Virtu-skeema

Virtu-luottamusverkoston yhteiset attribuutit ja attribuuttien muodostamisen ohjeistus

Versio	Päiväys	Editori	Muutokset
1.0	11.12.2009	Mikael Linden	Hyväksytty Virtu-käyttöönottohankkeen ohjausryhmässä
1.1	10.3.2011	Mikael Linden	Hetu ja Satu siirtyneet julkishallinnon yhteiseen skeemaan, johon tässä enää vain viitataan. VirtuHomeOrganization-arvotarkistus siirretty SAML-protokollaprofiilista tähän dokumenttiin ja oikaistu attribuutin virheellinen OID. Vähäisiä selvennyksiä (GUID-arvo virtuLocalID:ssä, muiden yksilöivien tunnisteiden käyttäminen).

Sisältö

1. Johdanto

Tässä dokumentissa

- kuvataan Virtu-luottamusverkostossa käytettävien yhteisten attribuuttien rakenne (syntaksi) ja merkitys (semantiikka).
- esitetään, kuinka osapuolet voivat muodostaa omia attribuuttejaan Virtu-luottamusverkoston kanssa yhteensopivalla tavalla.

Virtu-luottamusverkoston attribuutit –lukuun on sisällytetty joukko erilaisia attribuutteja. Lähtökohta on ollut määritellä varmuuden vuoksi erilaisia attribuutteja, joille on kuviteltavissa jossain vaiheessa käyttöä Virtu-luottamusverkostossa. Tarkoitus ei ole, että jokaisen Virtu-kotiorganisaation tulisi populoida jokainen attribuutti saati luovuttaa se jokaiseen Virtu-palveluun. Vain pakolliset attribuutit tulee olla populoitu Virtu-kotiorganisaation jokaiselle käyttäjälle. Palvelukohtaisesti määritellään, mitä attribuutteja palvelu tarvitsee kustakin loppukäyttäjästä.

Osapuolten omien attribuuttien muodostaminen tämän ohjeistuksen mukaan mahdollistaa sen, että attribuutti voidaan myöhemmin siirtää osaksi tätä dokumenttia.

2. Suhde muihin attribuuttimäärityksiin

Tässä luvussa kuvataan tämän määrityksen suhde muihin attribuuttimäärityksiin.

2.1. Julkishallinnon yhteinen SAML 2.0 –attribuuttiprofiili

Virtu-luottamusverkostossa käytetään julkishallinnon yhteisessä SAML 2.0 –attribuuttiprofiilissa (”SAML 2.0 Attribute Profile for the Finnish public sector, ver 1.1”, 21.2.2011) määriteltyjä attribuutteja.

Attribuutit on koottu liitteeseen A, jossa niitä täydennetään Virtun kannalta tarpeellisilla tiedoilla (attribuuttien pakollisuus).

~~2.~~ 2.2. JHS 133 –suosituksen henkilöä koskevat attribuutit

Virtu-luottamusverkostossa käytetään JHS 133 –suosituksen (”JHS 133 Hakemistotiedot ja niiden ylläpito”, 2.11.2006) luvussa 4.5. (”Henkilön tiedot”) määriteltyjä attribuutteja.

Attribuutit on koottu liitteeseen A, jossa niitä täydennetään Virtun kannalta tarpeellisilla tiedoilla (attribuuttien OID-tunniste ja pakollisuus).

3. Virtu-luottamusverkoston attribuutit

Tässä luvussa esitetään Virtu-luottamusverkostossa käytettävät attribuutit, joilla täydennetään edellisessä luvussa mainittuja määrityksiä. Attribuutit on koottu liitteeseen A~~jotka täydentävät JHS 133 -suositusta~~.

3.1. virtuHomeOrganization

Loppukäyttäjän kotiorganisaation yksilöivä tunniste, joka perustuu organisaation DNS-nimeen.

OID	LDAP-syntaksi	Moniarvoisuus	Pakollisuus
1.3.6.1.4.1.31350.1.5	DirectoryString	Ei	kyllä
SAML 2.0 –assertioesimerkki <Attribute			

```
   NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:uri”
   Name="urn:oid:1.3.6.1.4.1.31350.1.5"
   FriendlyName="virtuHomeOrganization">
   <AttributeValue>virastoy.fi</AttributeValue>
<Attribute>
```

Käyttötarkoitukset:

- loppukäyttäjän yksilöivän tunnuksen muodostaminen (katso luku 5.1)
- käyttövaltuuksien hallinnointi (esim. käyttövaltuuden antaminen kaikille tietyn organisaation loppukäyttäjille)

Organisaation on syytä valita attribuutille arvo, jonka vaihtuminen on mahdollisimman epätodennäköistä (vaikka ei täysin poissuljettua). Attribuutin arvo voi vaihdella saman organisaation eri yksikköön kuuluvien loppukäyttäjien välillä, ja attribuutti voi sisältää hierarkiaa (esim. yksikko1.virastoy.fi), mutta näitä ei suositella, koska tällöin mahdolliset organisaatiouudistukset aiheuttavat työläitä muutoksia loppukäyttäjän yksilöivään tunnisteeseen.

