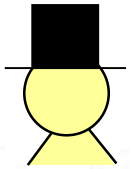
Federoidun identiteetinhallinnan periaatteet

CSC - Tieteen tietotekniikan keskus

- Valtion omistama osakeyhtiö
- Non-profit
- tuottaa keskitettyjä IT-palveluita korkeakouluille, tutkimuslaitoksille ja muille organisaatioille
  - Suurteholaskenta
  - Funet-verkko
- CSC ja identiteetinhallinta
  - Korkeakoulujen Haka-luottamusverkoston operointi ja koordinointi
  - Valtionhallinnon Virtu-luottamusverkoston operointi

Identiteetin ja pääsyn hallinta

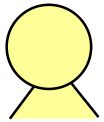
1. Henkilötietojen ylläpito (identity)
2. Käyttövaltuudet (authorisation)
3. Identiteetin todentaminen (authentication)
4. Jäljitettävyys/raportointi (audit)



Palvelun omistaja *esim. talous-hallinto*

2. ”Laitosjohtajat hyväksyvät matkalaskut”

4. Kenellä on oikeus?



3. Käyttäjätunnus
Salasana

Palvelu
(esim. matkanhallinta)

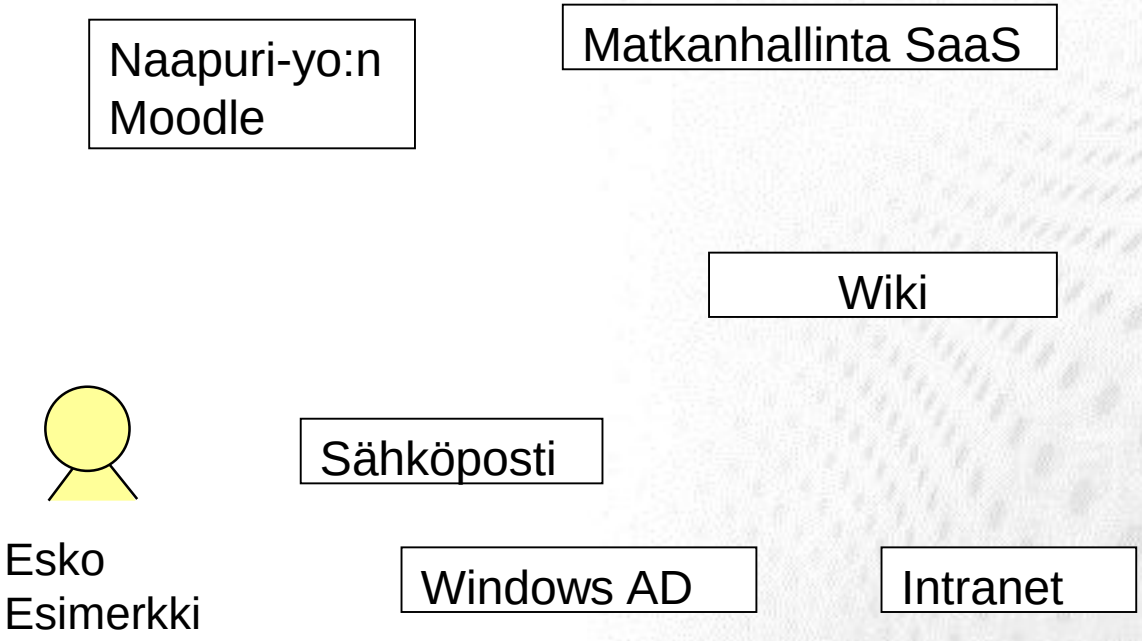
Esko Esimerkki

Nimi: Esko Esimerkki
Käyttäjätunnus: eesimerk
Rooli: laitosjohtaja

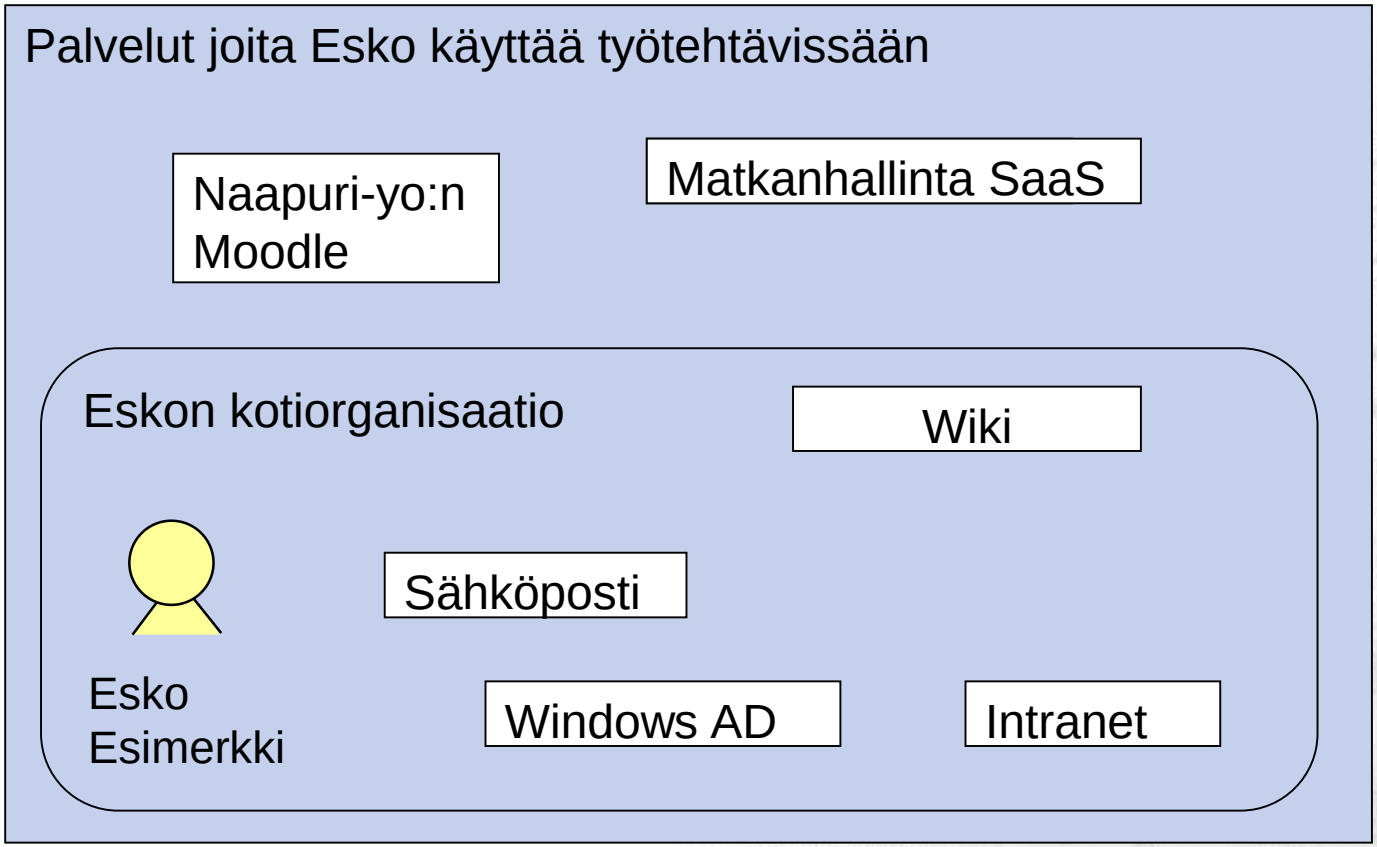
1. Eskon **henkilötiedot** viedään järjestelmään

