

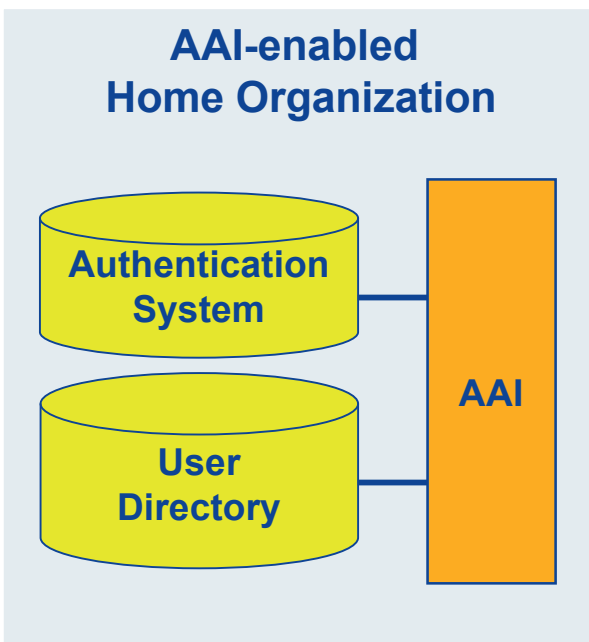
  

# SWITCH

The Swiss Education & Research Network

## **AAI Attributes**

**Thomas Lenggenhager, <[lenggenhager@switch.ch](mailto:lenggenhager@switch.ch)>**



- **Authentication System**
  - any Apache compatible authentication method: LDAP, PAM, RADIUS, TACACS, end-user certificates, Web SSO (e.g. Pubcookie), ...
  - any Tomcat compatible authentication method: e.g. Web SSO (CAS):
    - LDAP, end-user certificates, NIS, SQL database, Kerberos
  - any IIS compatible authentication method
- **User Directory**
  - Integration via Java APIs
    - LDAP via JNDI
    - Databases via JDBC

→ Username is the link between the two parts

SSO = Single Sign On

- **AAI transfers user attributes from a Home Organization to a Resource**
  - **Requires a common understanding of what a value means**
    - ➔ **Authorization Attribute Specification v1.1**  
[http://www.switch.ch/aai/docs/AAI\\_Attr\\_Specs.pdf](http://www.switch.ch/aai/docs/AAI_Attr_Specs.pdf)
- **A task force selected the attributes for SWITCHaai**
  - **minimal set to start with**
  - **attributes with pre-existing 'common understanding'**
  - **in line with foreign activities**
- **Descriptions are LDIF like, but use of LDAP not required**

# Authorization Attributes (2)

## Personal attributes

- **Unique Identifier**
- **Surname**
- **Given name**
  
- **E-mail**
- **Address(es)**
- **Phone number(s)**
- **Preferred language**
- **Date of birth**
- **Gender**

## Group membership

- **Name of Home Organization**
- **Type of Home Organization**
- **Affiliation (student, staff, faculty, ...)**
  
- **Study branch**
- **Study level**
- **Staff category**
- **Group membership**
- **Organization Path**
- **Organizational Unit Path**

- based on eduPerson specification
- study branch, study level, staff category are based on SHIS/SIUS
- username and password are missing  
⇒ only used locally!
- commonName is missing  
no common understanding on how to use it
- 'Matrikelnummer' is missing  
for data protection reasons

- Based on 'Schweizerisches Hochschulinformationssystem (SHIS/SIUS)'  
<http://www.bfs.admin.ch> (Fachbereich Bildung und Wissenschaft)

- Example for Universities of Applied Sciences

## **studyBranch1 (17 codes)**

40000 Landwirtschaft — Agriculture

## **studyBranch2 (64 codes)**

40200 Pflanzenproduktion — Production végétale

## **studyBranch3 (110 codes)**

40202 Obst-, Wein-, Gartenbau — Arboriculture fruitière/Horticulture

## **studyLevel**

40202-15 Studierende in der Studienphase, die zum Bachelor führt  
Etudiants réguliers se trouvant dans une phase d'études  
qui les conduit au titre de Bachelor

- **Only very broad categories, also derived from SHIS/SIUS**
- **Categories defined**

