



Federoidun identiteetin- hallinnan periaatteet

Haka/Virtu-käyttäjien
kokoontuminen 3.2.2010

Mikael Linden

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

CSC - Tieteen tietotekniikan keskus

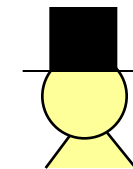


- Valtion omistama osakeyhtiö
- Non-profit
- Tehtävä tuottaa keskitettyjä IT-palveluita korkeakouluille ja tutkimuslaitoksille
 - Suurteholaskenta
 - Funet-verkko
- CSC ja identiteetinhallinta
 - Korkeakoulujen Haka-luottamusverkoston operointi ja koordinointi
 - Valtionhallinnon Virtu-luottamusverkoston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

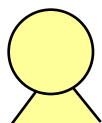
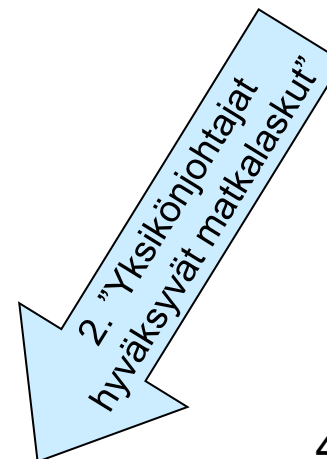
Identiteetin ja pääsyt hallinta



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



Palvelun omistaja
esim. *talous-*
hallinto



Esko
Esimerkki

3. Käyttäjätunnus
Salasana

Palvelu
(esim. matkanhallinta)

4. Kenellä on oikeus?



esim.
auditoija

1. Eskon **henkilötiedot**
viedään järjestelmään

Nimi: Esko Esimerkki
Käyttäjätunnus: eesimerk
Rooli: Yksikönjohtaja

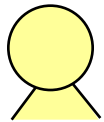
Tosielämässä palveluita on useita...



Hanselin
ekstranet

Matkanhallinta ASP

Wiki



Esko
Esimerkki

Sähköposti

Windows AD

Intranet

Osan niistä omistaa Eskon työnantaja, osan joku muu...



