

The logo for SWITCH, featuring the word "SWITCH" in a bold, sans-serif font. The letter "W" is stylized with a blue outline and an orange fill, while the other letters are solid blue.

The Swiss Education & Research Network

Integration of Web Applications

The AAI Team <aai@switch.ch>

- Introduction
- PHP and Java Integration
- Application and Database Integration
- AAIportal
- Group Management Tool
- WAYF



SWITCH

The Swiss Education & Research Network

Shibboleth Integration for Web Applications

Lukas Hämmerle, haemmerle@switch.ch

1. As **least invasive** as possible
 - Main developers don't like massive structural changes
 - If applications changes, your solution may have to be adapted as well
2. As **modular** as possible
 - Make Shibboleth just an additional authentication method
3. As **general** as possible
 - Solution should not only be developed for your own federation
 - Mapping for federation dependent attributes is generally necessary
 - API or hook to convert federation dependent attribute values
4. As **user-friendly** as possible
 - First-time users are registered/enrolled automatically/transparently
 - Auto-update of user data after login. Optionally prevent editing user data/password
 - Most of the times there still are users that don't have yet an AAI account

Feasibility

- Is the application open source?
- Can one get the source code for development (with NDA)?
- Is there a usable API?

Approach

- Authentication? Authorization? Auto-Enrollment?
- Dual login or Shibboleth only?

Sustainability

- Can modifications be integrated in the official source tree?
- What happens after version 1.0 and future versions in general?
- Can implementation be made part of official source tree?

1. Get the source code/API documentation
2. Learn how the application is used
 - Ask the administrators and users how they actually use the application
3. Learn how the application is programmed/structured
 - This is about 50% of the whole job
4. Evaluate the different implementation solutions
 - Cross check if the users/administrators need's are fulfilled
5. Implement the solution of choice
 - This is often the most straight forward part of the job
6. Thoroughly test the implementation
 - Even better: Let experienced users/administrators test the implementation
7. Contribute your patches to the official source tree
 - You may have to adapt your code to meet the main developers coding style...
 - This process may take a while, so don't get frustrated
8. Maintain your changes if necessary
 - Make sure you get a CVS account

- **Authorize with Apache:**

httpd.conf or .htaccess protect **<Files>**, **<Directory>** or **<Location>**:

```
AuthType shibboleth
ShibRequireSession On
ShibRequireAll On
require affiliation student
require homeOrganization unizh.ch ethz.ch
```

- **Authorize within Application:**

Shibboleth attributes in Apache environment variable or HTTP request header

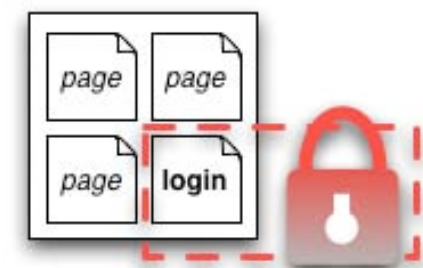
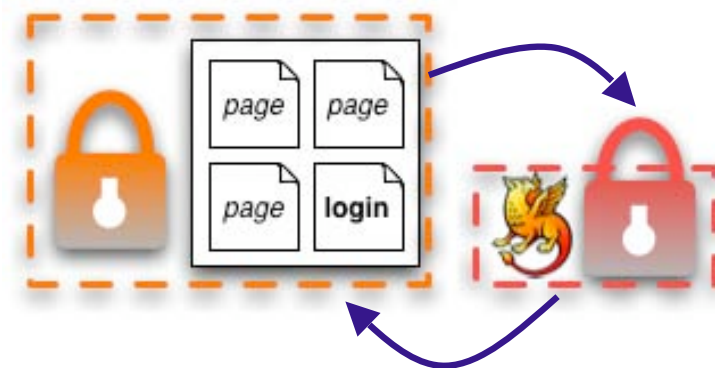
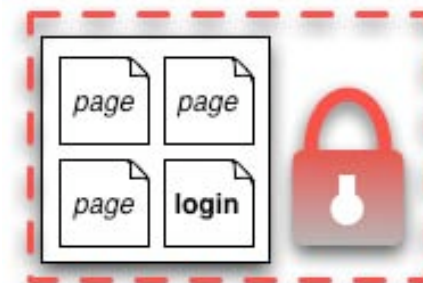
PHP: `if ($_SERVER['HTTP_SHIB_EP_AFFILIATION'] == 'staff') { authorizeUser();}`

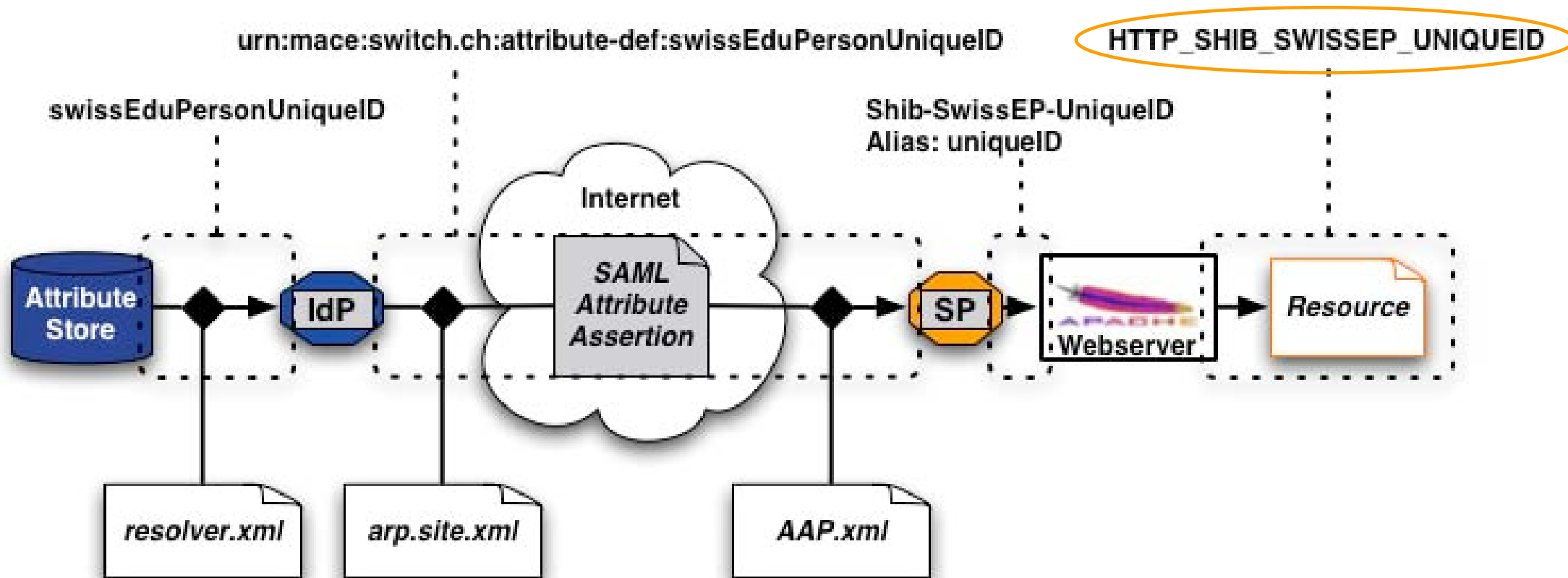
Perl: `if ($ENV{'HTTP_SHIB_EP_AFFILIATION'} == 'staff') { &authorizeUser();}`