Jos loppukäyttäjä on itse asiassa organisaation alihankkijan palveluksessa, mutta hänellä on organisaatiossa henkilökuntaan rinnastuva käyttäjätunnus ja käyttövaltuuksia, on tarkoituksenmukaista että hän saa saman virtuHomeOrganization-arvon kuin organisaation muut loppukäyttäjät. Tarvittaessa palvelussuhteen tyyppi osoitetaan virtuEmployeeType-attribuutilla. Esimerkki: virasto ostaa vahtimestaripalvelut alihankkijalta, jonka työntekijä toimii viraston tiloissa. Työntekijällä on todennäköisesti tarve henkilökuntaan rinnastuviin käyttöoikeuksiin, joten viraston virtuHomeOrganization-attribuutin arvon käyttäminen on tarkoituksenmukaista.

VirtuHomeOrganization-attribuutin arvoon tehtävät tarkistukset Virtu-luottamusverkostossa on esitetty luvussa 4.1.

3.2. virtuLocalID

virtuLocalID-attribuutti yksilöi loppukäyttäjän virtuHomeOrganization-attribuutin virittämässä nimiavaruudessa.

OID	LDAP-syntaksi	Moniarvoisuus	Pakollisuus
1.3.6.1.4.1.31350.1.8	DirectoryString	Ei	Kyllä

SAML 2.0 –assertioesimerkki

```
<Attribute
   NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:uri”
   Name="urn:oid:1.3.6.1.4.1.31350.1.8"
   FriendlyName="virtuLocalID">
   <AttributeValue>tammi03</AttributeValue>
</Attribute>
```

Käyttötarkoitukset:

virtuLocalID-attribuuttia käytetään loppukäyttäjän yksilöivän tunnisteen rakentamisessa. virtuLocalID-attribuutti on yhdessä virtuHomeOrganization-attribuutin kanssa globaalisti uniikki yli ajan, kuten luvussa 5.1 esitetään.

Sääntö uudelleenkäytöstä:

virtuLocalID-attribuutin arvo tulee valita niin, että vapautunutta virtuLocalID-attribuutin arvoa ei uudelleenkäytetä. Jos virtuLocalID-attribuutin arvon haltija poistuu organisaation palveluksesta, tulee

attribuutin arvo jäädyttää. Jäädytetty arvo voidaan ottaa uudelleen käyttöön vain, jos sama henkilö palaa jälleen organisaation palvelukseen.

Suositus vaihtumisesta:

Koska virtuLocalID-attribuuttia käytetään loppukäyttäjän yksilöivän tunnisteen rakentamisessa, tulee attribuutti pyrkiä valitsemaan niin, että sen arvon vaihtuminen on harvinaista (vaikka ei täysin poissuljettua). Jos käyttäjän virtuLocalID-attribuutin arvo vaihtuu, hukkuvatu käyttäjän tunnisteisiin palveluissa kiinnitetyt käyttäjäprofiilit ja käyttöoikeudet.

Suositus helppolukuisuudesta:

Voi tulla tilanteita, joissa ylläpitäjä tai loppukäyttäjä itse joutuu käsittelemään virtuLocalID-attribuutin arvoa, joten sen helppolukuisuus vähentää inhimillisen virheen mahdollisuuksia.

Esimerkkejä (käyttäjä Tauno Tammi):

Esimerkki	Huomioita
tammi	virtuLocalID on loppukäyttäjän käyttäjätunnus. Edellyttää, että vapautuneita käyttäjätunnuksia ei koskaan uudelleenkäytetä.
tammi2001	virtuLocalID on loppukäyttäjän käyttäjätunnus katenoituna vuoteen, jolloin se on annettu tälle käyttäjälle. Edellyttää, että käyttäjätunnus on jäädytettynä ainakin vuoden ennen uusiokäyttöä. Loukkaa hieman virkamiehen yksityisyyttä, koska saattaa paljastaa hänen virkaikänsä.
tammi3	virtuLocalID on loppukäyttäjän käyttäjätunnus katenoituna saman tunnuksen haltijan juoksevaan numeroon. Tässä tapauksessa Tauno Tammi on kolmas henkilö, jonka käyttäjätunnus organisaatiossa on ollut ”tammi”.
tauno.tammi	virtuLocalID on loppukäyttäjän sähköpostiosoitteen alkuosa. Jos käyttäjän nimi muuttuu tai organisaatioon tulee täyskaima, syntyy paine muuttaa myös virtuLocalID-arvoa. Sääntö uudelleenkäytöstä edellyttää, että sähköpostiosoite ei ole aikaisemmin kuulunut eri henkilölle.
92003011	virtuLocalID-arvo on sama kuin employeeNumber-attribuutin arvo, jota ei uudelleenkäytetä. Organisaation tulee kuitenkin tutkia ja ratkaista tapaukset, joissa loppukäyttäjällä ei ole employeeNumber-arvoa.
3F2504E0-4F89-11D3-9A0C-0305E82C3301	Organisaatio on valinnut virtuLocalID:ksi Windows-toimialueessa käyttäjälle annettavan GUID-arvon, jota ei vaihdeta tai uudelleenkäytetä. Haittapuolena on vaikealukuisuus. GUID-arvo saattaa myös muuttua, jos Windows-toimialuetta joudutaan muuttamaan organisaatiouudistuksen tai IT-toimintojen uudelleenjärjestelyn vuoksi.