Palvelut joita Esko käyttää työtehtävissään

Hanselin
ekstranet

Matkanhallinta ASP

Eskon kotiorganisaatio

Wiki



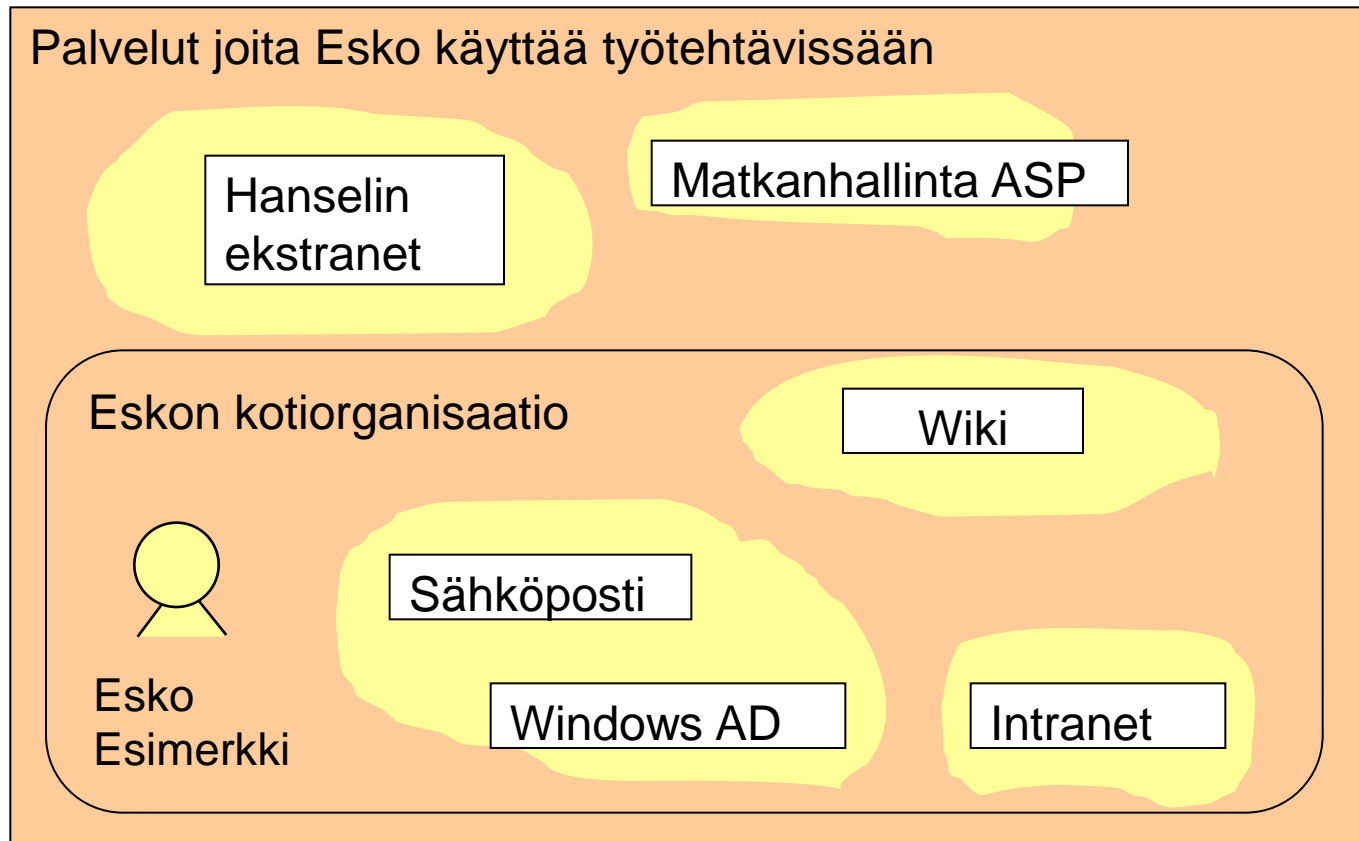
Sähköposti

Esko
Esimerkki

Windows AD