esim. Sisäinen tarkastaja

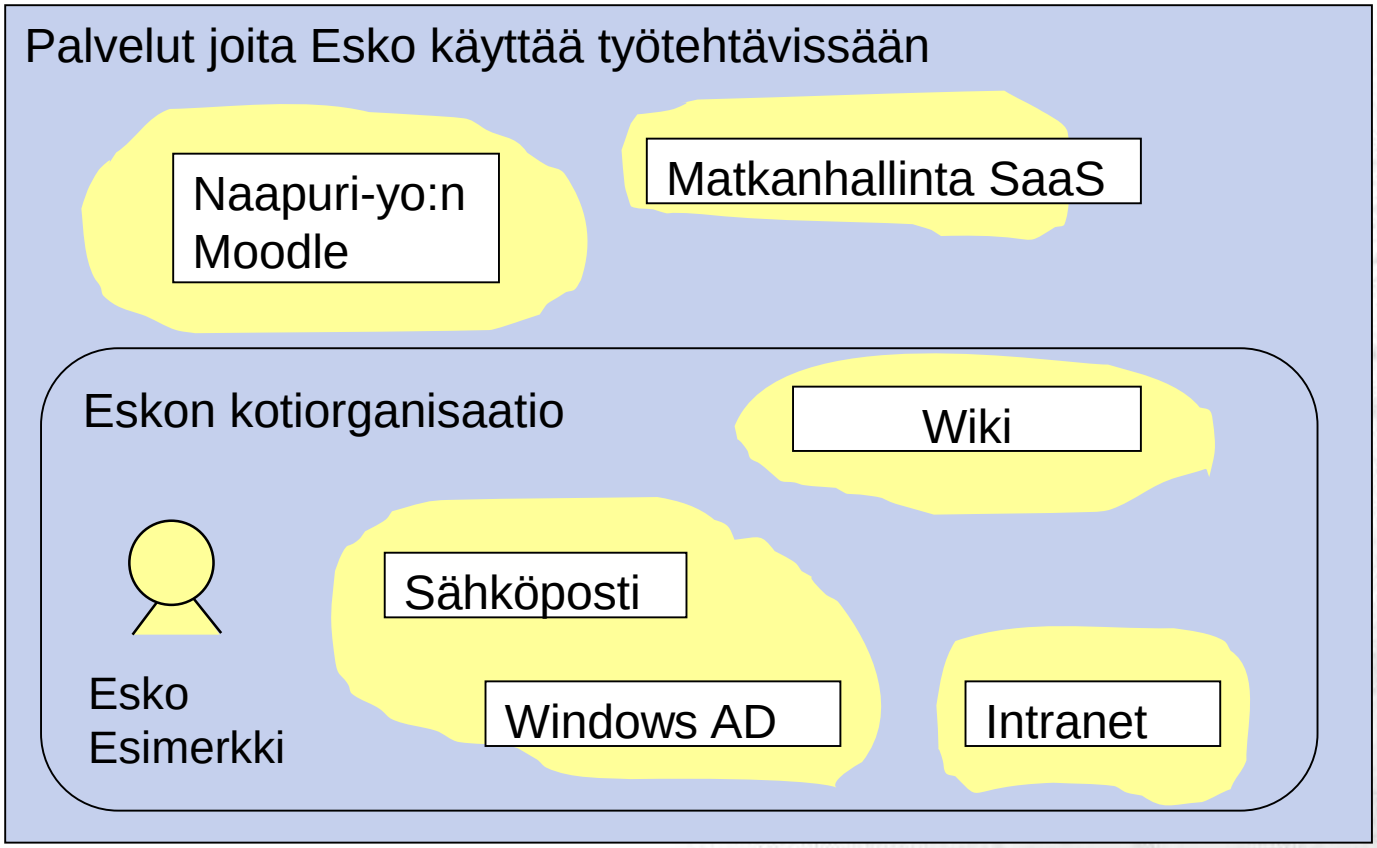
Tosielämässä palveluita on useita…



Osan niistä omistaa Eskon työnantaja, osan joku muu…