3.3. virtuHomeOrganizationType

Loppukäyttäjän kotiorganisaation tyyppi.

OID	LDAP-syntaksi	Moniarvoisuus	Pakollisuus
1.3.6.1.4.1.31350.1.7	DirectoryString	Kyllä	Kyllä

SAML 2.0 –assertioesimerkki (valtion virasto)

```
<Attribute
   NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:uri”
   Name="urn:oid:1.3.6.1.4.1.31350.1.7"
   FriendlyName="virtuHomeOrganizationType">
   <AttributeValue>valtionhallinto</AttributeValue>
</Attribute>
```

```
<Attribute
  NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:uri”
  Name="urn:oid:1.3.6.1.4.1.31350.1.7"
  FriendlyName="virtuHomeOrganizationType">
  <AttributeValue>virasto</AttributeValue>
</Attribute>
```

SAML 2.0 –assertioesimerkki (kunta)

```
<Attribute
  NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:uri”
  Name="urn:oid:1.3.6.1.4.1.31350.1.7"
  FriendlyName="virtuHomeOrganizationType">
  <AttributeValue>kunnallishallinto</AttributeValue>
</Attribute>
<Attribute
  NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:uri”
  Name="urn:oid:1.3.6.1.4.1.31350.1.7"
  FriendlyName="virtuHomeOrganizationType">
  <AttributeValue>kunta</AttributeValue>
</Attribute>
```

Käyttötarkoitus:

- käyttövaltuuksien hallinta

Sanastot:

Sektoria kuvaava sanasto:

valtionhallinto	organisaatio kuuluu valtion talousarviotalouteen
kunnallishallinto	organisaatio kuuluu kunnallishallintoon
valillinen-hallinto	organisaatio kuuluu välilliseen valtionhallintoon
muu	muu

Yhteisömuotoa kuvaava sanasto:

ministerio	organisaatio on ministeriö
virasto	organisaatio on valtion virasto
liikelaitos	organisaatio on valtion tai kunnan liikelaitos
kunta	organisaatio on kunta
kuntayhtyma	organisaatio on kuntayhtymä
osakeyhtio	organisaatio on osakeyhtiö
muu-organisaatio	muut organisaatiot

On varauduttava siihen, että palautettavia arvoja on monta.

Vain 7-bittisen ASCII merkistön arvot ovat sallittuja. Arvot eivät sisällä skandinaavisia merkkejä, vaan ne konvertoidaan: Ä->A, å ->a, ä->a, ö->o. Arvojen kirjasinkoolla ei ole merkitystä.

3.4. virtuEmployeeType

Loppukäyttäjän suhde kotiorganisaatioonsa.

OID	LDAP-syntaksi	Moniarvoisuus	Pakollisuus
1.3.6.1.4.1.31350.1.6	DirectoryString	Ei	Ei

SAML 2.0 –assertioesimerkki

```
<Attribute
  NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:uri”
  Name="urn:oid:1.3.6.1.4.1.31350.1.6"
  FriendlyName="virtuEmployeeType">
```

```
   <AttributeValue>virkamies</AttributeValue>
</Attribute>
```

Kotiorganisaatiolla tarkoitetaan virtuHomeOrganization-attribuutilla osoitettua organisaatiota.

Käyttötarkoitus:

- käyttövaltuuksien hallinta

Sanasto:

virkamies	Loppukäyttäjä on virkasuhteessa kotiorganisaatioonsa
tyontekija	Loppukäyttäjä on työsuhteessa kotiorganisaatioonsa
siviilipalvelus	Loppukäyttäjä suorittaa siviilipalvelustaan kotiorganisaatiossa
alihankkija	Loppukäyttäjä on kotiorganisaation alihankkijan palveluksessa
muu	Ei mikään näistä

Vain 7-bittisen ASCII merkistön arvot ovat sallittuja. Arvot eivät sisällä skandinaavisia merkkejä, vaan ne konvertoidaan: Ä->A, å ->a, ä->a, ö->o. Arvojen kirjasinkoolla ei ole merkitystä.