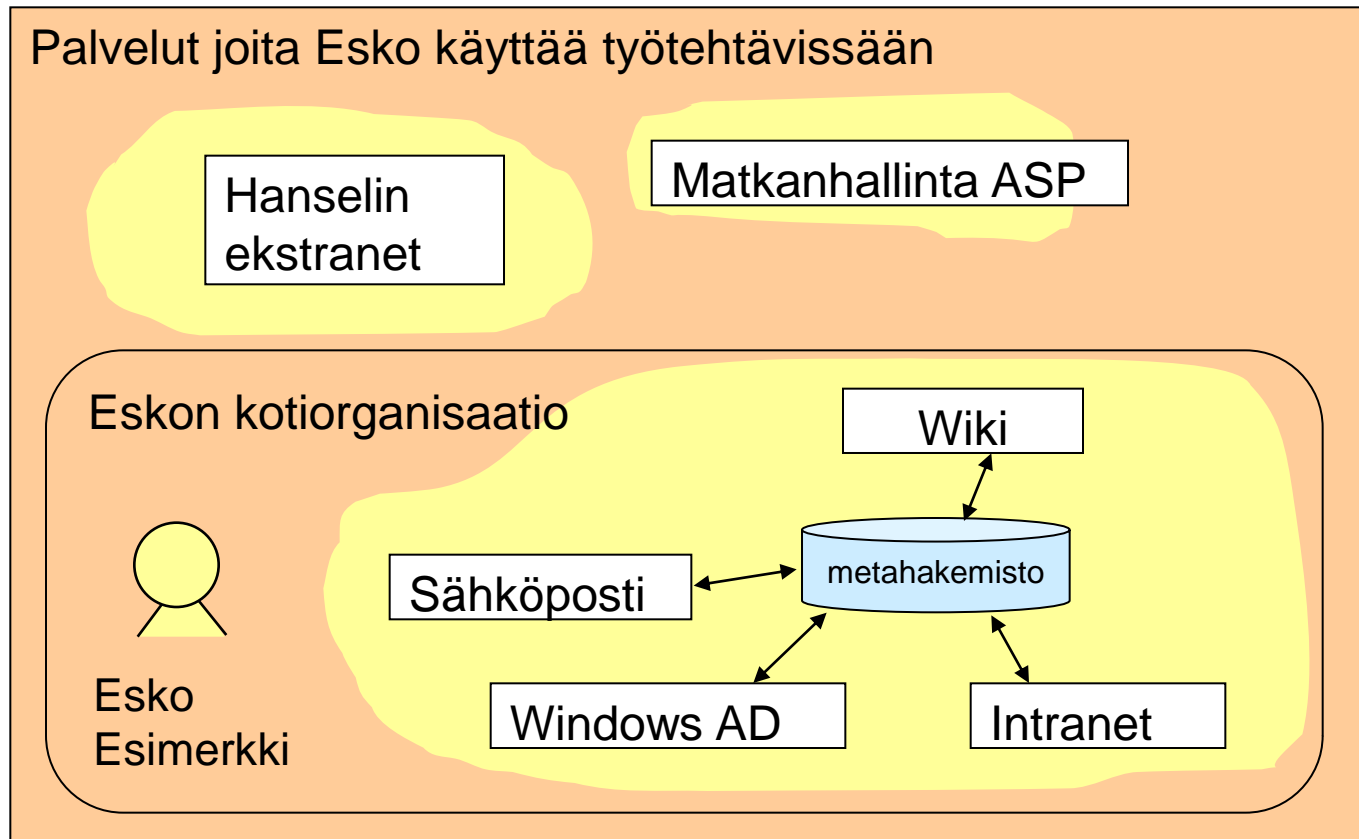
Intranet

Eskon tunnukset jokaisessa palvelussa tuppaa elämään omaa elämäänsä...



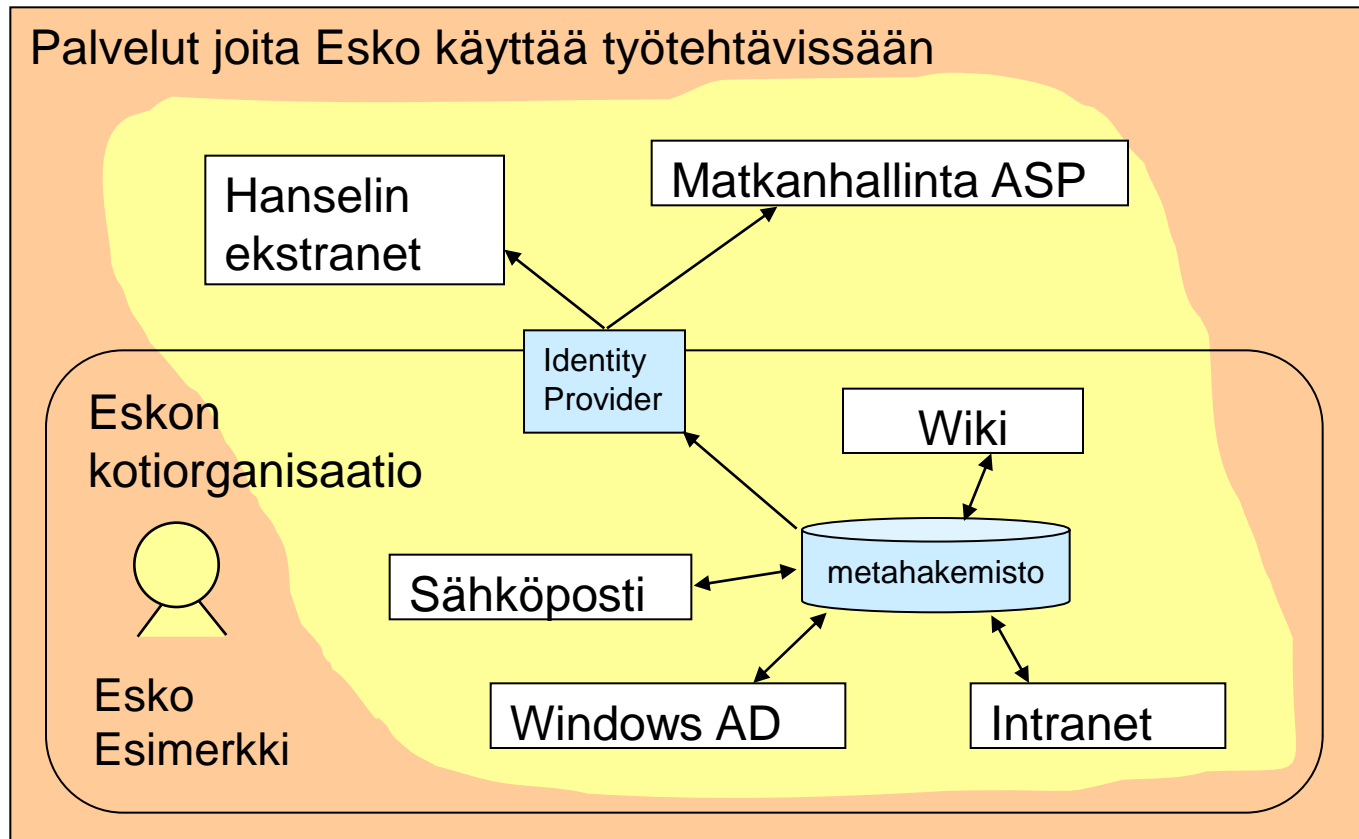
”Saarekkeinen identiteetinhallinta (isolated IdM)”

