SWITCH

The Swiss Education & Research Network

Group Management Tool

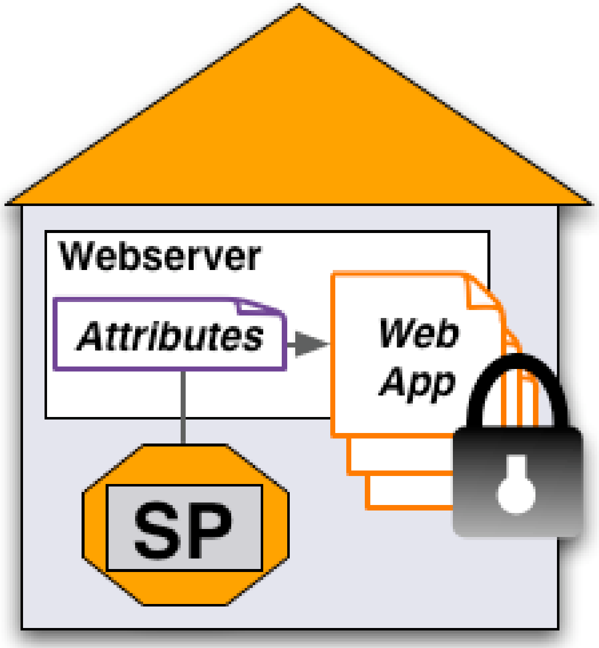
Lukas Haemmerle

haemmerle@switch.ch

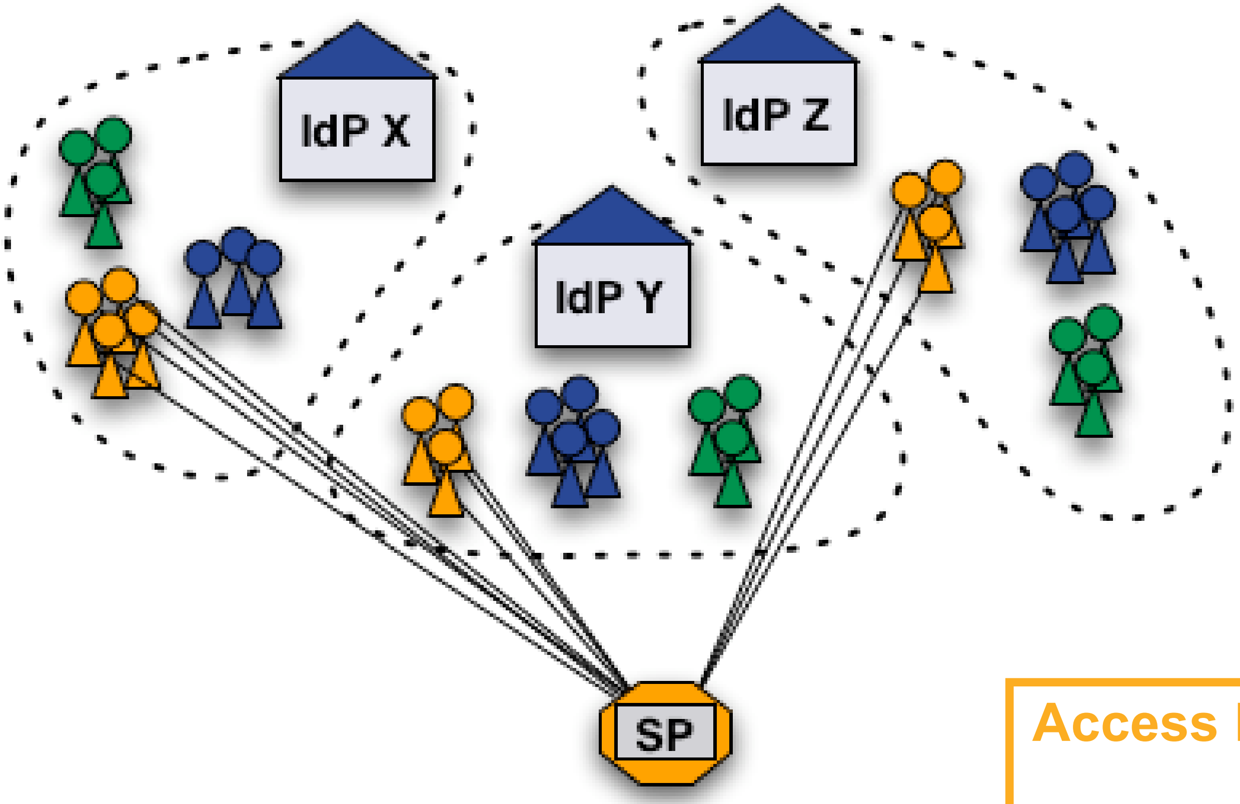
Situation

- Web application with more than 10 users
- Web application must be protected
- Access restricted to certain users
- Shibboleth SP is available on the same host

