

# Haka-luottamusverkosto

Virtuaalikorkeakoulupäivät 18.11.2009

CSC - Timo Mustonen  
timo.mustonen@csc.fi

CSC – Tieteen tietotekniikan keskus Oy  
CSC – IT Center for Science Ltd.



# CSC – Tieteen tietotekniikan keskus Oy

- Valtion omistama osakeyhtiö
- Non-profit
- IT-palveluiden tuottaminen korkeakouluille, tutkimuslaitoksille ja muille organisaatioille
  - Superlaskenta
  - Funet-verkko
- CSC operoi korkeakoulujen Haka-luottamusverkostoa

# Luottamusverkosto eli federaatio

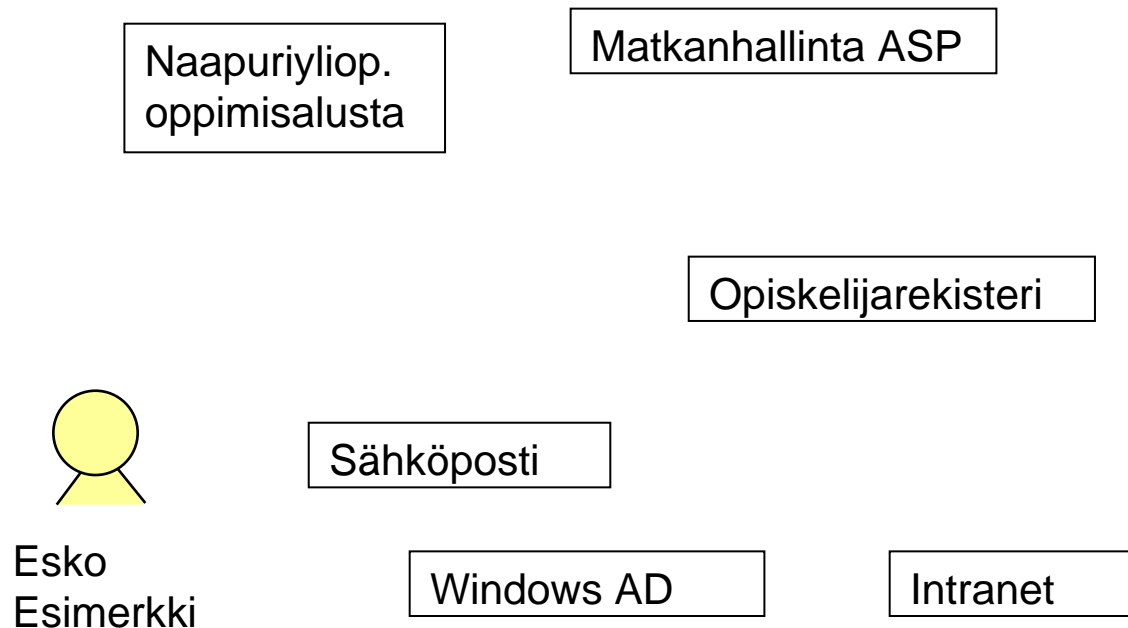
- Luottamusverkosto eli federaatio (engl. federation) on organisaatioiden muodostama yhteisö, joka päättää tehdä yhteistyötä käyttäjien tunnistamiseksi yli organisaatorajojen.
  - päättää käyttää siihen vaikka Shibboleth-tekniikkaa
- luottamusverkosto on siis organisatorinen (ei siis tekninen) olio
- löysässä puheessa federaatiolla tarkoitetaan myös luottamusverkoston käyttämää tekniikkaa (esim. Shibboleth)

# Kenelle Hakasta on hyötyä?

- Organisaatiot, joissa on paljon käyttäjiä ja/tai käyttäjän tunnistamista vaativia palveluja
- Verkostojen palvelut, joihin kirjautuu opiskelijoita ja työntekijöitä monesta korkeakouluista
- Keskitetysti tuotetut palvelut
  - Yhteiset oppimisalustat ja opetuksen tukityökalut
  - Kirjastojen yhteiset tietojärjestelmät
  - Vuokrasovellukset (ASP, SaaS)