Metahakemisto rationalisoi identiteetinhallintaa organisaation sisällä



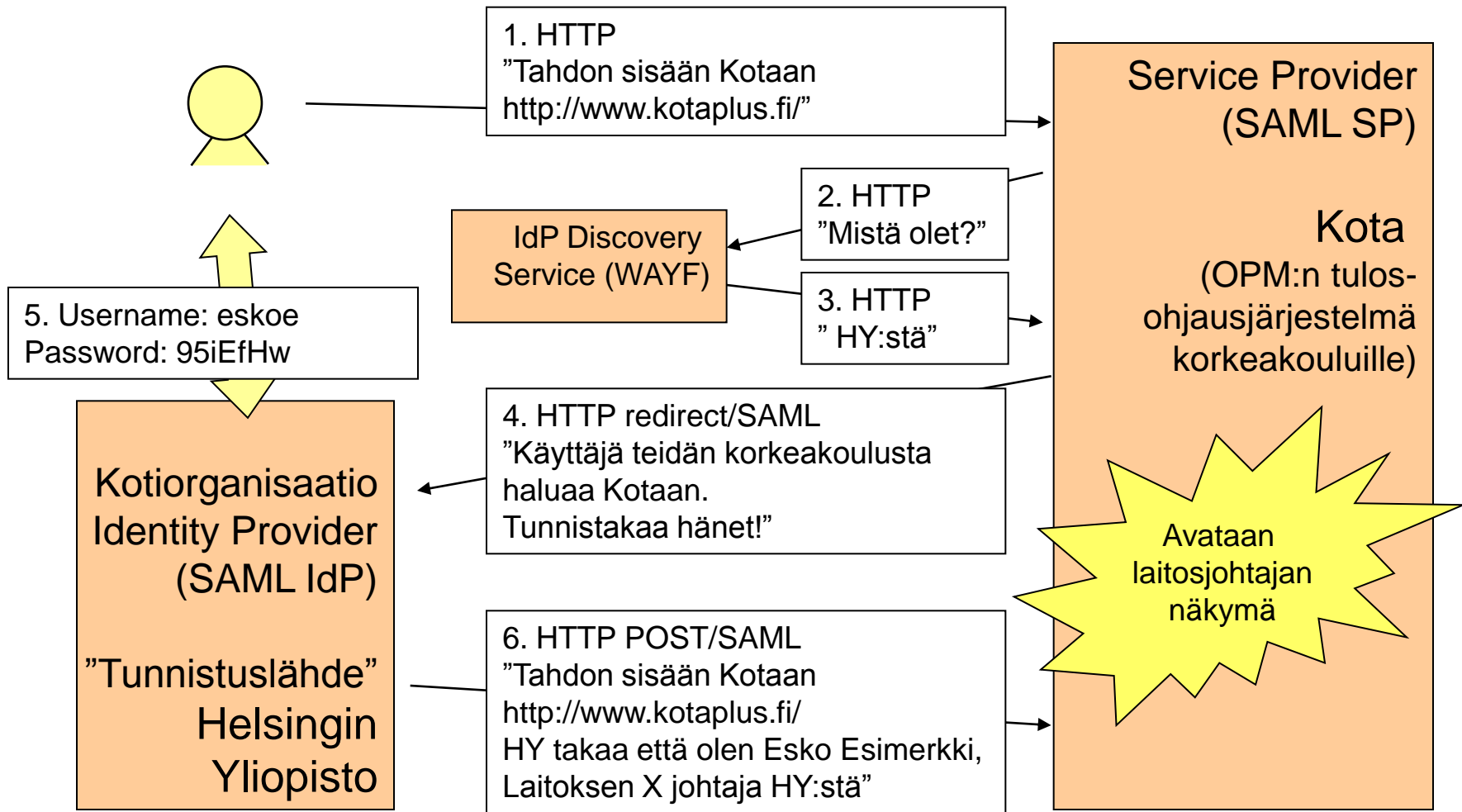
”Keskitetty identiteetinhallinta (centralised IdM)”