## **Teaching/Research**

101/201 Professors and Permanent Researchers

102/202 Oberer Mittelbau — Corps intermédiaire supérieur

103/203 Unterer Mittelbau — Corps intermédiaire inférieur

## **Administration/Support/Technical**

301 Administrative Personnel

302 Administrative Personnel: Apprentices and Interns

303 Technical Personnel

304 Technical Personnel: Apprentices and Interns

305 Janitors, Building Managers

306 Social and Wellness Personnel

307 Library Personnel

308 Safety Personnel



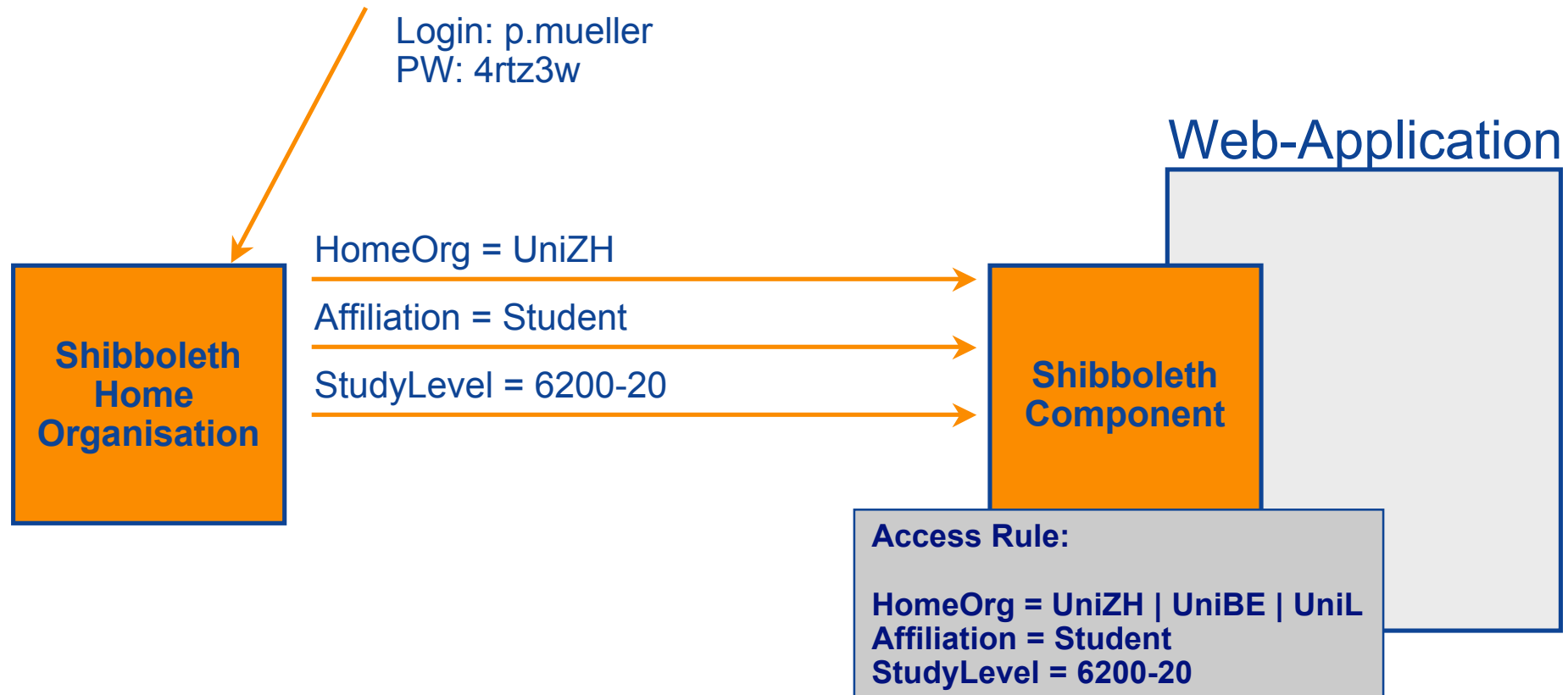
# SWITCH

The Swiss Education & Research Network

## Granting Access

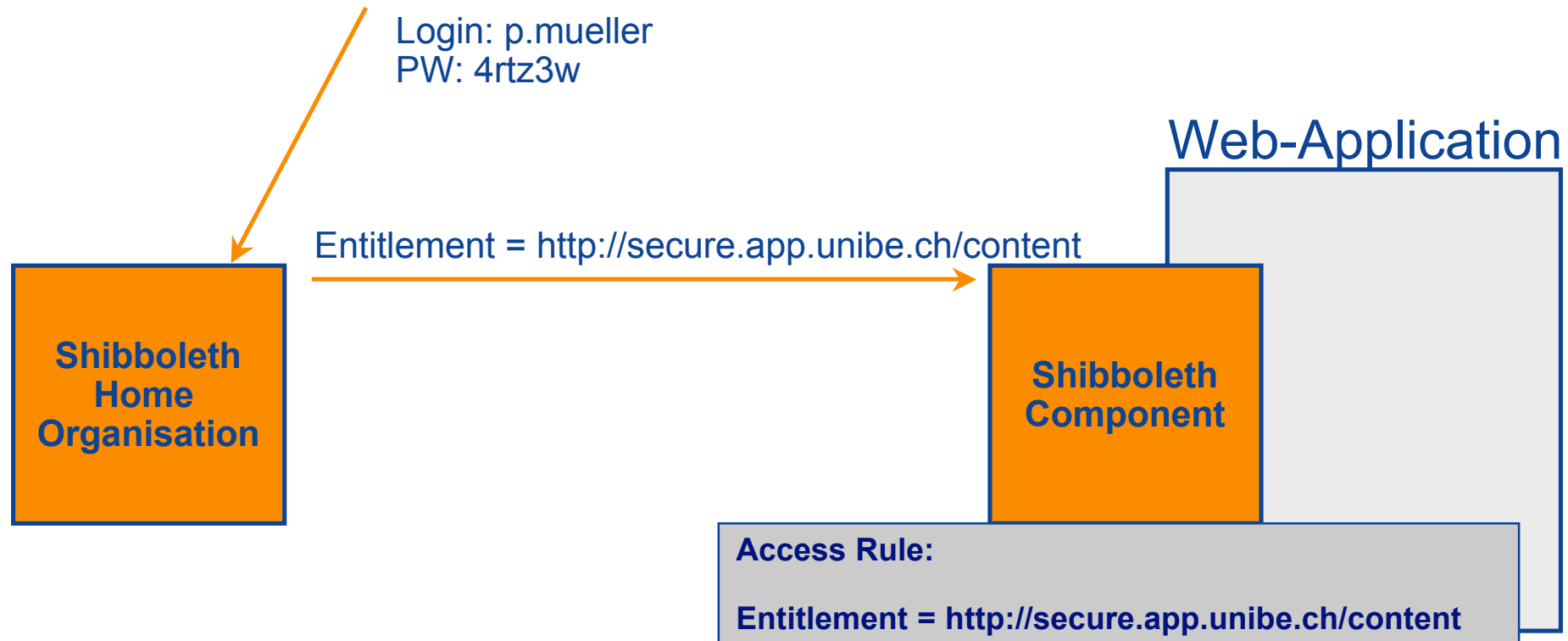
Ueli Kienholz, <[kienholz@switch.ch](mailto:kienholz@switch.ch)>