Java: `if (request.getHeader("Shib-EP-Affiliation").equals("staff")) { authorizeUser();}`

Where to require Shibboleth session

- **Whole application with “required” Shibboleth session**
 - Easiest way to protect a set of documents
 - No dual login possible in general
 - Not user friendly because no “login page” before login
 - Problems with lost HTTP POST requests
- **Whole application with “lazy” Shibboleth session**
 - Well-suited for dual login
 - Lazy sessions are more complicated
 - Authorization can only be done in application
- **Only page that sets up application session**
 - Well-suited for dual login
 - Application can control session time-out
 - **Generally the best solution**





Attribute Resolver:
What and how to read
from Attribute Store?

Attribute Acceptance Policy:
What attributes should be accepted
by IdP and forwarded to web server?

Attribute Release Policy:
What attributes should be sent to SP?

- Login name vs Username vs Screen name
 - There is no username/login name attribute available in AAI, but often a screen name is needed
 - Generate screen name (e.g. ILIAS) or ask user for one (e.g. OLAT)

- Password that is not available/used
 - Generate a random password. Won't be used in general

- Related non-Web services like WebDAV not (yet) Shib-compatible
 - Provide way for user to set password for that service

- Federation dependent attributes and values
 - Provide mapping between Shibboleth attributes and application attributes
 - Provide hook or API to do conversion/transformation

General

- Don't get frustrated. Shibboleth **is** a bit complex!
- Attend trainings and internal workshops
- Ask only for attributes you really need
- e-learning admins like SPs with integrated WAYF
- Adapt major applications to use Shibboleth if possible
- Convince application developers to support Shibboleth

Technical

- Set up a test SP for development
- Refresh your metadata regularly
- Keep log files (respect data protection)



SWITCH

The Swiss Education & Research Network

PHP and Java Integration

Valéry Tschopp <tschopp@switch.ch>

Attribute	Apache Environment Variable	HTTP Request Header
AAI UniqueID	HTTP_SHIB_SWISSEP_UNIQUEID	Shib-SwissEP-UniqueID
Surname	HTTP_SHIB_PERSON_SURNAME	Shib-Person-surname
Given Name	HTTP_SHIB_INETORGPERSO_N_GIVENNAME	Shib-InetOrgPerson-givenName
Email	HTTP_SHIB_INETORGPERSO_N_MAIL	Shib-InetOrgPerson-mail
Affiliation	HTTP_SHIB_EP_AFFILIATION	Shib-EP-Affiliation
Entitlement	HTTP_SHIB_EP_ENTITLEMENT	Shib-EP-Entitlement
Home Organization	HTTP_SHIB_SWISSEP_HOMEORGANIZATION	Shib-SwissEP-HomeOrganization
Home Organization Type	HTTP_SHIB_SWISSEP_HOMEORGANIZATIONTYPE	Shib-SwissEP-HomeOrganizationType

- Attributes are available as environment variables for PHP, Perl, ASP, ...
- Attributes are available as HTTP request header for Java

```
<?php
// read AAI uniqueID
$uniqueid= null;
// check if set and not empty
if (isset($_SERVER['HTTP_SHIB_SWISSEP_UNIQUEID']) and
    !empty($_SERVER['HTTP_SHIB_SWISSEP_UNIQUEID']))
{
    $uniqueid= $_SERVER['HTTP_SHIB_SWISSEP_UNIQUEID'];
    // decode UTF8 to Latin1 (Surname, Given Name, Address, ...)
    $uniqueid= utf8_decode($uniqueid);
    // continue processing...
}
else {
    // Error: attribute is missing!
}
?>
```

- PHP reads Shibboleth attributes as Apache environment variables
- Attribute value can be null or empty and are UTF-8 encoded

```
public class MyHttpServlet extends HttpServlet
{
    public void doPost(HttpServletRequest request, HttpServletResponse response)
        throws IOException, ServletException {
        // get the AAI uniqueID
        String uniqueid= request.getHeader("Shib-SwissEP-UniqueID");
        // check not null and not empty
        if ( uniqueid != null && !uniqueid.equals("") ) {
            // decode UTF8 to Latin1 (Surname, Given Name, Address, ...)
            uniqueid= new String( uniqueid.getBytes("ISO-8859-1"), "UTF-8");
            // continue processing...
        }
        else {
            // Error: attribute is missing!
            throw new ServletException("Shibboleth HTTP header 'Shib-SwissEP-UniqueID'
is missing");
        }
    }
}
```

- Java reads Shibboleth attributes as HTTP request header
- Attribute value can be null or empty and are UTF-8 encoded