User authorization with Shibboleth



Case 1: Users share common attributes

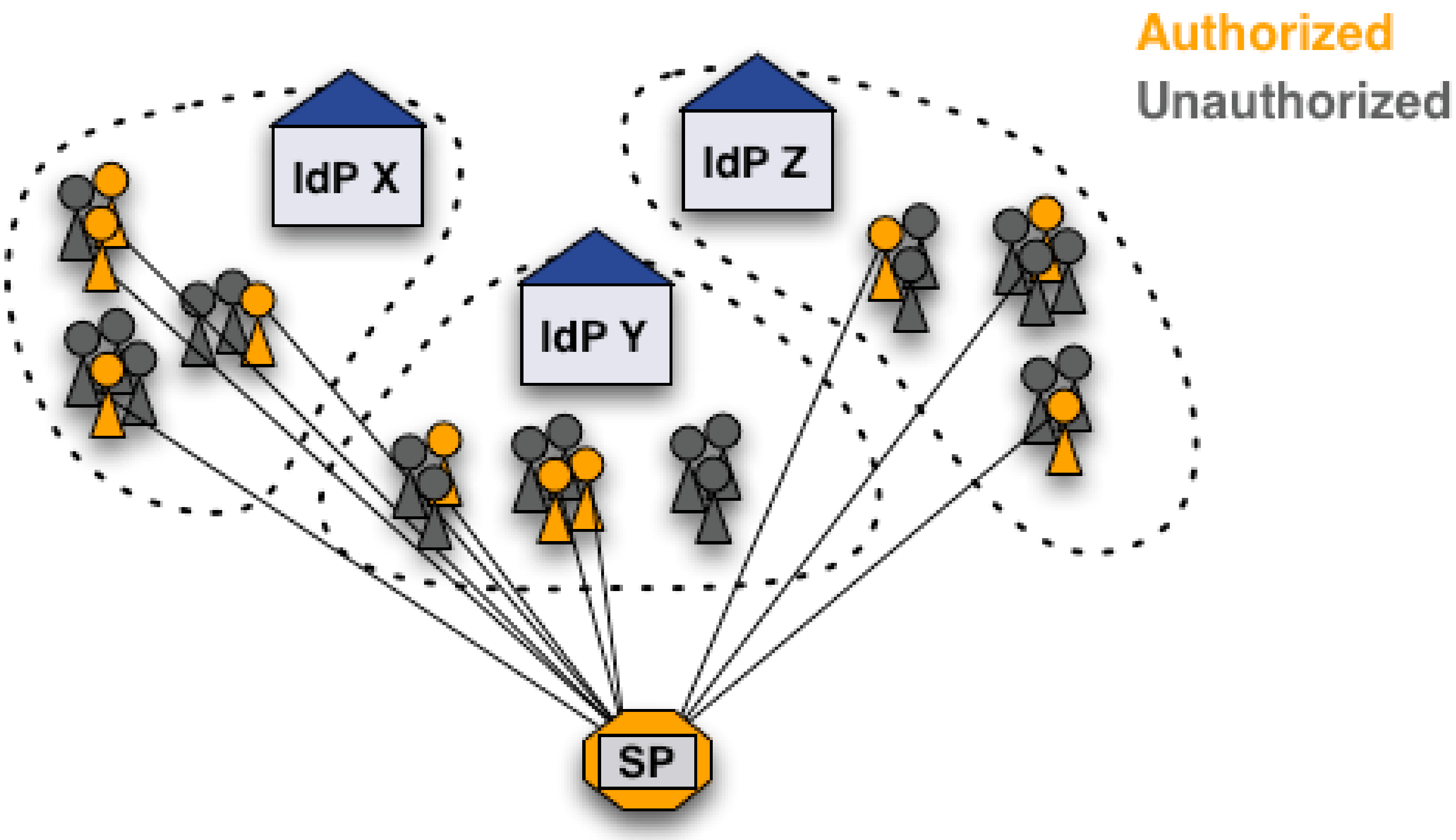


Medicine students (authorized)
Chemistry students
Staff

Access Rule

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

Case 2: No common user attributes



How can these users be authorized?