# Method 1: SWITCHaai Attributes

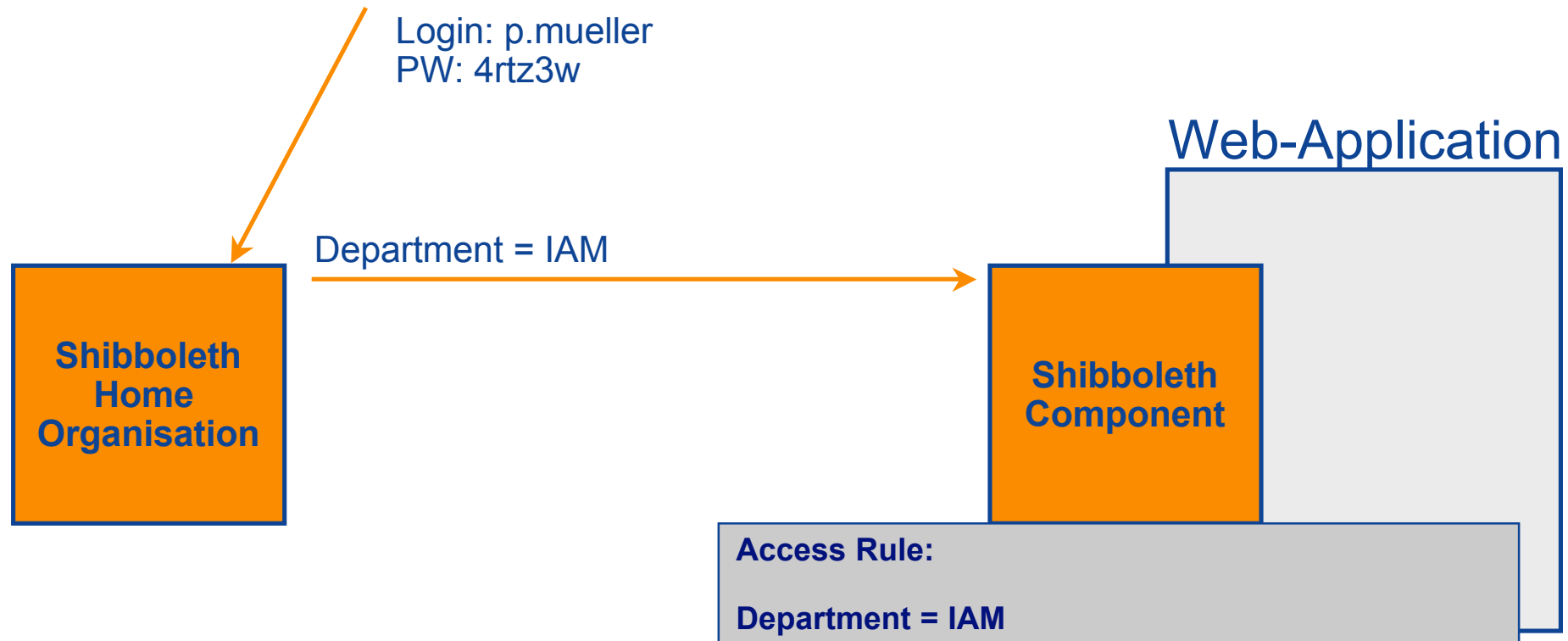




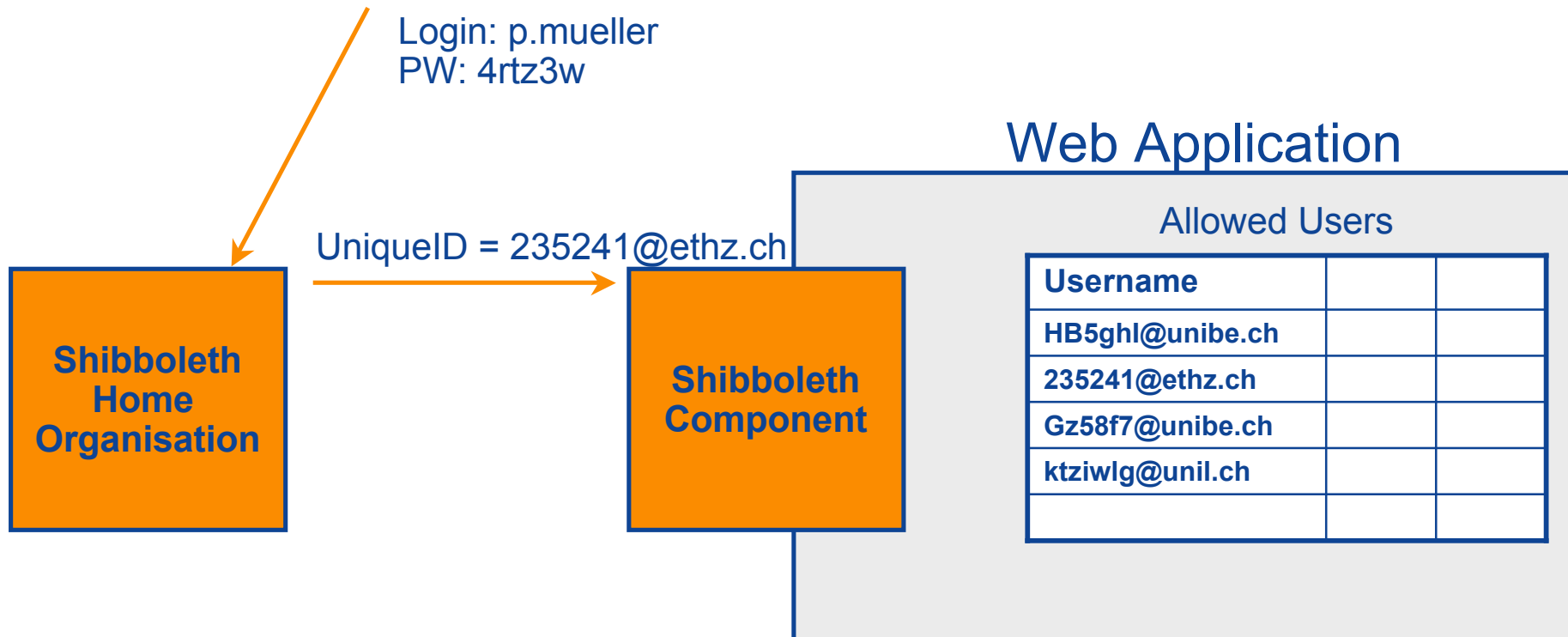
# Method 2: Entitlement



# Method 3: Definition of additional Attributes



# Method 4: Application has it's own Access Control



# SWITCH

The Swiss Education & Research Network

## System Requirements

Valéry Tschopp, <[tschopp@switch.ch](mailto:tschopp@switch.ch)>

# Supported Servers for Target Installations SWITCH

The Swiss Education & Research Network

## Server OS

- Windows NT, 2000, XP, 2003