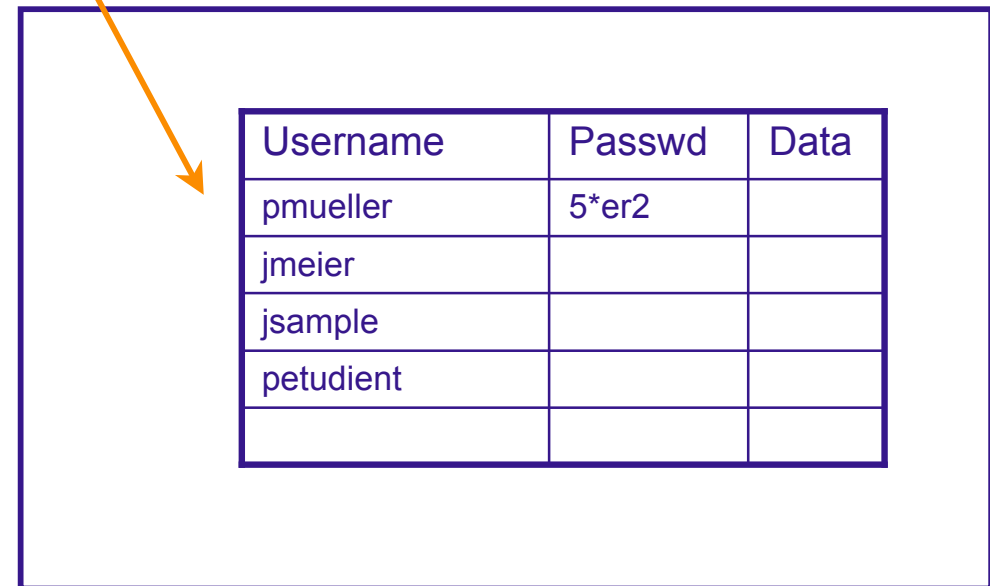
SWITCH

The Swiss Education & Research Network

Application and Database Integration

Valéry Tschopp <tschopp@switch.ch>

Username: pmueller
Password: 5*er2

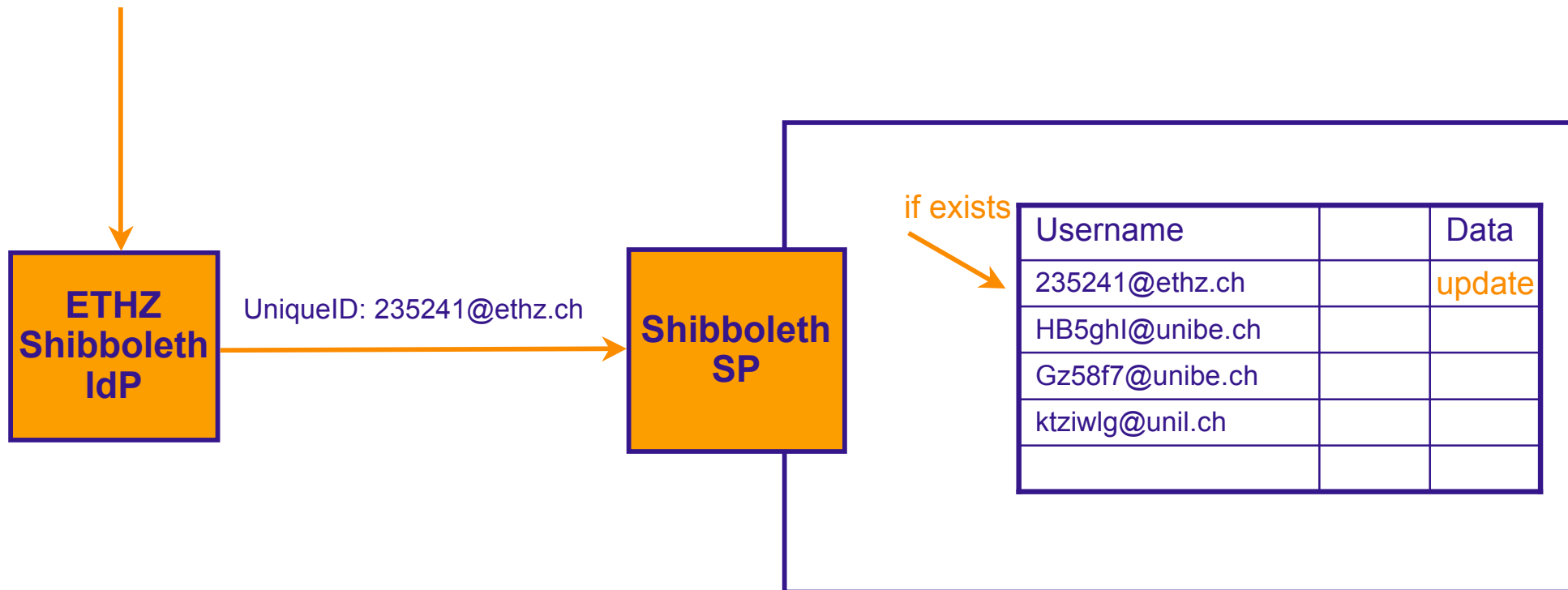


Username	Passwd	Data
pmueller	5*er2	
jmeier		
jsample		
petudiant		

- Existing application does the authorization
- It compare the username and password with the content of the database

Username: p.mueller
Password: 4rtz3w

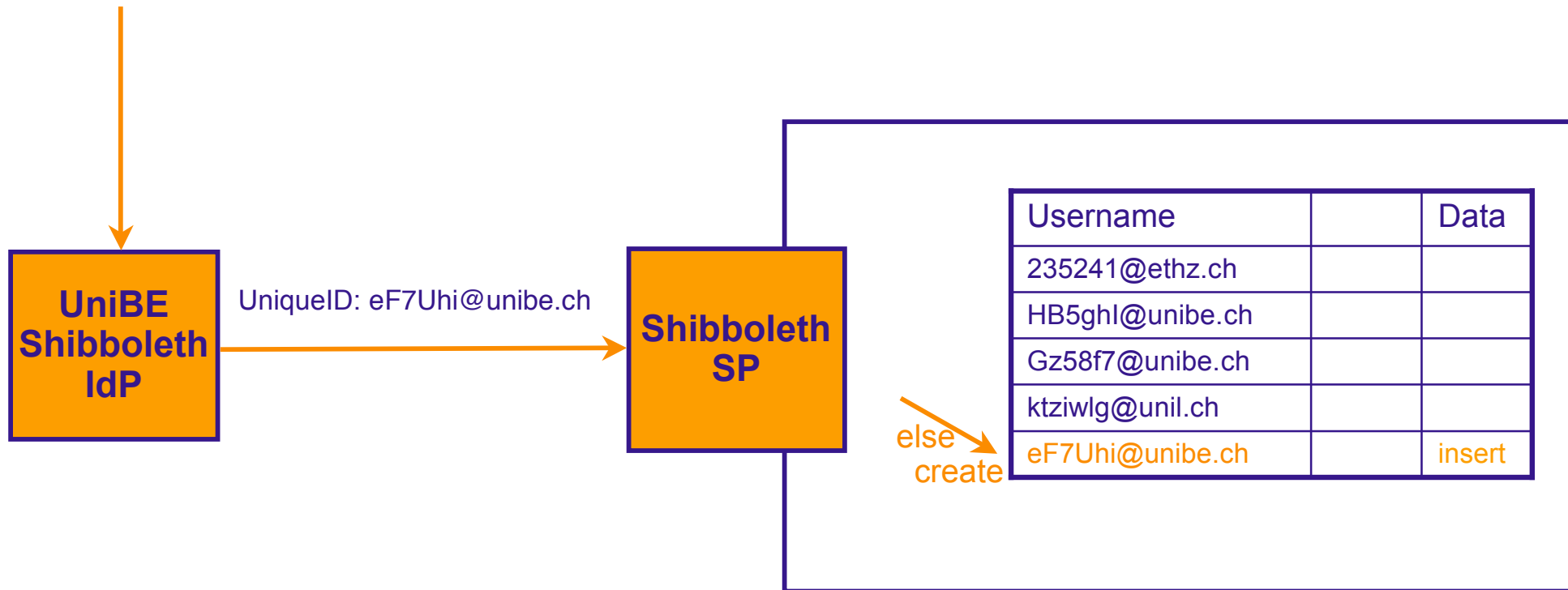
Existing user: if user exists then update data



