Federoitu identiteetti käyttäjähallinnon työjuhdaksi

Mikael Linden
Tieteen tietotekniikan keskus CSC

Haka-infrastruktuuri, Suomen korkeakoulujen ja tutkimuslaitosten yhteinen, ns. federoidua identiteettiä hyödyntävä käyttäjätunnistusjärjestelmä, on ollut käytössä elokuusta 2005 lähtien. Puolessa vuodessa siihen on liittynyt tusinan verran korkeakouluja, suurimmat yliopistot mukaan lukien. Infrastruktuurin piiriin on saatu kaksi kolmannesta yliopistojen loppukäyttäjistä, ja katsetta voidaan nyt kääntää käyttäjäpohjan laajentamisesta uusiin Haka-järjestelmää hyödyntäviin palveluihin.

ASP-käyttäjähallinto murheenkryyninä

Yliopistot osana valtionhallintoa ovat käyneet tehostamaan toimintaansa ulkoistamalla sovelluksiaan. ASP-palvelutarjontaan erikoistunut yritys pystyy suuruuden ekonomian kautta ehkä yliopistoja suurempaan kustannustehokkuuteen palvelun ylläpidossa, mutta varjopuoli on, että palveluntarjoajan konesalissa oleva tietojärjestelmä on vaikeampi kytkeä yliopiston muihin tietojärjestelmiin, esimerkiksi käyttäjätunnuksiin.

Jos loppukäyttäjän on tarpeen kirjautua ASP-palveluun, ovat käyttäjät tavallisesti saaneet palvelua varten omia käyttäjätunnus-salasana-pareja, joita jonkun yliopistossa pitäisi ehtiä myös ylläpitää. Olisikin houkuttelevaa, että uusien käyttäjätunnusten sijaan loppukäyttäjät voisivat käyttää olemassa olevia tunnuksia ja salasanoja, joilla he korkeakoulussaan kirjautuvat esimerkiksi työasemiin. Käyttäjien identiteetti pitäisi siis federoida identiteetintarjoajana (*Identity Provider, IdP*) toimivan kotikorkeakoulun järjestelmistä palveluntarjoajan (*Service Provider, SP*) ASP-palveluun.

Yliopistoilla on käytössä paljon yhteisiä ASP-palveluja. Valtiokonttori on sopinut Rondo-ohjelmiston käytöstä ostolaskujen kierrätykseen ja Persona Travel -ohjelmiston käytöstä matkanhallintaan. Yliopistot käyttävät myös muita Personec-yhtiön tuotteita, mm. Persona F -sovellusta (aiemmin Fortime) ja HR-ohjelmistoa. Näiden saaminen Haka-infrastruktuurin piiriin on ajankohtaista kuluvana vuotena.

Federoidun identiteetin hyödyntäminen

Federoidun identiteetin hyödyntämisessä on havaittavissa kolme astetta. Ensimmäinen askelma on käyttäjän henkilöllisyyden todentamisen eli autentikoinnin siirtäminen palvelusta kotiorganisaation IdP-palvelimelle. Loppukäyttäjälle tämä konkretisoituu siten, että hän pääsee palveluun kotiorganisaationsa käyttäjätunnuksella ja salasanalla. Käyttäjälle ylimääräisten tunnusten ja salasanojen muistaminen on monesti uusien sovellusten käyttöönoton päällimmäinen riesa, joka rasittaa myös ylläpitoa.

<kaavio>

Toisella portaalla myös käyttäjän henkilötietojen ylläpito siirretään palvelusta IdP-palvelimen tehtäväksi. Tällaisia tietoja ovat esimerkiksi nimi, sähköpostiosoite ja puhelinnumero. Tällöin muutokset tarvitsee tehdä vain kotikorkeakoulun identiteetintarjoajan käyttäjärekisteriin, josta ne federoituvat palveluun, kun käyttäjä seuraavan kerran kirjautuu siihen.

Federoidun identiteetin hyödyntämisen kolmas askel on sen ulottaminen auktorisointiin, eli käyttöoikeuksien hallintaan. Jos käyttöoikeus voidaan johtaa käyttäjän karkean roolitiedon perusteella, on oikeuden perustaminen federaation varaan melko suoraviivaista – esimerkiksi

käyttöoikeus yliopistokirjastojen lisensoimiin aineistoihin on opiskelijoilla ja henkilökunnalla, mikä voidaan tarkistaa vaikkapa identiteetintarjoajalta saatavan eduPersonAffiliation-attribuutin avulla.

Roolitieto voi myös kuvata käyttäjän suhdetta johonkin yliopiston opintojaksoon. Tampereen teknillisessä yliopistossa toteutettiin vuonna 2005 kokeiluhanke, jossa verkko-oppimisalustan käyttöoikeus sidottiin opiskelijan kurssi-ilmoittautumista kuvaavaan attribuuttiin: opiskelija sai käyttöoikeuden kurssiin oppimisalustassa, kun hän oli ilmoittautunut kyseiselle kurssille opiskelijarekisterissä. Kurssi-ilmoittautuminen ilmaistiin Internet2-yhteisön CourseID-työryhmän määrittelemällä eduCourseMember-attribuutilla, joka sanoi: ”Tämä käyttäjä on roolissa opiskelija kurssin MATHM-47250 syksyn 2005 toteutuksessa.”

