1 CDA R2 -asiakirjojen sähköisen allekirjoituksen määritys

Tämä dokumentti kokoaa yhteen ja täydentää CDA R2 -asiakirjojen sähköisistä allekirjoituksesta aiemmin annettuja määrityksiä.

CDA R2 -asiakirjojen sähköisiä allekirjoituksia koskevia määrityksiä ja ohjeita on tämän määrityksen julkaisemisen hetkellä seuraavissa dokumenteissa:
- tämä määritys
- XML-allekirjoituksen soveltamisopas v. 1.00
- CDA R2 Header v4.41

Niiltä osin kuin nämä dokumentit ovat keskenään ristiriitaisia, on dokumenttien soveltamisjärjestys seuraava:
- tämä määritys
- XML-allekirjoituksen soveltamisopas v. 1.00
- CDA R2 Header v4.41

Jatkossa dokumenttien sisältö yhtenäistetään.

1.1 Dokumentissa käytetyt merkinnät

Sähköiseen allekirjoitukseen liittyvät osuudet CDA-dokumentissa ovat kolmen eri nimiavaruuden (namespace) alla. Lisäksi allekirjoituksiin liittyy rakenteita joiden tietotyypit on määritelty XML Schemassa. Tässä määrityksessä käytetään selvyyden 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
ds	http://www.w3.org/2000/09/xmldsig#
cda	urn:hl7-org:v3
xs	http://www.w3.org/TR/2004/REC-xmlschema-2-20041028/

Tämän määrityksessä käytetään esimerkkinä pelkistettyä CDA-rakennetta jolla pyritään korostamaan allekirjoitukseen vaikuttavia keskeisiä rakenteita. Selkeyden vuoksi muut osat on piilotettu ...-merkin taakse.

2 Sähköisessä allekirjoituksessa sallitut menetelmät

Tämä määritys on sallittujen algoritmien osalta muuten yhdenmukainen OpenCDA Header 4.41 määrityksen kanssa, mutta sallittujen kanonikalisointimenetelmien joukkoon on palautettu http://www.w3.org/2001/10/xml-exc-c14n#WithComments -algoritmi[1].

[1] Kyseinen menetelmä oli kuvattu sallituksi ensimmäisissä julkaistuissa suosituksissa aiheesta, ja osa toteutuksista on toteutettu niiden mukaisesti.

Seuraavassa taulukossa on esitetty elementtikohtaisesti mitkä arvot ovat sallittuja parametreja CDA R2 -asiakirjan XML-allekirjoitusrakenteessa (***ds:Signature***) Elementit ovat kaikki ***ds:SignedInfo***-elementin lapsia. Vaihtoehtoisista arvoista suositeltu algoritmi on alleviivattu.

Taulukko 2

Elementti	Sallitut menetelmät
ds:CanonicalizationMethod	Exclusive XML Canonicalization version 1.0 (without comments) [http://www.w3.org/2001/10/xml-exc-c14n#] Canonical XML version 1.0 (without comments) [http://www.w3.org/TR/2001/REC-xml-c14n-20010315] Exclusive XML Canonicalization version 1.0 (with comments) [http://www.w3.org/2001/10/xml-exc-c14n#WithComments]
ds:SignatureMethod	RSAwithSHA1 [http://www.w3.org/2000/09/xmldsig#rsa-sha1]
ds:Reference/ ds:Transforms/ ds:Transform	Enveloped Signature Transform [http://www.w3.org/2000/09/xmldsig#enveloped-signature] XSLT Transform [http://www.w3.org/TR/1999/REC-xslt-19991116] XPath Filtering [http://www.w3.org/TR/1999/REC-xpath-19991116] Base64 [http://www.w3.org/2000/09/xmldsig#base64] XPath Filter-2 [http://www.w3.org/TR/2002/REC-xmldsig-filter2-20021108/] Exclusive XML Canonicalization version 1.0 (without comments) [http://www.w3.org/2001/10/xml-exc-c14n#] Canonical XML version 1.0 (without comments) [http://www.w3.org/TR/2001/REC-xml-c14n-20010315] Exclusive XML Canonicalization version 1.0 (with comments) [http://www.w3.org/2001/10/xml-exc-c14n#WithComments]
ds:Reference/ ds:DigestMethod	SHA1 [http://www.w3.org/2000/09/xmldsig#sha1]

2.1 Sähköisiä allekirjoituksia koskevat sitovat vaatimukset

Allekirjoituksissa käytettävien varmenteiden tulee olla voimassaolevan lain ja asetusten mukaisia[2].

[2] Terveydenhuollon varmenteita toimittavan Valviran varmenteisiin liittyvät määrittelyt löytyvät osoitteesta www.valtteri.fi.

Yksittäisen asiakirjan allekirjoituksessa ei saa käyttää moniallekirjoitusrakennetta

Kaikki järjestelmäallekirjoitukset tehdään yksittäisen asiakirjan allekirjoituksina.

Allekirjoittajan allekirjoitusvarmenne on liitettävä osaksi allekirjoitusta sekä yksittäin allekirjoitetuissa että moniallekirjoitetuissa dokumenteissa.

Allekirjoitettavan CDA R2 -asiakirjan pitää olla kulloinkin voimassa olevan virallisen CDA R2 skeeman mukainen sekä ennen allekirjoitusta, että allekirjoituksen jälkeen.

CDA R2-asiakirjan sisältämän XML-allekirjoituksen on oltava validi XML-allekirjoitusstandardin kokonaisuudessaan toteuttavaa allekirjoitusvalidaattoria vastaan, esimerkiksi SUNin tai Apachen xmlsec-implementaatio.

2.2 Sähköisiä allekirjoituksia koskevat suositukset

Suositellaan käyttämään allekirjoituksen kohdistamisessa paikallista viittausta (URI-viittaus ***ID***[3]-attribuutin arvoon).

Suositellaan asettamaan ***cda:structuredBody***-elementille ***ID***-attribuutti ja tälle arvo, vaikka allekirjoitusta muodostava järjestelmä ei tätä itse käytettäisi allekirjoitusta muodostettaessa (eli kohdistus tehdään Xpath tai Filter2 menetelmällä).

Suositellaan käyttämään kanonikalisointimenetelmää ”Exclusive XML Canonicalization version 1.0 (without comments)”.