- Shibboleth does the authorization
- Use the AAI UniqueID as username, if the user already exists update his data

Username: h.flueck
Password: 45\$iU2

New user: if user does not exist then insert data

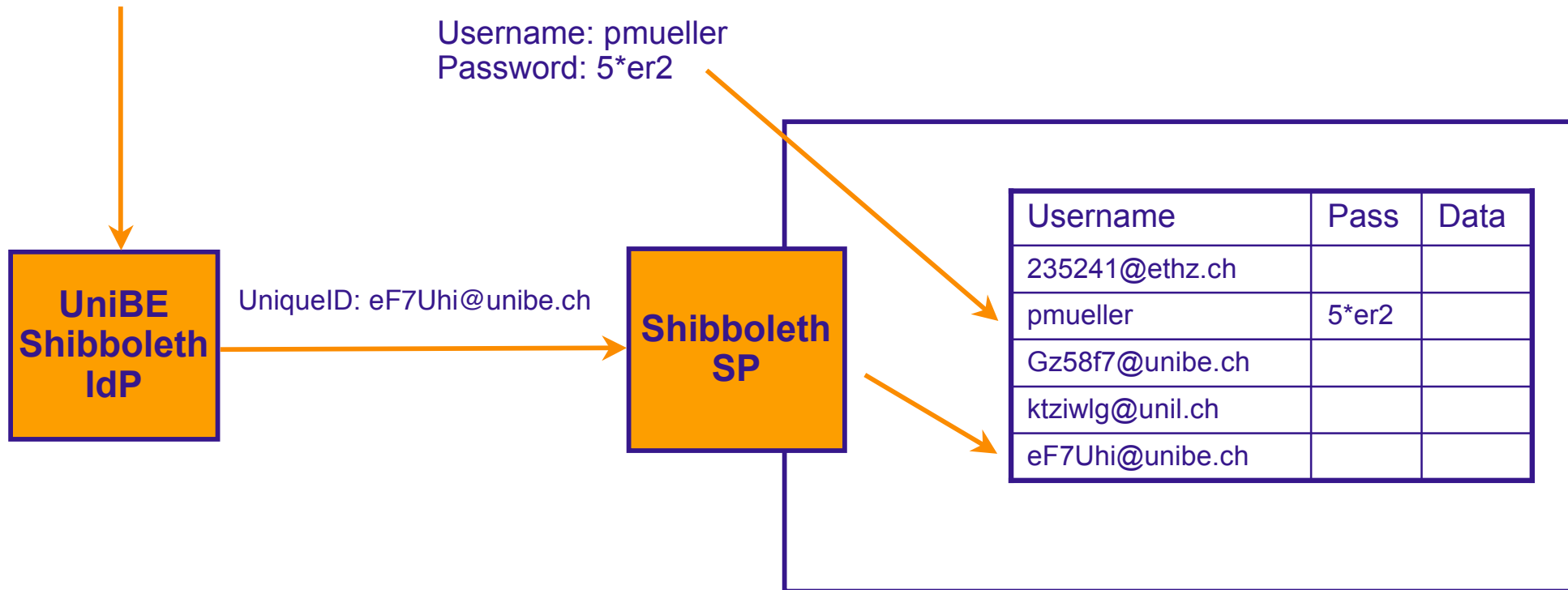


- Shibboleth does the authorization
- Use the AAI UniqueID as username, create the user if he doesn't exist (generate random password)

Username: h.flueck
Password: 45\$iU2

Dual login: Shibboleth and local users

Username: pmueller
Password: 5*er2



- Shibboleth and the application do the authorization
- For Shibboleth users update or insert data
- For local users same as before



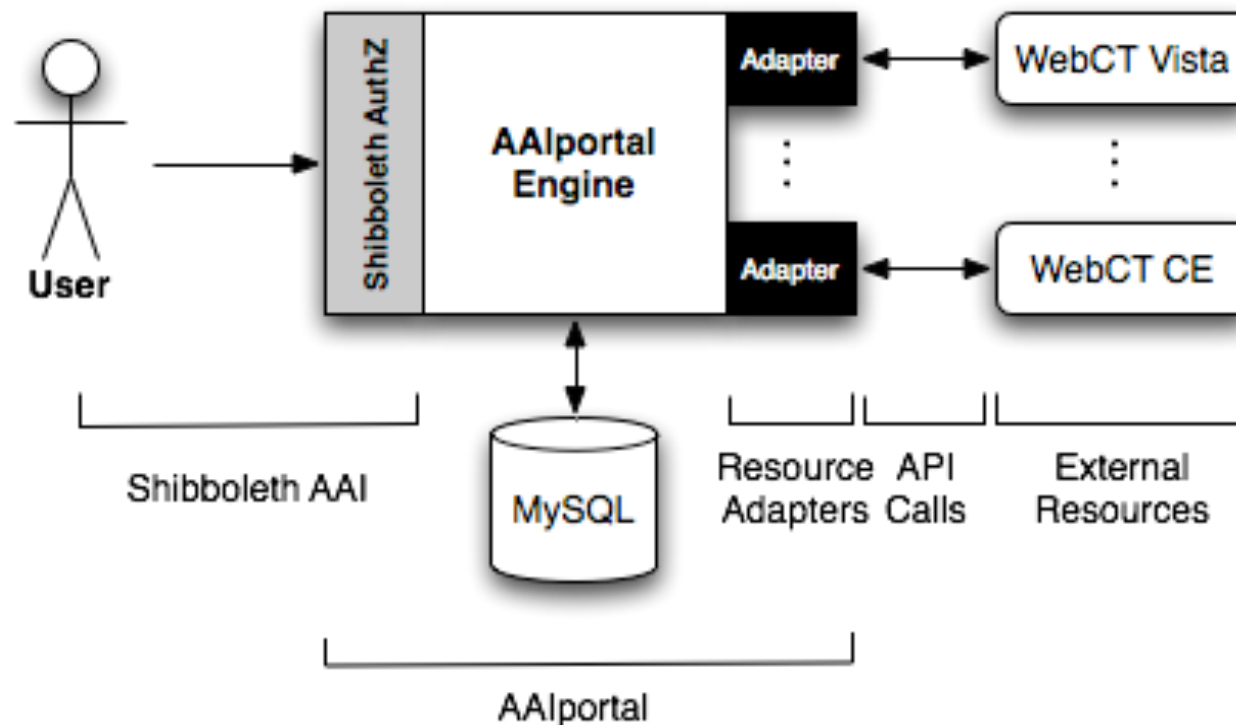
SWITCH

The Swiss Education & Research Network

AAIportal

Valéry Tschopp <tschopp@switch.ch>

- AAIportal to integrate WebCT CE 4, CE 6 and Vista
- Unified platform for course subscriptions management
- Interactive or transparent user mode