# Esko Esimerkki käyttää päivittäin useita palveluita



# Osan niistä omistaa Eskon kotikorkeakoulu, osan joku muu...

Palvelut joita Esko käyttää osana arkeaan korkeakoulussa

Naapuriyliop.  
oppimisalusta

Matkanhallinta ASP

Eskon kotikorkeakoulu

Opiskelijarekisteri



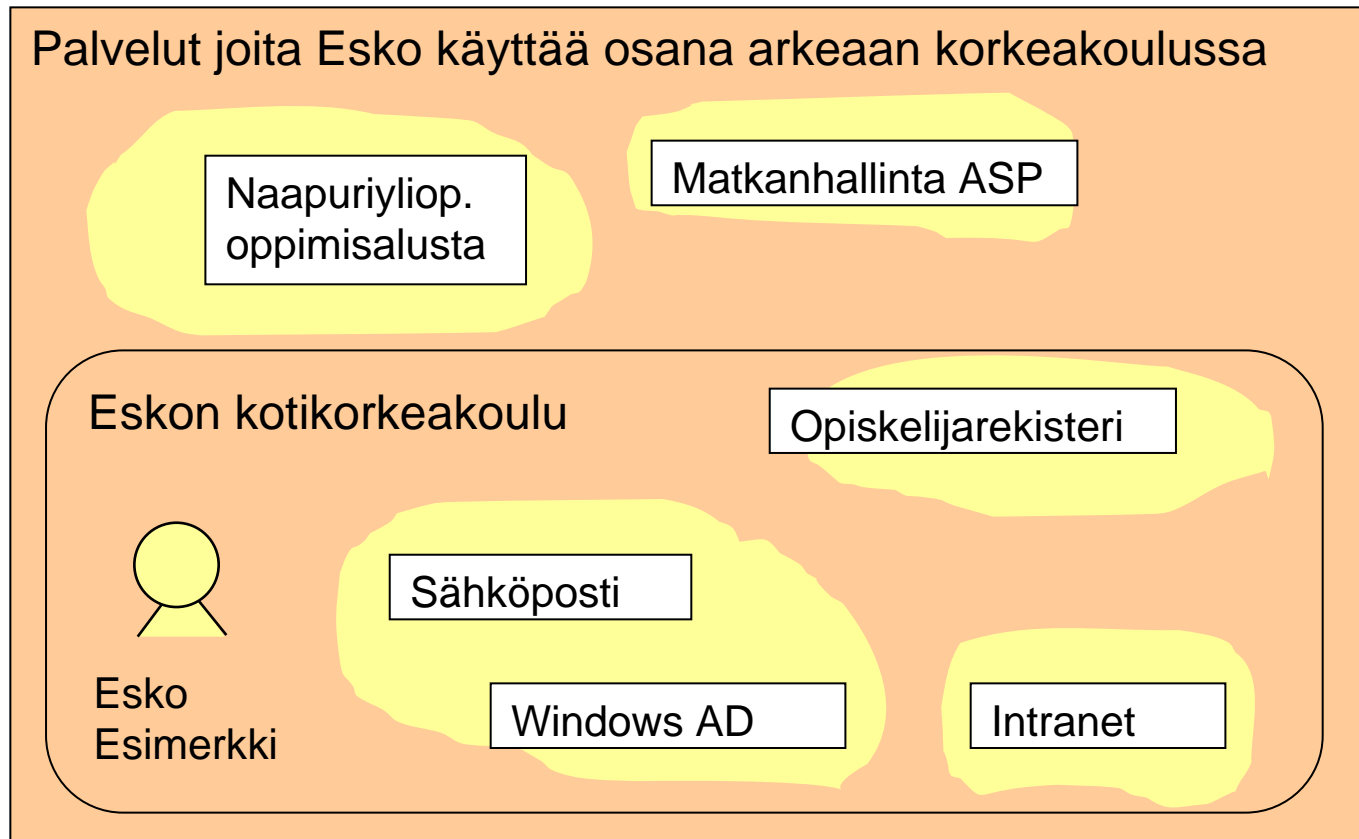
Sähköposti

Esko  
Esimerkki

Windows AD

Intranet

# Eskon tunnukset jokaisessa palvelussa tuppaa elämään omaa elämäänsä...



”Saarekkeinen identiteetin hallinta (isolated IdM)”

