SWITCH

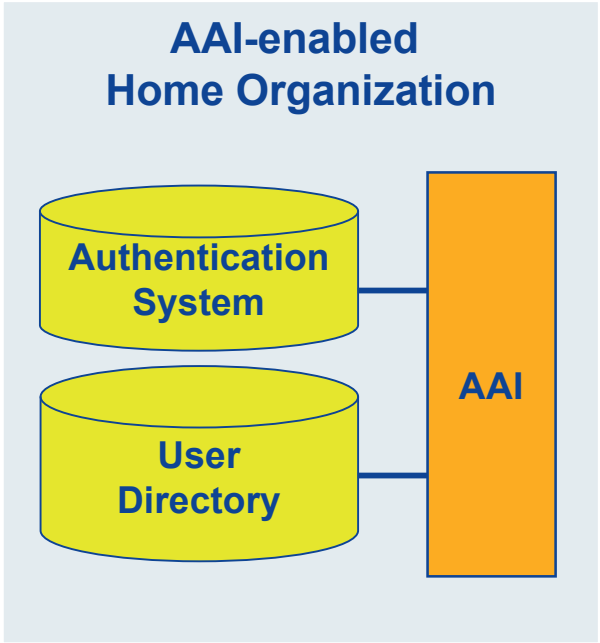
The Swiss Education & Research Network

AAI Attributes

Patrik Schnellmann, <schnellmann@switch.ch>

2005 © SWITCH

Directories within a AAI Home Organization



- 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

Authorization Attributes (1)

SWITCH
The Swiss Education & Research Network

- 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

- 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)

SWITCH
The Swiss Education & Research Network

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

studyBranch & studyLevel

SWITCH
The Swiss Education & Research Network

- **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

staffCategory

SWITCH
The Swiss Education & Research Network

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

Teaching/Reaserch

101/201 Professors and Permanent Researchers
102/202 Oberer Mittelbau — Corps intermédiare supérieur
103/203 Unterer Mittelbau — Corps intermédiare 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

