

Kuva-aineistojen arkiston tekninen määrittely

Liite 2: XUA-allekirjoituksen määrittely

Versio 1.02

Kela, Kanta-palvelut
29.9.2023

Muutoshistoria

Versio	Muutos	Tekijä	PVM
1.01	Muokattu Kvarkki –termi -> Kuva-aineistojen arkistoksi ei teknisiä muutoksia	Pekka Rinne	31.10.2017
1.02	Saavutettavuusmuutokset. Ei teknisiä muutoksia.	Kela, Kanta-palvelut	29.9.2023

Sisällys

Muutoshistoria	1
1 Johdanto.....	3
1.1 Dokumentissa käytetyt merkinnät	3
2 Allekirjoitusmenetelmät ja vaatimukset	4
2.1 Sähköisessä allekirjoituksessa sallitut menetelmät	4
2.2 Sähköisiä allekirjoituksia koskevat sitovat vaatimukset	5
2.3 Suositukset koskien merkistöjä ja erikoismerkkejä	5
3 SAML2-vakuutuksen sähköinen allekirjoitus.....	6
3.1 Allekirjoituksen rakenne	6
3.2 XML-allekirjoituksen kohdistuminen	7

1 Johdanto

Tämä määrittäminen kuvaa Kuva-aineistojen arkiston ITI-18, ITI-43 sekä RAD-69 (RAD-69:n kohdalla tarkastusta ei toistaiseksi tehdä) -transaktioihin liitettävän XUA-määrittämissä mukaisen SAML2-vakuutus-osion (assertion) sähköisen allekirjoituksen. XUA (Cross Enterprise User Assertion) on osa IHE IT Infrastructure -kohdealueen teknisiä määrittämiä ja määrittelee transaktion ITI-40.

XML-allekirjoitusstandardin soveltamistapa vastaa pääosin CDA R2 -asiakirjoille tehtävää allekirjoitusta mm. varmenteen osalta, mutta eroavaisuuksia tulee erityisesti allekirjoituksen kohdistamisessa. Allekirjoituksen kohde on vain SAML2-vakuutus eikä allekirjoitettavassa sisällössä välitetä asiakirjoja. Assertion allekirjoitetaan aina järjestelmän toimesta, eikä siinä käytetä CDA R2 -allekirjoituksen laajennoksia moniallekirjoitusta ja allekirjoitusaikaa. Allekirjoitus sijaitsee SAML2-vakuutuksen sisällä ja on tyypiltään 'enveloped' eli varsinainen tekninen allekirjoitus sijaitsee allekirjoituksen kohteen sisällä. Tässä määrittämissä ei ole toistettu kaikkia Sähköisen allekirjoituksen määrittämissä ja soveltamisohjeessa kuvattuja yksityiskohtia ja lukijaa pyydetään tarvittaessa tutustumaan siihen (www.kanta.fi/jarjestelmakehittajat/yhteiset-maarittelyt). Esimerkiksi ko. määrittämissä luku 3 'Taustaa' on poistettu kokonaan tästä määrittämisestä.

SAML2-vakuutuksen allekirjoitusta ei persistoida mihinkään tietovarastoon, vaan se hylätään tarkistuksen jälkeen haun kontekstietojen tarkastuksen yhteydessä. Tämän vuoksi allekirjoituksen tarvitsee olla validi vain osana lähetettävää sanomaa.

1.1 Dokumentissa käytetyt merkinnät

Sähköiseen allekirjoitukseen liittyvät osuudet SAML2-vakuutuksen sisällä ovat XML-allekirjoitukseen viittaavan nimiavaruuden (namespace) alla.

Taulukko 1. Sähköisen allekirjoituksen nimiavaruus

Etuliite (prefix)	Nimiavaruus (namespace)
ds	http://www.w3.org/2000/09/xmldsig#

Tässä määrittämissä käytetään esimerkeissä pelkistettyä XML-rakennetta, jolla pyritään korostamaan allekirjoitukseen vaikuttavia keskeisiä rakenteita.

2 Allekirjoitusmenetelmät ja vaatimukset

2.1 Sähköisessä allekirjoituksessa sallitut menetelmät

Seuraavassa taulukossa 2 on esitetty elementtikohtaisesti mitkä arvot ovat sallittuja parametreja XML-allekirjoitusrakenteessa (**ds:Signature**). Elementit ovat kaikki **ds:SignedInfo**-elementin alielementtejä. Vaihtoehtoisista suositellut parametrit on alleviivattu.

