



## 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) ]

## 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>

## 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



## Shibbolethin käyttöönotto Dreamsparkissa

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

**User Verification Type**  
**Shibboleth**  
 Details Settings Diagnostics

Relying Party\*  
 Haka  
 Federation or Identity Provider (IdP) providing Single SignOn authentication.  
 Identity Provider EntityID  
 https://idp.aalto.fi/idp/shibboleth  
 If the relying party is a federation yet a single IdP is to be used, enter its entityID so that discovery services (WAYF) is not used. The entityID value should be exactly as it is found in the metadata (i.e. urn:mace:incommon:myorg.edu or https://shibboleth.myorg.edu/).  
 UUV Administrator Email Address  
 servicedesk@aalto.fi  
 Email address of individual (or distribution list) who will receive error messages.  
 Hide Username  
 For the case when a screen-friendly username is not provided as part of the set of released attributes from the IdP. When checked, this setting prevents a user's unique identifier from being shown in several places in the webstore UI.  
 Logout Redirect URL  
 The URL a user will be redirected to following a logout from the webstore and the Shibboleth Service Provider.  
 Enable Diagnostic Mode  
 If enabled, access logs activity will be displayed on the Diagnostics tab. The detailed view of these may be useful in integration troubleshooting.  
 Restrict Eligibility Scope  
 If checked, eligibility attributes (e.g. eduPersonScopedAffiliation) will only be processed for users with accompanying organizational unit attributes (e.g. ou, eduPersonOrgUnitDN). The purpose of this is to reduce the scope of eligibility to a sub-organizational level, e.g. departmental webstores.



## Käyttövaltuuksien määrittäminen palvelussa organisaatiotasolla

- Ylläpidon www-käyttöliittymässä organization-sivun asetukset:
  - External Organization Code määrittelee tunnisteeseen, 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.”*

Organization Code

Identifier for organization assigned by organization it is managed by

External Organization Code

GroupCode

Code supplied by the organization itself or its parent to identify it in exchanges such as Integrated User Verification

## Käyttövaltuuksien määrittäminen palvelussa ryhmätasolla

- Luotiin uusi ryhmä webstore\_users, jolle määritettiin haluttu tunniste

**User Group**  
**webstore\_users**

Details Manage Members

Users > User Groups > Details

Name\*  
 webstore\_users

Languages...

Based on User Group  
 Students/Faculty/Staff

User Group Class\*  
 Academic Statuses

User Group Code  
 groupCode

Sector\*  
 Education

## Käyttövaltuuksienhallinta kotiorganisaatioissa

- 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

## 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!

## Q & A

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

# Kiitos!