- Linux (any distribution)
- Solaris
- Mac OS X

## Web Servers

- Apache 1.3.x
- Apache 2.x
- IIS 4.x, 5.x, 6.x

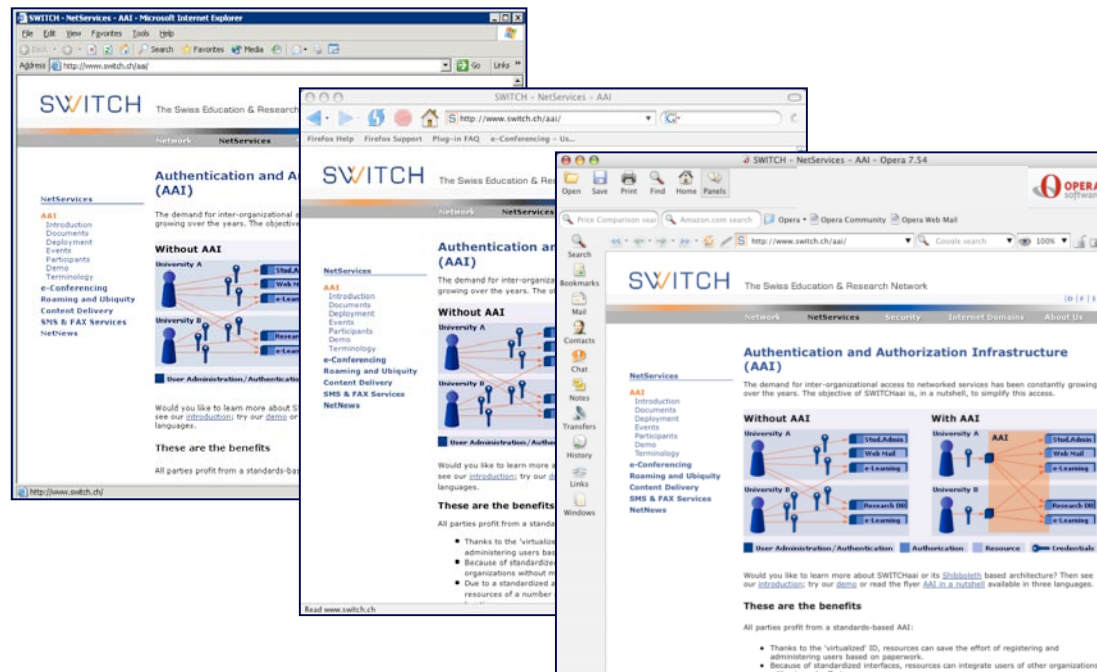
# Supported Applications

- ❑ **Static content on Apache**
- ❑ **Applications (PHP, Perl, ..) running on Apache**
- ❑ **Applications (ASP, PHP, ...) running on IIS Web Servers 4, 5, 6**
- ❑ **JAVA web-applications via mod\_jk and Apache / JK ISAPI redirector and IIS**
- ❑ **List of „shibbolized“ applications at <http://shibboleth.internet2.edu/seas.html>**