Solution 1: Create a common attribute

Add an entitlement attribute for specific users

Access Rule

Entitlement = https://www.host.ch/protected/app

⊕
- Clean solution to a difficult problem

⊖
- Additional work for user directory administrator
- Difficult to efficiently manage many entitlement values

Solution 2.a: Use uniqueIDs or email

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

Access Rule

uniqueID = 465@idpx.ch | 234@idpy.ch | …
email = hans.muster@idpx.ch | pierre.m@idpz.ch | …

➕

- Straight-forward and efficient solution

➖

- Unique ID is unknown to administrator
- Email address must be AAI email address!
- Difficult to efficiently manage for many users

Solution 2.b: Use SWITCH GMT

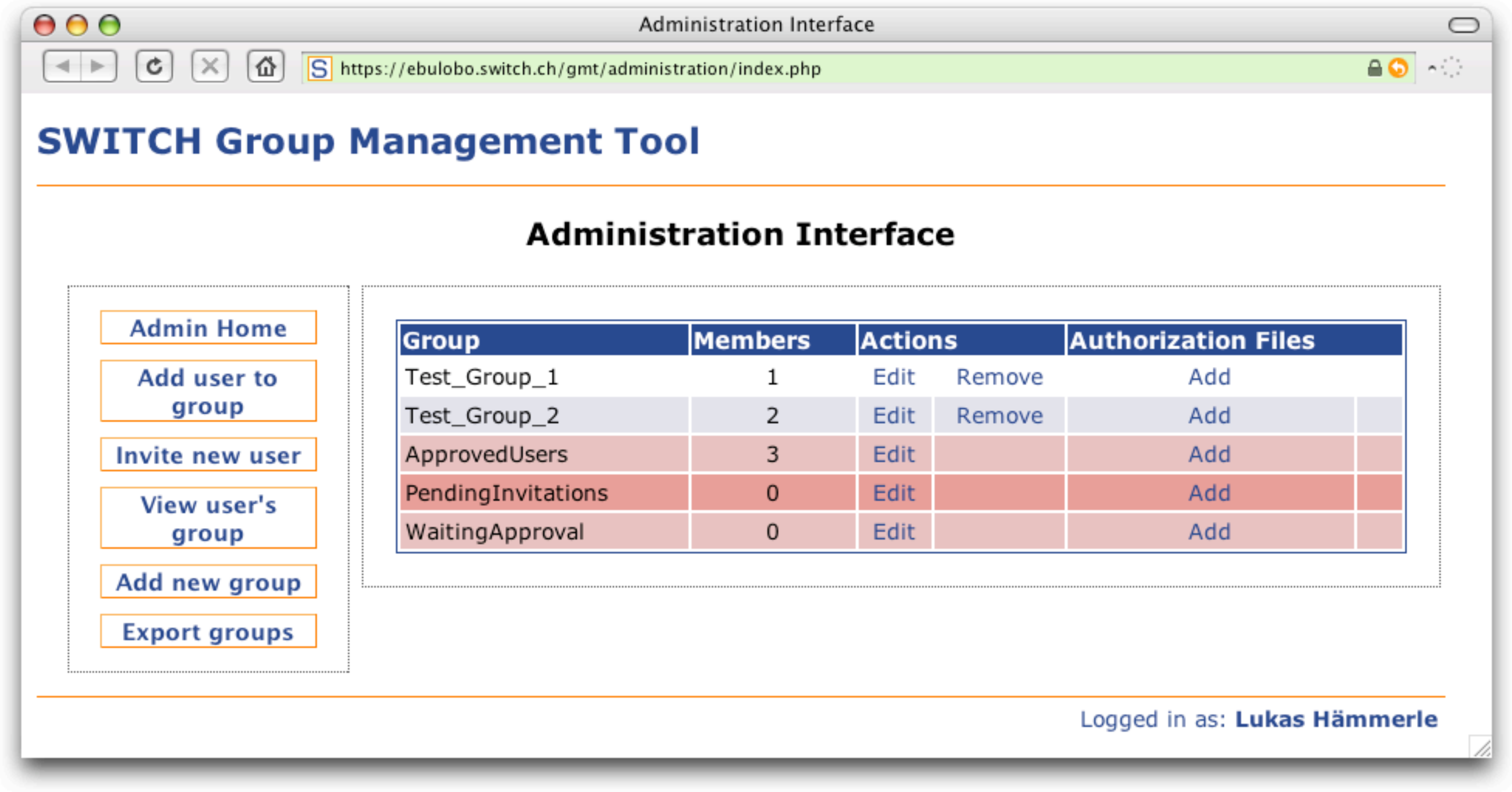
- Open Source, software (BSD license)
- Easy to install
- Light-weight PHP application
- Text files to store group data

Features

- Manage multiple groups
- Three user/admin roles with different privileges
- Invite new users to join group via email
- User can request to join a group (self-registration)
- Transfer privileges to other users
- Generate authorization files (Apache .htaccess)
- Interface for remote hosts