Suositellaan varmistumaan käytettävän kohdistuksen oikeellisuudesta.

Suositellaan että ***ds:Signature*** -elementille asetetaan ***ID***-attribuutti ja tälle yksilöivä arvo, vaikka allekirjoitusta tuottava järjestelmä ei tätä arvoa itse käyttäisi mihinkään.

Suositellaan noudattamaan soveltamisohjeen yhteentoimivuuteen liittyviä ohjeita.

2.3 Moniallekirjoituksessa käytettävät menetelmät

Moniallekirjoitusrakenteen sisältämien hajautussummien muodostamisessa pitää hyödyntää samoja algoritmeja kuin moniallekirjoitusrakenteeseen itseensä kohdistuvassa ds:Rerefence-elementissä on käytetty. Sijainnin osoittamiseen käytettäviä menetelmiä (XPath ja Filter2) ei tarvitse soveltaa.

Ne algoritmit joiden soveltamiseen tulee varautua moniallekirjoituksia muodostettaessa ja tarkistettaessa on eritetty seuraavassa taulukossa:

Taulukko 3

elementti	Moniallekirjoitukseen periytyvät algoritmit
ds:Reference/ ds:Transforms/	http://www.w3.org/2000/09/xmldsig#enveloped-signature http://www.w3.org/TR/1999/REC-xslt-19991116 http://www.w3.org/2001/10/xml-exc-c14n#

[3] Jotta viittaus toimii yhdenmukaisesti eri ympäristöissä tulee käytettävän ***ID***-attribuutin olla määritetty ***xs:ID*** -tyyppiseksi ja näin määrittelevän skeeman/dtd:n olla allekirjoitusympäristön käytettävissä allekirjoituksia muodostettaessa ja tarkistettaessa.
(***xs:ID***-tyyppisen solmun yksilöintiin käytettävän attribuutin kirjoitusasu on CDA-määrityksissä ***ID*** ja XML-allekirjoituksen määrityksissä ***Id***).

elementti	Moniallekirjoitukseen periytyvät algoritmit
ds:Transform	http://www.w3.org/2001/10/xml-exc-c14n#WithComments http://www.w3.org/TR/2001/REC-xml-c14n-20010315
ds:Reference/ ds:DigestMethod	http://www.w3.org/2000/09/xmldsig#sha1

Moniallekirjoituksen kohdistamisesta on käsitelty yksityiskohtaisemmin luvussa 5.2. Moniallekirjoituksen muodostamisesta ja tarkistamisesta on yksityiskohtainen kuvaus luvuissa 6.3 ja 6.4

3 CDA-allekirjoituksen rakenne

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

hl7fi:signatureCollection -elementti sisältää nolla tai useampia ***hl7fi:signature*** -elementtejä joista kukin sisältää yhden allekirjoituksen tiedot. Kaikki erityyppiset 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 tyypin. Tyypin kuvaamiseen käytettävä koodisto on: ”Sähköisen allekirjoituksen tyyppi” ja sen OID-tunnus on 1.2.246.537.5.40127.2006. Koodisto jaellaan THL:n koodistopalvelun kautta muiden vastaavien CDA-koodistojen tavoin.

Esimerkki ***hl7fi:signatureDescription*** -elementistä:

```
<hl7fi:signatureDescription code="1"
        codeSystem="1.2.246.537.5.40127.2006"
        codeSystemName="Sähköisen allekirjoituksen tyyppi"
        displayName="ammattihenkilön tekemä normaali allekirjoitus"/>
```

Esimerkki koodiston 1.2.246.537.5.40127 (KanTa-palvelut - Sähköisen allekirjoituksen tyyppi) arvolistasta:

Id	Short name
1	Ammattihenkilön tekemä tavanomainen allekirjoitus
2	Ammattihenkilön tekemä moniallekirjoitus
3	Järjestelmäallekirjoitus / perusjärjestelmä
4	Järjestelmäallekirjoitus / KanTa
5	Potilaan sähköinen allekirjoitus

Id	Short name
6	Luotettavalla tavalla varmennettu aikaleima

(koodiston ajantasainen versio on jakelussa THL:n ylläpitämässä koodistopalvelussa)

hl7fi:signatureTimestamp-elementti sisältää kellonajan sekunnin tarkkuudella. Elementti on tyyppiä ***xs:dateTime***[4] ja sillä on pakollinen attribuutti ***ID***. Aikaleiman muodostaminen on kuvattu yksityiskohtaisemmin luvussa 4.

Esimerkki ***hl7fi:signatureTimestamp*** -elementistä:

```
<hl7fi:signatureTimestamp ID="TSid001">2008-11-21T12:18:06Z</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:structuredBody***-elementistä laskettu hajautussumma. Hajautussumman laskemisessa käytetään samoja kanonikalisointi- ja hajautusalgoritmeja kuin moniallekirjoitusrakenteeseen kohdistuvassa allekirjoituksessa.

Esimerkki hl7fi:multipleDocumentSignature -elementistä:

```
<hl7fi:multipleDocumentSignature ID="MDSid001">
        <hl7fi:Ref OID="1.2.246.10.98765432.93.2009.1" hash="biiFiCL6NjvIw4tlwCTAvfYsiLM="/>
        <hl7fi:Ref OID="1.2.246.10.98765432.93.2009.2" hash="MZIz+sdPtKCORLFvyxf6IiInXt0="/>
        <hl7fi:Ref OID="1.2.246.10.98765432.93.2009.3" hash="B9/F5tiIs5o/xOiQmkQiijEXYxU="/>
</hl7fi:multipleDocumentSignature>
```

