen on mahdollista toteuttaa XML allekirjoituksen tukemien menetelmien avulla käyttämällä XSL-suodatinta joka poistaa allekirjoitettavasta asiakirjasta ylimääräiset tyhjät merkit ennen allekirjoituksen laskemista. Käytännössä tämä on mahdollista *normalize-space()* -funktion avulla.

*Normalize-space()* funktio korvaa kaikki yhden tai useamman tyhjän merkin ilmentymät yhdellä välilyönnillä. Erityisesti on huomion arvoista että allekirjoitus ei tällöin ota huomioon rivinvaihtoja, joilla saattaa olla joissain erikoistapauksissa merkitystä tietosisällölle. Rivinvaihdot jäävät huomioimatta kuitenkin vastaavasti myös esitettäessä CDA asiakirja HTML -muodossa.

<sup>4</sup> Erilaisten rivinvaihtomerkkien historiaan voi tutustua esimerkiksi wikipedian artikkelista: <http://en.wikipedia.org/wiki/Newline>



## Esimerkki **ds:Transform**

```
<ds:Transform Algorithm="http://www.w3.org/TR/1999/REC-xslt-19991116">
  <xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform" version="1.0">
    <xsl:template match="*|@*|comment()">
      <xsl:copy>
        <xsl:apply-templates select="*|@*|text()|comment()" />
      </xsl:copy>
    </xsl:template>
    <xsl:template match="text()">
      <xsl:value-of select="normalize-space(.)" />
    </xsl:template>
  </xsl:stylesheet>
</ds:Transform>
```

## 4.2 Kommentit

XML:n semanttisen luonteen takia asiakirjan kommentteihin ei pitäisi sisällyttää merkitsevää tietoa. Niiden sisällyttäminen allekirjoitukseen puolestaan saattaa aiheuttaa lisäongelmia tyhjen merkkien takia sekä siksi, että käytetyt työkalut saattavat ennalta-arvaamattomasti "kuoria" ne pois käsittelyketjuissa.

Kommentit eivät ole ongelma CDA -asiakirjojen allekirjoituksissa käytettäessä kanonikalisointi-algoritmeja, jotka suodattavat kommentit pois ennen allekirjoituksen muodostamista ja tarkistamista.

## 4.3 Nimiöiden käyttö

XML:n siirtäminen esimerkiksi SOAP-kääreessä ja muu käsitteleminen saattaa lisätä rakenteeseen ennalta-arvaamattomasti nimiöitä.

CDA asiakirjojen allekirjoituksissa hyväksyttäviksi on määritetty kaksi nimiöitä eri tavalla käsittelevää kanonikalisointi-algoritmia. Inclusive-kanonikalisointia käytettäessä allekirjoitusta muodostettaessa ja tarkistettaessa nimiöt otetaan huomioon. Exclusive-kanonikalisointia käytettäessä nimiöt vastaavasti jätetään huomiotta allekirjoitusta muodostettaessa ja tarkistettaessa.

Inclusive-kanonikalisointia käytettäessä tulee varmistua että asiakirjassa esiintyy vain tarvittavat nimiöt ja puhdistaa asiakirja ylimääräisistä nimiöistä tarvittaessa.

Nimiöiden käyttöä XML-allekirjoituksessa käytettävissä XPatheissa tulee pyrkiä välttämään samoista syistä. Tämä on mahdollista esimerkiksi käyttämällä *local-name()* -funktiota seuraavasti:

```
//*[local-name()='structuredBody']
```

joka vastaa seuraavia nimiöiden tiettyyn käsittelytapaan nojaavia XPath:ejä:

```
//cda:structuredBody
```

```
//structuredBody
```

```
//muu:structuredBody
```



## 4.4 Merkitöt

Jotta merkitömuunnoksissa tapahtuvat virheet vältettäisiin, *suositellaan* käytettäväksi allekirjoitettavissa asiakirjoissa UTF-8 -merkitöä.