Administror view

SWITCH
The Swiss Education & Research Network



SWITCH Group Management Tool

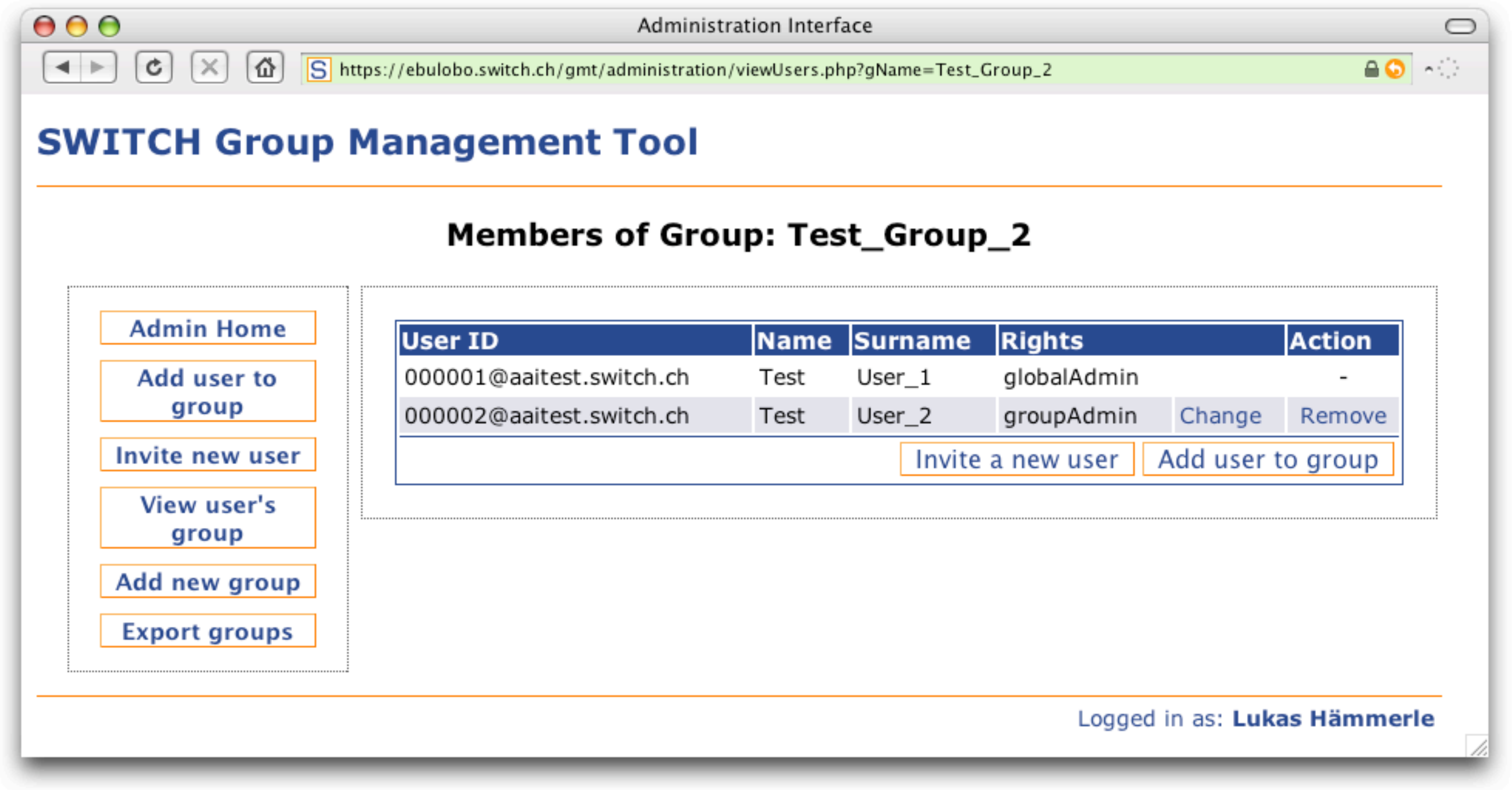
Administration Interface

Group	Members	Actions		Authorization Files
Test_Group_1	1	Edit	Remove	Add
Test_Group_2	2	Edit	Remove	Add
ApprovedUsers	3	Edit		Add
PendingInvitations	0	Edit		Add
WaitingApproval	0	Edit		Add

Logged in as: **Lukas Hämmerle**

Manage a group

SWITCH
The Swiss Education & Research Network



Administration Interface
https://ebulobo.switch.ch/gmt/administration/viewUsers.php?gName=Test_Group_2

