

# Solutions for Access Control

Light weight group management, access control and authorization



# SWITCH

SWITCHaai Team  
aai@switch.ch

## Agenda

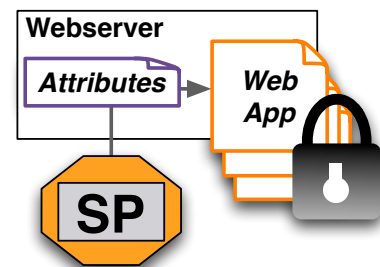
- The problem statement
- Two major cases
  - common attribute value(s) exists
  - no common attribute value(s) exists
- Two solutions
  - Introduce a common attribute value
  - Still no common attribute
    - \* Manage the group 'by hand'
    - \* Manage it with 'Group Management Tool' or 'Toolbox'

## Situation

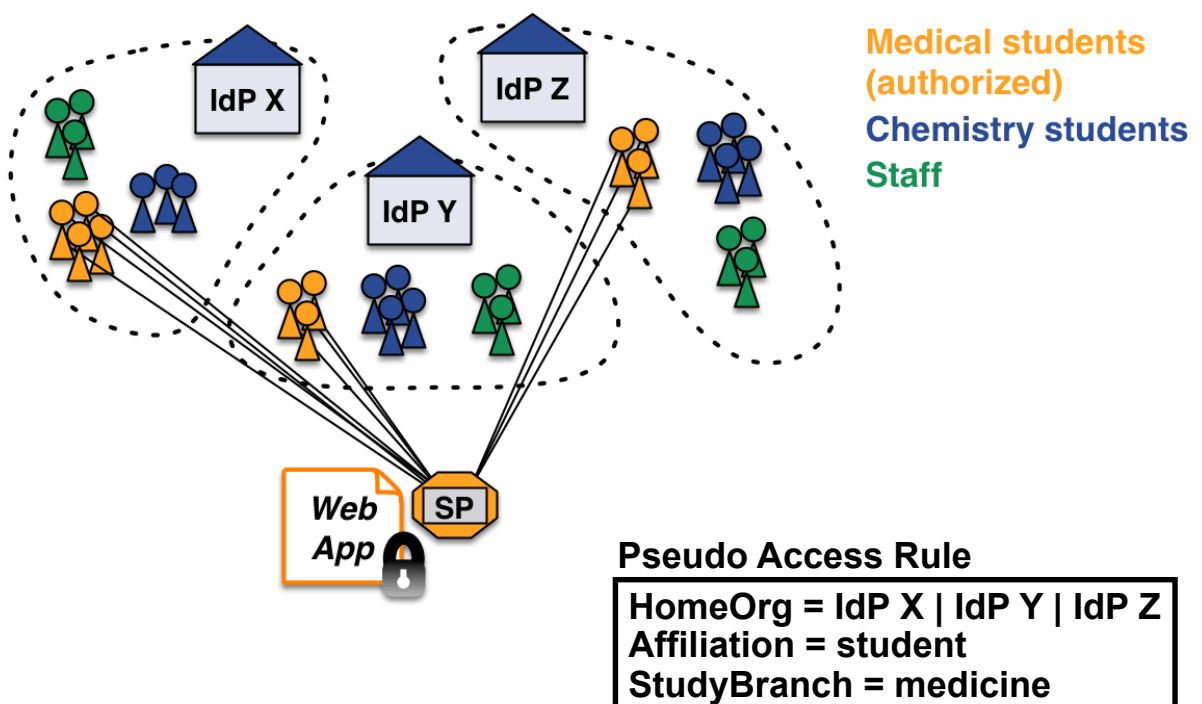
- Grant access to a specific group of people
- All users have an AAI account
- Overhead for group administration should be small

