Solutions for Access Control

Light weight group management, access control and authorization

SWITCH
Serving Swiss Universities

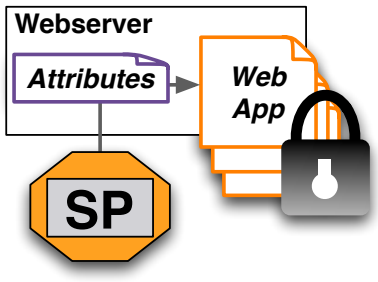
SWITCHaai Team
aai@switch.ch

Situation

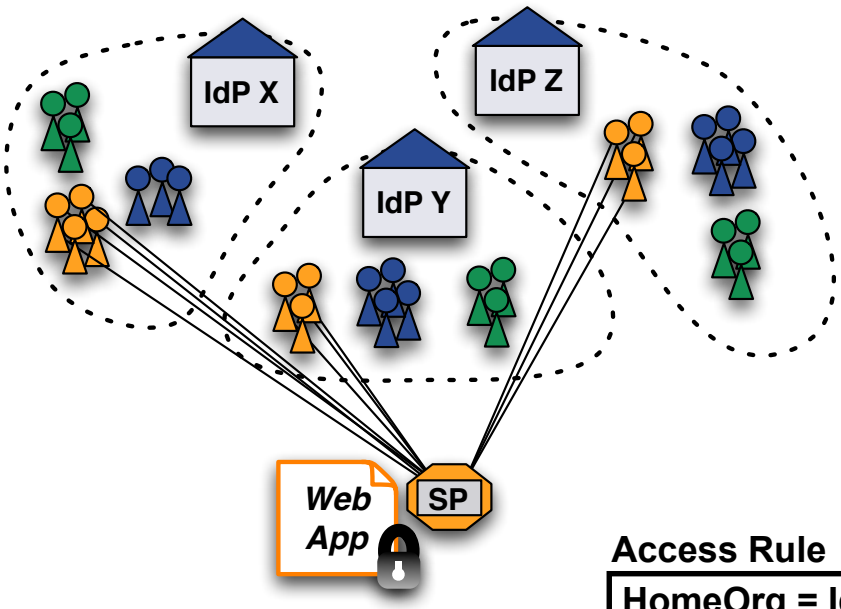
- Grant access to specific group of people
- All users have an AAI account
- Overhead for group administration should be small

- **Real life example:**

  The slides/photos of this workshop shall only be accessible by all people who attended this meeting.