## 4.5 Paikallinen viittaus XPointerilla

Käytettäessä XPointerin paikallista viittausmuotoa (**URI**="#ID-arvo") edellyttää tämä käytettävän XML-ympäristön tunnistavan kohteena olevan attribuutin ID -tyyppiseksi arvoksi. Käytännössä tämä edellyttää joko DTD tai Schema tiedoston liittymistä käsiteltävään XML-asiakirjaan siten että se on allekirjoituksen muodostamiseen ja tarkistamiseen käytettävän ympäristön hyödynnettävissä. Eri XML-ympäristöt eroavat standardin noudattamistavoiltaan eikä XPointerin yhdenmukainen toimiminen ole aina taattua.

Paikallisen viittausmuodon käyttö CDA asiakirjojen XML allekirjoituksissa saattaa jossain tapauksissa aiheuttaa ongelmia jotka ovat vältettävissä käyttämällä muita kohdistustapoja.

## 5. ESIMERKIT

CDA-asiakirja voidaan allekirjoittaa esimerkiksi alla kuvatulla tavalla. Tämä esimerkki ei ole sitova eikä ainoa toimiva tapa allekirjoittaa CDA-asiakirja. Esimerkin tarkoitus on kuvittaa ja täydentää yllä kuvattua sitovaa määritystä sekä ongelmien välttämiseen tarkoitettua ohjeistusta.

Esimerkeissä 1, 2 ja 3 käytetty CDA -asiakirja on tiedostossa EsimerkkiAsiakirja1.xml  
Esimerkissä 3 lisäksi käytetyt CDA -asiakirjat ovat tiedostoissa EsimerkkiAsiakirja2.xml ja EsimerkkiAsiakirja3.xml