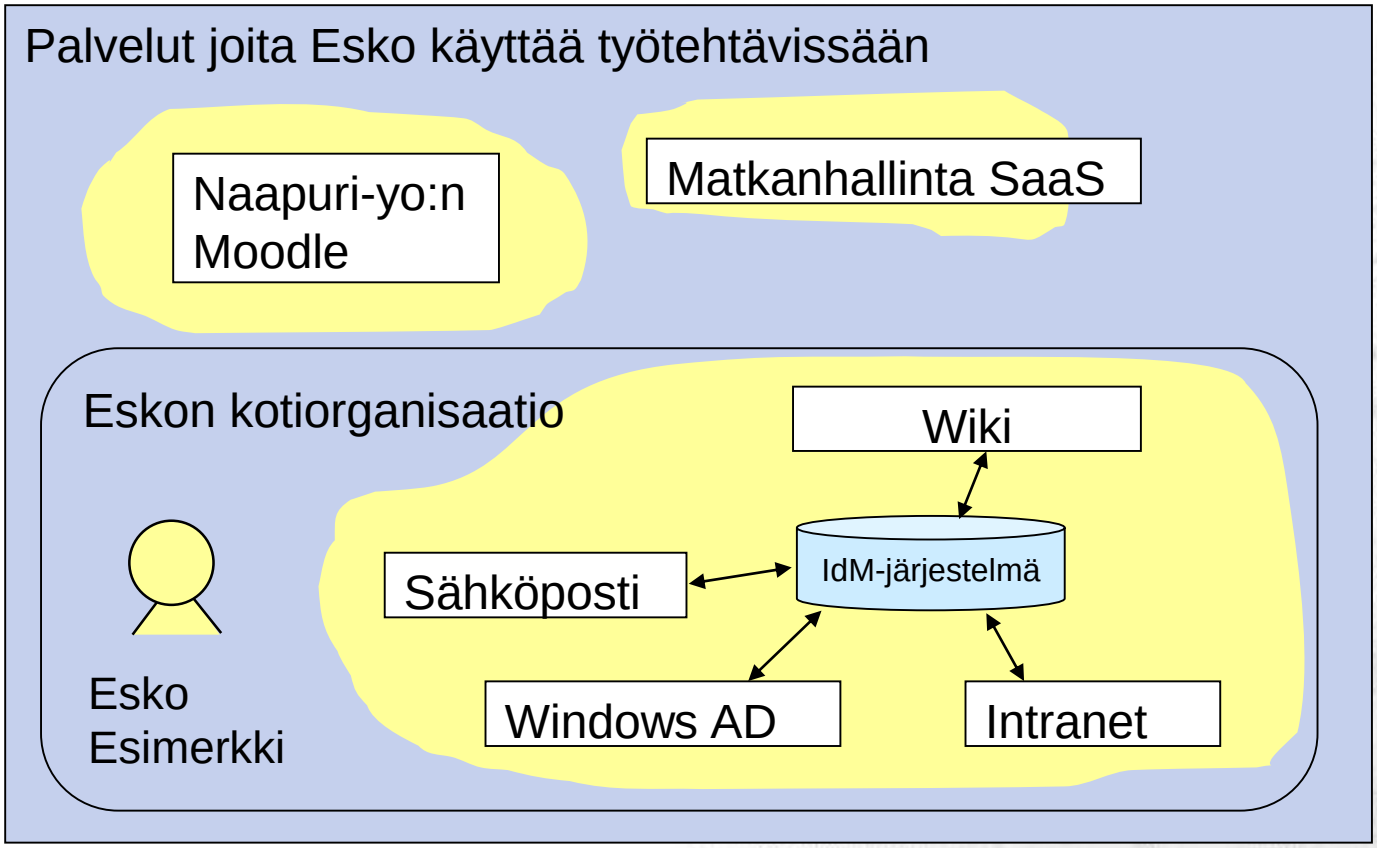


Eskon tunnukset joka palvelussa tuppaa elämään omaa elämäänsä…



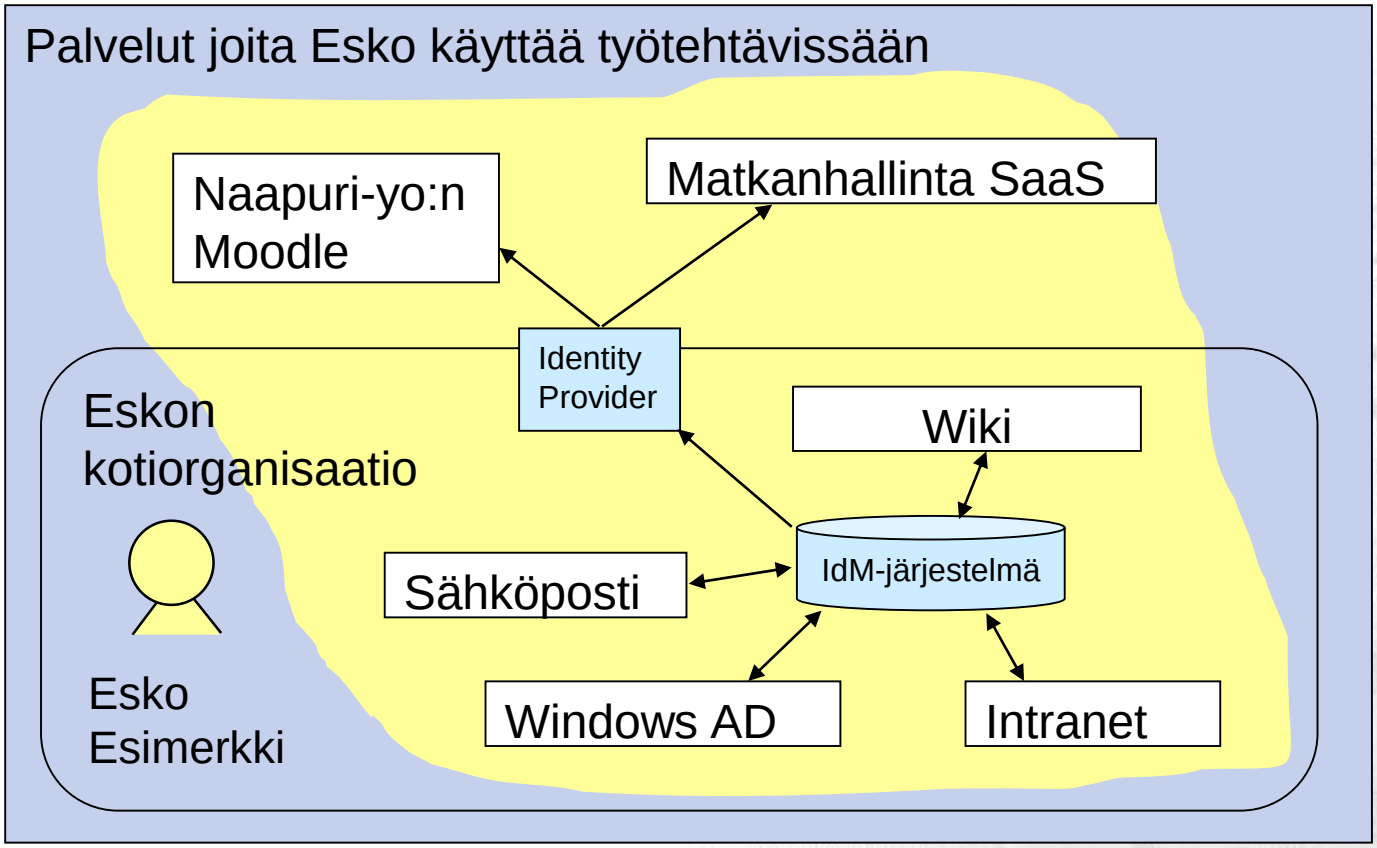
”Saarekkeinen identiteetinhallinta (isolated IdM)”