Case 1: Users share common attributes

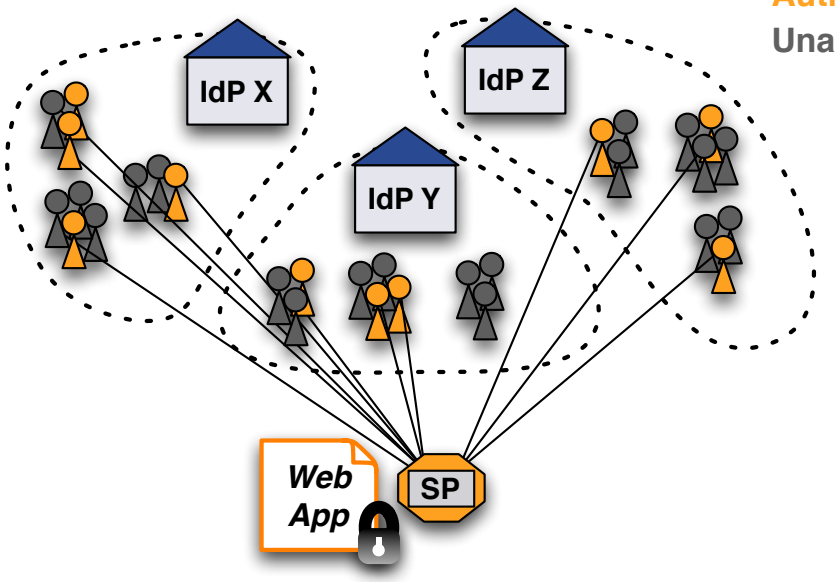


Medicine students (authorized)
Chemistry students
Staff

Access Rule

HomeOrg = IdP X| IdP Y| IdP Z
Affiliation = Student
StudyBranch = Medicine

Case 2: No common user attributes



Authorized
Unauthorized

Without a shared user attribute, no simple access control rule can be created

Solution 1: Create a common attribute

- Add a common atttribute to user's identity, e.g. an entitlement attribute

Access Rule

Require entitlement *urn:mace:rediris.es:entitlement:wiki:jra5*

⊕
- Very simple solution

⊖
- Additional work for user directory administrator
- Difficult to efficiently manage many entitlement values
- Only IdP admin can manage access
- **Only works for users from same organisation**

Solution 2.a: Use uniqueIDs or email

1. Get unique IDs or (AAI) email addresses from users
2. Create access rules like:

Access Rule

require uniqueID *465@idp-x.ch 234@idp-y.ch* […]
require email *hans.muster@idpx.ch pierre.m@idpz.ch* […]

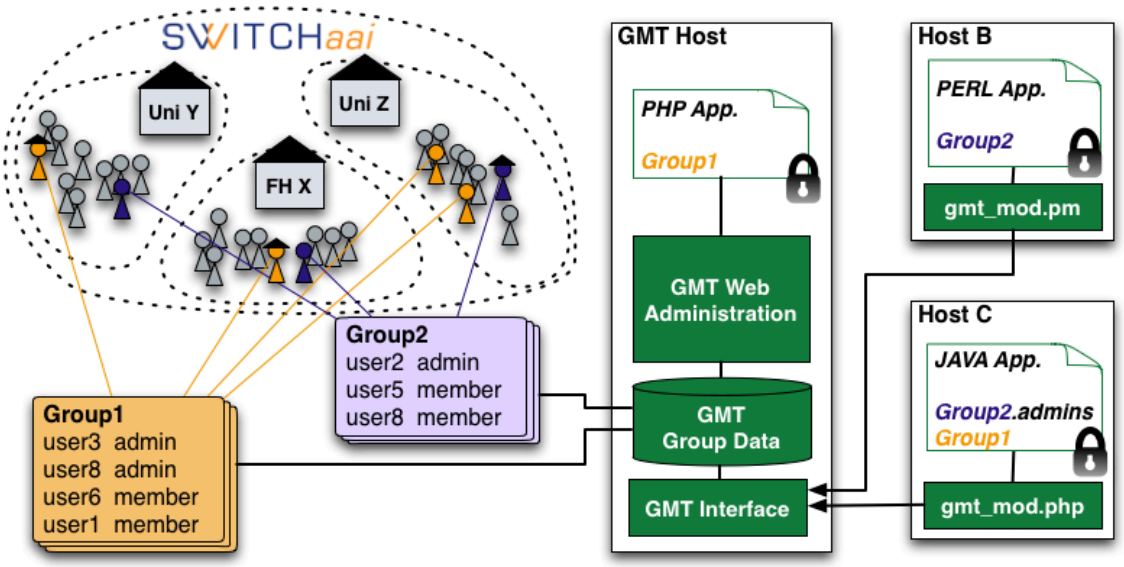
⊕
- Straight-forward solution

⊖
- SP administrator must know unique ID/Email address
- Difficult to efficiently manage for many users/apps
- **Only SP admin can manage access**