Federointi tuo myös talon ulkopuoliset järjestelmät saman identiteetin piiriin



”Federoitu identiteetin hallinta (Federated IdM)”

Virtun ja 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
- 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
 - Perusrekisterit (VTJ ym)
 - Korkeakoulukirjastojen palvelut ym
- Kollaborointi
 - Ryhmätyöalustat, wikit ym
 - Oppimisalustat ym

Hyödyntämistavat



Auktorisointi

Myös käyttövaltuudet palvelussa tuodaan federoidusti.

Provisiointi

Uusien käyttäjien perustaminen palveluun lennosta.
Käyttäjätietojen ylläpito

Autentikointi

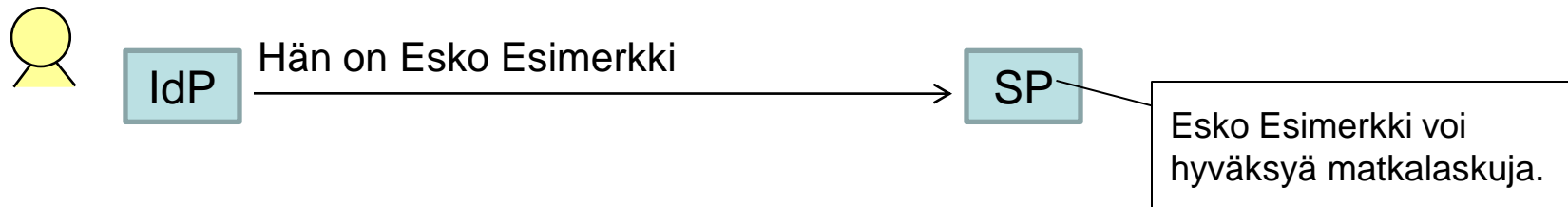
Kirjautuminen kotiorganisaation tunnuksella ja salasanaalla.
Ei palvelukohtaista käyttäjätunnus/salasana-paria.

Kuinka monennelle portaalle haluat palvelusi nostaa?

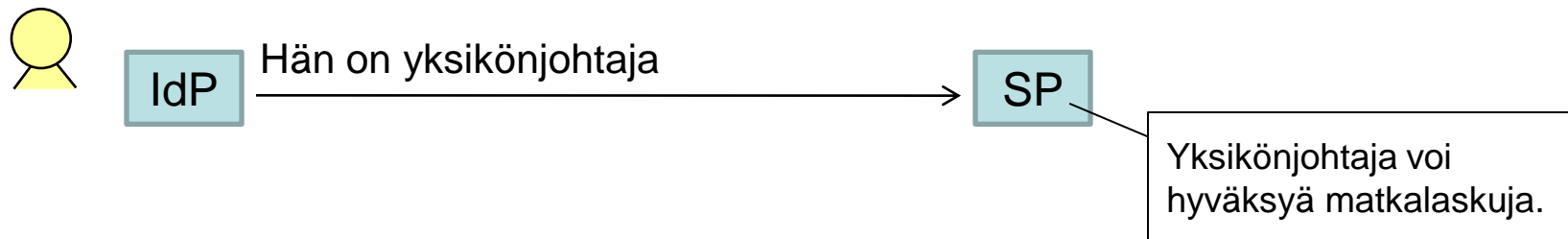
Valtuuksien federoitu hallinta



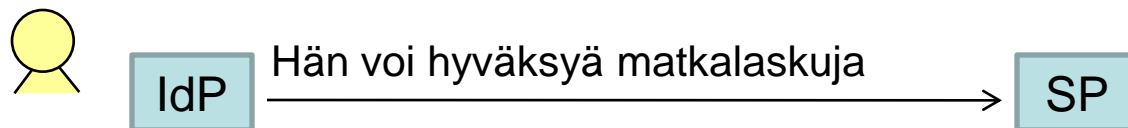
A. Perinteinen: valtuudet hallitaan SP-päässä