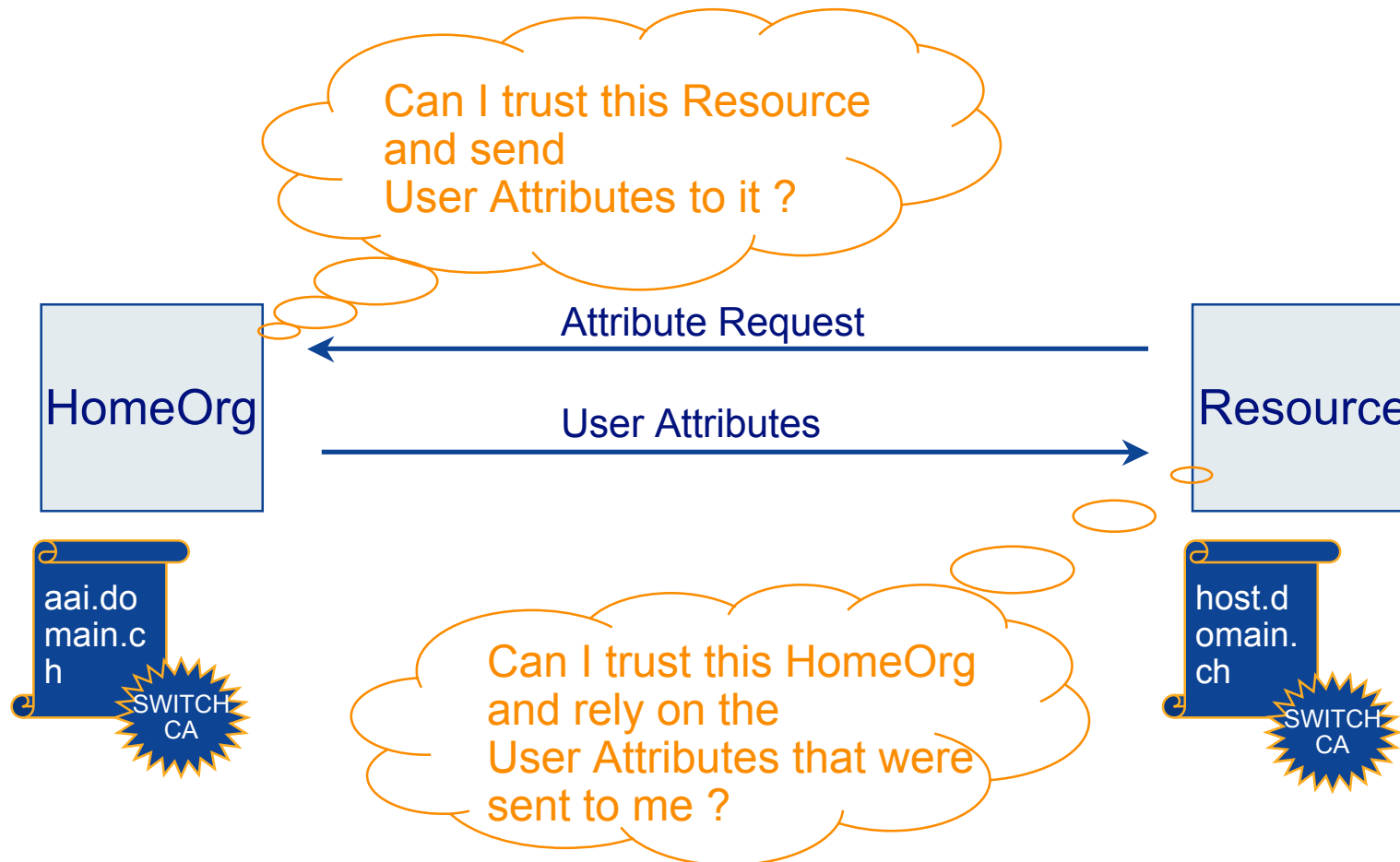
- \* ArtSTOR
- \* Blackboard
- \* CSA
- \* Darwin Streaming Server
- \* eAcademy
- \* EBSCO Publishing
- \* Elsevier ScienceDirect
- \* ExLibris - SFX
- \* Fedora
- \* Gale
- \* Higher Markets
- \* JSTOR
- \* Napster
- \* NSDL
- \* OCLC
- \* Ovid Technologies Inc.
- \* Proquest Information and Learning
- \* SYMPA
- \* TWiki
- \* Useful Utilities - EZProxy
- \* Web Assign
- \* WebCT (Campus Ed./Vista)
- \* Zope4Edu