3.5. virtuPersonEntitlement

URI, joka yksilöi resurssin, johon loppukäyttäjällä on käyttöoikeus. Voi sisältää myös käyttäjää koskevaa rooli- ja muuta informaatiota resurssissa.

OID	LDAP-syntaksi	Moniarvoisuus	Pakollisuus
1.3.6.1.4.1.31350.1.4	DirectoryString	Kyllä	Ei

SAML 2.0 –assertioesimerkki

```
<Attribute
   NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:uri”
   Name="urn:oid:1.3.6.1.4.1.31350.1.4"
   FriendlyName="virtuPersonEntitlement">
   <AttributeValue>http://valtiokonttori.fi/rondo/TTY/1234/hyvaksyja</AttributeValue>
</Attribute>
<Attribute
   NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:uri”
   Name="urn:oid:1.3.6.1.4.1.31350.1.4"
   FriendlyName="virtuPersonEntitlement">
   <AttributeValue>
   http://secure.personec.com/travel/vk?kustannuspaikka=3244&rooli=matkasihteeri
   </AttributeValue>
</Attribute>
```

URI-tunniste voi olla keinotekoinen (ei resolvoi todelliseen www-sivuun), mutta sen tulee olla yksilöllinen eikä se saa olla päällekkäinen toisen organisaation kanssa tai viitata toisen organisaation hallinnoimaan verkkopalveluun.

Käyttötarkoitukset:

- attribuutin avulla kotiorganisaatio voi osoittaa loppukäyttäjälle käyttövaltuuden tiettyyn palveluun

Julkaisu:

Virtu-skeemakuvauksen yhteydessä Virtu-luottamusverkoston kotisivuilla, josta löytyy tieto tai linkki eri palveluntarjoajien käyttämiin arvoihin.

3.6. businessCode

Loppukäyttäjän edustaman organisaation Y-tunnus.

OID	LDAP-syntaksi	Moniarvoisuus	Pakollisuus
1.2.246.10	DirectoryString	Ei	Ei
SAML 2.0 –assertioesimerkki <Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" Name="urn:oid:1.2.246.10" FriendlyName="businessCode"> <AttributeValue>204819-8</AttributeValue> </Attribute>			

~~3.7. electronicIdentificationNumber~~

~~Väestörekisterikeskuksen loppukäyttäjälle antama sähköinen asiointitunnus (satu).~~

~~OID~~	~~LDAP-syntaksi~~	~~Moniarvoisuus~~	~~Pakollisuus~~
~~1.2.246.22~~	~~DirectoryString~~	~~Ei~~	~~Ei~~
~~SAML 2.0 –assertioesimerkki~~ ~~<Attribute~~ ~~NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"~~ ~~Name="urn:oid:1.2.246.22"~~ ~~FriendlyName="electronicIdentificationNumber">~~ ~~<AttributeValue>012345678N</AttributeValue>~~ ~~</Attribute>~~			

~~Käyttötarkoitus:~~

- ~~loppukäyttäjän yksilöiminen~~

~~3.8. nationalIdentificationNumber~~

~~Väestörekisterikeskuksen loppukäyttäjälle antama henkilötunnus.~~

~~OID~~	~~LDAP-syntaksi~~	~~Moniarvoisuus~~	~~Pakollisuus~~
~~1.2.246.21~~	~~DirectoryString~~	~~Ei~~	~~Ei~~
~~SAML 2.0 –assertioesimerkki~~ ~~<Attribute~~ ~~NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"~~ ~~Name="urn:oid:1.2.246.21"~~ ~~FriendlyName="nationalIdentificationNumber">~~ ~~<AttributeValue>010191-123A</AttributeValue>~~ ~~</Attribute>~~			

~~Käyttötarkoitus:~~

- ~~loppukäyttäjän yksilöiminen~~

~~3.9.~~3.7. employeeNumber

Organisaation loppukäyttäjälle antama henkilönumero.

OID	LDAP-syntaksi	Moniarvoisuus	Pakollisuus
2.16.840.1.113730.3.1.3	DirectoryString	Ei	Ei
SAML 2.0 –assertioesimerkki			

```
<Attribute
   NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:uri”
   Name="urn:oid:2.16.840.1.113730.3.1.3"
   FriendlyName="employeeNumber">
   <AttributeValue>92003011</AttributeValue>
</Attribute>
```

Suositellaan käytettäväksi henkilöstöhallinnon numeroa. Voi sisältää myös muita merkkejä kuin numeroita.

employeeNumber-attribuutin tulee liittyä yksikäsitteisesti henkilöön, jolle se on annettu, eikä sitä saa uudelleenkäyttää eri henkilön henkilönumerona.

Attribuutti on yksiarvoinen. Tämä ei kuitenkaan estä sitä, että saman henkilön employeeNumber-attribuutin arvo voi vaihtua.