- Courses Management
- Subscriptions Management
 - Waiting list
 - Automatic subscription
 - Password subscription
- Users Management

- Interactive User Mode
- Transparent User Mode
 - Login URL: <https://aaiportal.example.ch/user/aai/login?rid=234.ADFASFASDF>

Online Demo: <https://demo.aaiportal.switch.ch/>
AAIportal Home Page: <http://aai-portal.sourceforge.net/>



SWITCH

The Swiss Education & Research Network

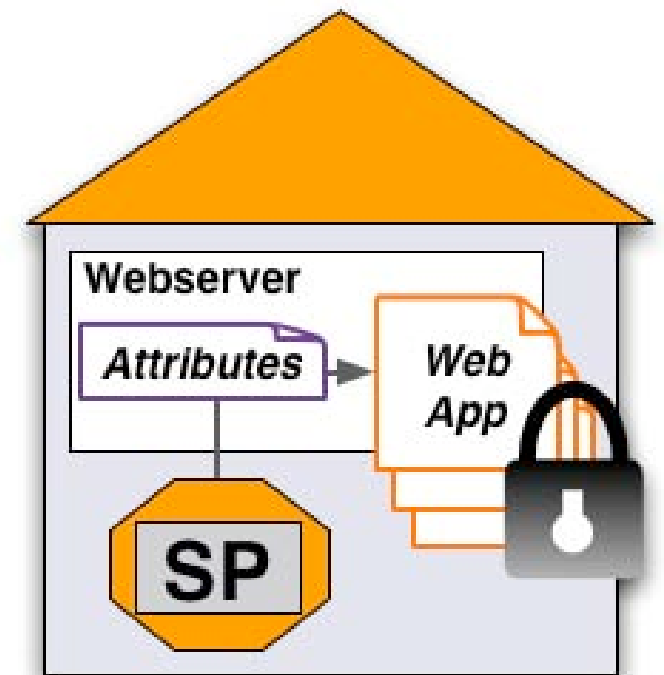
Group Management Tool

Lukas Hämmerle, haemmerle@switch.ch

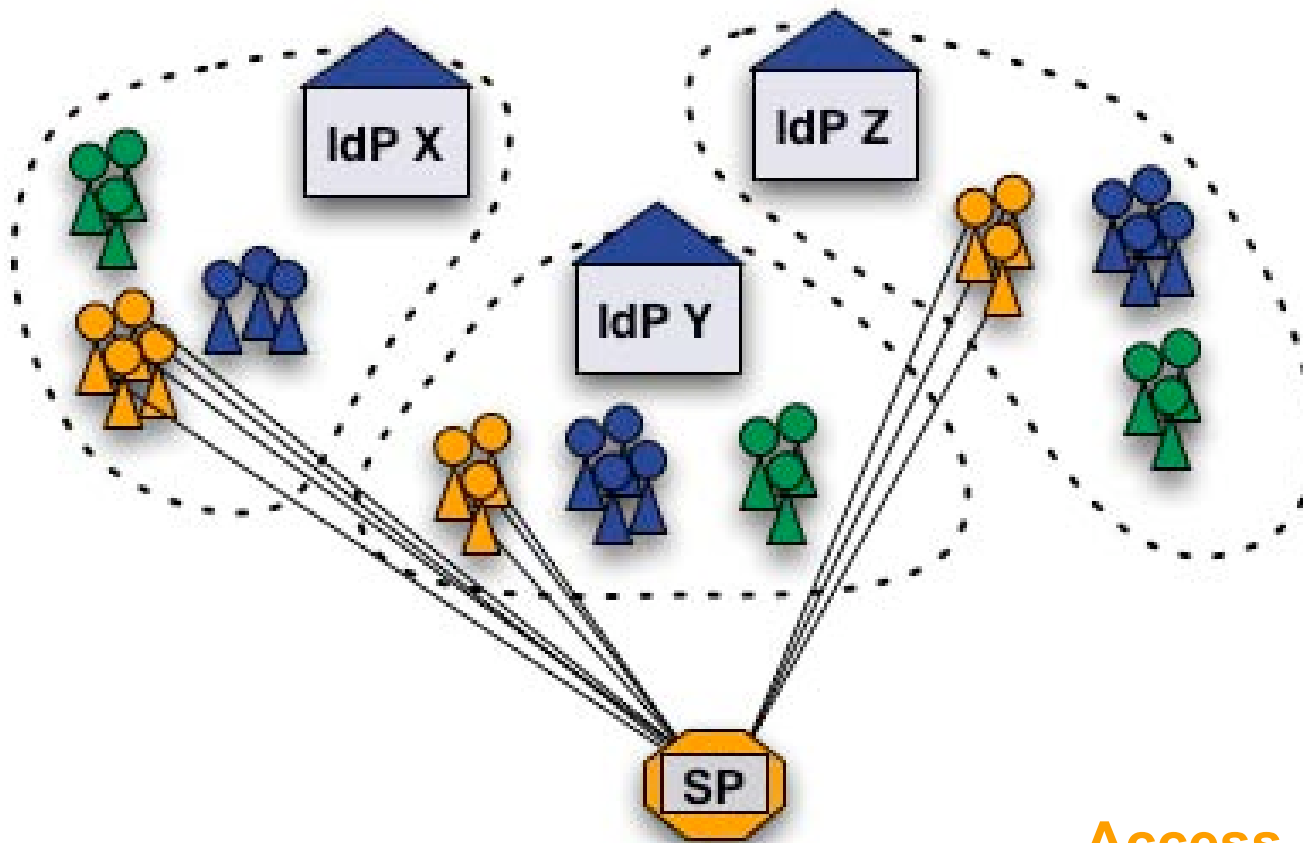
- Web application that must be protected
- Access/authorization shall be based on user groups
- Overhead for group administration shall be small
- Shibboleth/Other FIM solution available

Example:

The slides of this presentation shall only be accessible by all people attending this meeting.



