

## <Kainalojuttu: Shibboleth>

### Yliopisto ja Haka-infrastruktuuri

**Minna Harjuniemi**

Tietotekniikkaosasto

Haka-infrastruktuuri on Suomen yliopistojen ja ammattikorkeakoulujen yhteinen käyttäjätunnistusjärjestelmä, johon liittyneiden yhteisöjen loppukäyttäjät pääsevät yhdellä käyttäjätunnuksella korkeakoulusektorin palveluihin riippumatta niiden tuottajasta. Infrastruktuurin käyttö edellyttää liittymistä luottamusverkostoon.

Luottamusverkostolla tarkoitetaan eri organisaatioiden – tässä tapauksessa yliopistojen ja ammattikorkeakoulujen – muodostamaa yhteisöä, joka tekee yhteistyötä käyttäjien tunnistamiseksi yli organisaatorajojen. Nimensä mukaisesti toiminta perustuu luottamukseen: eri organisaatiot luottavat siihen, että toiset toimivat sovitulla tavalla ja että niiden käyttäjähallinto on sellaisella tasolla, että siellä käyttäjätunnistus tapahtuu riittävän uskottavasti.

Tämän luottamuksen takaamiseksi on muotoiltu yhteinen sopimus, johon on kirjattu ne ehdot, jotka verkoston jäsenet toiminnassaan on täytettävä. Helsingin yliopisto on ollut jäsenenä alusta alkaen, ja ollut mukana myös sen perustamista edeltäneissä hankkeissa.

Luottamusverkostolla on kahdenlaisia jäseniä: kotiorganisaatioita, joiden käyttäjät verkoston palveluita hyödyntävät – siis yliopistoja ja ammattikorkeakouluja – sekä palveluntarjoajia, jotka haluavat tarjota palveluitaan kotiorganisaatioiden käyttäjille. Luottamusverkossa on jäseniä tällä hetkellä 13, joista seitsemän toimii myös kotiorganisaationa. Suurin osa palveluntarjoajista on ainakin tällä hetkellä yliopistoja, mutta jatkossa heitä löytynee muualtakin: esimerkiksi sähköisiä aineistoja tai talous- ja henkilöstöhallinnan järjestelmien käyttöpalveluita myyvistä yrityksistä (esimerkiksi Elsevier tai Fortime).

Koska verkoston toiminta perustuu luottamukselle, on sen säilyttämiseksi sovittu yhteisistä toimintatavoista ja toiminnan reunaehdoista käyttäjähallinnossa. Suoraan käyttäjiä koskevia asioita ovat esimerkiksi:

- \* Käyttäjätietojen ajantasaisuus:  
*Helsingin yliopistossa tämä on hoidettu käyttölupajärjestelmän kytkennällä erilaisiin taustajärjestelmiin (Oodi, Fortime/Persona F).*
- \* Käyttäjätunnuksen voimassaolo on rajoitettu:  
*Yliopistolla henkilökunnan tunnus on voimassa enintään puolitoista vuotta kerrallaan, opiskelijalla läsnäololukukauden tai -vuoden loppuun. Mikäli henkilön käyttölupa työsuhteen päättyessä halutaan pitää voimassa, häneltä poistuu henkilökuntastatus.*
- \* Tietoturvallisuuteen liittyviä asioita:  
*Salasanan minimipituus on kahdeksan merkkiä. Tästä syystä myös unix-ympäristössä on otettu käyttöön salasanan vaihtopakko vuoden välein. Tänä aikana kaikki salasanat vaihtuvat 8-merkkisiksi. Tämä vaikeuttaa myös huomattavasti salasanan murtamista brute force -menetelmällä (ks. sivu XX)*
- \* Henkilöllisyyden todentaminen käyttöluvan myöntämisen tai salasanan luovutuksen yhteydessä:

*Tältä osin sääntöjä on tiukennettu myös yliopiston omalla päätöksellä (hallintojohtajan päätös X/Y). Koska henkilökunnan ja opiskelijan tunnus-salasanaparilla pääsee sähköpostin lisäksi muihinkin luottamuksellisiin tietoihin, vaikkapa WebOodiin tai UPJWebiin, on varmistuttava siitä, että salasana luovutetaan juuri oikealle henkilölle. On ollut tilanteita, jossa laitoksella on tutunnäköinen henkilö pyytänyt uutta salasanaa, eikä atk-yhdyshenkilö ole kehdannut varmistua henkilöllisyydestä. Kiusalliset tilanteet voidaan välttää, kun hallintojohtajan päätöksen mukaisesti henkilöllisyys aina varmistetaan virallisella henkilöllisyystodistuksella lupatietoja käsiteltäessä.*

#### **Lisätietoa**

*<http://www.csc.fi/suomi/funet/middleware/haka/index.phtml>*