B. Rooliin perustuva pääsynvalvonta

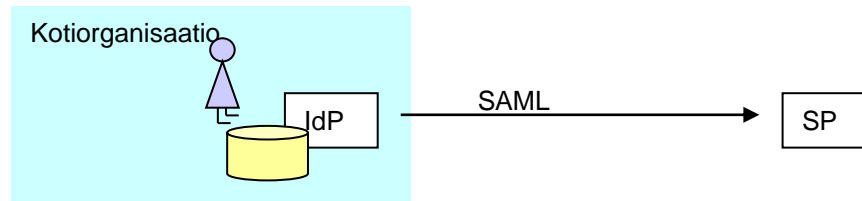


C. Valtuudet hallitaan IdP-päässä

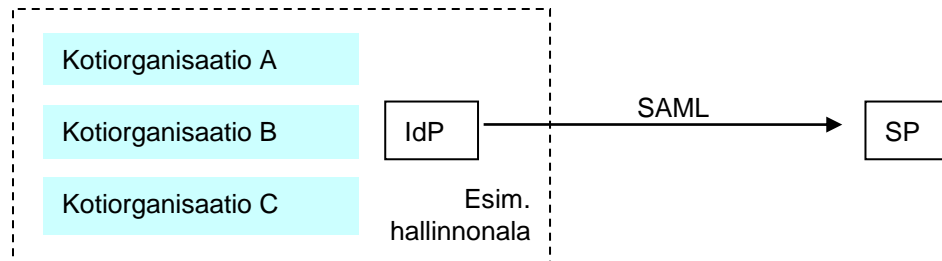


IdP-pään toimintamalleja

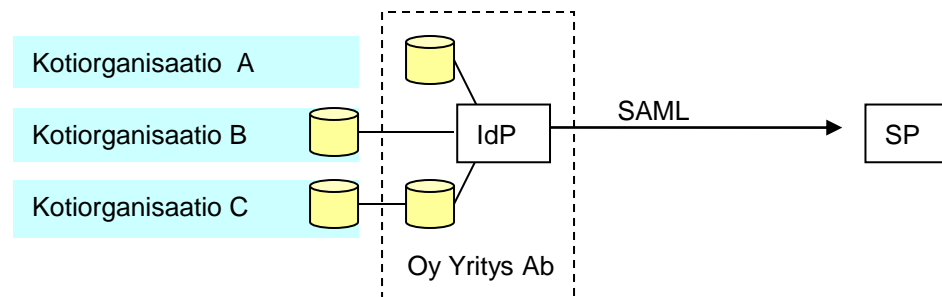
Organisaatiolla oma IdP-palvelin



Organisaatioilla yhteinen IdP

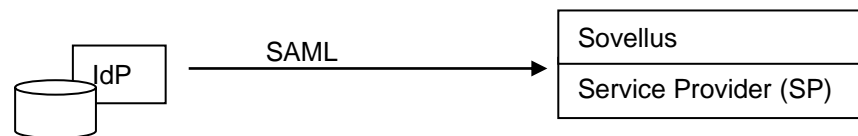


IdP SaaS

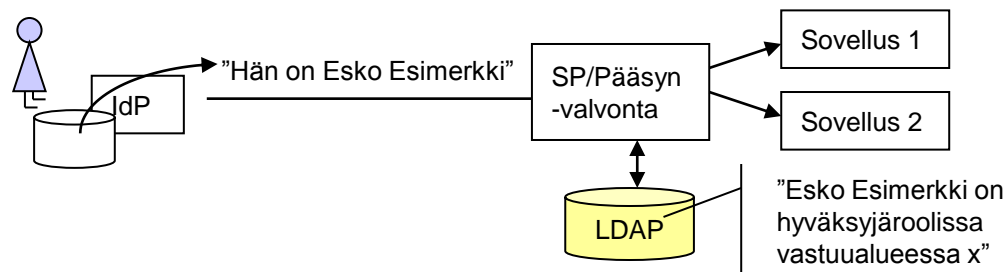


SP-pään toimintamalleja

SAML SP viety suoraan palvelimeen



SAML SP erillisessä pääsynvalvonta-palvelimessa



SAML SP proxyssä, joka on protokollamuunnin