Case 1: Users share common attributes



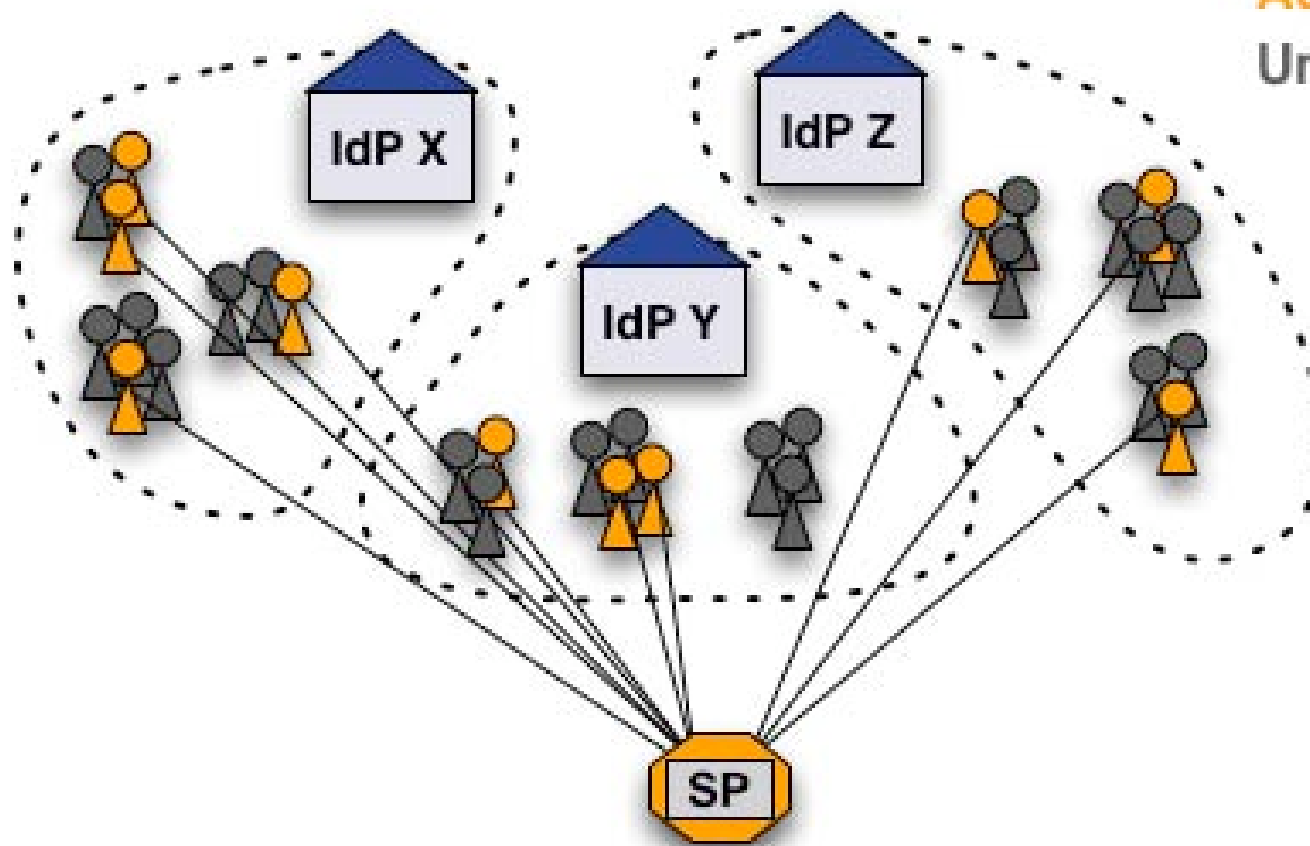
Medicine students
(authorized)

Chemistry students
Staff

Access Rule

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

Case 2: No common user attributes



How can these users be authorized?

Add an entitlement attribute for specific users

Access Rule

Require entitlement *urn:mace:dir:entitlement:common-lib-terms*

- ⊕ Easy solution for a difficult problem
- ⊖
 - Additional work for user directory administrator
 - Difficult to efficiently manage many entitlement values
 - Only IdP admin can manage access**