```
<cda:ClinicalDocument xmlns:cda="urn:hl7-org:v3">
  ...
  <cda:id root="1.2.246.10.2164623.93.2009.1"/>
  ...
  <hl7fi:localHeader xmlns:hl7fi="urn:hl7finland">
    ...
    <hl7fi:signatureCollection>
      <hl7fi:signature ID="CDA-allekirjoitus-esimerkki">
        <hl7fi:signatureDescription code="1" codeSystem="1.2.246.537.5.40127.2006"/>
        <hl7fi:signatureTimestamp ID="CDA-aikaleima">2009-11-10T12:01:01+02:00</hl7fi:signatureTimestamp>
        <ds:Signature Id="XML-signature" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          ...
        </ds:Signature>
      </hl7fi:signature>
    </hl7fi:signatureCollection>
  </hl7fi:localHeader>
  <cda:component>
    <cda:structuredBody ID="CDA-allekirjoituksen-kohde">...</cda:structuredBody>
  </cda:component>
</cda:ClinicalDocument>
```

Kuva 1 Pelkistetty esimerkki sähköisestä allekirjoituksesta CDA R2 -asiakirjassa

Sähköisen allekirjoituksen skeematiedosto on osa CDA R2 Header kokonaisuutta. CDA Header 4.41 versiossa sähköisen allekirjoituksen rakenne on skeematiedostossa hl7fi_extensions_cdar2header.xsd.

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

XML-allekirjoitusstandardi määrittää kolme erilaista allekirjoitustyyppiä sen mukaan miten sähköinen allekirjoitus sijoittuu suhteessa allekirjoituksen kohteena olevaan sisältöön. CDA R2 -asiakirjoissa käytettävä allekirjoitustyyppi on detached[5].

3.1 Moniallekirjoituksen rakenne

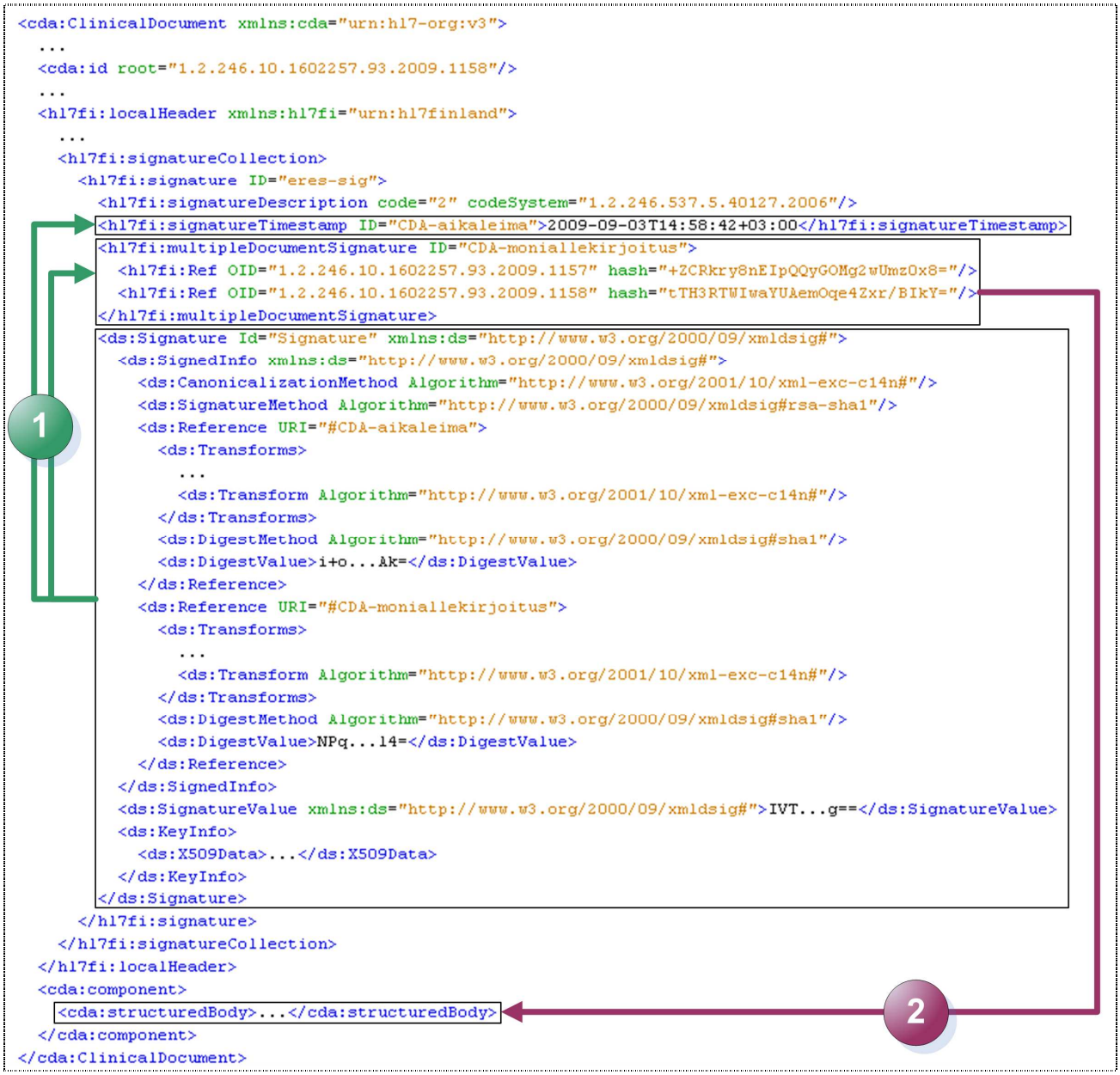
Moniallekirjoitus eroaa yksittäisestä allekirjoituksesta seuraavilta osin:

- ***hl7fi:signatureDescription*** -elementissä määritelty allekirjoituksen tyyppi on arvoltaan 2, eli ammattihenkilön tekemä moniallekirjoitus.
- käytössä on ***hl7fi:multipleDocumentSignature*** -elementti
- toinen ***ds:Reference*** - elementeistä ei kohdistu ***cda:structuredBody*** -elementtiin, vaan ***hl7fi:multipleDocumentSignature*** -elementtiin
- kaikki yhdellä kertaa moniallekirjoitetut asiakirjat sisältävät saman ***hl7fi:signatureCollection*** -elementin. Erityisesti on huomioitavaa, että ***hl7fi:signatureTimestamp*** -elementti ja sen sisältämä aika on sama kaikissa asiakirjoissa.

Tästä seuraa se, että allekirjoituksen XML-allekirjoitusosuus ei enää takaa suoraan varsinaisen tietosisällön, eli ***cda:structuredBody*** elementin ja tämän alipuun, eheyttä. Tietosisällön eheyden takaaminen tapahtuu ***hl7fi:multipleDocumentSignature***-elementin sisältämän ***hl7fi:Ref*** -elementin kautta vastaavilla menetelmillä kuin yksittäisessä allekirjoituksessa. Kohteena olevan sisällön muuttumattomuuden takaa moniallekirjoitusrakenteeseen muodostettu hajautussumma, jonka muuttamattomuuden takaa XML-allekirjoitus.

Kuvassa 1 on esitetty allekirjoituksen kohdistuminen ja eheyden takaaminen moniallekirjoituksessa. 1-Nuolet kuvaavat XML-allekirjoituksen sisältämiä kohdistuksia. 2-Nuoli kuvaa moniallekirjoitusrakenteen sisältämää kohdistusta.

[5] detached-muoto sallisi allekirjoituksen sijoittamisen eri tiedostoon kuin missä allekirjoitettava tietosisältö on, mutta tämä ominaisuus ei ole käytössä CDA R2 -asiakirjojen allekirjoittamisessa. detached-muodon määritelmä: http://www.w3.org/TR/xmldsig-core/#def-SignatureDetached



Kuva 2 Moniallekirjoituksen kohdistumiset - allekirjoitus takaa nuolen kohteina olevien alueiden muuttumattomuuden

4 Allekirjoituksen aikaleima

hl7fi:signatureTimestamp -elementin tietosisältö sisältää allekirjoituksen ajankohdan sekunnin tarkkuudella. Käytetty ajan esitystapa noudattaa tyyppiä ***xs:dateTime***[6]

Esimerkkejä ***hl7fi:signatureTimestamp*** -elementistä:

```
<hl7fi:signatureTimestamp ID="TSid001">2009-11-11T20:18:06Z</hl7fi:signatureTimestamp>
<hl7fi:signatureTimestamp ID="TSid002">2009-11-11T22:18:06+02:00</hl7fi:signatureTimestamp>
<hl7fi:signatureTimestamp ID="TSid003">2009-07-07T07:07:07+03:00</hl7fi:signatureTimestamp>
```

[6] XML Schema Part 2: Datatypes Second Edition. W3C Recommendation 28 October 2004, http://www.w3.org/TR/xmlschema-2/#dateTime, luku 3.2.7

```
<hl7fi:signatureTimestamp ID="TSid004">2009-07-07T04:07:07Z</hl7fi:signatureTimestamp>
```

Esimerkin ensimmäinen ja toinen sekä kolmas ja neljäs rivi kuvaavat keskenään samaa aikaa.

Aikaleimassa voidaan ilmaista myös sekunnin murto-osat tai aikavyöhyke. Aikavyöhyke ilmoitetaan erotuksena UTC-aikaan, joten on huomioitava että esimerkiksi Suomen aikavyöhyke on kesäajan voimassa ollessa +03:00 ja muutoin +02:00 (UTC ei noudata kesäaikaa). Ohjelmointiympäristöt ja välineet saattavat hoitaa tämän tosin automaattisesti. Jotta aikaan liittyvät vertailut voidaan tehdä yksikäsitteisesti - on suositeltavaa että aikaleimassa ilmaistaan aikavyöhyke tai aikaleima annetaan UTC ajassa (aikavyöhyke -00:00, +00:00 tai Z). Jos aikaleimasta puuttuu aikavyöhyketieto, ohjelmointiympäristöt voivat tulkita sen olevan sama kuin paikallinen aikavyöhyke, mistä voi seurata aikahetken vääristyminen.

On suositeltavaa että järjestelmien kello on synkronoitu NTP-protokollan avulla oikeaan aikaan. NTP-palvelimia on tarjolla sekä ilmaiseksi että kaupallisten toimijoiden toimesta. Mittatekniikan keskus Mikes tarjoaa Suomen viralliseen aikaan synkronoitua NTP-palvelua eri tasoilla.

Moniallekirjoituksessa kaikilla yhdellä kertaa allekirjoitetuilla asiakirjoilla on sama aikaleima.

Sähköinen allekirjoitus kohdistuu aikaleimarakenteeseen. Tästä seuraa että aikaleima pitää muodostaa ennen allekirjoittamista ja että aikaleiman sisältöä ei saa muokata allekirjoittamisen jälkeen.

5 Sähköisen allekirjoituksen kohdistuminen

Yksittäinen allekirjoitus ja moniallekirjoitus sisältävät molemmat XML-allekirjoitusrakenteen, joka sisältää kaksi kohdistusta allekirjoitettavaan tietoon. Yksi kohdistuksista osoittaa aikaleimarakenteeseen, toinen asiakirjan tietosisältöön.

Yksittäinen allekirjoitus kohdistuu XML-allekirjoituksesta suoraan asiakirjan tietosisältöön. Moniallekirjoituksessa XML-allekirjoitus kohdistuu moniallekirjoitusrakenteeseen. Moniallekirjoitusrakenne kohdistuu kunkin moniallekirjoitetun asiakirjan tietosisältöön. Moniallekirjoitusrakenne on paikallinen laajennus.

5.1 XML-allekirjoituksen kohdistuminen

XML-allekirjoitus muodostuu kahdesta päällekkäisestä kerroksesta. Sisempänä on ***ds:SignedInfo***-rakenne ja sen sisältämät ***ds:Reference***-solmut, jotka sisältävät viittauksen allekirjoitettavaan sisältöön. Ulompana on varsinaisen julkisen avaimen allekirjoituksen kerros.

Julkisen avaimen kerroksen allekirjoituksessa allekirjoitettava sisältö on ***ds:SignedInfo***-rakenne. Ennen allekirjoittamista ***ds:SignedInfo***-rakenne kanonikalisoidaan ***ds:CanonicalizationMethod***-solmun mukaisella menetelmällä. Allekirjoituksessa käytetty algoritmi määritetään ***ds:SignatureMethod***-solmussa. Allekirjoituksessa käytetyn avaimen tiedot esitetään ***ds:KeyInfo***-solmussa. Allekirjoituksen arvo tallennetaan ***ds:SignatureValue***-solmuun.