SWITCH Group Management Tool

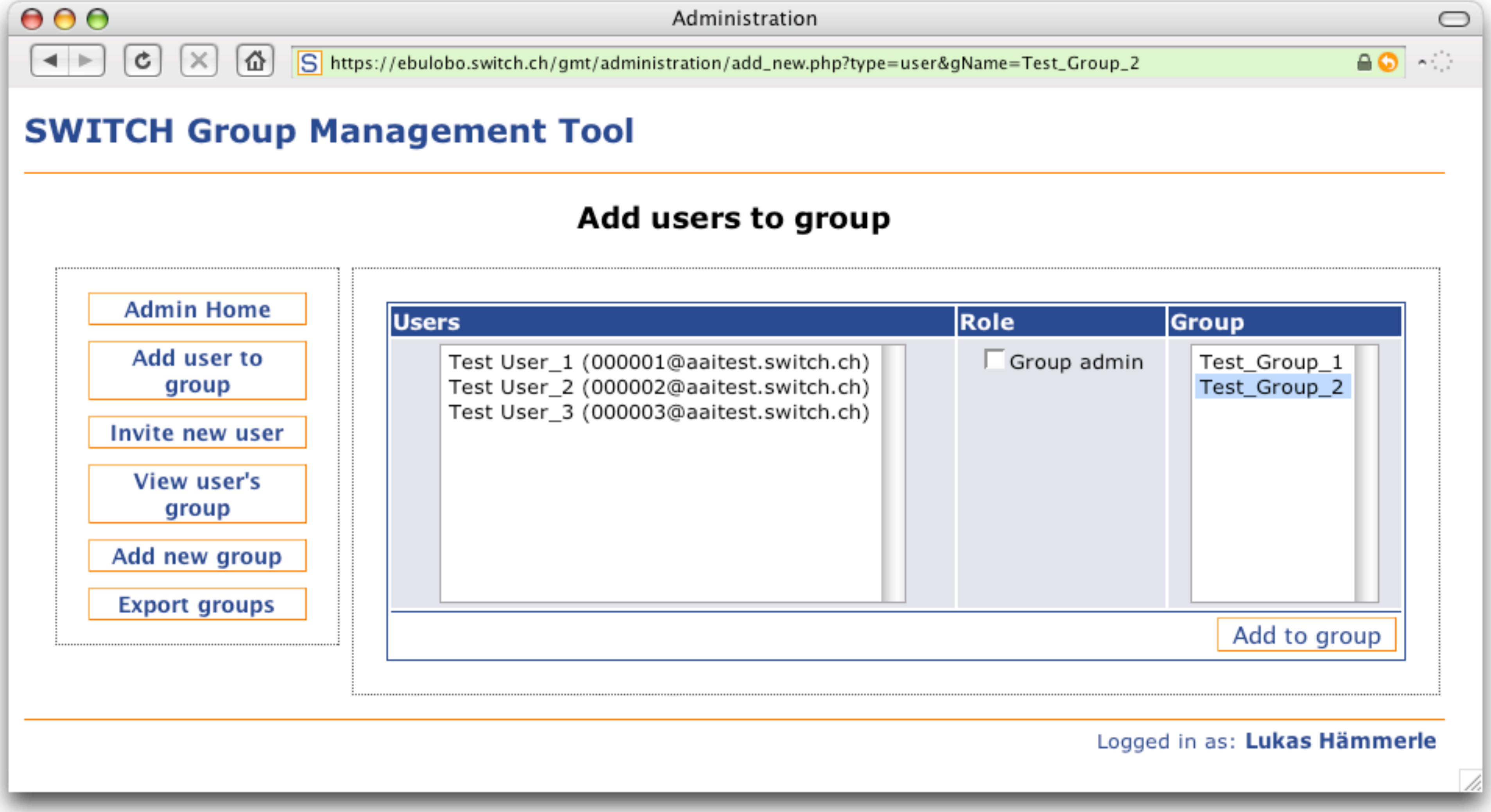
Members of Group: Test_Group_2

User ID	Name	Surname	Rights		Action
000001@aaitest.switch.ch	Test	User_1	globalAdmin		-
000002@aaitest.switch.ch	Test	User_2	groupAdmin	Change	Remove

Logged in as: **Lukas Hämmerle**

Adding users to a group

SWITCH
The Swiss Education & Research Network



Administration
https://ebulobo.switch.ch/gmt/administration/add_new.php?type=user&gName=Test_Group_2