Käyttötarkoitus:

- loppukäyttäjän yksilöiminen

~~3.10.~~3.8. preferredLanguage

Loppukäyttäjän haluama asiointikieli.

OID	LDAP-syntaksi	Moniarvoisuus	Pakollisuus
2.16.840.1.113730.3.1.39	DirectoryString	Ei	Ei

SAML 2.0 –assertioesimerkki

```
<Attribute
   NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:uri”
   Name="urn:oid:2.16.840.1.113730.3.1.39"
   FriendlyName="preferredLanguage">
   <AttributeValue>fi</AttributeValue>
</Attribute>
```

Käyttötarkoitus:

- personointi; attribuutin perusteella palvelu voi avautua automaattisesti loppukäyttäjän toivomalla kielellä.

4. Attribuuteille tehtävät tarkistukset

4.1. VirtuHomeOrganization

virtuHomeOrganization-attribuutille tehtävän tarkistuksen tavoite on varmistaa, että murrettu tai huonosti käyttäytyvä Identity Provider –palvelin ei vaaranna loppukäyttäjien identiteettejä muissa Identity Provider –palvelimissa. SAML Identity Provider –palvelimelle sallitut virtuHomeOrganization-arvot osoitetaan Virtu-luottamusverkoston metadatassa seuraavasti:

- Jokainen Virtu-metadatan IDPSSODescriptor –elementti sisältää täsmälleen yhden Attribute-elementin, jonka arvona on virtuHomeOrganization:
  <Attribute name=”urn:oid:1.3.6.1.4.1.31350.1.5”>
- Attribute-elementti sisältää täsmälleen yhden AttributeValue-elementin jokaiselle virtuHomeOrganization-attribuutin arvolle, jota kyseinen Identity Provider saa käyttää SAML-assertiossa.

Yhdellä organisaatiolla voi olla nolla, yksi tai useita Identity Provider –palvelimia. Sama virtuHomeOrganization-arvo voi siis esiintyä usean eri Identity Providerin Virtu-metadatassa.

Esimerkki:

Oletetaan, että Hallinnon tietotekniikkakeskus Haltik operoi Identity Provider –palvelinta kolmelle organisaatiolle: Haltik (virtuHomeOrganization: haltik.fi), sisäasiainministeriö (intermin.fi) ja vähemmistövaltuutettu (omf.fi). Haltikin Identity Provider –palvelimen SAML 2.0 –metadataelementti näyttää seuraavalta:

```
<EntityDescriptor entityID="https://idp.haltik.fi/">
    <IDPSSODescriptor ...>
        <Attribute Name="urn:oid: 1.3.6.1.4.1.31350.1.5">
            <AttributeValue>haltik.fi</AttributeValue>
            <AttributeValue>intermin.fi</AttributeValue>
            <AttributeValue>omf.fi</AttributeValue>
        </Attribute>
    </IDPSSODescriptor>
</EntityDescriptor>
```

Jos Identity Providerin lähettämä SAML-assertio sisältää virtuHomeOrganization-attribuutin, Service Providerin tulisi tarkistaa, että attribuutin arvo täsmää johonkin kyseisen Identity Providerin SAML-metadatan sille sallimaan arvoon. Jos metadata osoittaa, että kyseinen Identity Provider ei voi käyttää kyseistä virtuHomeOrganization-arvoa, Service Providerin tulee hylätä assertio.

Esimerkki (jatkoa):

Kun Service Provider vastaanottaa SAML-assertion Identity Providerilta, jonka entityID on https://idp.haltik.fi/, Service Providerin tulisi tarkistaa, että assertion mahdollisesti sisältämä virtuHomeOrganization-attribuutti sisältää jonkun seuraavista arvoista: haltik.fi, intermin.fi tai omf.fi.

4.5. Loppukäyttäjän yksilöivät tunnisteet

Tämä luku esittelee Virtu-luottamusverkostossa käytettäviä loppukäyttäjän yksilöintiin tarkoitettuja tunnisteita, niiden käyttöä ja ominaisuuksia.