### 5.1 Allekirjoitus kohdistettuna paikallisella viittauksella

Alla esimerkki XPointer menetelmän avulla kohdistetusta CDA allekirjoitusrakenteesta. Kaikki kolme kanonikalisoitua (SignedInfo-, signatureTimestamp- ja StructuredBody-rakenteet) ovat esimerkissä Inclusive -kanonikalisoitimenetelmän (Canonical XML version 1.0 (without comments) ) mukaisia. Esimerkissä käytetään tyhjän tilan siistimiseen XSLT -transformaatiota. Allekirjoitukseen käytetty varmenne on omana rakenteenaan ja varmenteen tietoja on esitetty myös avattuna. Allekirjoitettu asiakirja on kokonaisuudessaan tiedostossa esimerkkiAllekirjoitus1.xml

```
<hl7fi:signature ID="esimerkkiAllekirjoitus1">
<hl7fi:signatureDescription code="1" codeSystem="1.2.246.537.5.40127.2006" codeSystemName="Sähköisen
allekirjoituksen tyyppi" displayName="ammattihenkilön tekemä normaali allekirjoitus" />
<hl7fi:signatureTimestamp ID="esimerkkiAika1">2008-12-02T12:05:00+02:00</hl7fi:signatureTimestamp>
<ds:Signature Id="Signature" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo xmlns="urn:hl7-org:v3" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:hl7fi="urn:hl7finland" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
<ds:Reference URI="#esimerkkiAika1">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/TR/1999/REC-xslt-19991116">
<xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform" version="1.0">
<xsl:template match="*|@*|comment()" />
<xsl:copy>
<xsl:apply-templates select="*|@*|text()|comment()" />
</xsl:copy>
```



```
</xsl:template>
<xsl:template match="text()">
<xsl:value-of select="normalize-space(.)" />
</xsl:template>
</xsl:stylesheet>
</ds:Transform>
<ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<ds:DigestValue>x39qsJ+ / +kmfwEbhtVoxApHiiVo=</ds:DigestValue>
</ds:Reference>
<ds:Reference URI="#esimerkkiStructuredBody1">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/TR/1999/REC-xslt-19991116">
<xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform" version="1.0">
<xsl:template match="*|@*|comment()">
<xsl:copy>
<xsl:apply-templates select="*|@*|text()|comment()" />
</xsl:copy>
</xsl:template>
<xsl:template match="text()">
<xsl:value-of select="normalize-space(.)" />
</xsl:template>
</xsl:stylesheet>
</ds:Transform>
<ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<ds:DigestValue>IQBCiHGDUGcb2tMwXh60UeLNips=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
spQ2ObIOhflK3fhYeW2w/nnzJsLia/DqLvSb+ATl6pBrMtMiBMy05zMANKL0V210vM93MwGk8UNqaiXhkIAbaAxTc07yZBQ8
c5KBF105JRG1ZiRDZwG1S2zqqnOAYUYUWjS6YldHsq9p6TF+df6C0lk0wf/qf/4K8p/4erBm5DeoNzIxHuhLiSw2gkiKuZ2mHU
ygV8Hpe9yTJOBTZCYBTVMelJWQ5JYHAFQO2MF4ZuOWTE+rpmXLLP/ksko1VR6iDMyNeEdeHqrlcKmsJtlenhmXN25kdAi