# Metahakemisto rationalisoi identiteetinhallintaa organisaation sisällä

Palvelut joita Esko käyttää osana arkeaan korkeakoulussa

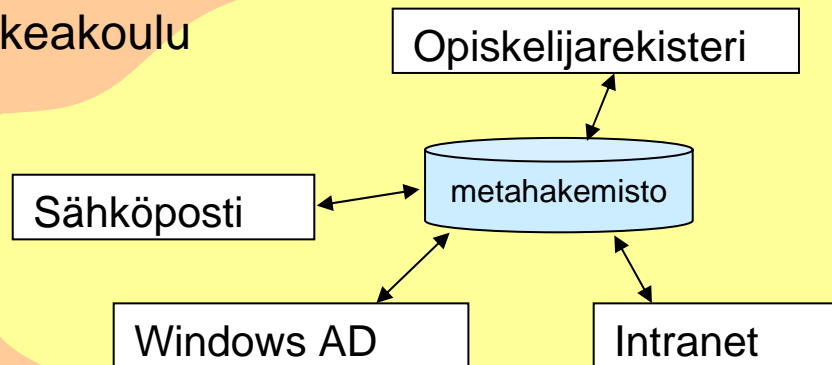
Naapuriyliop.  
oppimisalusta

Matkanhallinta ASP

Eskon kotikorkeakoulu

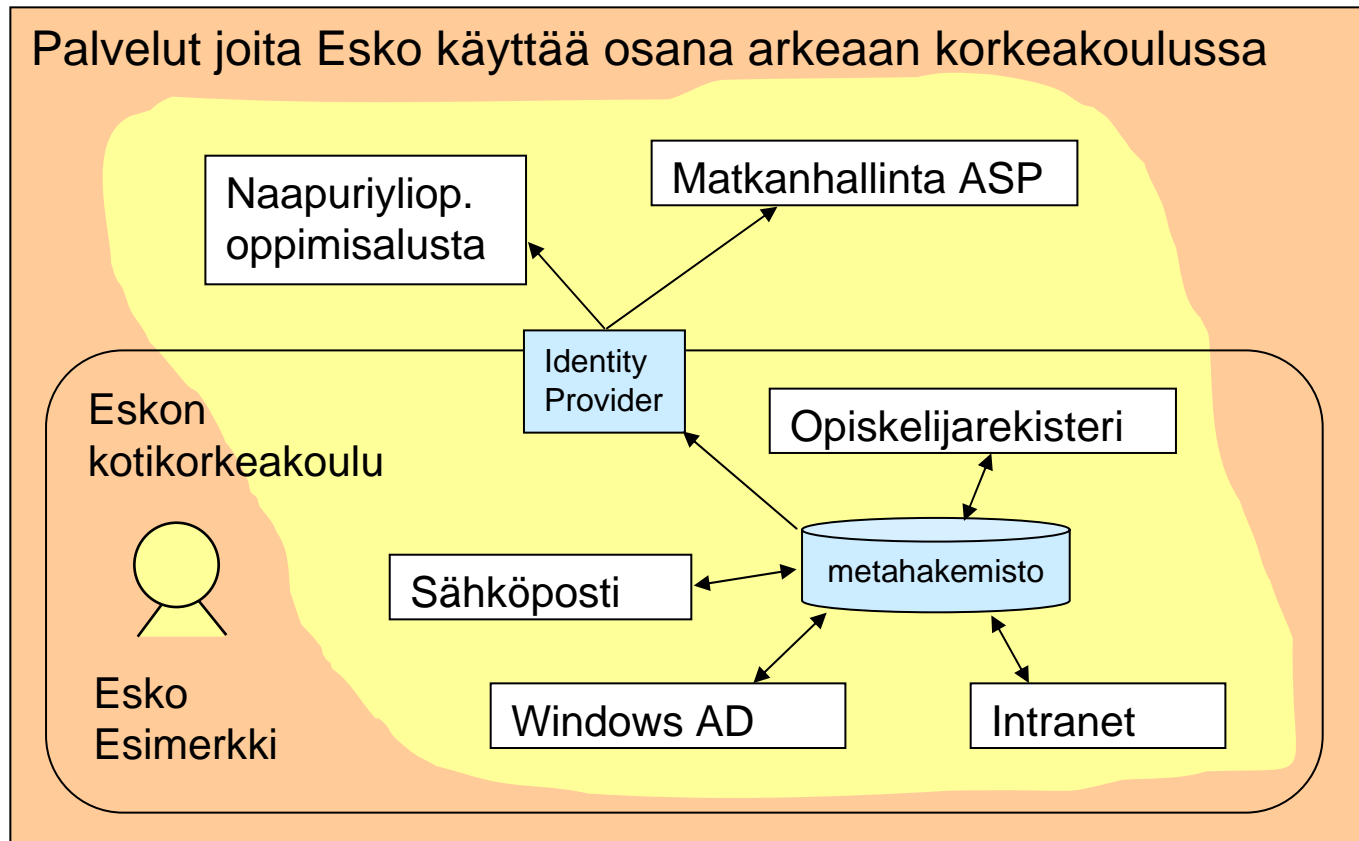


Esko  
Esimerkki



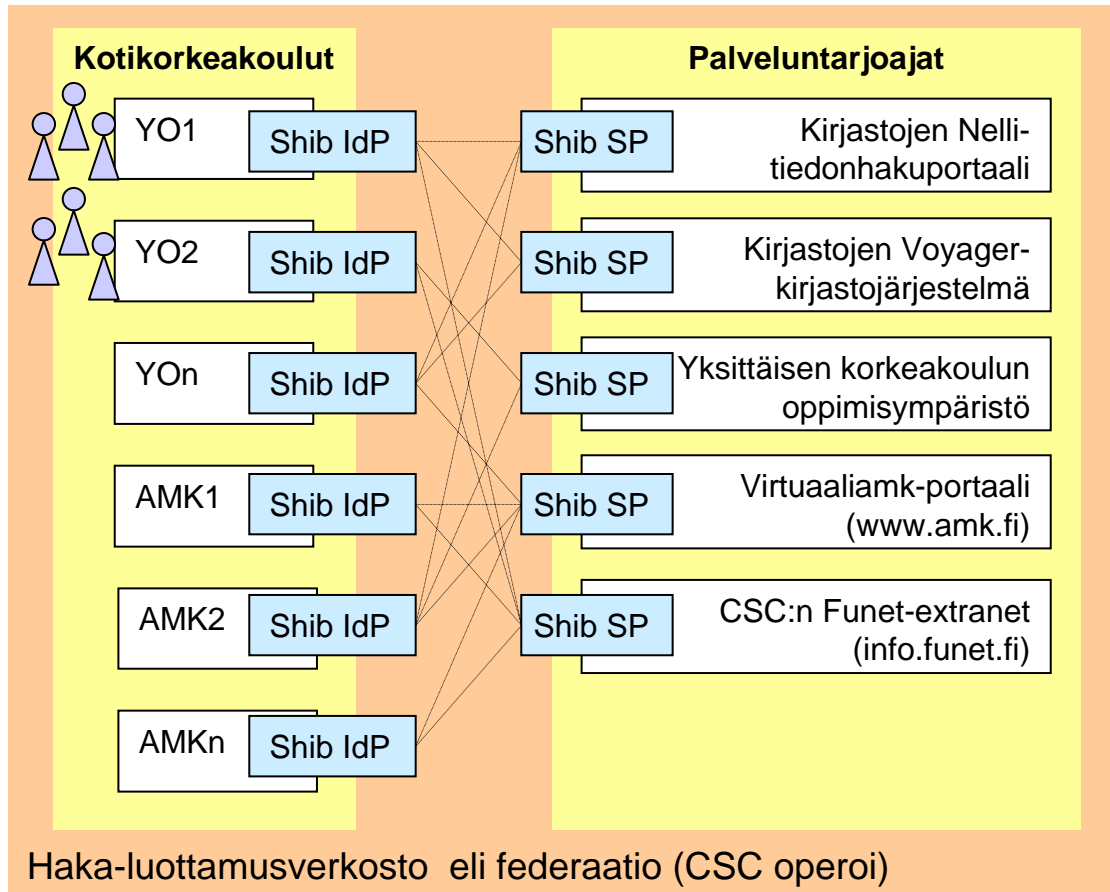
”Keskitetty identiteetinhallinta (centralised IdM)”