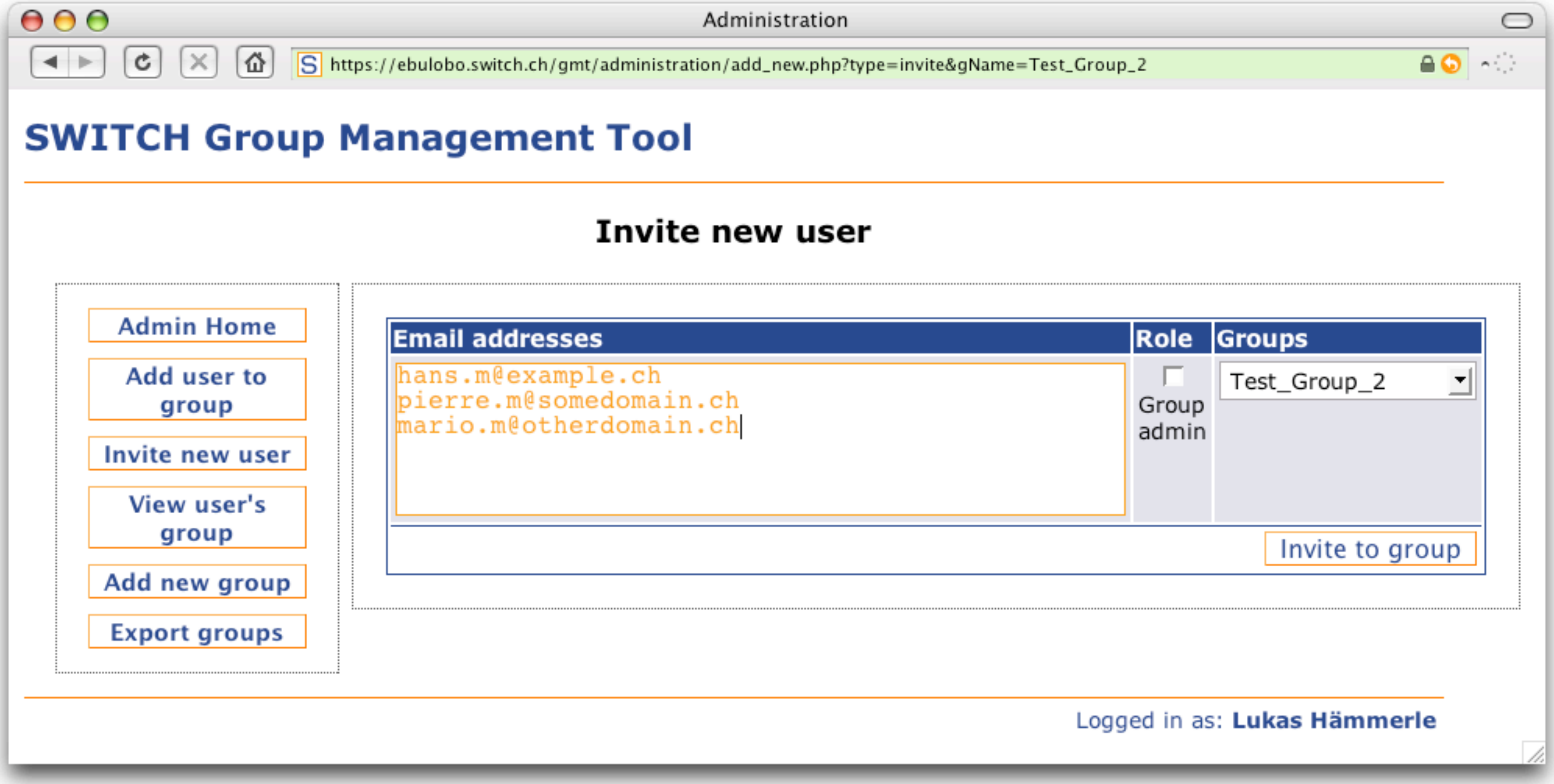
SWITCH Group Management Tool

Add users to group

Users	Role	Group
Test User_1 (000001@aaitest.switch.ch) Test User_2 (000002@aaitest.switch.ch) Test User_3 (000003@aaitest.switch.ch)	□ Group admin	Test_Group_1 Test_Group_2

Logged in as: **Lukas Hämmerle**

Inviting new users



Administration

https://ebulobo.switch.ch/gmt/administration/add_new.php?type=invite&gName=Test_Group_2