m3X27kYrhN1FBXKQeoJyhORRI245dWQEJYtMNLQsC+i5A6HCv1s7t5g==
</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509IssuerSerial>
<ds:X509IssuerName>C=FI, O=TEO TEST, OU=Terveystieteiden tutkimuskeskus, CN=TEO TEST
CA</ds:X509IssuerName>
<ds:X509SerialNumber>124464345</ds:X509SerialNumber>
</ds:X509IssuerSerial>
<ds:X509SKI>m4MI979NUHO60gFm4CQSQ2sLTKc=</ds:X509SKI>
</ds:X509Data>
<ds:X509Data>
<ds:X509SubjectName>C=FI, OID.2.5.4.65=100024, T=Erikoislääkäri, SERIALNUMBER=00198704009, G=Paavo
Gideon, SN=Ämmälä Tes, CN=Ämmälä Tes Paavo Gideon 00198704009</ds:X509SubjectName>
</ds:X509Data>
<ds:X509Data>
<ds:X509Certificate>
MIIFqDCCBJCgAwIBAgIEB2ss2TANBgkqhkiG9w0BAQUFADBfMQswCQYDVQQGEwJGSTERMA8GA1UEChMIVEVPIFRFU1Q
xJzAIBgNVBAsThIRlcnZleWRlbmh1b2xsb24gdGVzdG12YXJtZW5uZTEUMBIGA1UEAxMLVEVPIFRFU1QgQ0EwHhcNMjM0Mj
A5MjIwMDAwWWhcNMTxMjEwMjE1OTU5WjCBsDELMAKGA1UEBhMCRRkxZDANBgNVBEETBjEwMDA5NDEaMBGGA1UEDAw
RRXJpa29pc2ZDpMOKa8OkcmkxZDASBgNVBAUcZAwMTk4NzA0MDA5MRUwEwYDVQQLQwEwYWF2byBHAWRlb24xZjAU
BgNVBAQMDCoEbw3DpGzDpCBUZXMxLzAtBgNVBAMMJsOEbW3DpGzDpCBUZXMgUGFhdm8gR2lkZW9uIDAwMTk4NzA0
MDA5MIIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwTfUZPdDlCpYpQboZ4IQ5e13HEjHpVfyV6SHWYbbRocVh3
uiTS3YDkK17MNLz2iWf7MuGQYtn523MPyQLP3wRgjt3G4D8A9RIOMjcbmvYB54IeNTfSnf5xYoyY+mvG8ifgY94H0BtgJSiw
9YcZcZLBFJYQ8RSOo6AR0IY3peil0tuL9idRkp7iB61yoeWClfJNRxuL3pgPjf5wjV6QiyPjeULxqcMCvvXz/HudQYuX55rNkjbv
PY1uBC9SxolrTQBTt3gdJvDtGottKOWb9sQFgqbt7hckAtDHCIE71nbSxFEaW8Isd6tAeM0BY+yqyr+WZsuUxgF54d+YGJ
e6QQIDAQABo4ICGDCCAqHwHwYDVR0jBBgwFoAULMp7wIEF48FpfkM1TL+31OIayoYwHQYDVR0OBBYEFJuDCPe/TVBzut
IBZuAkEkNrC0ynMA4GA1UdDwEB/wQEAwIGQDCBIQYDVR0gBIGNMIGKMIIGHBgwqgXaEJ2MBAGPvVswdzBLBggrBgEFB
QcCAjA/Gj1WYXJtZW5uZXBvbG10aWlra2Egb24gc2FhdGF2aWxsYSBodHRwOi8vd3d3LnZhbHR0ZXJpLmZpL2Nwczk5MCG
GCCsGAQUFBwIBFhxdHRwOi8vd3d3LnZhbHR0ZXJpLmZpL2Nwczk5MGA8GA1UdEwEB/wQFMAMBAQAwgYwGA1UdHwSB
hDCBgTBjoh2ge4Z5bGRhcdovL2xkYXAudGVvLmZpZjM4OS9DTj1URU8IMjBURVNUJTIwQ0EsT1U9VGydmV5ZGVuaHVv
bGxvbiUyMHRlc3RpdMfYbWVubmUsTz1URU8IMjBURVNULEM9Rkk/Y2VydGlmawNhdGVVSXZyZ2F0aW9uTGldZDCBiQYI
KwYBBQUHAQEFTB7MHkGCCsGAQUFBzAChm1sZGFwOi8vbGRhcdC50ZW8uZmk6Mzg5L0NOPVRFTYUyMFRFU1Q1QIMjBDQ
SxPVT1UZXXJ2ZXlkZW5odW9sbG9uJTIwZGVzdG12YXJtZW5uZSxPPVRFTYUyMFRFU1Q1Q1GST9jYUNlcnRpZmljYXRIMA0
GCSqGSIb3DQEBAQUAA4IBAQAfytotxuLUcDPWJb6ksJgI65AeKwrl9nV/+WlJoYpK9I8hkFlyfBQbDNDorpuvgNbIsb42cLS1I
```





```
4SCgfzbdInq66n3vTwptD8PkyN19pJFBhHkawGvXyyt7tY1SuvNppyKPNploE70ODPukYMacOEko25H3l+TXd58Z85UIJ2hqc  
gq/YLI/IO1bkfo0olclIejn3wJAio5QXS+dLF+3GVnqew+My/fhxEspDJcRYwGIU3d+F91m1gmqDPufQpr842iRchBkMIG2CTp  
5h2oO6IXYhmvZWKHV/KDn0snLjI0bpTgt50gNFuBqNUa/CI0Lhj6W1uT0JJVYIzvKtTPAzAq  
</ds:X509Certificate>  
</ds:X509Data>  
</ds:KeyInfo>  
</ds:Signature>  
</hl7fi:signature>
```