Solution 2.a: Use uniqueIDs or email

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

Access Rule

```
require uniqueID 465@idpx.ch 234@idpy.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**

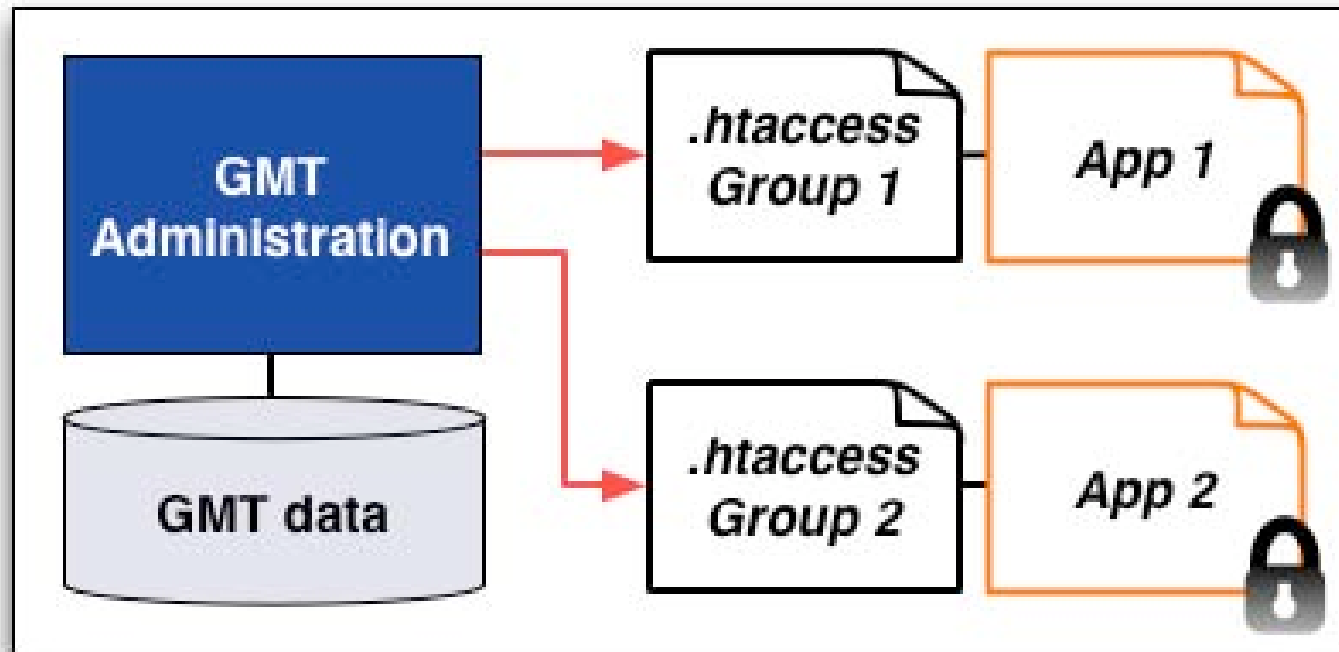
- Open Source, software (BSD license)
- Easy to install
- Light-weight PHP application
- Human readable text files to store group data

Features

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

Generate authorization files

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

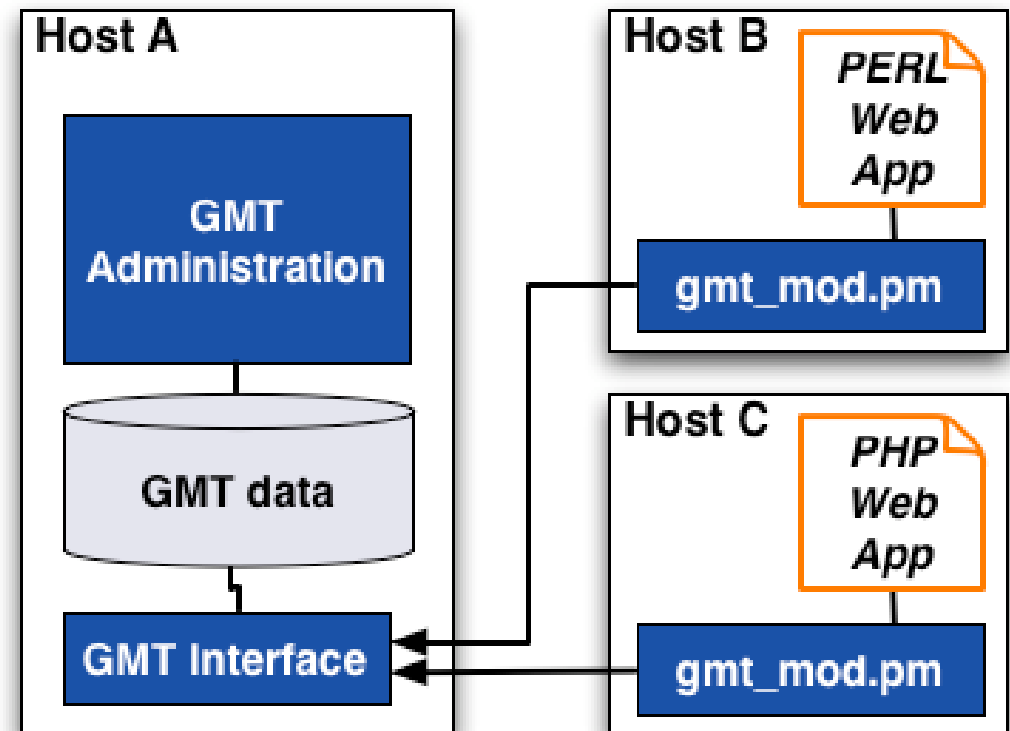


PHP/PERL functions:

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

Secure REST queries:

- Over SSL
- Encrypted with shared key
- Limited to allowed hosts



Summary

- Convenient management of “virtual” groups
- Roles can be transferred
- Users can request to join a group with self-registration
- Authorize users on remote servers
- Libraries available for PHP and Perl

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

Outlook

- Generation of Shibboleth XML authorization files
- New API functions
- Probably new name (“grot”, “groopy”, ...)

The logo for SWITCH, featuring the word "SWITCH" in a bold, sans-serif font. The letter "W" is stylized with a blue outline and an orange fill, while the other letters are solid blue.

The Swiss Education & Research Network

IdP Discovery Service (a.k.a „WAYF“)

Lukas Hämmerle, haemmerle@switch.ch

SWITCH^{aai}

[About AAI](#) : [About SWITCH](#) : [FAQ](#) : [Help](#) : [Privacy](#)

Select your SWITCH^{aai} Home Organization

In order to access a Resource on host 'kelut.switch.ch' you must authenticate yourself.

Select the Home Organization you are affiliated with ...

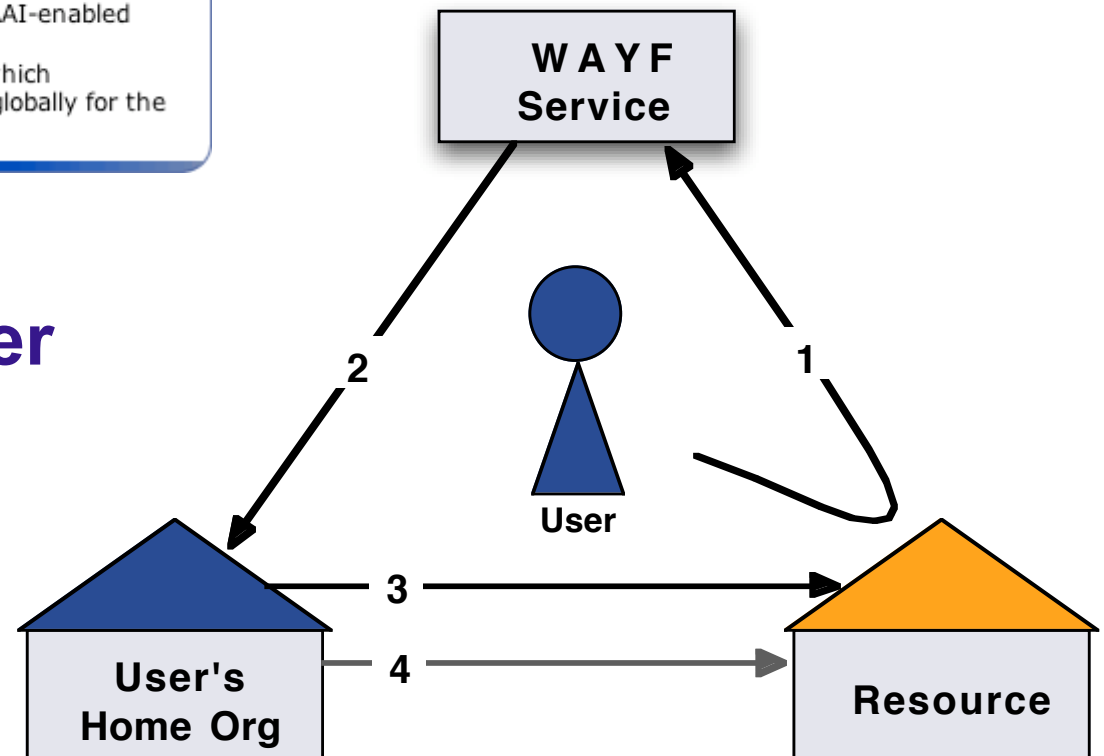
Remember selection for this web browser session.

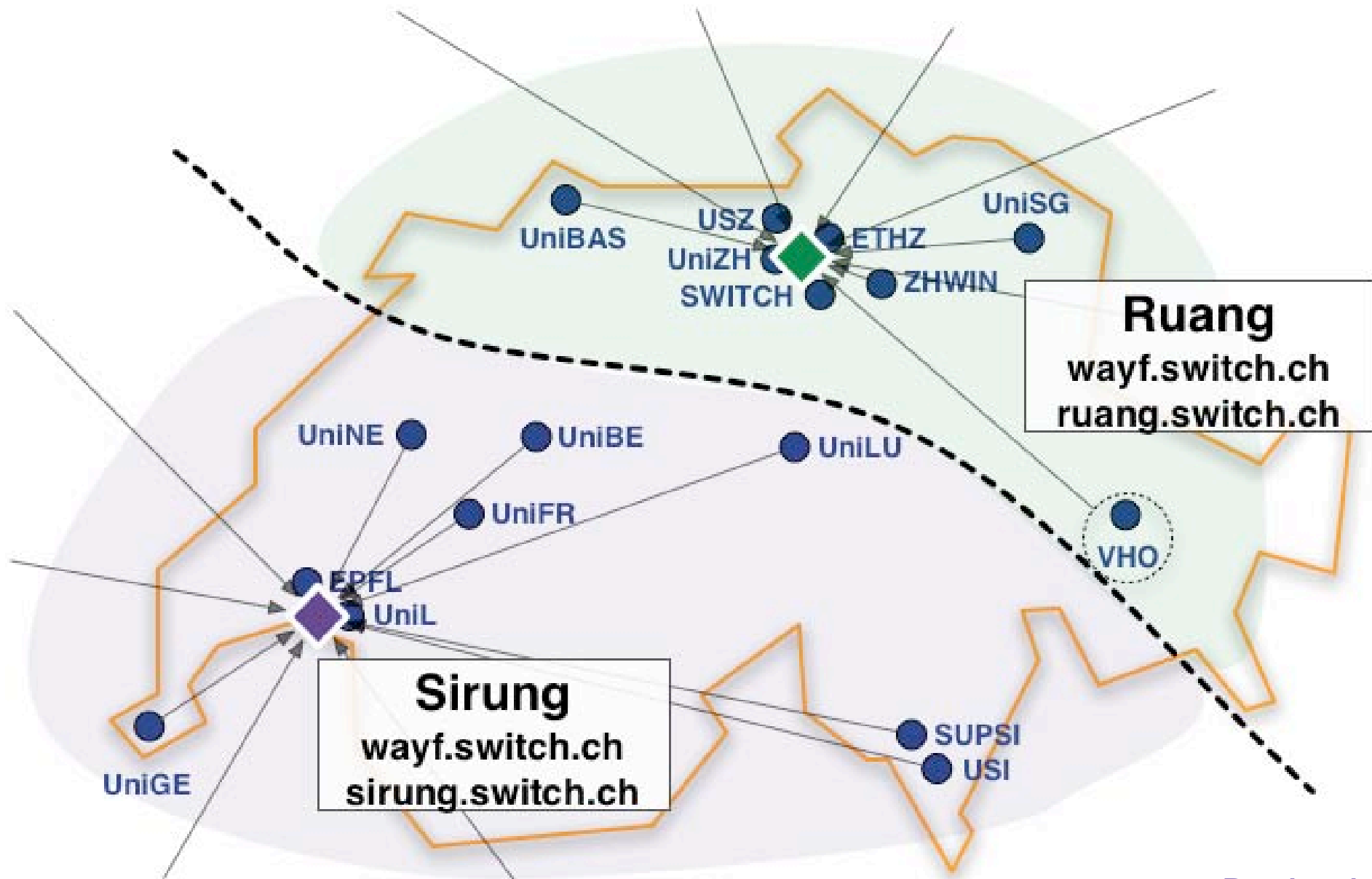
- ▶ SWITCH recommends [importing the 'SwissSign Root CA Certificate'](#) into your web browser. That way, your web browser can seamlessly establish secure connections to AAI-enabled web servers.
- ▶ The [SWITCH](#) Foundation operates the Swiss Education & Research Network which guarantees high-speed connectivity to the Internet and to science networks globally for the benefit of higher education in Switzerland.

⇒ **The WAYF guides the user to his Identity Provider**

Facts about WAYF:

- Stateless requests
- Two requests per visit
 1. (Show drop-down list)
 2. Redirect User to IdP





Routing dependent