SWITCH Group Management Tool

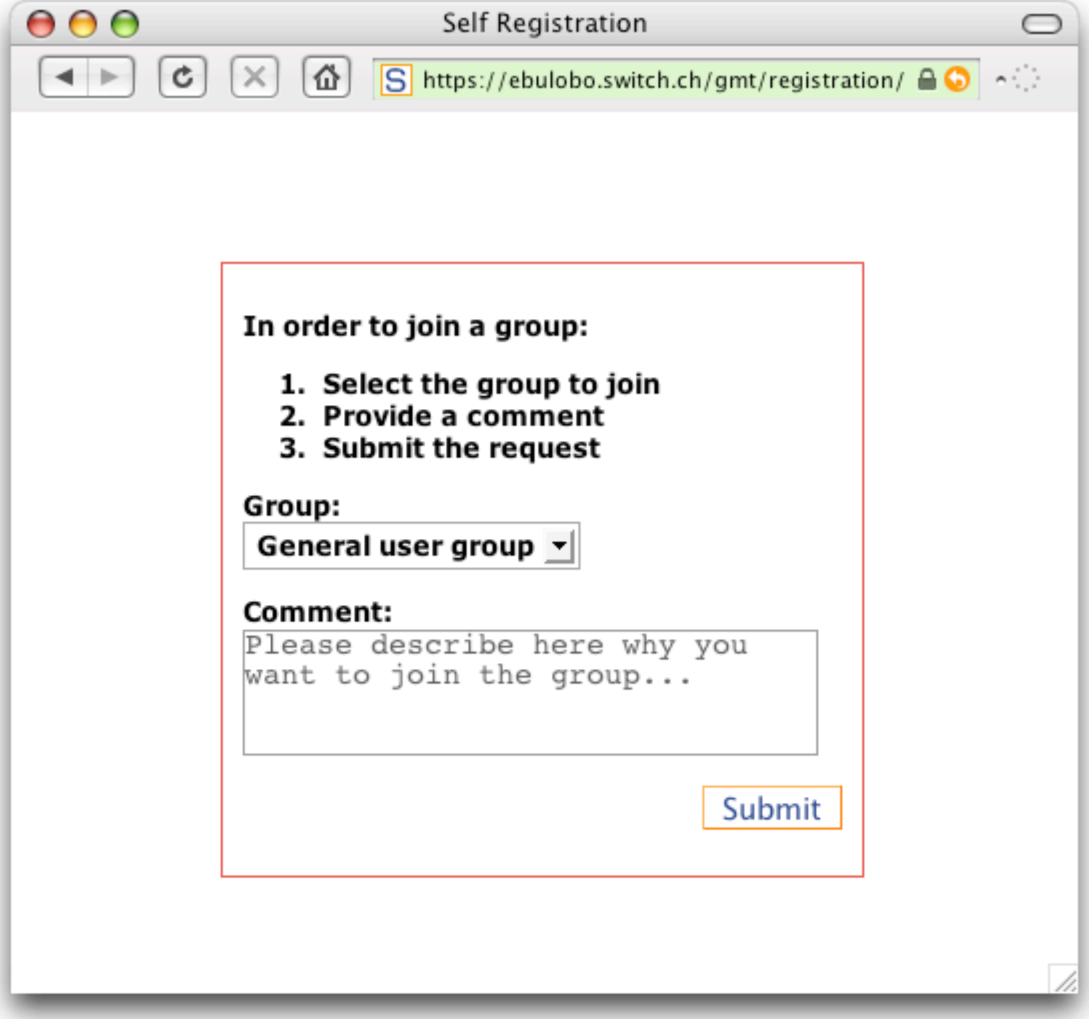
Invite new user

Email addresses	Role	Groups
hans.m@example.ch pierre.m@somedomain.ch mario.m@otherdomain.ch	□ Group admin	Test_Group_2

Logged in as: **Lukas Hämmerle**

Request to join a group

SWITCH
The Swiss Education & Research Network



In order to join a group:

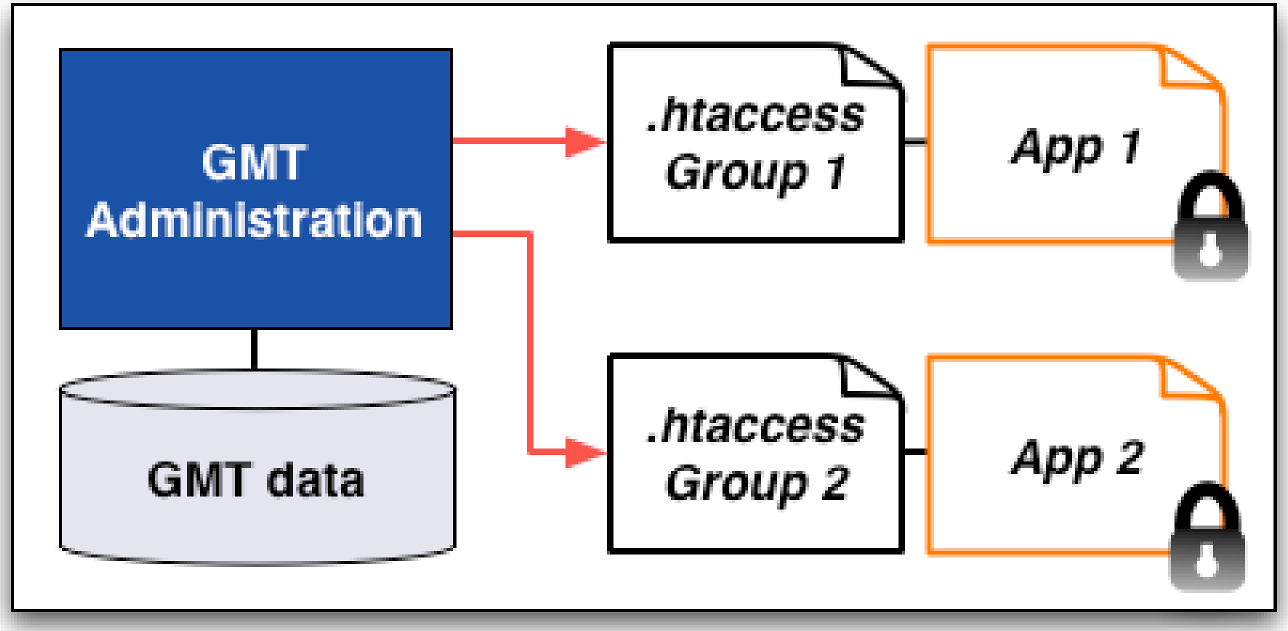
1. Select the group to join
2. Provide a comment
3. Submit the request

Group:
General user group

Comment:
Please describe here why you want to join the group...

Generate authorization files

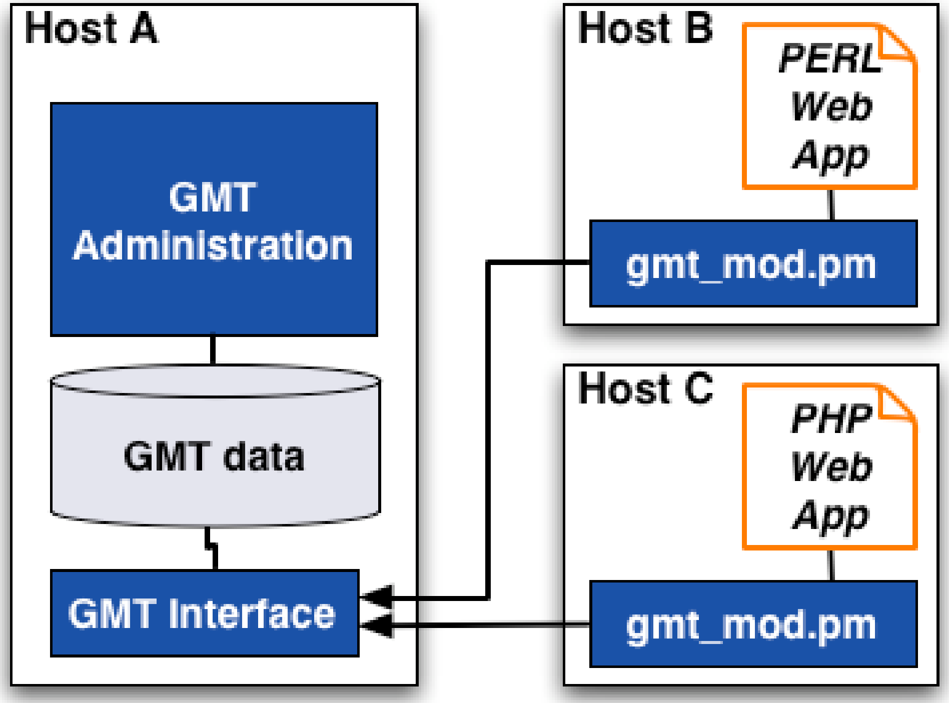
- Multiple authorization files can be generated per group
- Files are updated automatically on changes



Interface for remote hosts

PHP/PERL functions:

- *isInGroup($uniqueID, $gName)*
- *getGroupModifyURL($gName)*
- *getUserGroups($uniqueID)*
- *getStatus()*
- *getError()*



Secure queries:

- Over SSL
- Encrypted with shared key

Summary and outlook

Summary

- Convenient management of “virtual” groups
- Privileges can be transferred
- Users can request to join a group with self-registration
- Authorize users on remote servers
- Libraries available for PHP and Perl
- GMT will be available in the next few days on

http://www.switch.ch/aai/gmt

Outlook

- Generation of Shibboleth XML authorization files
- Your requested features (feedback appreciated!)

Questions

SWITCH
The Swiss Education & Research Network

Q & A

GO http://www.switch.ch/aai

aai@switch.ch