## 5.2 Allekirjoitus kohdistettuna Filter2 suodatuksella

Alla esimerkki Filter2 -menetelmän avulla kohdistetusta CDA allekirjoitusrakenteesta. Kaikki kolme kanonikalisoitua (SignedInfo-, signatureTimestamp- ja StructuredBody-rakenteet) ovat esimerkissä Inclusive -kanonikalisoitimenetelmän (Canonical XML version 1.0 (without comments) ) mukaisia. Esimerkissä käytetään tyhjän tilan siistimiseen XSLT -transformaatiota. Allekirjoitukseen käytetty varmenne on omana rakenteenaan eikä varmenteen tietoja ole esitetty erikseen avattuna. Esimerkissä esiintyy lisäksi XML-allekirjoituksen mukainen Object-lisärakenne. Allekirjoitettu asiakirja on kokonaisuudessaan tiedostossa esimerkkiAllekirjoitus2.xml

```
<hl7fi:signature ID="esimerkkiAllekirjoitus2">  
<hl7fi:signatureDescription code="1" codeSystem="1.2.246.537.5.40127.2006" codeSystemName="Sähköisen  
allekirjoituksen tyyppi" displayName="ammattihenkilön tekemä normaali allekirjoitus" />  
<hl7fi:signatureTimestamp ID="esimerkkiAika1">2008-12-02T12:05:00+02:00</hl7fi:signatureTimestamp>  
<ds:Signature Id="Signature" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">  
<ds:SignedInfo xmlns="urn:hl7-org:v3" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"  
xmlns:hl7fi="urn:hl7finland" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">  
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />  
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />  
<ds:Reference URI="">  
<ds:Transforms>  
<ds:Transform Algorithm="http://www.w3.org/TR/1999/REC-xslt-19991116">  
<xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform" version="1.0">  
<xsl:template match="*|@*|comment()">  
<xsl:copy>  
<xsl:apply-templates select="*|@*|text()|comment()" />  
</xsl:copy>  
</xsl:template>  
<xsl:template match="text()">  
<xsl:value-of select="normalize-space(.)" />  
</xsl:template>  
</xsl:stylesheet>  
</ds:Transform>  
<ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">  
<dsig-xpath:XPath xmlns:dsig-xpath="http://www.w3.org/2002/06/xmldsig-filter2"  
Filter="intersect">//*[ @ID='esimerkkiAika1']</dsig-xpath:XPath>  
</ds:Transform>  
<ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />  
</ds:Transforms>  
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />  
<ds:DigestValue>x39qsJ+/-+kmfwEbhtVoxApHiiVo=</ds:DigestValue>  
</ds:Reference>  
<ds:Reference URI="">  
<ds:Transforms>  
<ds:Transform Algorithm="http://www.w3.org/TR/1999/REC-xslt-19991116">  
<xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform" version="1.0">  
<xsl:template match="*|@*|comment()">  
<xsl:copy>  
<xsl:apply-templates select="*|@*|text()|comment()" />  
</xsl:copy>  
</xsl:template>  
<xsl:template match="text()">  
<xsl:value-of select="normalize-space(.)" />  
</xsl:template>  
</xsl:stylesheet>
```



```
</ds:Transform>
<ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
  <dsig-xpath:XPath xmlns:dsig="http://www.w3.org/2002/06/xmldsig-filter2"