IdM-järjestelmä rationalisoi identiteetin-hallintaa organisaation sisällä



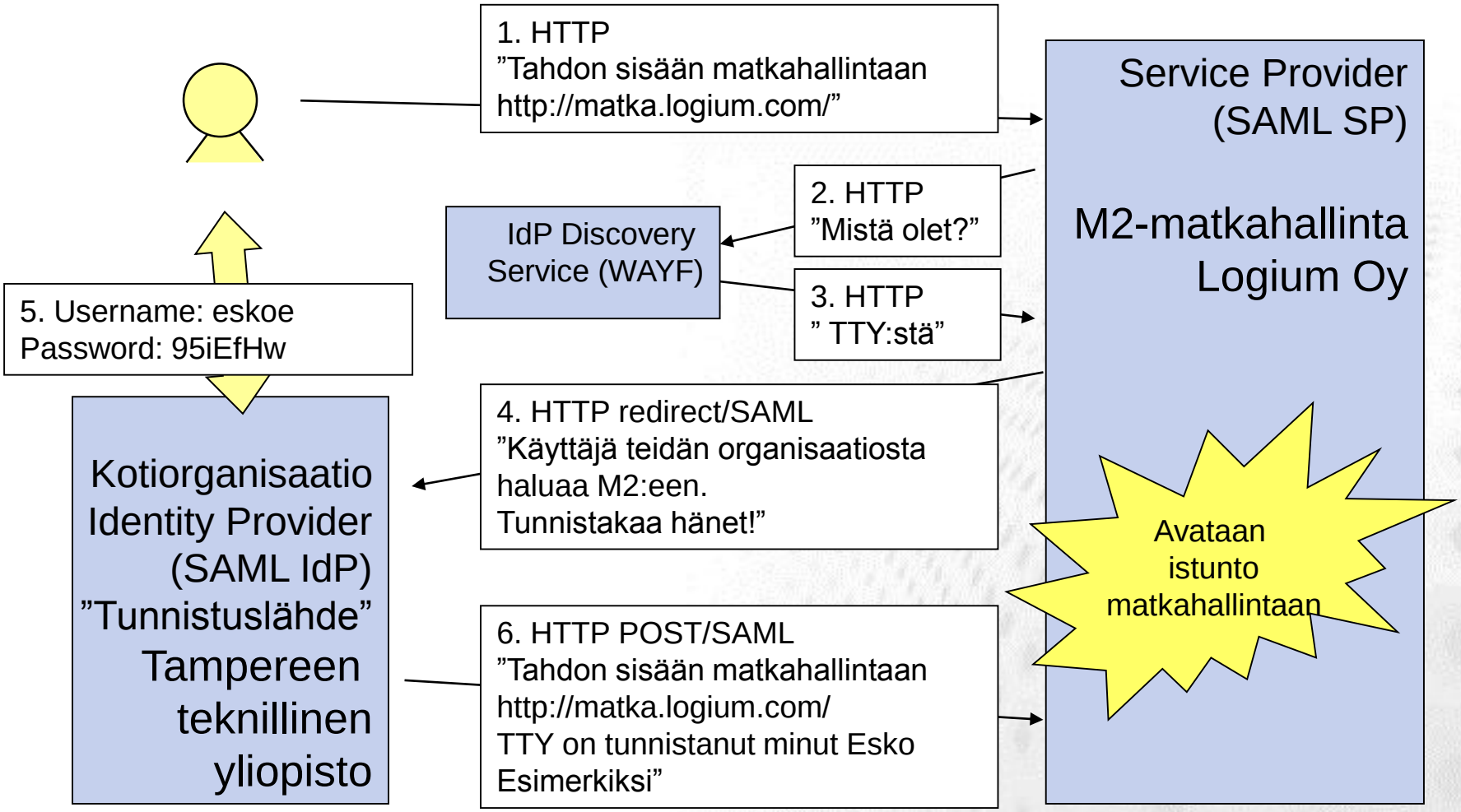
”Keskitetty identiteetinhallinta (centralised IdM)”

Federointi tuo myös talon ulkopuoliset järjestelmät saman identiteetin piiriin



”Federoitu identiteetinhallinta (Federated IdM)”

Hakan tekniikka: SAML2.0



SAML IdP ja SP –toteutuksille on laaja kaupallinen ja OSS-tarjonta

SAML 2.0 on XML-kieli

```
 <saml:AuthnStatement AuthnInstant="2004-12-05T09:22:00Z"
SessionIndex="b07b804c-7c29-ea16-7300-4f3d6f7928ac">
   <saml:AuthnContext>
      <saml:AuthnContextClassRef>
       urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
      </saml:AuthnContextClassRef>
   </saml:AuthnContext>
</saml:AuthnStatement>
<saml:AttributeStatement>
   <saml:Attribute
xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
   x500:Encoding="LDAP"
   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
   Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1"
FriendlyName="eduPersonAffiliation">
      <saml:AttributeValue
xsi:type="xs:string">member</saml:AttributeValue>
      <saml:AttributeValue
xsi:type="xs:string">staff</saml:AttributeValue>
   </saml:Attribute>
</saml:AttributeStatement>
```

- **OASIS-standardi vuodelta 2005**

Mitä hyötyä federoinnista?