Using an integrated WAYF service in your web application can enhance ease-of use.



WAYF Look&Feel can be adapted to application
User feels more “at home”



List of Home Organizations has to maintained
No redirection to IdP when accessing another Resource
No high availability (in general)

Examples of integrated WAYFs

OLAT@UZH

OLAT
Login
Gastzugang
Browsercheck
Über Cookies
Über OLAT

OLAT - Online Learning And Training

Bitte wählen Sie Ihre Hochschule.
Für die Authentifizierung werden Sie weitergeleitet.

Hochschule: SWITCH - The Swiss Education & Rese

Login

Gastzugang
Passwort vergessen

Alternative Möglichkeiten für Login.
Gehören Sie keiner der oben aufgelisteten Hochschulen an?
Weiter

Nicht eingeloggt (242 OLAT-Benutzer sind online)

ILIAS@ETH

ILIAS®

3.6.8 2006-11-27

Sie melden sich bei ILIAS an. Zur Authentifizierung wählen Sie bitte aus der Liste die Hochschule, der Sie angehören.

University: I'm a member of ...

- I'm a member of ...
- ETH Zürich
- Universität Zürich
- Universität Basel
- Universität Bern
- Université de Fribourg - Universität Freiburg
- Université de Genève
- EPFL Lausanne
- Université de Lausanne
- Universität Luzern
- Université de Neuchâtel
- Università della Svizzera Italiana
- Virtual Home Organisation
- Zürcher Hochschule Winterthur

In case you are not a member of a given university and you need access to a course, please contact AAI Support.

SWITCH aai enabled provided by NET Network for Educational Technology

Several WAYF implementations available, e.g.

- WAYF from Internet 2, Java
 - Comes with Shibboleth IdP
 - Uses same metadata format as Shibboleth
- SWITCH WAYF, PHP
 - Enhanced ease-of use for the user
 - Light-weight implementation of a WAYF service
 - Uses PHP instead of JSP
 - Multilingual (Currently en, fr, de, it)
 - Ready for push-update from Resource Registry (not used yet)
 - OpenSource (BSD License)

<http://www.switch.ch/aai/support/tools/wayf.html>

Goal is at most one click per session for HomeOrg selection

Two Cookies:

- Short term: Optionally skipping WAYF for current browser session
- Long term: Remembers past choices (100 days). Can be used to preselect Home Organization in following sessions.

Resource hints the WAYF with URN:

Append part of your IdP providerID (URN) to WAYF URL

<https://wayf.switch.ch/SWITCHaai/WAYF/unige.ch?shire=...>

Transparent mode:

Users never see the WAYF. Append 'redirect' to WAYF URL

<https://wayf.switch.ch/SWITCHaai/WAYF/redirect/unizh.ch?shire=...>