XML-allekirjoitus kohdistuu allekirjoitettavaan sisältöön ***ds:Reference***-rakenteella siten että kohteesta muodostettu tiiviste (hajautussumma) tallennetaan ***ds:DigestValue*** -solmun arvoksi. Kohdistuminen tapahtuu määrittämällä kohteena olevan XML-rakenteen

sijainti suhteessa allekirjoitukseen ja suodatukset jotka rakenteelle tehdään ennen tiivisteen laskemista.

CDA R2-asiakirjassa sähköinen allekirjoitus on osa samaa XML-rakennetta kuin ne rakenteet joihin allekirjoitus kohdistuu. Kohteen sijainti voidaan esittää ***ds:Reference*** -elementin ***URI***-attribuutissa URI-viittauksella. Vaihtoehtoisesti ***URI***-attribuutti voi viitata XML-rakenteen juureen ja tarkka sijainti määritetään suodattamalla. Tämän määrityksen esimerkeissä käytetään tilan säästämiseksi URI-viittausta.
ds:reference-elementtejä on kaksi, joista yksi kohdistuu aina aikaleimaan (***hl7fi:signatureTimestamp*** -elementti). Toinen ***ds:reference***-elementti kohdistuu yksittäisissä allekirjoituksissa ***cda:structuredBody***-elementtiin.

Kohdistaminen voi tapahtua joko pelkällä URI-atribuutilla tai URI-atribuutin ja Filter-suodatuksen yhdistelmällä.

Soveltamisoppaassa on tarkempi kuvaus eri kohdistamismenetelmistä esimerkkeineen. Alla on esitetty yksittäisen sähköisen allekirjoituksen kohdistuminen (Kuva 3).

Hajauttamisessa käytettävä algoritmi määritetään ***ds:DigestMethod*** solmussa.

Ennen hajauttamista kohteena oleva XML-rakenne suodatetaan ***ds:Transform***-solmujen mukaisilla menetelmillä. Suodatusmenetelmät ovat jaettavissa neljään osajoukkoon käyttötarkoituksen mukaisesti. Käyttötarkoitukset ja näitä vastaavat algoritmit on esitetty alla taulukossa:

Taulukko 4

ID	käyttötarkoitus	Algoritmi
1	XML-allekirjoitusten suodattaminen	http://www.w3.org/2000/09/xmldsig#enveloped-signature
2	Kohdistaminen / kohteen rajaaminen	http://www.w3.org/2002/06/xmldsig-filter2 http://www.w3.org/TR/1999/REC-xpath-19991116]
3	Suodattaminen XSLT-merkintäkielen avulla	http://www.w3.org/TR/1999/REC-xslt-19991116
4	Kanonikalisointi	http://www.w3.org/2001/10/xml-exc-c14n# http://www.w3.org/2001/10/xml-exc-c14n#WithComments http://www.w3.org/TR/2001/REC-xml-c14n-20010315

XML-allekirjoitusten suodattaminen -toiminnallisuudella XML-allekirjoitukset suodatetaan pois allekirjoituksen kohteena olevasta XML-rakenteesta. Tämänhetkisissä CDA-asiakirjojen allekirjoituksissa allekirjoitusten suodattaminen ei ole tarpeen, mutta tästä ei myöskään ole mitään haittaa.

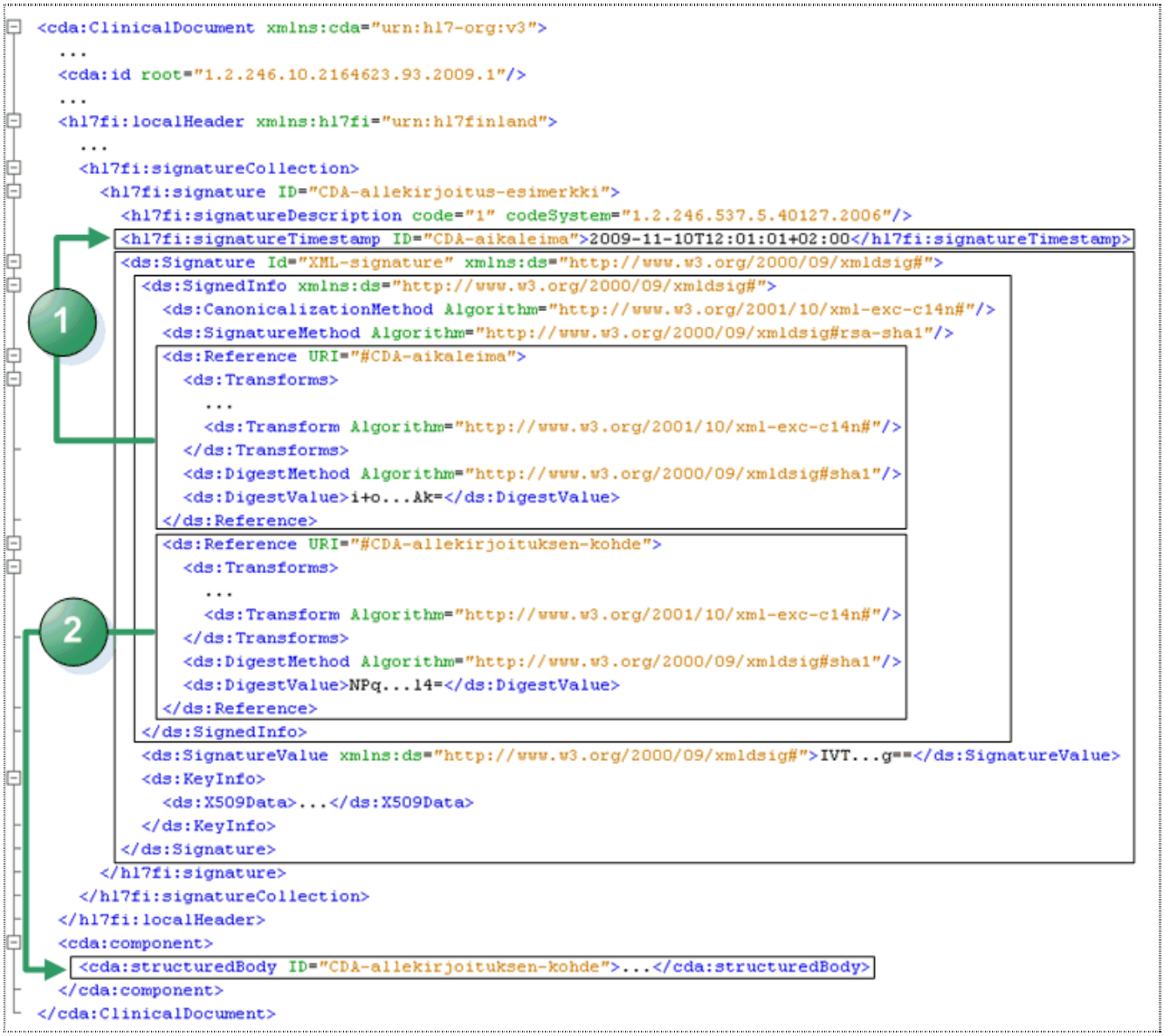
Kohdistaminen / kohteen rajaaminen -toiminnallisuudella allekirjoituksen kohdistus XML-rakenteeseen voidaan rajata yksityiskohtaisesti suodatusmenetelmälle annettujen parametrien mukaisesti. Tuetut menetelmä (Xpath ja Filter2) ovat kuvausvoimaltaan vastaavia, mutta Filter2 -menetelmän mukaiset toteutukset ovat tyypillisesti tehokkaampia, ja siksi se on menetelmistä suositeltavampi.

Suodattaminen XSLT-merkintäkielen avulla -toiminnallisuudella allekirjoituksen kohteena oleva XML-rakennetta voidaan suodattaa yksityiskohtaisesti menetelmälle annettujen parametrien mukaisesti.

Kanonikalisointi -toiminnallisuudella allekirjoituksen kohteena oleva XML-rakenne voidaan yhdenmukaistaa ennen allekirjoituksen muodostamista. Kanonikalisointi tulee

tehdä suodatusmenetelmistä viimeisenä, jotta muut sen jälkeen sovellettavat menetelmät eivät sotke yhdenmukaistettua järjestystä.