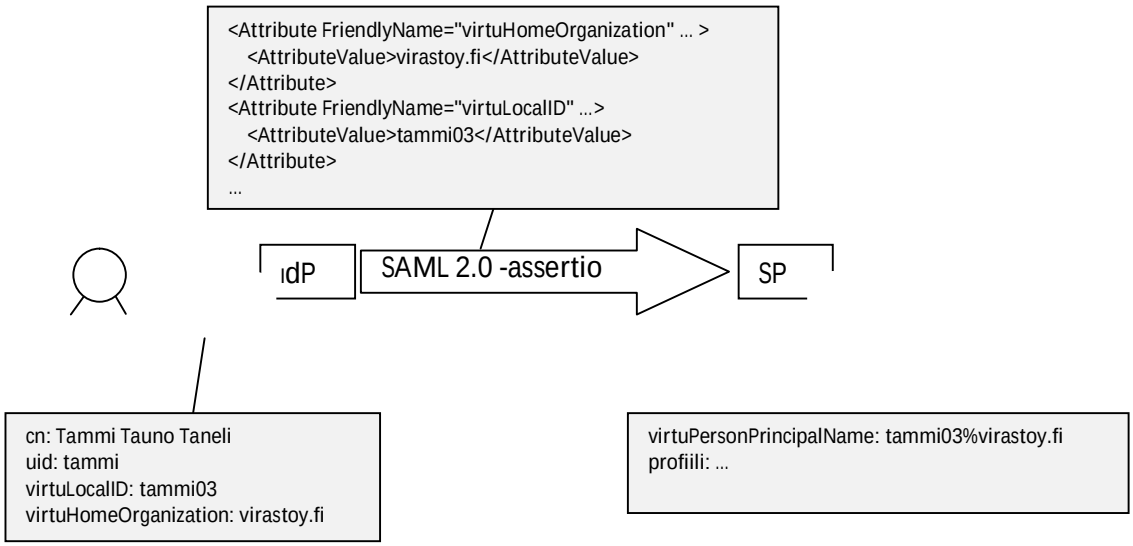
4.1.5.1. virtuPersonPrincipalName

virtuPersonPrincipalName-tunniste koostuu kahdesta attribuutista: virtuHomeOrganization (luku 3.1) ja virtuLocalID (luku 3.2). Toisin kuin luvuissa 2-3 esitetyt attribuutit, virtuPersonPrincipalName-tunnistetta ei kuljeteta SAML 2.0 –assertiossa omana itsenäisenä attribuuttina. Virtu-luottamusverkoston Identity Provider –palvelin luovuttaa molemmat attribuutit (virtuHomeOrganization ja virtuLocalID), ja Service Provider –palvelin yhdistää ne käyttäjän yksilöiväksi tunnisteeksi sovellusta varten.

virtuPersonPrincipalName-tunnisteen jakaminen kahteen osaan johtuu Virtu-luottamusverkoston tietoturvamallista. ~~Virtu SAML 2.0 Profile –dokumentissa on esitetty, kuinka v~~Vain tietty SAML Identity Provider –palvelin voi antaa tietyn virtuHomeOrganization –arvon, ja ~~kuinka~~ kunkin SAML Service Provider –palvelimen tulisi~~ee~~ suorittaa arvoa koskeva tarkistus, joka on esitetty luvussa 4.1.~~. Näin~~

~~varmistetaan, että murrettu tai huonosti käyttäytyvä Identity Provider –palvelin ei vaaranna loppukäyttäjien identiteettejä muissa Identity Provider –palvelimissa.~~

~~Esimerkki:~~



Esimerkissä Tauno Tammi –niminen käyttäjä virastosta Y kirjautuu palveluun. Viraston Y sisällä Taunon käyttäjätunnus on ”tammi”, mutta koska viraston toimintakäytännöt sallivat vapautuneiden käyttäjätunnusten uudelleenkäytön, on virasto populoinut virtuLocalID-attribuutin katenoimalla Taunolle sen loppuun arvon ”03”, joka viraston Y toimintakäytäntöjen puitteissa riittää takaamaan tunnisteen ikuisen yksikäsitteisyyden.

Service Provider –palvelimen saama SAML 2.0 –assertio sisältää sekä virtuHomeOrganization-arvon ”virastoy.fi” että virtuLocalID-arvon ”tammi03”. Service Provider –palvelin suorittaa virtuHomeOrganization-attribuutille ~~”Virtu SAML 2.0 Profile” –dokumentin~~ luvun 4.1 mukaiset tarkistukset, jonka jälkeen Service Provider yhdistää attribuutit yhdeksi, %-merkillä erotetuksi virtuPersonPrincipalName-attribuutiksi, johon sovellus kiinnittää loppukäyttäjän profiilin.

~~4.2.~~5.2. SAML 2.0 Persistent Identifier

~~Virtu SAML 2.0 Profile mahdollistaa myös~~ SAML 2.0 ~~–määritys mahdollistaa myös –määrityksen mukaisen~~ Persistent Identifier –tunnisteen käyttämisen loppukäyttäjän yksilöivänä tunnisteena. SAML 2.0 Persistent Identifier –tunnisteen nameQualifier-attribuutti sisältää aina sen antaneen Identity Provider –palvelimen tunnisteen (entityID), jonka vastaavuuden SAML 2.0 –yhteensopiva Service Provider tarkistaa automaattisesti. Esimerkiksi:

<NameID nameQualifier="idp.virastoy.fi">_df1ef64b-87db-44a6-a437-b6f4967121b2</NameID>

SAML 2.0 Persistent Identifieriä voidaan käyttää loppukäyttäjän yksilöivänä tunnisteena myös Virtu-luottamusverkostossa, mutta tällöin palvelun toteuttajan tulee huomioida, että kotiorganisaatioiden Identity Provider –järjestelyt saattavat muuttua esimerkiksi organisaation tietohallinnon tai IT-ulkoistusten uudelleen järjestelyjen tuloksena. Tällöin loppukäyttäjien Persistent Identifier –tunnisteet todennäköisesti muuttuvat, minkä seurauksena myös tunnisteisiin kiinnitetyt loppukäyttäjien profiilit palveluissa hukkuvat.