Jos käyttöoikeus sen sijaan on erikseen nimetyillä käyttäjillä, on tilanne monisyisempi. Esimerkkinä tästä on yliopistojen sähköinen JOO-hakujärjestelmä (joustava opinto-oikeus), jossa opiskelijoiden hakemuksia käsittelevät opintoasiainhallinnon virkamiehet opintotoimistoissa tai tiedekunnissa. Keväällä 2005 kokeilukäyttöön otetussa sähköisessä JOO-hakujärjestelmässä käyttöoikeuksia hallinnoidaan järjestelmän sisällä, vaikka henkilöllisyyden todentamisessa ja henkilötietojen ylläpidossa tukeudutaan IdP-palvelimen antamiin tietoihin.

Jos palvelujen käyttöoikeudet annetaan käyttäjälle henkilökohtaisesti ilman, että niitä voidaan johtaa hänen roolitiedoistaan, esimerkiksi laitostiedosta ja virka-asemasta, tullaan käyttöoikeuksien hallinnan peruskysymysten äärelle. Jos hallinta siirretään palvelusta identiteetintarjoajalle, pitäisi federaation jokaisen kotiorganisaation rakentaa mekanismit tämän tiedon ylläpitämiseksi esimerkiksi IdP-palvelimensa yhteydessä olevassa LDAP-hakemistossa. Vaikka tällaisia tekniikoita on kehitteillä myös yliopistoissa (esim. Internet2-konsortion Signet-projekti), on epäselvää, tuleeko käyttöoikeuksien hallinta koskaan siirtymään täysin sovellusten ulkopuolelle. Monessa tilanteessa jo pelkkä henkilöllisyyden todentamisen rakentaminen federaation varaan on riittävä helpotus käyttäjälle ja yliopistolle.

Käyttäjätunnistus globalisoituu

Haka-infrastruktuuria vastaavia kansallisia luottamusverkostoja on syntynyt korkeakouluihin myös Yhdysvalloissa, Sveitsissä, Norjassa ja Espanjassa, ja lukuisissa Euroopan maissa on aiheeseen liittyviä kehitysprojekteja. Yliopistojen toiminta ja yhteistyö on kuitenkin globaalia. Tutkimusyhteisöt muodostavat ylikansallisia virtuaaliorganisaatioita, ja ylikansalliset toimijat – esimerkiksiksi kirjastojen aineistontarjoajat – palvelevat asiakkaita monessa maassa.

Seuraava askel onkin kansallisten luottamusverkostojen kytkeminen yhteen. EU:n rahoittaman GN2-projektin JRA5-tutkimushankkeessa kehitetään eduGAIN-tekniikkaa, jonka avulla kansalliset tutkimusverkot voidaan kytkeä yhteen erityisen sillan kautta. Tekniikka tukeutuu SAML-kieleen (*Security Assertion Markup Language*), joka on XML-pohjainen kieli ja yhteyskäytäntö käyttäjätunnistukseen liittyvien väittämien vaihtamiseen IdP- ja SP-palvelinten välillä. Teknisen yhteensopivuuden lisäksi on kuitenkin ratkaistava myös koko joukko poliittisia ja tietosuojaan liittyviä kysymyksiä.

Kohti kaupallista tarjontaa

Tällä hetkellä kaikki Haka-infrastruktuuriin kytketyt palvelimet ovat Shibboleth-palvelimia. Shibboleth-protokolla on SAML-kielen version 1.1 profiili, jonka Yhdysvalloissa tehty avoimen lähdekoodin toteutus tukeutuu OpenSAML-kirjastoon ja edelleen muihin avoimen lähdekoodin tuotteisiin, kuten Apache, Tomcat, OpenSSL ja Xerces.

Jatkossa Haka-infrastruktuurin ja Shibboleth-tekniikan välillä ei kuitenkaan enää välttämättä ole yhtäsuuruusmerkkejä. Heinäkuussa 2005 Shibboleth-kehittäjät testasivat onnistuneesti Shibboleth-toteutuksen yhteensopivuutta kuuden kaupallisen tuotteen kanssa. Ensimmäiset SAML-yhteensopivat kaupalliset tuotteet ovat nyt päätymässä kauppojen hyllyille. Shibboleth 2.0:n toteutus on tekeillä, ja sen sisältämä SAML 2.0 -tuki avaa tien Shibbolethin ja Liberty-tekniikan yhteensopivuudelle.

Vahvan tunnistuksen merkitys kasvaa

Haka-infrastruktuurissa käyttäjän henkilöllisyyden todentaminen tapahtuu tällä hetkellä salasanan avulla. Myös korkeakouluissa on hapuiltu tukevampien autentikointimenetelmien suuntaan. Mm. HSTYA-projekti tutki toimikorttiin perustuvaa varmennetunnistusta vuosina 2000–2002. Tähän mennessä vahvaa tunnistusta ei ole korkeakouluissa kuitenkaan otettu laajemmassa mittakaavassa käyttöön. Tarve sille ei ole ollut kustannuksiin nähden riittävä.

Salasana-autentikoinnin heikkouksiin perustuvat hyökkäykset ovat saaneet viimeaikoina huomiota Suomessakin, kun verkkopankkien asiakkaita on huijattu paljastamaan kertakäyttösalasanansa kalastelijoille. Identiteettifederaatiossa yhdellä salasanalla avautuu entistä suurempi joukko palveluja, ja kalastajan verkkoihin takertumisesta seuraava vahinko kasvaa. Niinpä identiteettifederaatio on lopulta myös osaltaan vauhdittamassa vahvaan tunnistukseen siirtymistä.