eduuni-ID

Verkostojen identiteetinhallinta

Haka-seminaari 14.2.2013
Kehityspäällikkö Sami Saarikoski
Opetus- ja kulttuuriministeriö

eduuni

Lähtötilanne

- Yliopistojen ja korkeakoulujen kesken on laajalti omaksuttu verkostomainen sähköinen työskentely.
- Erilaisia verkostoitumisen alustoja otetaan käyttöön itsetuotettuina tai valmiina palveluina.
  - Confluence, SharePoint, Google Drive, Yammer jne.
- Luottamusverkostot (Haka, Virtu jne.) luovat perustan verkostojen identiteetinhallinnalle.

eduuni

Verkosto

- Verkoston voi muodostaa yhteisö, työryhmä, hanke, projekti tms.
- Verkostossa on yleensä aina jäseniä useista eri organisaatioista
  - Mukana voi olla myös yksityishenkilöitä
- Hyvin organisoiduilla verkostoilla on käytössään oma sivusto tai työtila tarvittavine toiminnallisuuksineen.
  - Valitettavan usein verkostoitumisen väline on edelleen sähköposti, koska se koetaan ainoaksi helpoksi tavaksi saada ulkopuoliset käyttäjät mukaan.
- Verkoston jäsenyyksiä hallinnoi verkoston ns. omistaja, joka voi olla kuka tahansa ja mistä tahansa.

eduuni

Eduunin kehitys

- OKM:n hallinnonalan tietohallintostrategia 2006–2015
  - Sähköinen työskentely ja verkostomainen toimintatapa
- Syyskuussa 2009 otettiin käyttöön OKM:n hallinnonalan työryhmäpalvelu (SharePoint 2007)
  - Haka-kirjautuminen ei onnistunut (Shibboleth-ADFS extensions), joten AD-luottosuhteet luotiin 7 organisaation välille.
  - Ulkopuolisten käyttäjähallinto hajautettiin asiakasorganisaatioihin.
  - Toimi hyvin sisäisille työryhmille, mutta salasanojen hallinnointi aiheutti ongelmia.
    - Sähköposti oli edelleen helpompi väline verkostoille
- Syyskuussa 2011 otettiin käyttöön Eduuni-työtilat OKM:n toimialalle (SharePoint 2010)
  - Eduuni-työtilat käyttää Eduuni-ID:tä tunnistuslähteenä (IdP)
  - Eduuni-työtiloissa on tällä hetkellä 2400 rekisteröitynyttä käyttäjää 320 eri organisaatiosta.

eduuni

Verkostojen käyttäjähallinnon vaatimukset

- Käyttäjätunnuksen muoto oltava yleisesti tunnettu, yksilöivä ja mahdollisimman informatiivinen.
  - Ainoaksi vaihtoehdoksi jää sähköpostiosoite.
  - Parhaassa tapauksessa sähköpostiosoitteesta selviää myös käyttäjän nimi ja organisaatio.
- Verkostojen käyttäjien ja valtuuksien hallintaan ei ole olemassa keskitettyjä resursseja.
  - Hajautettu malli (kirjautuminen, identiteetti ja valtuudet)
  - Täysin automatisoitu itsepalvelu
  - Ei siis keskitettyä tunnus- ja salasanahallintoa

eduuni

Eduuni-ID:n hajautettu malli

Kirjautuminen

haka
VIRTU
Google
Microsoft
YAHOO!

Käyttäjä valitsee kirjautumistavan itse

Identiteetti

Käyttäjä täyttää rekisteröitymislomakkeen
- etu- ja sukunimi
- **Sähköpostiosoite = ID**
- organisaatio

Käyttäjän antama sähköpostiosoite varmistetaan vahvistusviestin avulla.

Kirjautumistapa liitetään rekisteröintitietoihin

Valtuutus

- Käyttöoikeuksien hallinta on verrattavissa sähköpostin lähetykseen.
- Verkoston jäsenten ei tarvitse olla rekisteröityneitä.

SharePoint
CONFLUENCE

Verkoston omistaja antaa käyttöoikeuksia suoraan sähköpostiosoitteille

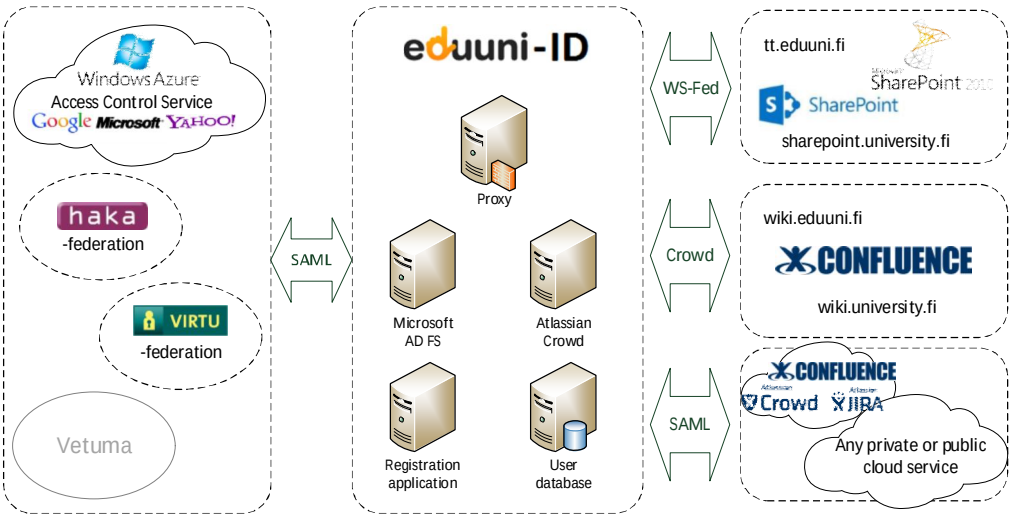
eduuni

Demo

- Eduuni-ID
  - Rekisteröinti
  - Kirjautuminen
  - Valtuutus

eduuni

Arkkitehtuuri



eduuni

Luottamusverkostojen haasteet palveluntarjoajalle

- Attribuuttien sisältö ei aina yhtenäistä
- Palveluntarjoajan on sovittava organisaatiokohtaisesti palvelun käyttöönotosta (tarvittavat attribuutit)
  - Ei sovellu verkostojen palveluille (kollaboraatioalustat)
- Luottamus ei sisällä teknistä yhteen toimivuutta
  - Haka – Shibboleth toimii hyvin, AD FS tarkempi
  - Virtu – eri federointitekniikat haasteellisia
  - Tekninen toimimattomuus käännetään usein palvelun syyksi, vaikka oman organisaation IdP olisi huonosti ylläpidetty
- Laajojen verkostojen luottamuksen taso
  - eduGAIN vs. Google

eduuni

Haka + Eduuni-ID =

- Tasa-arvoinen ID
  - Ei erikseen sisäisiä ja ulkoisia käyttäjiä
  - Mahdollistaa yksinkertaisen valtuutuksen
- Kokonaan eroon salasanahallinnoinnista
  - Isot toimijat osaa homman (Google, Microsoft…) ja jos ei osaa, niin siitä kyllä kuullaan.
- ”Proxy” luottamusverkostoihin
  - Testattu ja ylläpidetty SP luottamusverkostoihin
  - Palveluiden liittäminen helpottuu

eduuni

Demo

- Eduuni-ID
  - Ryhmähallinta (virtuaaliorganisaatiot)
- Keskustelua
  - Käyttötapauksia

eduuni

Kiitos!

sami.saarikoski@minedu.fi

eduuni