# Federointi tuo myös talon ulkopuoliset järjestelmät saman identiteetin piiriin



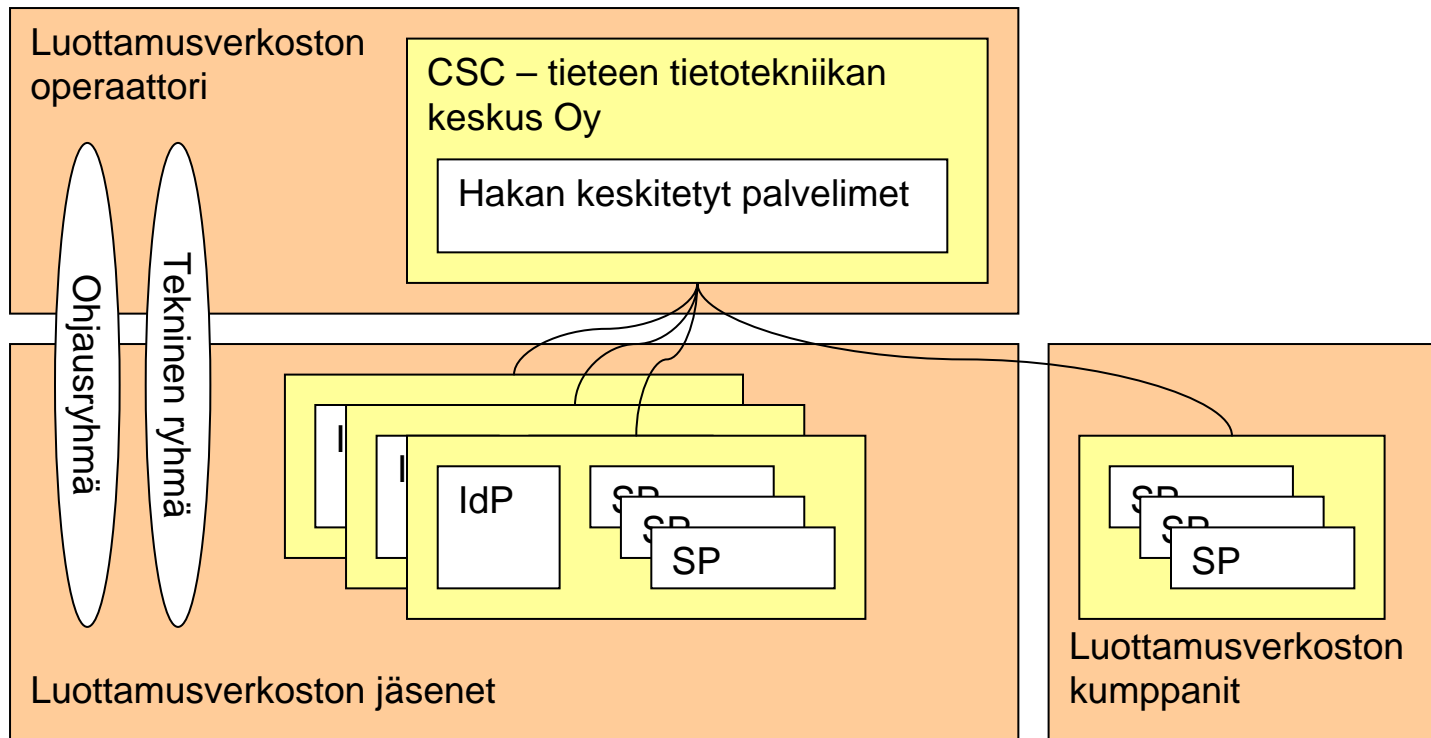
"Federoitu identiteetin hallinta (Federated IdM)"

# Haka-luottamusverkosto



- Kotikorkeakoulu ylläpitää käyttäjän **perustietoja** (nimi, yhteystiedot, rooli, opintosuunta ym)
- Kotikorkeakoulu **autentikoi** käyttäjän (esim. salasanalla)
- Kotikorkeakoulu **luovuttaa** (käyttäjän suostumuksella) henkilötietoja palveluntarjoajalle
- Palveluntarjoaja päättää henkilötietojen perusteella, **millainen näkymä** käyttäjälle avautuu palvelussa

# Haka-luottamusverkosto on CSC:n palvelu korkeakouluille



Hakaan liitytään allekirjoittamalla palvelusopimus CSC:n kanssa

# Hakan hyödyt loppukäyttäjille, kotiorganisaatioille ja palvelujen tarjoajille

- Loppukäyttäjällä yksi tunnus-salasanapari kaikkiin Haka-palveluihin helposti ja turvallisesti
- Turha ja päällekkäinen käyttäjätunnusten ylläpitotyö poistu
- Haka on ilmainen palveluntarjoajille korkeakouluissa
- Palvelun käyttäjätunnusten ylläpito korkeakoulun IT-yksikön hoidettavaksi
  - Palveluntarjoaja voi keskittyä palvelunsa sisältöön
- Luotettavat ja ajantasaiset käyttäjätiedot  
Tiedot kotikorkeakoulun tietojärjestelmistä (opiskelijarekisteri, henkilökuntarekisteri), esim. nimi, sähköpostiosoite, rooli (opisk/hlökunta), opintosuunta, kurssi-ilmoittautuminen
- Palvelun käyttöoikeuksien rajaaminen tai profilointi mahdollista, esim. palvelu avautuu vain psykologian opiskelijoille