- **Real life example:**

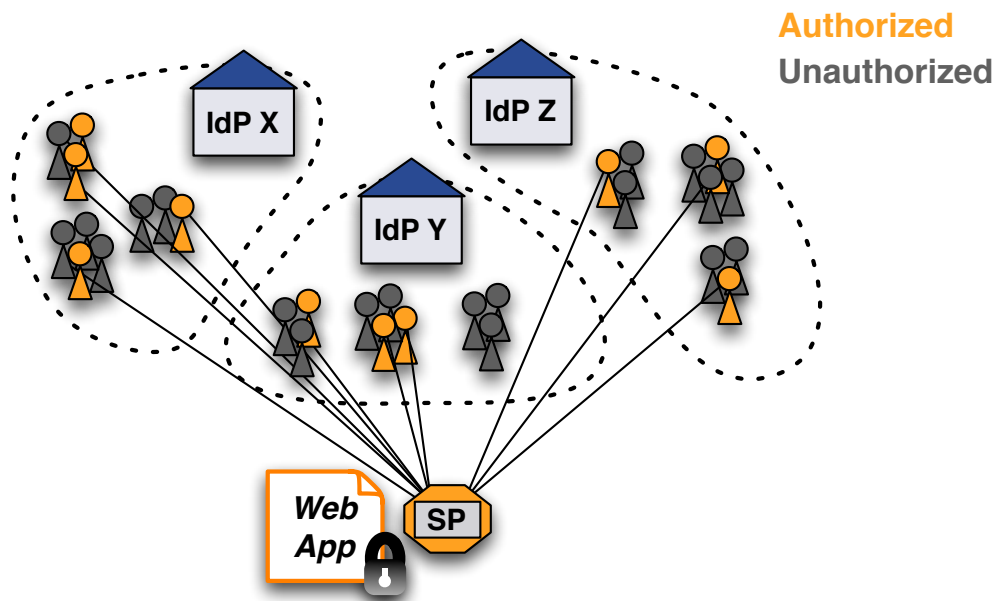
*The slides/photos of this workshop shall only be accessible by all people who attended this meeting.*



## Case 1: Users share common attributes



## Case 2: No common user attributes



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

## Solution 1: Create a common attribute

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

### Pseudo 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 email addresses from users
2. Create access rules like:

**Note:** Email address is less suited, it might get reassigned!

### Pseudo Access Rule

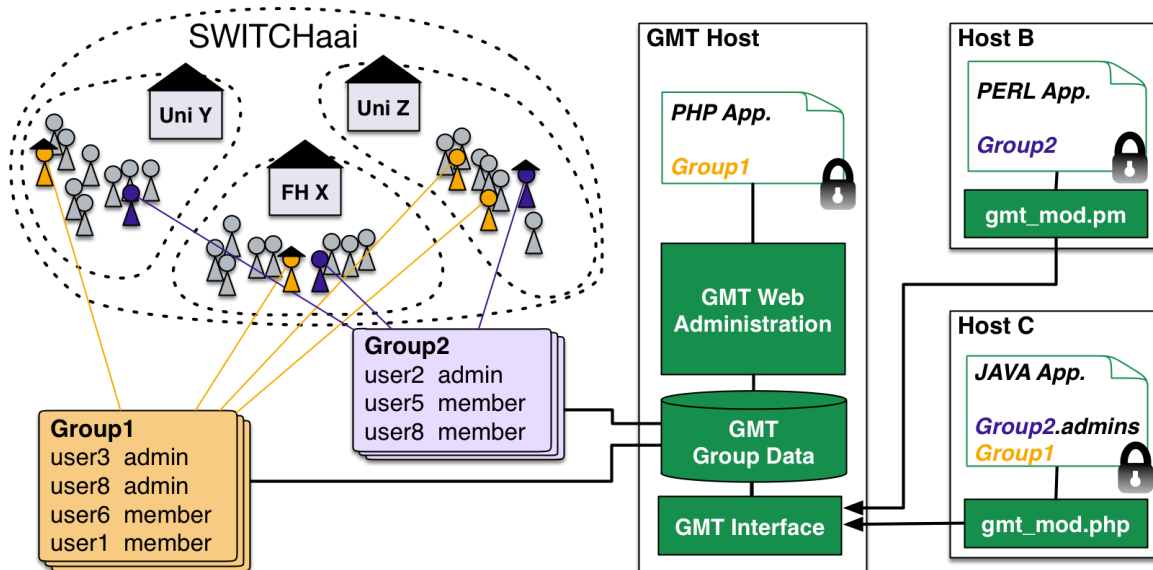
```
require uniqueID 465@idp-x.ch 234@idp-y.ch [...]  
require email hans.muster@idpx.ch pierre.m@idpz.ch [...]
```