5.3. Muut yksilöivät tunnisteet

Service Provider voi harkintansa mukaan käyttää myös muita tunnisteita loppukäyttäjän yksilöintiin, kunhan huomioi niihin liittyvät rajoitteet ja riskit, kuten

- employeeNumber-attribuuttia ei välttämättä ole henkilöllä, joka ei ole palvelussuhteessa
- nationalIdentificationNumber (hetu) ja electronicIdentificationNumber (satu) –attribuuttia ei ole henkilöllä, jota ei ole kirjattu väestötietojärjestelmään
- mail-attribuutti saattaa vaihtua, ja vapautunut arvo voidaan myöhemmin antaa eri henkilölle
- edellä mainitut attribuutit eivät ole pakollisia, joten kaikki Identity Providerit eivät ole välttämättä populoineet niitä loppukäyttäjilleen

~~5.~~6. Omat attribuutit

Organisaatiot voivat muodostaa myös omia attribuutteja ja julkaista niiden määritykset WWW:ssä muita organisaatioita varten.

~~5.1.~~6.1. Oman attribuutin muodostaminen

Oman attribuutin muodostaminen tapahtuu seuraavasti:

1. Selvitä attribuutin OID-tunniste tai määritä se itse. OID-tunniste voidaan luoda esimerkiksi JHS 159[1]-suositusta noudattaen.
2. Kuvaa attribuutin arvot, niiden merkitykset ja käyttötilanteet suhteessa loppukäyttäjään.
3. Muodosta esimerkki SAML 2.0 Attribute Assertionista malliksi todenmukaisessa käyttötilanteessa
4. Julkaise kuvaus ja esimerkki Virtu-luottamusverkoston WWW-sivuilla

~~5.2.~~6.2. Esimerkki: uusi attribuutti, jolla on sanasto

On tunnistettu tarve ilmaista loppukäyttäjän toimenkuva suhteessa organisaationsa Virtu-jäsenyyteen. Toimenkuvia on kolme: hallinnollinen yhteyshenkilö, tekninen yhteyshenkilö ja laskutusyhteyshenkilö.

1. OID:n muodostaminen

   Virtu-koordinaattori on rekisteröinyt oman OID-juuren 1.3.6.1.4.1.31350, josta se on varannut attribuutin nimelle 1.10. OID-juuria saa esimerkiksi Suomen Standardisoimisliitto SFS ry:n[2] tai IANA:n[3] kautta.

2. Semantiikan määrittely Virtussa

   Attribuutilla kuvataan henkilön toimenkuva organisaatiossa suhteessa Virtu-luottamusverkostoon. Sanasto:

Arvo	Selitys
hallinnollinen yhteyshenkilö	Edustaa organisaatiotaan Virtu-luottamusverkostoa koskevissa sopimuksellisissa ja hallinnollisissa asioissa
tekninen yhteyshenkilö	Edustaa organisaatiotaan Virtu-luottamusverkoston teknisissä asioissa, kuten palvelimen ylläpidossa ja sen tietoturva-asioissa
laskutusyhteyshenkilö	Organisaationsa yhteyshenkilö laskutukseen liittyvissä asioissa

3. SAML Attribute Assertion -esimerkki

[1] JHS 159 ISO OID-yksilöintitunnuksen soveltaminen julkishallinnossa, http://www.jhs-suositukset.fi/web/guest/jhs/recommendations/abstracts#JHS159

[2] SFS, Kortinantajan-, AID-, RID- ,OID- ja NSAP-tunnukset, http://www.sfs.fi/palvelut/tunnukset/

[3] IANA, Private Enterprise Number (PEN) Request Template, http://pen.iana.org/pen/PenApplication.page

```
<Attribute
  NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:uri”
  Name="urn:oid:1.3.6.1.4.1.31350.1.10"
  FriendlyName="virtuOrgContactType">
  <AttributeValue>hallinnollinen yhteishenkilö</AttributeValue>
</Attribute>
```

4. Julkaisu

   Virtu-operaattorin palvelun tuottaja ylläpitää sivustollaan määrittelyä, johon on linkki Virtu-luottamusverkoston skeemakuvauksen yhteydessä Virtu-luottamusverkoston kotisivuilla.