Edellä kuvatuista toiminnallisuuksista kanonikalisointi on ainoa jonka käyttäminen allekirjoituksia muodostettaessa on pakollista. Muiden toiminnallisuuksien käyttäminen allekirjoituksia muodostettaessa on valinnanvaraista.



Kuva 3 yksittäisessä allekirjoituksessa XML-allekirjoitus kohdistuu aikaleimaan (1) ja asiakirjan sisältöön (2)

5.2 Moniallekirjoituksen kohdistuminen

Moniallekirjoitusrakenteen ***hl7fi:Ref***-rakenne vastaa käyttötarkoitukseltaan XML-allekirjoituksen ***ds:Reference***-rakennetta. ***ds:Reference***-rakenteessa käytetty kohdistaminen erilaisine vaihtoehtoisine parametreineen on kuvattu luvussa 5.1.

hl7fi:Ref -elementin osoittaman rakenteen sijainti, käytettävä hajautusmenetelmä ja käytettävät suodatukset määräytyvät seuraavasti:

hl7fi:Ref -elementin kohteena oleva XML-rakenne on ***OID***-attribuutin arvoa vastaavan CDA R2-asiakirjan ***cda:structuredBody*** ja tämän alipuu. Kohteesta muodostettu hajautussumma tallennetaan ***hash***-attribuutin arvoksi.

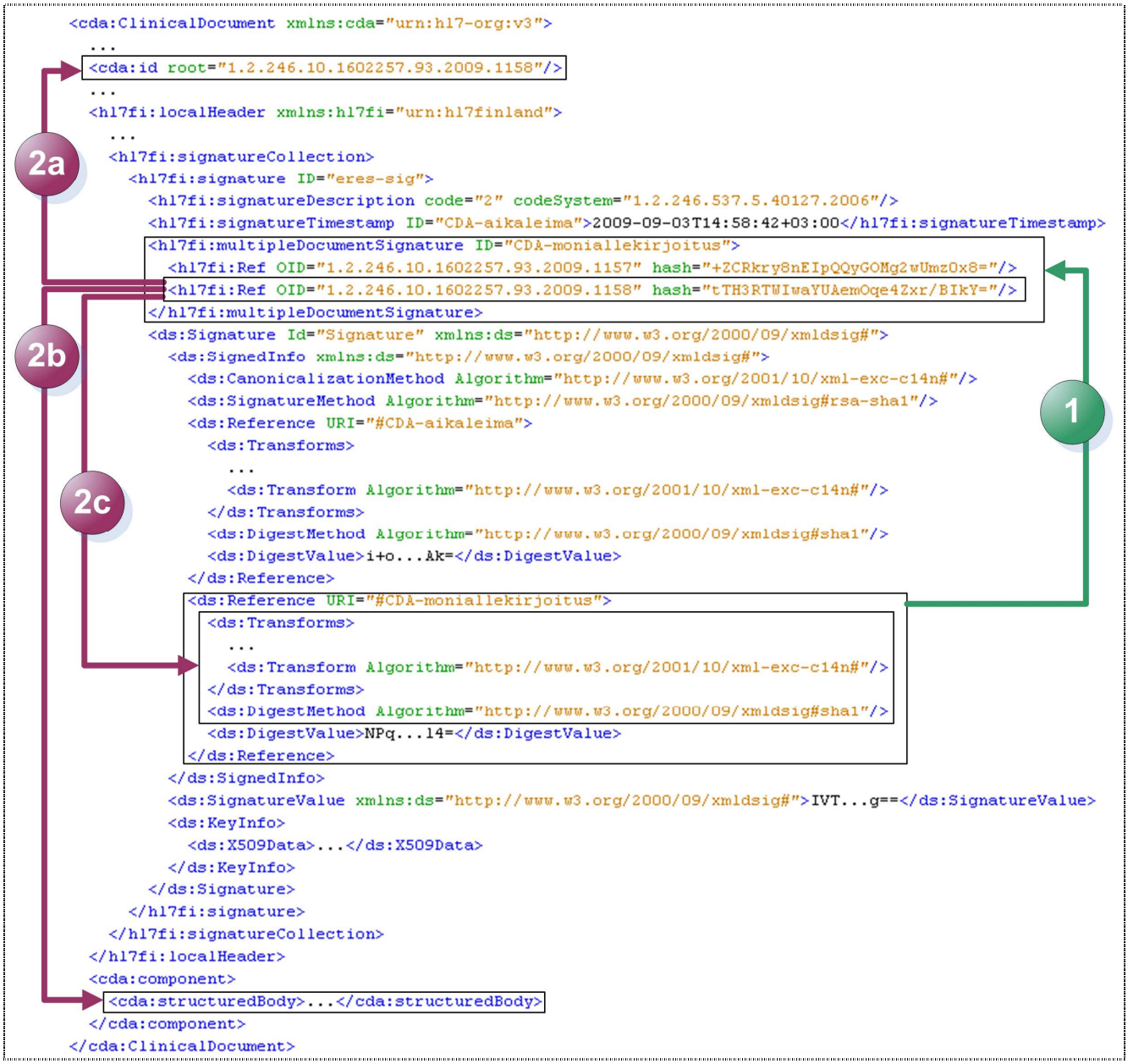
CDA-dokumentin yksilöintitunnuksena käytetty OID sijaitsee asiakirjan ***cda:id*** -solmussa. Oikean dokumentin valinta ja ***cda:structuredBody*** -rakenteen kohdistamiseen käytettävä menetelmä ovat toteutuskohtaisesti vapaasti valittavissa sallittujen menetelmien joukosta.

cda:structuredBody -rakenteen suodattamiseen käytetään ***hl7fi:multipleDocumentSignature***-elementtiin kohdistuneen ***ds:Reference***-rakenteen mukaisia ***ds:Transform*** -solmujen menetelmiä. Luvussa 2.3 on esitetty ne menetelmät joita tämä koskee (Taulukko 3).

ds:Transform -solmujen menetelmiä sovellettaessa tulee huomioida se, että menetelmien järjestyksellä on merkitystä[7]. Menetelmät tulee soveltaa samassa järjestyksessä kuin ne sovelletaan XML-allekirjoituksessa. Erityisesti suositellaan huolehtimaan siitä, että kanonikalisointi suoritetaan menetelmistä viimeisenä ennen tiivisteen laskemista.

Moniallekirjoituksen kohdistuminen on esitetty kuvassa 2. Nuoli 2a kuvaa ***hl7fi:Ref*** solmun ***OID***-elementin mukaista viittausta dokumentin ***cda:id***-solmuun. Nuoli 2b kuvaa edellisen nuolen mukaista viittausta ***cda:structuredBody*** -rakenteeseen. Nuoli 2c kuvaa moniallekirjoituksen riippuvuutta ***ds:Reference*** -rakenteen ***ds:Transfom***-rakenteista.

[7] Juuri ennen hajautusta tehtynä kanonikalisointi takaa yhdenmukaisen rakenteen esitystavan. Muiden menetelmien osalta rakenteen esitystapa eri ympäristöissä voi vaihdella.



Kuva 4 moniallekirjoitusrakenne on riippuvainen punaisten nuolten kohteista

6 Käyttötapaukset

6.1 Henkilökohtaisen yksittäisen allekirjoituksen muodostaminen

Yksittäisen allekirjoituksen muodostamisen prosessi on seuraava:

1. **Käyttäjä** valitsee asiakirjan allekirjoituksen suoritettavaksi (voi tapahtua myös implisiittisesti)
2. **Sovellus** muodostaa asiakirjan tiedoista CDA R2 -asiakirjan
3. **Sovellus** muodostaa aikaleimarakenteen ja liittää tämän asiakirjaan
4. **Sovellus** muodostaa XML-allekirjoituksen, joka kohdistuu aikaleimarakenteeseen ja CDA R2 -asiakirjan ***cda:structuredBody***-rakenteeseen.

   a. **Sovellus** välittää allekirjoitettavasta sisällöstä muodostetun hajautussuman käyttäjän toimikortille allekirjoitettavaksi
   b. **Käyttäjä** syöttää PIN2-koodin ja kortti tekee allekirjoituksen.