1. Tietoturvallisuus
   - Tunnusten keskitetty sulkeminen, kun henkilö lähtee
   - Yksi salasana, parempi salasana?
   - Salasanan korvaaminen vahvalla tunnistuksella keskitetysti
   - Identity Providerille lisäsuojaa sijoittamalla se sisäverkkoon
   - Jäljitettävyys ja raportointi helpottuu
2. Tuottavuus
   - Sähläys tunnus/salasana-parien kanssa vähenee (käyttäjä)
   - Salasanojen resetointi vähenee (IT-helpdesk)
   - Päällekkäinen tietojen ylläpito vähenee ja tiedon laatu paranee
   - Palvelunomistaja voi keskittyä palveluunsa, tietohallinto hoitaa tunnukset
3. Uudet toimintatavat
   - Tukee esim. SaaS-palveluiden käyttöä

Käyttötilanteet

- SaaS-palvelut
  - Ostolaskut, matkalaskut, HR-järjestelmät
- Keskitetyt järjestelmät
  - Korkeakoulukirjastojen portaalit ja palvelut ym
  - CSC:n palvelut (Tutkijan käyttöliittymä, Funet-extra…)
- Kollaborointi
  - Oppimisalustat ym
  - Ryhmätyöalustat, wikit ym
  - Adobe connect, Funet filesender…
  - Tutkimusresurssit

Hyödyntämistavat

Auktorisointi

Myös käyttövaltuudet palvelussa tuodaan federoidusti.

Provisiointi

Uusien käyttäjien perustaminen palveluun lennosta.
Käyttäjätietojen ylläpito.

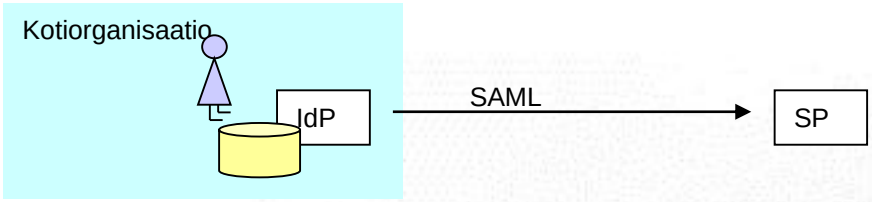
Autentikointi

Kirjautuminen kotiorganisaation tunnuksella ja salasanalla.
Ei palvelukohtaista käyttäjätunnus/salasana-paria.

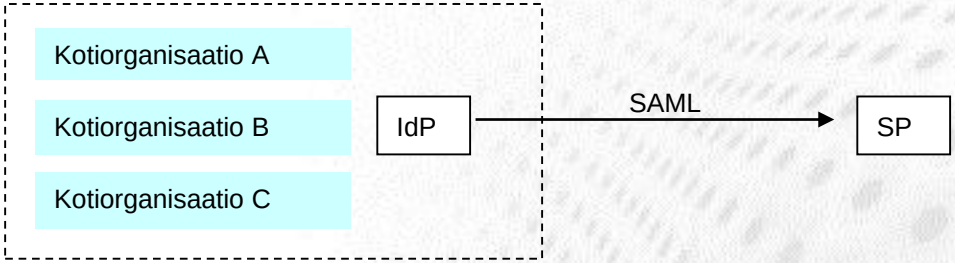
Kuinka monennelle portaalle haluat palvelusi nostaa?