6. Soveltamisohje

Jos myöhemmässä vaiheessa tarvitaan uusi attribuutti, tai ilmenee päällekkäisiä vastaavaan tarkoitukseen tarkoitettuja attribuutteja, noudatetaan priorisoinnissa seuraavaa järjestystä:

1. Virtu-skeeman määritystä
2. X.500 person skeeman luokista (esim. inetOrgPerson) johdettua attribuuttia
3. Vastaavaa Virtu-luottamusverkostossa julkaistua skeeman ulkopuolista attribuuttia
4. Omaa attribuuttia ja sen koodistoa

LIITE A: Virtu-luottamusverkostossa käytettävät attribuutit

Taulukkoon on koottu tämän määrityksen sekä JHS 133-suosituksen attribuutit, niiden nimet sekä pakollisuus Virtu-luottamusverkostossa.

Henkilön tieto	Attribuutti	Attribuutin nimi	Pakollisuus
SAML 2.0 Attribute Profile for the Finnish public sector ~~Julkishallinnon yhteinen SAML 2.0 -attribuuttiprofiili~~, ver 1.1 (21.2.2011)			
Henkilön nimi	cn	urn:oid:2.5.4.3	Kyllä
Sähköinen asiointitunnus	electronicIdentificationNumber	urn:oid:1.2.246.22	Ei
Henkilötunnus	nationalIdentificationNumber	urn:oid:1.2.246.21	Ei
Autentikointipalvelun tarjoaja	authenticationProvider	urn:oid:1.3.6.1.4.1.31350.1.11	Ei
JUHTA JHS 133 (2.11.2006) ~~-~~ attribuutit ~~-~~ ~~-~~ ~~-~~			
~~Henkilön nimi~~	~~cn~~	~~urn:oid:2.5.4.3~~	~~Kyllä~~
Sukunimi	sn	urn:oid:2.5.4.4	Kyllä
Etunimi / etunimet	givenName	urn:oid:2.5.4.42	Kyllä
Sähköpostiosoite	mail	urn:oid:0.9.2342.19200300.100.1.3	Ei
Puhelinnumero	telephoneNumber	urn:oid:2.5.4.20	Ei
Organisaation nimi	o	urn:oid:2.5.4.10	Ei
Organisaation yksikön nimi	ou	urn:oid:2.5.4.11	Ei
Nimen alkukirjaimet	initials	urn:oid:2.5.4.43	Ei
Näyttönimi	displayName	urn:oid:2.16.840.1.113730.3.1.241	Ei
Tehtävänimike	title	urn:oid:2.5.4.12	Ei
Matkapuhelimen numero	mobile	urn:oid:0.9.2342.19200300.100.1.41	Ei
Faksinumero	facsimileTelephoneNumber	urn:oid:2.5.4.23	Ei
Organisaation verkkosivuston URI-osoite	labeledURI		Ei
Katuosoite	street	urn:oid:2.5.4.9	Ei
Postilokero	postOfficeBox	urn:oid:2.5.4.18	Ei
Postinumero	postalCode	urn:oid:2.5.4.17	Ei
Postiosoite	postalAddress	urn:oid:2.5.4.16	Ei

Paikkakunta	l	urn:oid:2.5.4.7	Ei
Kuvaus	description	urn:oid:2.5.4.13	Ei
Toimiala	businessCategory	urn:oid:2.5.4.15	Ei
Organisaatiovarmenne (henk.koht.)	userCertificate	urn:oid:2.5.4.36	Ei

Virtu-luottamusverkoston omat attribuutit			
Kotiorganisaatio	virtuHomeOrganization	urn:oid:1.3.6.1.4.1.31350.1.5	Kyllä
Yksilöivä tunniste kotiorganisaatiossa	virtuLocalID	urn:oid:1.3.6.1.4.1.31350.1.8	Kyllä
Kotiorganisaation tyyppi	virtuHomeOrganizationType	urn:oid:1.3.6.1.4.1.31350.1.7	Kyllä
Palvelussuhteen tyyppi	virtuEmployeeType	urn:oid:1.3.6.1.4.1.31350.1.6	Ei
Henkilön valtuutukset	virtuPersonEntitlement	urn:oid:1.3.6.1.4.1.31350.1.4	Ei
Y-tunnus	businessCode	urn:oid:1.2.246.10	Ei
~~Sähköinen asiointitunnus~~	~~electronicIdentificationNumber~~	~~urn:oid:1.2.246.22~~	~~Ei~~
~~Henkilötunnus~~	~~nationalIdentificationNumber~~	~~urn:oid:1.2.246.21~~	~~Ei~~
Henkilö~~kunta~~numero	employeeNumber	urn:oid:2.16.840.1.113730.3.1.3	Ei
Toivottu asiointikieli	preferredLanguage	urn:oid:2.16.840.1.113730.3.1.39	Ei