5. **Sovellus** muodostaa ja liittää XML-allekirjoituksen asiakirjaan

6.2 Yksittäisen allekirjoituksen tarkistaminen

Yksittäisen allekirjoituksen tarkistamisen prosessi on seuraava:

1. **Sovellus** tarkistaa XML-allekirjoituksen eheyden. XML-allekirjoituksen tarkistaminen tarkistaa allekirjoituksen kohteena olevien tietojen sisällön muuttumattomuuden.
2. **Sovellus** tarkistaa XML-allekirjoituksen sisältämän varmenteen eheyden ja luotettavuuden (varmenteen tulee olla luotetun ja hyväksytyn varmentajan myöntämä)
3. **Sovellus** tarkistaa allekirjoituksen muodostamisajan ja vertaa tätä varmenteen voimassaoloaikaan. Aikaleima ei saa olla nykyhetkestä katsottuna tulevaisuudessa eikä varmenteen voimassaoloajan ulkopuolella (ennen varmenteen voimassaolon alkamista tai voimassaolon päättymisen jälkeen tehty)

Allekirjoituksesta voidaan haluttaessa tarkistaa myös seuraavia osioita:

4. **Sovellus** tarkistaa että allekirjoitus kohdistuu määritysten mukaisesti aikaleimaan ja ***cda:structuredBody***-osioon.
5. **Sovellus** tarkistaa että allekirjoituksessa käytetyt menetelmän ovat tämän määrityksen mukaisia.

6.3 Moniallekirjoituksen muodostaminen

Moniallekirjoituksen muodostamisen prosessi on seuraava:

1. **Käyttäjä** valitsee tai merkitsee allekirjoitettavat asiakirjat käyttämänsä sovelluksen käyttöliittymästä
2. **Käyttäjä** valitsee moniallekirjoituksen suoritettavaksi (voi tapahtua myös implisiittisesti)
3. **Sovellus** muodostaa moniallekirjoitusrakenteen
4. **Sovellus** muodostaa kutakin asiakirjaa vastaavan rivin moniallekirjoitusrakenteeseen
   a. Asiakirjan ***cda:structuredBody***-osiosta lasketaan tiiviste[8]. Tiivisteen laskemisessa käytettävät menetelmät ovat samat kuin moniallekirjoitusrakenteeseen itseensä kohdistuvassa ***ds:Reference*** -elementissä (6)
      i. Poikkeuksena kohdistamisessa käytettävät menetelmät (URI, xpath, filter2). Näiden osalta ei käytetä ***ds:Reference***-elementin arvoja.
      ii. Menetelmien soveltamisjärjestys on sama kuin ***ds:Reference*** -elementissä
      iii. Muodostettu Tiiviste tallennetaan Base64-muodossa ***hash***-attribuutin arvoksi.
   b. Asiakirjan tunniste (OID) ja hajautussumma liitetään yhteen
5. **Sovellus** muodostaa yhden aikaleimarakenteen

[8] cda:structuredBody -elementtiin kohdistamiseen käytettävällä menetelmällä ei ole merkitystä koska oikein käytettynä kaikki menetelmät palauttavat saman rakenteen.

6. **Sovellus** muodostaa XML-allekirjoituksen, joka kohdistuu aikaleimarakenteeseen ja moniallekirjoitusrakenteeseen
    c. **Sovellus** välittää allekirjoitettavasta sisällöstä muodostetun hajautussuman käyttäjän toimikortille allekirjoitettavaksi
    d. **Käyttäjä** syöttää PIN2-koodin ja kortti tekee allekirjoituksen.
7. **Sovellus** muodostaa yhden allekirjoitusrakenteen joka sisältää XML-allekirjoituksen, moniallekirjoitusrakenteen ja aikaleiman, sekä kopioi tämän saman rakenteen jokaiseen moniallekirjoituksen kohteena olleeseen asiakirjaan

Lähetettäessä moniallekirjoitettu asiakirja KanTa-järjestelmään, liittyy allekirjoituksen muodostamiseen vielä seuraavat vaiheet:

8. **Sovellus** lähettää allekirjoitetun asiakirjan arkistoon
9. **KanTa** tarkistaa asiakirjassa olevan moniallekirjoituksen oikeellisuuden
10. **KanTa** allekirjoittaa asiakirjan järjestelmäallekirjoituksella