IdP-pään toimintamalleja

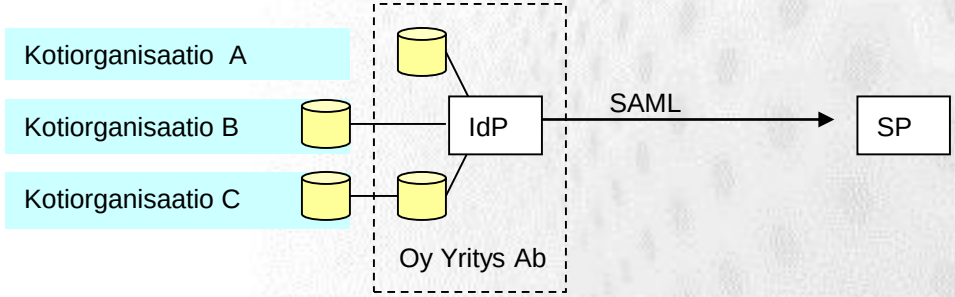
Organisaatiolla oma IdP-palvelin



Organisaatioilla yhteinen IdP



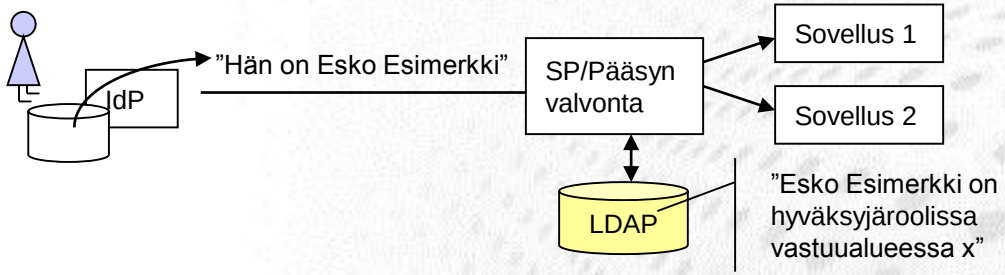
IdP SaaS



SP-pään toimintamalleja

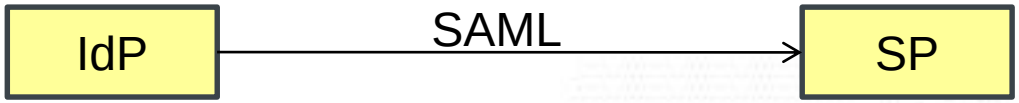
SAML SP viety suoraan palvelimeen

SAML SP erillisessä pääsynvalvonta-palvelimessa



Johdatus luottamusverkostoihin

Federointi on sopimista

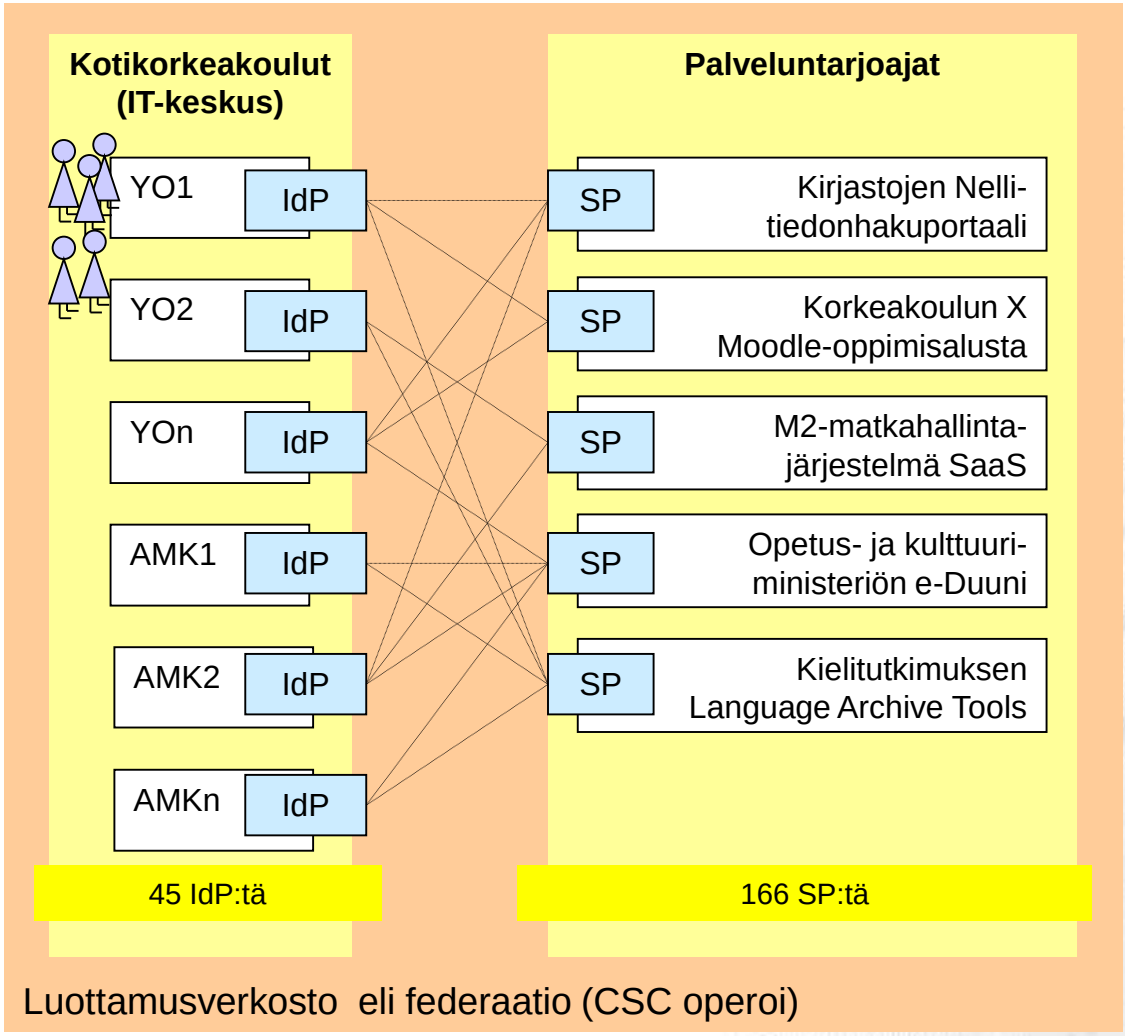


- Tekniset asiat
  - Protokolla (SAML-profiili)
  - Varmenteet
  - Ym
- Henkilötiedot eli attribuutit
  - Semantiikka
  - Sanastot
- Luottamus
  - IdP:n käyttäjätietojen laatu
  - Autentikoinnin tukevuus
- Vaatimustenmukaisuus
  - Henkilötietolaki
  - Tietoturva-asetus
- Sopimusasiat
  - Oikeudet ja velvollisuudet

Miksi luottamusverkosto

- Sopimukset voivat tietysti olla kahdenvälisiä
  - Mutta niitä tulee tolkuttomasti, jos organisaatioita on paljon
  - esim. nyt Hakassa 45 IdP:tä ja 166 SP:tä, 45x166=7470
- Helpommalla pääsee, kun organisaatiot muodostavat yhteisön, joka sopii porukalla pelisäännöistä (”policy”)
  - syntyy luottamusverkosto eli federaatio (engl. federation, Circle of Trust)
- Suomen korkeakoulujen ja tutkimuslaitosten luottamusverkosto on nimeltään Haka
- Valtion virastojen luottamusverkosto on nimeltään Virtu