Taulukko 2. Sallitut parametrit XML-allekirjoitusrakenteessa

Elementti	Sallitut menetelmät
ds:CanonicalizationMethod	<u>Exclusive XML Canonicalization version 1.0 (without comments)</u> <u>[http://www.w3.org/2001/10/xml-exc-c14n#]</u> 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	RSASignatureWithSHA256 [http://www.w3.org/2001/04/xmldsig-more#rsa-sha256]
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] <u>Exclusive XML Canonicalization version 1.0 (without comments)</u> <u>[http://www.w3.org/2001/10/xml-exc-c14n#]</u> 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	SHA256 [http://www.w3.org/2001/04/xmldsig-more#sha256]

2.2 Sähköisiä allekirjoituksia koskevat sitovat vaatimukset

Allekirjoituksissa käytettävien varmenteiden tulee olla voimassaolevan lain ja asetusten mukaisia. Allekirjoitusvarmenteena käytetään DVV:n myöntämää järjestelmäallekirjoitusvarmennetta (testi- & tuotantovarmennet ympäristökohtaisesti), jonka Subject-osion serialNumberiksi annetaan organisaation OID-tunniste.

Allekirjoittajan allekirjoitusvarmenne on liitettävä osaksi allekirjoitusta. Käytettävä rakenne on ***ds:Signature/ds:KeyInfo/ds:X509Data/ds:X509Certificate***

SAML-valtuutuksen sisältämän XML-allekirjoituksen on oltava validi XML-allekirjoitusstandardin kokonaisuudessaan toteuttavaa allekirjoitusvalidaattoria vastaan, esimerkiksi Oraclen tai Apachen Santuario-implementaatio.

Allekirjoituksen kohteena (***ds:Reference***-viittaus) olevalle rakenteelle pitää antaa ***ID***-attribuutti ja tälle arvo.

2.3 Suositukset koskien merkistöjä ja erikoismerkkejä

Jotta merkistömuunnoksissa tapahtuvat virheet havaitaan mahdollisimman aikaisessa vaiheessa, on suositeltavaa käyttää testiaineistoa joka sisältää erikoismerkkejä. UTF-8 merkistössä on syytä käyttää sekä kaksi- että useampitavuisia erikoismerkkejä. Esimerkiksi €-merkki on UTF-8:ssa kolmitavuihin.

Vastaavasti myös ääkkösiä sisältävien testivarmennetiden käyttö on suositeltavaa.

3 SAML2-vakuutuksen sähköinen allekirjoitus

3.1 Allekirjoituksen rakenne

ds:Signature-rakenne sisältää yhden **ds:Reference**-elementin, joka kohdistuu SAML2-juureen siihen määritellyn ID-attribuutin perusteella.

SAML2-vakuutukseen kohdistuvan allekirjoituksen rakenne:

```
<wsse:Security>
  <saml2:Assertion ID>
    <ds:Signature>
      <ds:SignedInfo/>
      <ds:SignatureValue/>
      <ds:KeyInfo/>
    </ds:Signature>
  </saml2:Assertion>
</wsse:Security>
```

(**ds:Signature** on XML-allekirjoituksen rakenteen mukainen)

```
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/ws-sx/2004/01/oasis-200401-ws-security-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/ws-sx/2004/01/oasis-200401-ws-security-util-1.0.xsd" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <saml2:Assertion ID="ALLEKIRJOITUKSEN_KOHDE" IssueInstant="2017-03-15T12:28:34" Version="2.0" xsi:type="saml2:AssertionType" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
    <saml2:Issuer>ISSUER</saml2:Issuer>
    <ds:Signature Id="ID" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
        <ds:Reference URI="#ALLEKIRJOITUKSEN_KOHDE">
          <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            <ds:InclusiveNamespaces PrefixList="saml2" xmlns:ds="http://www.w3.org/2001/10/xml-exc-c14n#" />
          </ds:Transforms>
          </ds:Reference>
        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha256" />
        <ds:DigestValue>TIIVISTEEN_ARVO</ds:DigestValue>
      </ds:SignedInfo>
      <ds:SignatureValue>ALLEKIRJOITUKSEN_ARVO</ds:SignatureValue>
      <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate>VARMENNE BASE64-MUODOSSA</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </ds:Signature>
  </saml2:Assertion>
</wsse:Security>
```

Kuva 1. Pelkistetty esimerkki sähköisestä allekirjoituksesta SAML2-vakuutuksen yhteydessä

XML-allekirjoitusstandardi määrittää kolme erilaista allekirjoitustyyppiä sen mukaan miten sähköinen allekirjoitus sijoittuu suhteessa allekirjoituksen kohteena olevaan sisältöön. SAML2-vakuutuksissa käytettävä allekirjoitustyyppi on enveloped.