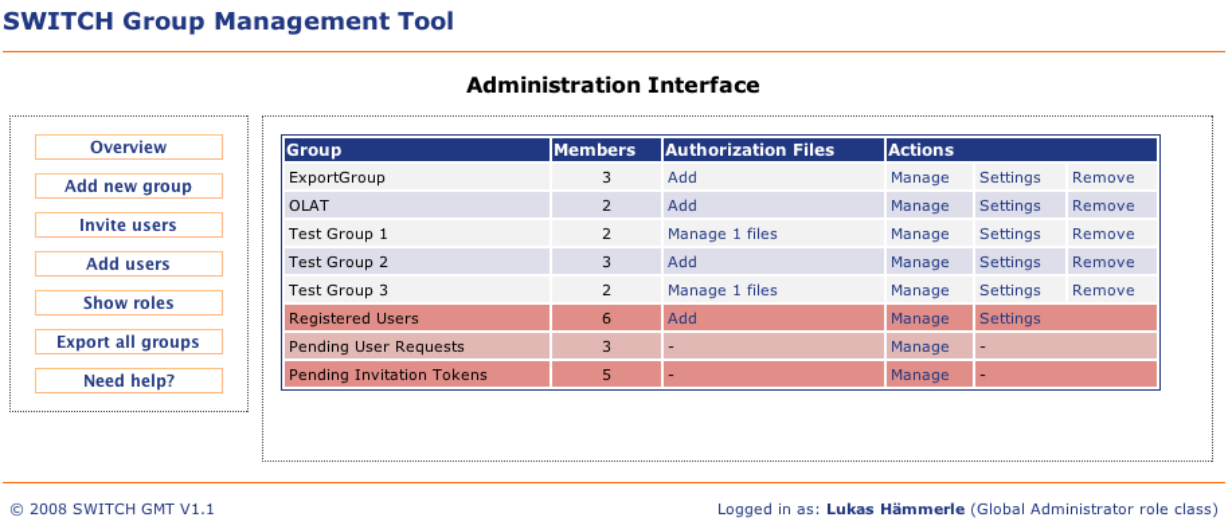
Solution 2.b: Group Management Tool

- Web based OpenSource PHP tool develop by SWITCH
- Manages multiple groups to protect multiple applications
- Users can be:
  - Invited to a group via email
  - Added to a group with a password
  - Added to a group based on their attributes
  - Moderated after they request to join a group
- GMT generates authorization files (Apache and Shibboleth)
  - Only works same host as GMT
- API and libraries for authorization on remote hosts

GMT Overview



GMT Administration Interface



GMT Authorization File Example

- Multiple groups can write to same authorization file
- Example of an .htaccess file

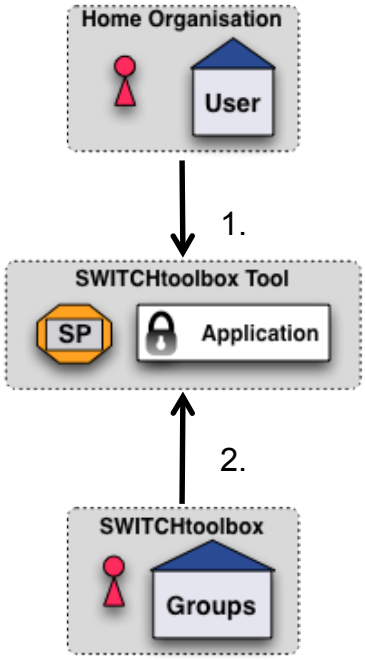
```
# Group Management Tool: Apache Authorization File
# DON'T EDIT LINES THAT CONTAIN ###
# AND ALSO DON'T REMOVE THE FOLLOWING TWO DIRECTIVES
AuthType shibboleth
ShibRequireSession On

require placeholder never.match

###START:Test_Group_1###
require uniqueID 023sdf-345fdg-23401@unizh.ch
require uniqueID 3141324sdd592@ethz.ch
###END:Test_Group_1###
```