# Browser Requirements

- ❑ Cookies
- ❑ Browser redirect
- ❑ SSL
- ❑ If no JavaScript: additional click necessary

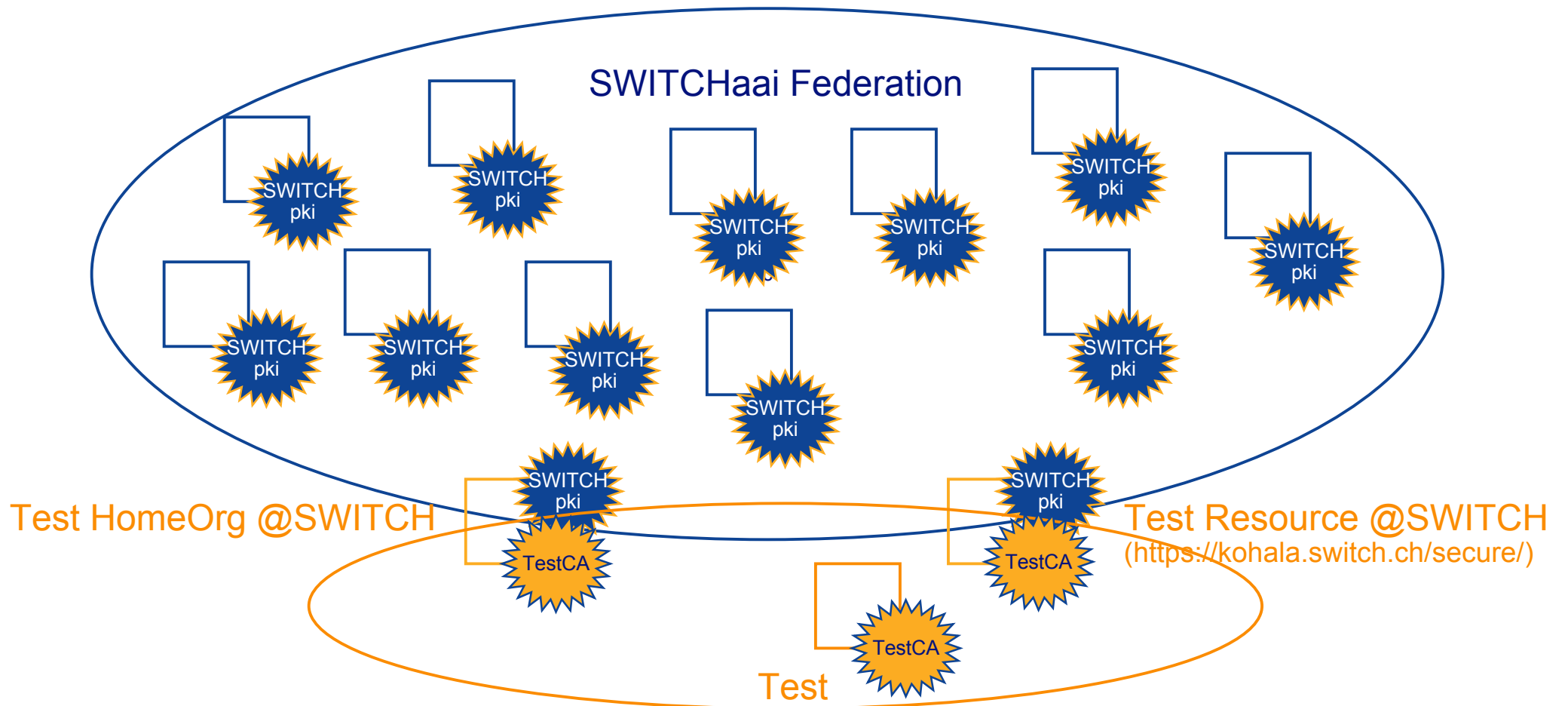


# Requirement: SWITCHpki Server Certificates