  Filter="intersect">//*[ @ID='esimerkkiStructuredBody1']</dsig-xpath:XPath>
</ds:Transform>
<ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<ds:DigestValue>IQBCIhGDUGcb2tMwXh60UeLNips=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
spQ2ObIOhflK3fhYeW2w/nnzJsLia/DqLvSb+ATl6pBrMtMiBMy05zMANKL0V21OvM93MwGk8UNqaiXhkIAbaXtC07yZBQ8
c5KBFI05JRG1ZIRDZwq5SzzqnOAYUYUWjS6YldHsq9p6TF+df6C0lk0wf/qf/4K8p/4erBm5DeoNzIxhLiSW2gkiKuZ2mHU
ygV8Hpe9yTJOBTzCYBTVMelJWQ5JYHAFQO2MFn4ZuOWTE+rpmXLLP/ksko1VR6iDMYNeEdehQrlcKmSjTlenhmXN25kdAi
m3X27kYrhN1FBXKQeoJyh0RRI245dWQJEJYtMNLQsC+i5A6HCv1s7t5g==
</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>
MIIFqDCCBJCgAwIBAgIEB2ss2TANBgkqhkiG9w0BAQUFADBfMQswCQYDVQQGEwJGSTERMA8GA1UEChMIVEVPIFRFU1Q
xJzAlBgNVBAAsTHRlcnZleWRlbnhm1b2xsxb24gdGVzdGI2YXJtZW5uZTEUMBIGA1UEAxMLVEVPIFRFU1QgQ0EwHhcNMDcxMj
A5MjIwMDAwWWhcNMTIxMjEwMjE0TU5WjCBsDELMAkGA1UEBhMCRCkxZDANBgNVBETBjEwMDAyNDEaMBGGA1UEDAw
RRXJpa29pc2Z2DpMOKa8OkcmkxFDASBgNVBAUcZAwMTk4NzA0MDA5MRUwEwYDVQQQEWxYWYWF2byBHAWRlbn24xZjAU
BgNVBAQMDCOEbW3DpGzDpCBUZXMXLzAtBgNVBAMMJsOEbW3DpGzDpCBUZXMGUGFhdm8gR2lkZW9uIDAwMTk4NzA0
MDA5MIIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAWtFuzPdDlCypQboZ4IQ5e13HEjHpVfyV6SHWYbbRocVh3
uitT53YDKk17MNLZ2iWf7MuGQYtn523MPyQLP3wRgjt3G4D8A9RI0mjbcmvYB54IeNTfSnf5xYoyY+mvG8ifgY94H0BtgJSiw
9YcZcZLBfJYQ8RSOo6AR0IY3peil0tuL9idRkp7iB61yoeWClfJNRxuL3pgPjf5wJv6QiyPjeULxqcMCvvXz/HudQYuX55rNkjvvh
PY1uBC9SxolrTQBTt3gdJvDtGottKOWb9sQFGqbt7hcKAtDHCIEN71nbSxFeaW8Isd6tAeM0BY+yqyr+WZsuUxgF54d+YGJ
e6QQIDAQABo4ICGDCCAqHwHwYDVR0jBBgwFoAULMp7wIEf48FpfkM1TL+31OIayoYwHQYDVR0OBBYEFJuDCPe/TVBzut
IBZuAkEkNrC0ynMA4GA1UdDwEB/wQEAwIGQDCBIQYDVR0gBIGNMIGKMGHGBgwqgXaEJ2MBAgGPVwswdzBLBggrBgEFB
QCCAJA/Gj1WYXJtZW5uZXBvbGl0aWlra2Egb24gc2FhdGF2aWxsYSBodHRwOi8vd3d3LnZhbHR0ZXJpLmZpL2Nwczk5MCG
GCCsGAQUFBwIBFhxodHRwOi8vd3d3LnZhbHR0ZXJpLmZpL2Nwczk5MA8GA1UdEwEB/wQFMAMBAQAwwYGA1UdHwSB
hDCBgTB/oH2ge4Z5bGRhcdovL2xkYXAudGVvLmZpOjM4OS9DTj1URU8IMjBURVNULEM9Rkk/Y2VydGlmawNhdGVSSXZvY2F0aW9uTGldZDCBiQYI
KwYBBQUHAQEFTB7MHkGCCsGAQUFBzACHm1sZGFwOi8vbGRhcC50ZW8uZmk6Mzg5L0NOPVRFTyUyMFRFU1QIMjBDQ
SxPVT1UZjZjZlIkdW5odW9sbG9uJTIwdGVzdGI2YXJtZW5uZSxPPVRFTyUyMFRFU1QsQz1GST9jYUNlcnRpZmljYXRIMA0
GCSqGSIb3DQEBBQUAA4IBAQAfytzXuLUcDPWJb6ksJgI65AeKwrl9nV/+WlJoYpK9I8hkFlyfBQbDNDorpuvgNbIsb42cLSlI
4SCgfzbdlnq66n3vTwptD8PkyN19pJfBhHkawGvXyyt7tY1SuvNppyKPNploE70ODPukYMacOEko25H3l+TXd58Z85UIJ2hqc
qq/YLI/I01bkf00lclIejn3wJAio5QXS+dLF+3GVnqeq+My/fhxEspDJcRYwGIU3d+F91m1gmqDPufQpr842iRchBkMIG2CTp
5h2oO6IXYhmVZWKHV/KDn0snLjI0bpTgt50gNFuBqNUa/Ci0Lhj6W1uT0JJVYIzvKtTPAzAq
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
<ds:Object Id="Timestamp-1">
<ds:SignatureProperties>
<ds:SignatureProperty Target="#Signature">
<timestamp version="1.2" type="unsigned">
<formattedDateTime>2008-12-03T14:59:51+0200</formattedDateTime>
</timestamp>
</ds:SignatureProperty>
</ds:SignatureProperties>
</ds:Object>
</ds:Signature>
</hl7fi:signature>
```