Solution 2.c: SWITCHtoolbox

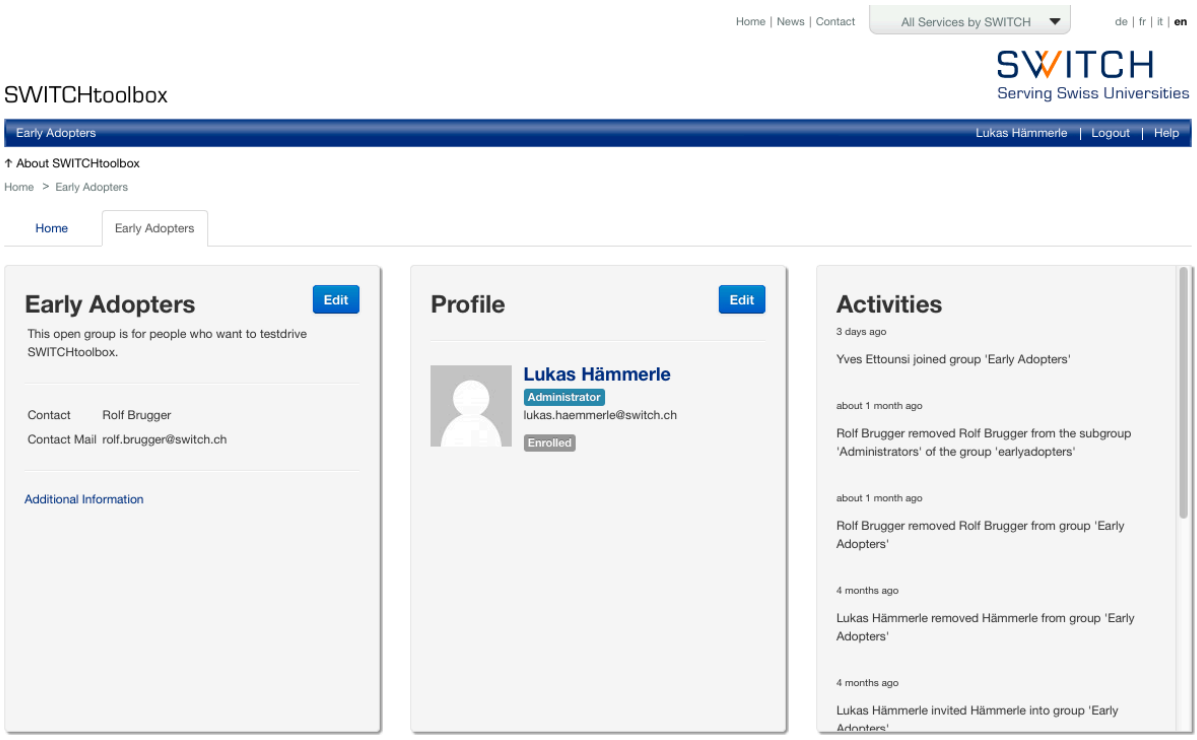
- Service Provider aggregates:
  - identity information from users's IdP
  - group information from SWITCHtoolbox IdP
- Application receives group membership information like any other Shibboleth attribute
- Everybody can create groups
- Allows easy access control rules



Access Rule

require isMemberOf https://toolbox.switch.ch/mygroup

SWITCHtoolbox Administration



Add a Service as Tool

- SP needs only minor configuration change to be tool
- Tool can be public or private
  - Public tools can be subscribed/accessed by many different groups
- SWITCH offers already three public tools:
  - Wiki, Document Storage, Mailinglist
- Webpage: http://www.switch.ch/toolbox/

Summary

- GMT and SWITCHtoolbox are very similar
- GMT has to be installed and maintained yourself
  - Allows customization
  - Suited for few groups with few users
  - Only protects applications on same host or requires libraries
- SWITCHtoolbox is a service offered by SWITCH
  - Allows easier integration of application
  - Can manage hundreds of groups and sub groups
  - No software libraries required to protect remote applications
  - Multilingual
- **SWITCHtoolbox recommended in the long term!**