-  Straight-forward solution
-  SP administrator must know unique ID/email address
  - Difficult to efficiently manage for many users/apps
  - **Only the SP admin can manage access**

## Solution 2.b: Group Management Tool

- Web based open source PHP tool developed by SWITCH
- Manages multiple groups to protect multiple applications
- Users can be:
  - invited to a group via email
  - added to a group with a shared group password
  - added to a group based on their attributes
  - moderated after they request to join a group
- GMT generates authorization files (for Apache and Shibboleth SP)
  - this option only works on the same host as the GMT
- API and libraries for authorization on remote hosts

# GMT Overview



<https://www.switch.ch/aai/gmt>

# GMT Administration Interface

## SWITCH Group Management Tool

### Administration Interface

- [Overview](#)
- [Add new group](#)
- [Invite users](#)
- [Add users](#)
- [Show roles](#)
- [Export all groups](#)
- [Need help?](#)

Group	Members	Authorization Files	Actions		
ExportGroup	3	Add	Manage	Settings	Remove
OLAT	2	Add	Manage	Settings	Remove
Test Group 1	2	Manage 1 files	Manage	Settings	Remove
Test Group 2	3	Add	Manage	Settings	Remove
Test Group 3	2	Manage 1 files	Manage	Settings	Remove
<b>Registered Users</b>	<b>6</b>	<b>Add</b>	<b>Manage</b>	<b>Settings</b>	
Pending User Requests	3	-	Manage	-	
Pending Invitation Tokens	5	-	Manage	-	

## 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

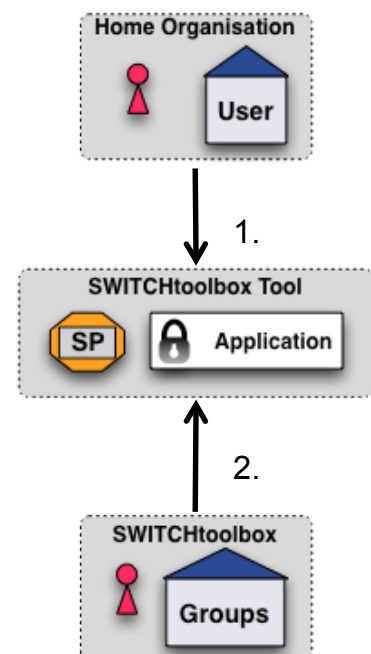
###START:Test_Group_1###
require uniqueID 023sdf-345fdg-23401@unizh.ch
require uniqueID 3141324sdd592@ethz.ch
###END:Test_Group_1###
```

## 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

### Pseudo Access Rule

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



## Early Adopters

Edit

This open group is for people who want to testdrive SWITCHtoolbox.

Contact Rolf Brugger  
Contact Mail rolf.brugger@switch.ch

Additional Information

## Profile

Edit



**Lukas Hämmerle**

Administrator  
lukas.haemmerle@switch.ch

Enrolled

## Activities

3 days ago

Yves Ettoussi joined group 'Early Adopters'

about 1 month ago

Rolf Brugger removed Rolf Brugger from the subgroup 'Administrators' of the group 'earlyadopters'

about 1 month ago

Rolf Brugger removed Rolf Brugger from group 'Early Adopters'

4 months ago

Lukas Hämmerle removed Hämmerle from group 'Early Adopters'

4 months ago

Lukas Hämmerle invited Hämmerle into group 'Early Adopters'

## Add a Service as Tool

- SP needs only minor config changes to become a tool
- Tool can be public or private
  - Public tools can be subscribed/accessed by many different groups
- SWITCH offers these public tools:
  - Document Filing, Discussion Forum, Mailinglist, SWITCHinteract, SWITCHcast, Wiki

<https://www.switch.ch/toolbox/>

## Summary

- GMT and SWITCHtoolbox are 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 many of groups and sub groups of moderate size
  - No software libraries required to protect remote applications
  - Multilingual