Aalto University

Attribuuttipohjainen käyttövaltuuksien hallinta Case Dreamspark Premium

Jari Kotomäki
Aalto University IT

Käyttövaltuuksien hallinta eli auktorisointi

- Prosessi, jossa on kyse käyttäjän tunnistamisen (autentikoinnin, engl. authentication) jälkeisestä käyttäjän valtuuksien (pyydetyn toiminnon suorittamiseen tarvittavan oikeuden) tarkastamisesta (auktorisointi, engl. authorization)

Pääsynvalvontamenetelmiä

- Rooliin perustuva pääsynvalvonta (role based access control, RBAC)
  - Käyttäjän ja käyttövaltuuden väliin luotu abstraktio
  - Käyttäjälle annetaan rooleja ja rooleille käyttövaltuuksia
- Attribuuttiin perustuva pääsynvalvonta (attribute based access control, ABAC)
  - Perustuu roolien sijasta mihin tahansa käyttäjän, palvelun, operaation tai ympäristön attribuuttiin
  - Ei tarvita suurta määrää eri rooleja
  - Mahdollistaa haluttaessa myös anonyymin käytön
- Pakotettu pääsynvalvonta (mandatory access control, MAC)
  - No read-up
  - No write-down
- [Jäljitettävyyteen perustuva pääsynvalvonta (accountability based access control)]

Aalto University

Mikä Dreamspark Premium?

- ”DreamSpark is a Microsoft Program that supports technical education by providing access to Microsoft software for learning, teaching and research purposes.”
- “DreamSpark Standard is for all types of institutions from primary to tertiary educations. DreamSpark Premium has a wider software catalog of over 500 products and is for qualifying technical departments only.”
- https://www.dreamspark.com/What-Is-Dreamspark.aspx

Aalto University

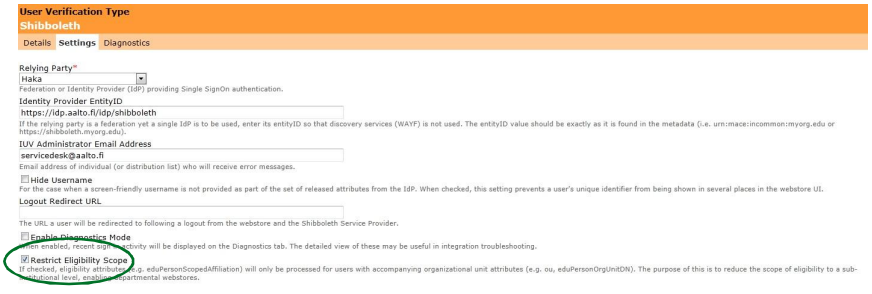
Dreamspark Premium Hakassa

- Dreamspark Premium verkkokauppa Haka-luottamusverkossa, entityID=https://e5.onthehub.com
- Hakan attribuuttifiltterin perusteella luovutetaan attribuutit:
  - **eduPersonEntitlement**
  - **eduPersonPrimaryAffiliation**
  - **eduPersonTargetedID**
  - **ou**
- Aalto IT käyttää tällä hetkellä kuitenkin vain eduPersonEntitlement-attribuuttia käyttövaltuuksien perusteena

Aalto University

Shibbolethin käyttöönotto Dreamsparkissa

- Ylläpidon www-käyttöliittymässä webstore -> verification -> shibboleth -> settings



Aalto University

Käyttövaltuuksien määritys palvelussa organisaatiotasolla

- Ylläpidon www-käyttöliittymässä organization-sivun asetukset:
  - External Organization Code määrittelee tunnisteen, jonka perusteella käyttäjät tunnistetaan tietyn organisaation jäseniksi ”*When a match is made, a user verification will be created for the user linking them to the organization with any corresponding user groups.*”

Aalto University

Käyttövaltuuksien määritys palvelussa ryhmätasolla

- Luotiin uusi ryhmä webstore_users, jolle määritettiin haluttu tunniste

Aalto University

Käyttövaltuuksienhallinta kotiorganisaatiossa

- Lupajärjestelmään tehtiin skripti, joka automaattisesti päivittää tiettyjen kriteerien mukaan käyttäjien eduPersonEntitlement-attribuutin arvoksi:
  - http://e-academy.com/eligibility/aalto.fi/groupCode
- Arvo poistetaan, jos kriteerit eivät enää seuraavalla suorituksella täyty

Aalto University

Kohdattuja haasteita

- eduPersonEntitlement-attribuutin kuvaus ohjeissa:
  - “Values are URIs of the form http://[SP]/eligibility/[IdP]/[code]. Example: *http://e-academy.com/eligibility/example.edu/compSciSoftware*.“
- Todellisuudessa attribuutin validointi tehdään säännöllisellä lausekkeella:
  - "^http://e-academy.com/eligibility/[\w\.\d]+/(?<GroupCode>.*)$”
- Ohjeiden [SP] ei tarkoita palvelun entityID:tä Hakassa eikä näin ollen vastaa validoinnissa käytettyä osoitetta!

Aalto University

Q & A

- Onko mahdollista rajata eduPersonEntitlement –attribuutin arvojen luovutusta niin että vain kohdepalveluun liittyvät arvot luovutetaan?
  - Vaatii yhteisen määrityksen siitä missä muodossa entitlement-arvot esitetään, esim. palvelun ylläpitäjä määrittelee resurssirekisterissä minkä muotoisia entitlement-arvot kyseisessä palvelussa ovat
  - Onko ollut jo esillä Hakan työryhmissä?

Aalto University

Kiitos!

Aalto University