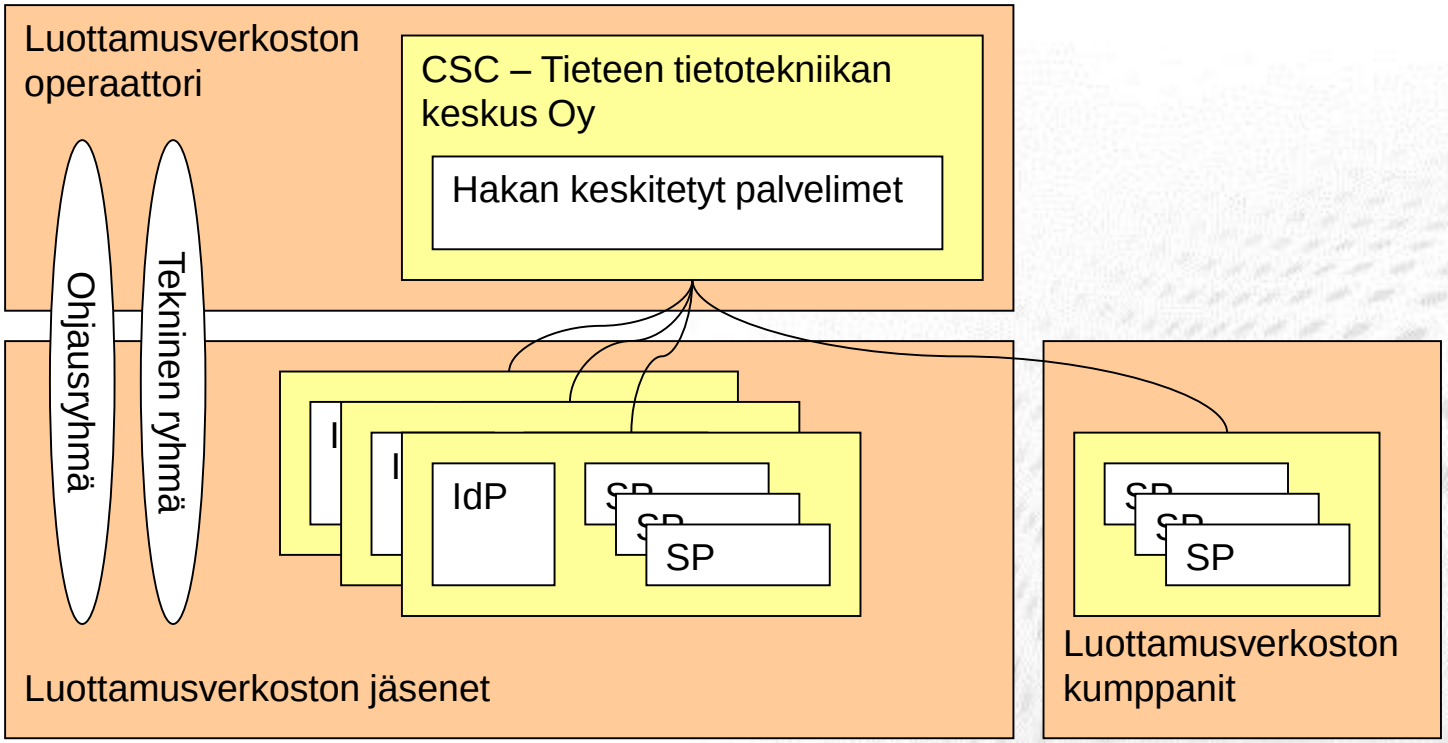
Haka-luottamusverkosto



Luottamusverkosto eli federaatio (CSC operoi)

- 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

CSC:n tehtäviä Haka-operaattorina

Tekninen operointi

- Ylläpitää luottamusverkoston SAML2-metatietoa
  - mitä organisaatioita, IdP:tä ja SP:tä on
  - mitä attribuutteja kukin SP tarvitsee
  - tekniset yhteystiedot ja –henkilöt
  - luotetut varmentajat ym
- Ylläpitää IdP Discovery Serviceä
- Tarjoaa testipalvelimet
- Tarjoaa tukea IdP/SP-ylläpitäjille

Luottamusverkoston koordinointi

- Solmii sopimuksen luottamusverkoston osapuolten kanssa
- Organisoi ohjausryhmän ja teknisen ryhmän toiminnan
- Suunnittelee toimintaa ohjausryhmän kanssa
- Koordinoi viestintää
- Ylläpitää kansainvälisiä yhteyksiä
- Järjestää koulutusta

Lisätietoa

Haka

- www.csc.fi/haka
- Haka-tiedotus-postilista, postit.csc.fi

Virtu

- http://www.valtori.fi/fi-FI/Palvelut/Kayttopalvelut