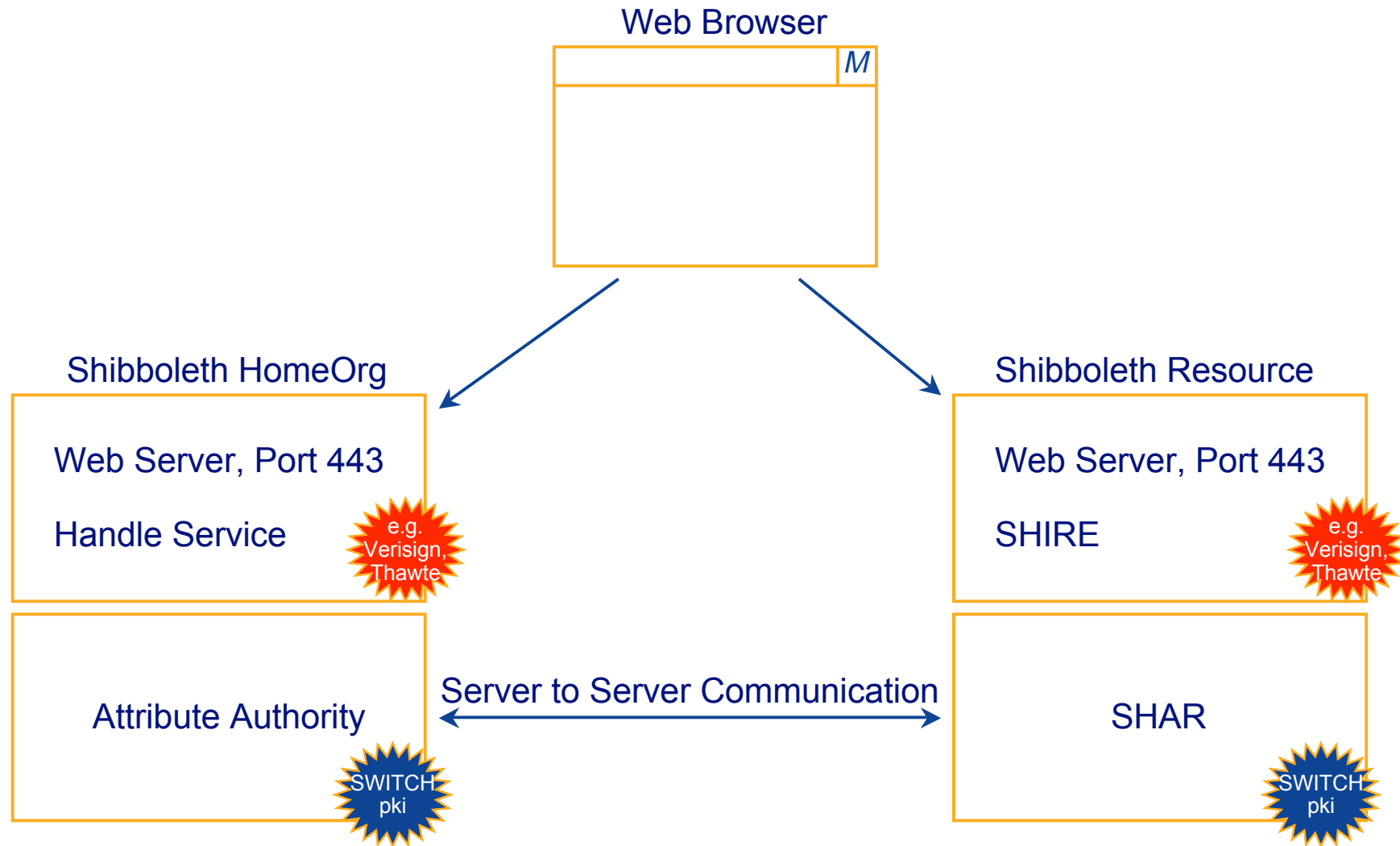




# Exception 1: Mere Test-Purposes



# Exception 2: SSL connection from Browser



Q & A

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

[aai@switch.ch](mailto:aai@switch.ch)