11. **KanTa** tallentaa asiakirjan arkistoon (mukana molemmat allekirjoitukset)

6.4 Moniallekirjoituksen tarkistaminen

Moniallekirjoituksen tarkistamisen prosessi on seuraava:

1. **Sovellus** tarkistaa asiakirjan sisältämien XML-allekirjoitusten eheyden. XML-allekirjoituksen tarkistaminen tarkistaa allekirjoituksen kohteena olevien tietojen sisällön muuttumattomuuden.
2. **Sovellus** tarkistaa XML-allekirjoituksen sisältämien varmenteiden eheyden ja luotettavuuden (varmenteen tulee olla luotetun ja hyväksytyn varmentajan myöntämä)
3. **Sovellus** tarkistaa kunkin allekirjoituksen muodostamisajan ja vertaa tätä kyseisen allekirjoituksen varmenteen voimassaoloaikaan. Aikaleima ei saa olla nykyhetkestä katsottuna tulevaisuudessa eikä varmenteen voimassaoloajan ulkopuolella (ennen varmenteen voimassaolon alkamista tai voimassaolon päättymisen jälkeen tehty)
    a. **Sovellus** muodostaa asiakirjan ***structuredBody***-osiosta tiivisteen ja vertaa tätä asiakirjan moniallekirjoitusrakenteessa vastaavan rivin ***hash***-attribuutin arvoon.
    b. **Sovellus** valitsee tarkastettavan rivin siten että OID-attribuutti vastaa tarkistettavan CDA R2 asiakirjan tunnistetta (***cda:ClinicalDocument/cda:id*** -elementin ***root*** ja ***extension*** -attribuuttien mukainen arvo)
    c. Tiivisteen laskemisessa käytetään soveltuvin osin samoja menetelmiä samassa järjestyksessä kuin tarkistettavaan moniallekirjoitusrakenteeseen kohdistuvassa ***ds:Reference***-elementissä käytetään.
        i. Poikkeuksena kohdistamisessa käytettävät menetelmät (URI, xpath, filter2). Näiden osalta ei käytetä ***ds:Reference***-elementin arvoja.
        ii. Menetelmien soveltamisjärjestys on sama kuin ***ds:Reference*** -elementissä
        iii. Muodostettua tiivistettä verrataan Base64-muodossa ***hash***-attribuutin arvoon.

Tiivisteen muodostamisessa suositellaan käytettävän hyödyksi XML-allekirjoitustoteutusta siten, että asiakirjasta muodostetaan järjestelmäallekirjoitus käyttäen ***cda:sctucturedBody***-osioon kohdistuvassa ***ds:Reference***-elementissä samoja menetelmiä ja näiden parametreja kuin tarkistettavassa allekirjoituksessa käytetään moniallekirjoitusrakenteeseen kohdistuvassa allekirjoituksessa. Poikkeuksena tähän

kuitenkin kohdistaminen, jotta kohteena on ***cda:sctucturedBody***-osio eikä moniallekirjoitusrakenne.

Allekirjoituksesta voidaan haluttaessa tarkistaa myös seuraavia osioita:

4. **Sovellus** tarkistaa että allekirjoitus kohdistuu määritysten mukaisesti aikaleimaan ja moniallekirjoitusrakenteeseen.
5. **Sovellus** tarkistaa että allekirjoituksessa käytetyt menetelmän ovat tämän määrityksen mukaisia.

Jos sovellus ei pysty tarkistamaan moniallekirjoitusta, niin riittää, että sovellus tarkistaa KanTa-järjestelmän tekemän järjestelmäallekirjoituksen. Tämä tarkoittaa implisiittisesti sitä, että sovellus ja käyttäjä luottavat KanTa-järjestelmän tarkistaneen moniallekirjoituksen oikein (luku 6.3, kohdat 9-11).

Versiohistoria

Versio	Pvm	Tekijä	Muutos
0.8	11.11.2009	Mikael Himanka	Toinen luonnos
1.0		Kela	Ensimmäinen julkaistu versio.
1.1	31.12.2009	Mikael Himanka	Soveltamisoppaan päivittämisen yhteydessä täydennetty versio (ei muutoksia sallittuihin tai vaadittaviin menetelmiin)
1.1.1	11.1.2010	Mikael Himanka	XML-esimerkit siistitty ja yhtenäistetty (muutoksia ID-attribuutin kirjoitusasuun)