### 5.3 Moniallekirjoitus

Alla esimerkki moniallekirjoitusrakenteesta. Käytetty kanonikalisointimenetelmä on Exclusive (Exclusive XML Canonicalization version 1.0 (without comments) ). Esimerkissä käytetään tyhjän tilan siistimiseen XSLT -transformaatiota. Allekirjoitukseen käytetty varmenne on omana rakenteenaan eikä varmenteen tietoja ole esitetty erikseen avattuna.

Allekirjoitetut asiakirjat ovat tiedostoissa esimerkkiMoniAllekirjoitus1.xml, esimerkkiMoniAllekirjoitus2.xml, esimerkkiMoniAllekirjoitus3.xml

```
<hl7fi:signature ID="esimerkkiMoniallekirjoitus1">
```



```
<hl7fi:signatureDescription code="2" codeSystem="1.2.246.537.5.40127.2006" codeSystemName="Sähköisen  
allekirjoituksen tyyppi" displayName="ammattihenkilön tekemä moniallekirjoitus" />  
<hl7fi:signatureTimestamp ID="esimerkkiMoniallekirjoitusAika1">2008-12-  
02T12:05:00+02:00</hl7fi:signatureTimestamp>  
<hl7fi:multipleDocumentSignature ID="esimerkkiMoniallekirjoitusRakenne1">  
<hl7fi:Ref OID="1.2.246.10.98765432.93.2007.16" hash="MzeK/E61NLqvi3VpxK3vd/Dog3k=" />  
<hl7fi:Ref OID="1.2.246.10.98765432.93.2007.2" hash="ypYAj0cZSDsVKSgJ4EHJ8XFPxU8=" />  
<hl7fi:Ref OID="1.2.246.10.98765432.93.2007.3" hash="sxNAmtgoHF5EKniNjSLZFue9dg=" />  
</hl7fi:multipleDocumentSignature>  
<ds:Signature Id="Signature" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">  
<ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">  
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />  
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />  
<ds:Reference URI="">  
<ds:Transforms>  
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />  
<ds:Transform Algorithm="http://www.w3.org/TR/1999/REC-xslt-19991116">  
<xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform" version="1.0">  
<xsl:template match="*|@*|comment()">  
<xsl:copy>  
<xsl:apply-templates select="*|@*|text()|comment()" />  
</xsl:copy>  
</xsl:template>  
<xsl:template match="text()">  
<xsl:value-of select="normalize-space(.)" />  
</xsl:template>  
</xsl:stylesheet>  
</ds:Transform>  
<ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">  
<dsig-xpath:XPath xmlns:dsig-xpath="http://www.w3.org/2002/06/xmldsig-filter2"  
Filter="intersect">//*[ID='esimerkkiMoniallekirjoitusAika1']</dsig-xpath:XPath>  
</ds:Transform>  
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />  
</ds:Transforms>  
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />  
<ds:DigestValue>5CN3Ii2POs27zSbNN1t1QU+z1zQ=</ds:DigestValue>  
</ds:Reference>  
<ds:Reference URI="">  
<ds:Transforms>  
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />  
<ds:Transform Algorithm="http://www.w3.org/TR/1999/REC-xslt-19991116">  
<xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform" version="1.0">  
<xsl:template match="*|@*|comment()">  
<xsl:copy>  
<xsl:apply-templates select="*|@*|text()|comment()" />  
</xsl:copy>  
</xsl:template>  
<xsl:template match="text()">  
<xsl:value-of select="normalize-space(.)" />  
</xsl:template>  
</xsl:stylesheet>  
</ds:Transform>  
<ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">  
<dsig-xpath:XPath xmlns:dsig-xpath="http://www.w3.org/2002/06/xmldsig-filter2"  
Filter="intersect">//*[ID='esimerkkiMoniallekirjoitusRakenne1']</dsig-xpath:XPath>  
</ds:Transform>  
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />  
</ds:Transforms>  
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />  
<ds:DigestValue>ewZFtmI0+m2XHM9Wu+kpaY/TBlg=</ds:DigestValue>  
</ds:Reference>  
</ds:SignedInfo>  
<ds:SignatureValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">  
NJYPtm1oAu2buJy14ytFvXzhlrWkChNIUOW92bPcZ4/aRSDKy2WgJLlVKAf0xr71s60+i4zLkAzkkHLSxtA26cDdxUW8ihW  
j98a+kP3ztr0eNBNEFWfHvI28vvt+tRIJvZNs00V4MdlzwsILKC04mY/U7yIvpGE3fZgszgotA8LID9qlzYpFlutLurJ4xFcj9aj1I  
XLdFkQ2rrCbjLlwQTp3VdsP1Y/7nrOLCx1bk9B1YR1L8NPuoHWFriY9sgejE8nr/qOfOQzc7Tcl72IgXc8q6YTs8mu69pjEL  
CieW8T0U1PZLXDe6Pj9xkYlZynk/qCjPnXclvwb1Ow==  
</ds:SignatureValue>  
<ds:KeyInfo>  
<ds:X509Data>
```





```
<ds:X509Certificate>
MIIFqDCCBJCgAwIBAgIEB2ss2TANBgkqhkiG9w0BAQUFADBfMQswCQYDVQQGEwJGSTERMA8GA1UEChMIVEVPIFRFU1Q
xJzAIBgNVBAsTHIRlcnZleWRlbnh1b2xsb24gdGVzdGI2YXJtZW5uZTEUMBIGA1UEAxMLVEVPIFRFU1QgQ0EwHhcNMDCxMj
A5MjIwMDAwWWhcNMTIxMjEwMjE1OTU5WjCBsDELMAkGA1UEBhMCRCkxZzANBgNVBEETBjEwMDAyNDEaMBGGA1UEDAw
RRXJpa29pc2Z2DpMOKa8OkcmkxFDASBgNVBAUTCzAwMTk4NzA0MDA5MRUwEwYDVQQQeWwQYWF2byBHaWRlb24xZjAU
BgNVBAQMDcOEbW3DpGzDpCBUZXMXLzAtBgNVBAMMJsOEbW3DpGzDpCBUZXMGUGFhdm8gR2lkZW9uIDAwMTk4NzA0
MDA5MIIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCGKCAQEAWtFUPdDlCypQboZ4IQ5e13HEjHpVfyV6SHWYbbRocVh3
uiTS3YDkK17MNLz2iWf7MuGQYtn523MPyQLP3wRgjt3G4D8A9RIOmjcbmvYB54IeNTfSnf5xYoyY+mvG8ifgY94H0BtgJSiw
9YcZcZLBFJYQ8RSOo6AR0IY3peil0tuL9idRkp7iB61yoeWClfJNRxuL3pgPjf5wjV6QiyPjeULxqcMCvvXz/HudQYUx55rNkjvvh
PY1uBC9SxolrTQBTt3gdJvDtGottKOWb9sQFGqbt7hcAtdHCiEN71nbSxFEaW8Isd6tAeM0BY+yqyr+WZsuUxgF54d+YGJ
e6QQIDAQABO4ICGDCCAqHwHwYDVR0jBBGwFoAULMp7wIEf48FpfkM1TL+31OIayoYwHQYDVRO0BBYEFJuDCPe/TVBzut
IBZuAkEkNrC0ynMA4GA1UdDwEB/wQEAwIGQDCBIQYDVR0gBIGNMIGKMIGHBgwqgXaEJ2MBAgGPVwswdzBLBgggBgEFB
QcCAJA/Gj1WYXJtZW5uZXBvbGloaWlra2Egb24gc2FhdGF2aWxsYSBodHRwOi8vd3d3LnZhbHR0ZXJpLmZpL2Nwczk5MCg
GCCsGAQUFBwIBFhxodHRwOi8vd3d3LnZhbHR0ZXJpLmZpL2Nwczk5MA8GA1UdEwEB/wQFMAMBAQAwgYwGA1UdHwSB
hDCBgTB/oH2ge4Z5bGRhcDovL2xkYXAudGVvLmZpOjM4OS9DTj1URU8IMjBURVNUJTIwQ0EsT1U9VGvYdmV5ZGVuaHVv
bGxvbiUyMHRlc3RpdmFybWVubmUsTz1URU8IMjBURVNULEM9Rkk/Y2VydGlmaWNhdGV5ZXZvY2F0aW9uTGldZDCBiQYI
KwYBBQUHAQEETB7MHkGCCsGAQUFBzAChm1sZGFwOi8vbGRhcC50ZW8uZmk6Mzg5L0NOPVRFTyUyMFRFU1QIMjBDQ
SxPVT1UZXR2ZXJkZW5odW9sbG9uJTIwdGVzdGI2YXJtZW5uZSxPPVRFTyUyMFRFU1QsQz1GST9jYUNlcnRpZmljYXRIMA0
GCSqGSIb3DQEBBQUAA4IBAQAfyotzXuLUcDPWJb6ksJgI65AeKWrl9nV/+WlJoYpK9I8hkFlyfBQbDNDorpuvgNbIsb42cLSl
4SCgfbzDlnq66n3vTwptD8PkyN19pJFBhHkAwGvXyyt7tY1SuvNppyKPNploE70ODPukYMacOEko25H3l+TXd58Z85UIJ2hqc
gq/YLI/IO1bkfo0olclIejn3wJAio5QXS+dLF+3GVnqew+My/fhxEspDJcRYwGIU3d+F91m1gmqDPufQpr842iRchBkMIG2CTp
5h2oO6IXYhmvZWKHV/KDn0snLjI0bpTgt50gNfubqNUa/Cl0Lhj6W1uT0JJVYIzvKtTPAZAq
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
</hl7fi:signature>
```