3.2 XML-allekirjoituksen kohdistuminen

Seuraavassa on esimerkki ID-attribuutilla tehtävästä kohdistamisesta:

- Suora kohdistus **ds:Reference**-elementillä **ID**-attribuuttiin

```
<ds:Reference URI="#ID_KOHDISTUS">...</ds:Reference>
```

Alla kuvassa 2 on havainnollistettu yksittäisen sähköisen allekirjoituksen kohdistuminen ja kuvassa 3 vihreällä värillä korostettuna varsinainen allekirjoitettava sisältö. Enveloped-tyyppinen allekirjoitus ottaa huomioon sen, että itse allekirjoitusrakenne on allekirjoituksen kohteen sisällä ja jättää sen pois allekirjoituslaskennasta.



```
<wss:Security xmlns:wss="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <saml2:Assertion ID="ALLEKIRJOITUKSEN_KOHDE" IssueInstant="2017-03-15T12:28:34" Version="2.0" xsi:type="saml2:AssertionType" xmlns:saml2="urn:oasis:names:tc:saml:2.0:assertion" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <saml2:Issuer>ISSUER</saml2:Issuer>
    <ds:Signature Id="ID" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
          <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
          <ds:Reference URI="#ALLEKIRJOITUKSEN_KOHDE">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                <ds:InclusiveNamespaces PrefixList="saml2" xmlns:ds="http://www.w3.org/2001/10/xml-exc-c14n#">
                </ds:Transform>
              </ds:Transforms>
              <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig#sha256"/>
              <ds:DigestValue>IIIVISTEEN ARVO</ds:DigestValue>
            </ds:Reference>
          </ds:SignedInfo>
          <ds:SignatureValue>ALLEKIRJOITUKSEN ARVO</ds:SignatureValue>
          <ds:KeyInfo>
            <ds:X509Data>
              <ds:X509Certificate>VARMENNE BASE64-MUODOSSA</ds:X509Certificate>
            </ds:X509Data>
          </ds:KeyInfo>
        </ds:Signature>
      </saml2:Signature>
    </saml2:Assertion>
  </wss:Security>
```

Kuva 2. Allekirjoituksen kohdistaminen



```
<wss:Security xmlns:wss="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <saml2:Assertion ID="3CD97577F8C35798F113905644956476" IssueInstant="2017-03-15T12:28:34" Version="2.0" xsi:type="saml2:AssertionType" xmlns:saml2="urn:oasis:names:tc:saml:2.0:assertion" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <saml2:Issuer>ISSUER</saml2:Issuer>
    <ds:Signature Id="MPS_ee78fb8a5d84-9a6539da-95e0-423c-adb1-00d4776ffc1c-df203628524a" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <saml2:Subject>
        <saml2:AttributeStatement>
          <saml2:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:organization-id">[]</saml2:Attribute>
          <saml2:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:organization">[]</saml2:Attribute>
          <saml2:Attribute Name="urn:kanta:kvarkki:organization-unit">[]</saml2:Attribute>
          <saml2:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:subject-id">[]</saml2:Attribute>
          <saml2:Attribute Name="urn:oasis:names:tc:xspa:2.0:subject:npi">[]</saml2:Attribute>
          <saml2:Attribute Name="urn:oasis:names:tc:xacml:2.0:resource:resource-id">[]</saml2:Attribute>
          <saml2:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse">[]</saml2:Attribute>
          <saml2:Attribute Name="urn:kanta:kvarkki:special-reason-expl">[]</saml2:Attribute>
          <saml2:Attribute Name="urn:oasis:names:tc:xacml:2.0:subject:role">[]</saml2:Attribute>
          <saml2:Attribute Name="urn:ihe:iti:xca:2010:homeCommunityId">[]</saml2:Attribute>
          <saml2:Attribute Name="urn:kanta:kvarkki:custodian-id">[]</saml2:Attribute>
          <saml2:Attribute Name="urn:kanta:kvarkki:registry-code">[]</saml2:Attribute>
          <saml2:Attribute Name="urn:kanta:kvarkki:registry-specifier">[]</saml2:Attribute>
          <saml2:Attribute Name="urn:kanta:kvarkki:encounter-id">[]</saml2:Attribute>
        </saml2:AttributeStatement>
      </saml2:Subject>
    </saml2:Assertion>
  </wss:Security>
```

Kuva 3. Allekirjoitettava sisältö