# Mistä luottamusverkoston pitää sopia

- Luottamus, kuinka osapuolet luottavat toisiinsa
  - Käyttäjätiedot kotikorkeakoulussa ajan tasalla
  - Palveluntarjoajan järjestelmä tietoturvallinen
  - Käyttäjän yksityisyyttä ei loukata (henkilötietolaki)
  - Luottamusverkostoa operoidaan sovittujen pelisääntöjen mukaan
- Skeema eli attribuuttien esitystapa:
  - funetEduPerson
  - esim. kuinka ilmaistaan ”lääketieteen opiskelija”
  - esim. kuinka Matti Virtanen erotetaan kaimoistaan
- Protokolla:
  - *esim. SAML1.1, SAML2.0, OpenID*
- Tietoturvainfrastruktuuri:
  - PKI=palvelinvarmenteet, esim. *Sonera CA*

# Haka-palvelusopimus: CSC luottamusverkoston operaattorina

- ylläpitää luottamusverkoston metatietoa ja WAYF:ä
  - mitä organisaatioita, IdP:tä ja SP:tä on
  - mitä attribuutteja kukin SP tarvitsee
  - tekniset yhteystiedot ja –henkilöt
  - luotetut varmentajat ym.
- organisoii ohjausryhmän ja teknisen ryhmän toiminnan
- suunnittelee luottamusverkoston toimintaa ohjausryhmän avulla
- ylläpitää kansainvälisiä yhteyksiä
- ylläpitää testilaitteistoa ja testaa ohjelmakomponentteja
- järjestää koulutusta ja edistää tunnettavuutta
- helpdesk IdP/SP-ylläpitäjille

# Haka-palvelusopimus: luottamusverkoston jäsenet

- Haka-jäseneksi voivat hakea:
  - yliopistot ja ammattikorkeakoulut
  - tieteen ja taiteen toimielimet, viranomaiset ja tutkimuslaitokset
  - yliopistolliset sairaalat
  - em. organisaatioiden opetus- ja tutkimustoimintaa tukevat organisaatiot
- voivat pystyttää yhden IdP:n ja useita SP:tä
  - siis vain yksi IdP/korkeakoulu
- nimeävät hallinnollisen yhteyshenkilön
- huolehtivat SAML/Shibboleth-palvelimiensa asennuksesta ja ylläpidosta
- hankkivat palvelinvarmenteen luottamusverkoston hyväksymältä varmentajalta (Sonera CA)
- Huolehtivat metatiedon päivityksestä

# Haka-palvelusopimus: kotiorganisaationa toimiva

- kytkee SAML/Shibboleth IdP:n paikalliseen käyttäjätietokantaan
- antaessaan käyttäjätunnuksen varmistaa hakijan henkilöllisyyden
- autentikoi ainakin salasanalla ja huolehtii niiden turvallisuudesta
- tarjoaa *vain ajantasaisia* attribuutteja noudattaen funetEduPersonia
- ylläpitää Site ARP:a ja User ARP:a
- tarjoaa käyttäjälle mahdollisuuden tutustua palvelun tietosuojaselosteeseen ennen kuin pyytää käyttäjältä suostumuksen henkilötietojen luovutukseen
- kerää lokia ja informoi käyttäjää lokitietojen käytöstä
- järjestää loppukäyttäjälle helpdesk-pisteen
- laatii käyttäjähallinnostaan kuvauksen luottamusverkoston muita jäseniä varten

# Haka-palvelusopimus: palveluntarjoajana toimiva

- asentaa SAML/Shibboleth SP:n ja integroi sen palveluun
- ilmoittaa operaattorille
  - mitkä attribuutit ovat palvelun kannalta tarpeellisia
  - tietosuojaselosteen URL:n
- suorittaa palvelunsa pääsynvalvontaa
- kerää lokia ja luovuttaa sitä tarvittaessa kotiorganisaatiolle väärinkäytösten selvittämistä varten

# Haka numeroin

- Operationaalinen toiminta alkoi 3.8.2005
- 36 IdP palvelinta (mm. kaikki yliopistot) ja 76 SP-palvelinta (17.11.2009)
- 750 000 palveluun kirjautumista 10/2009
- Odotettavissa ~ 5,0 miljoonaa kirjautumista vuoden 2009 aikana
- Volyymiltään suurimmat palvelut: kirjastot ja e-opetus
  - myös hyvin pienten kirjautumismäärien palveluja on

# Lisätietoja

- <http://www.csc.fi/haka>
- [timo.mustonen@csc.fi](mailto:timo.mustonen@csc.fi)