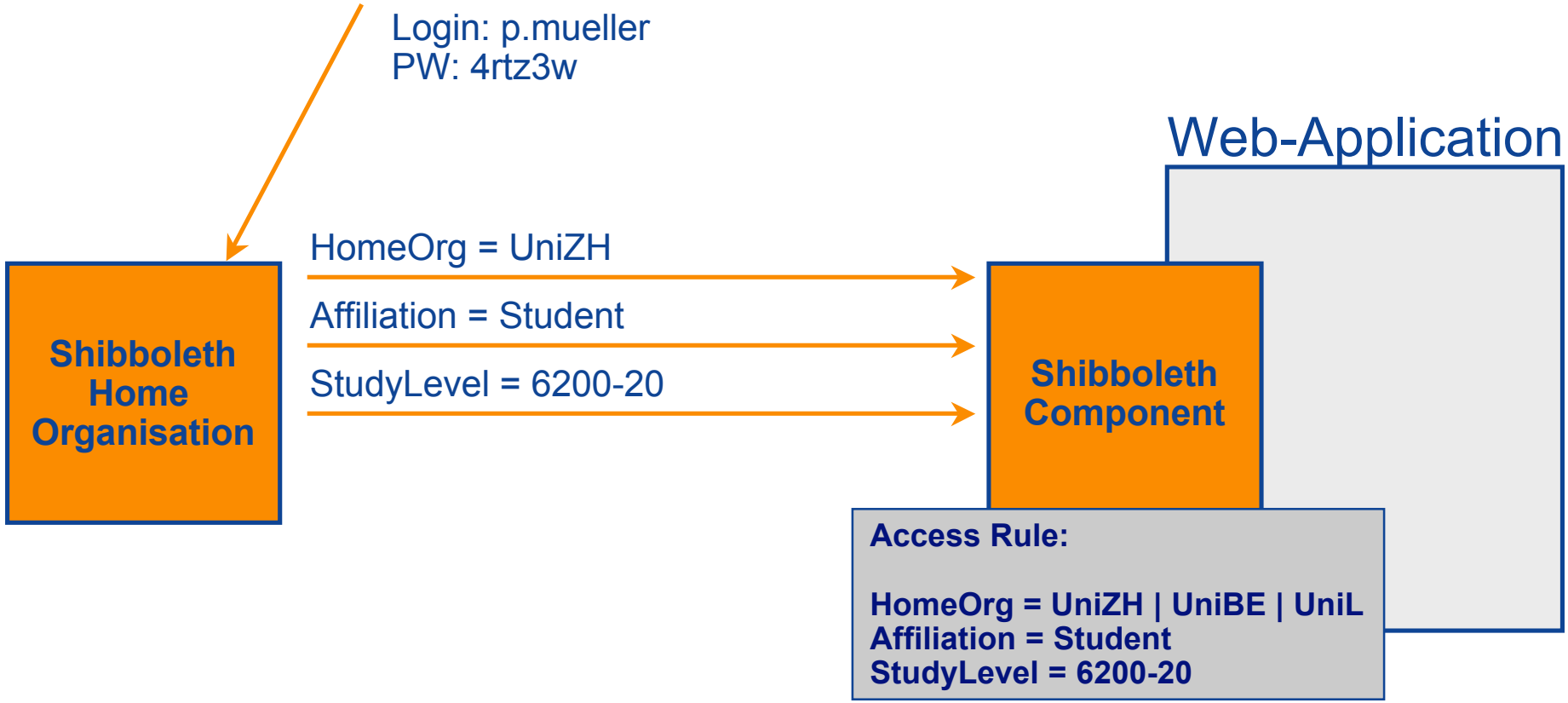
The Swiss Education & Research Network

Authorization

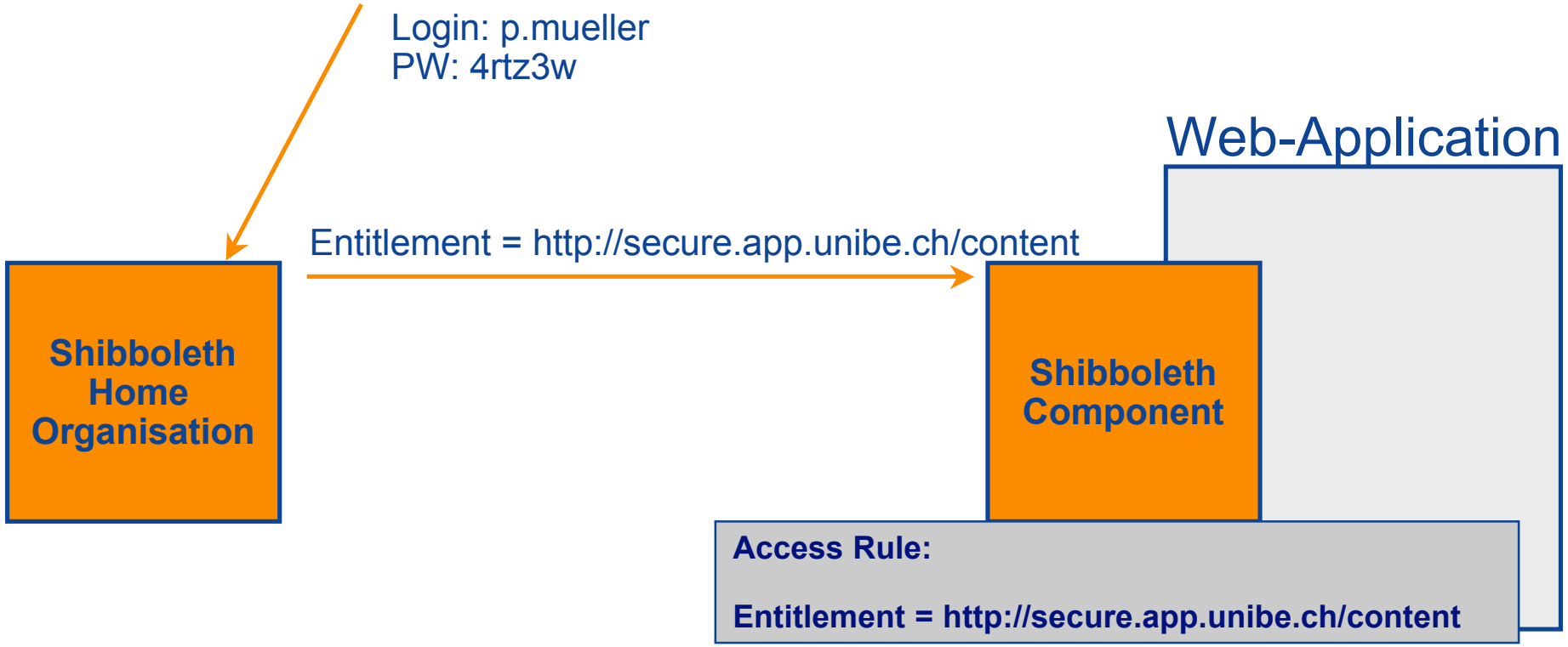
Ueli Kienholz, <kienholz@switch.ch>

2005 © SWITCH

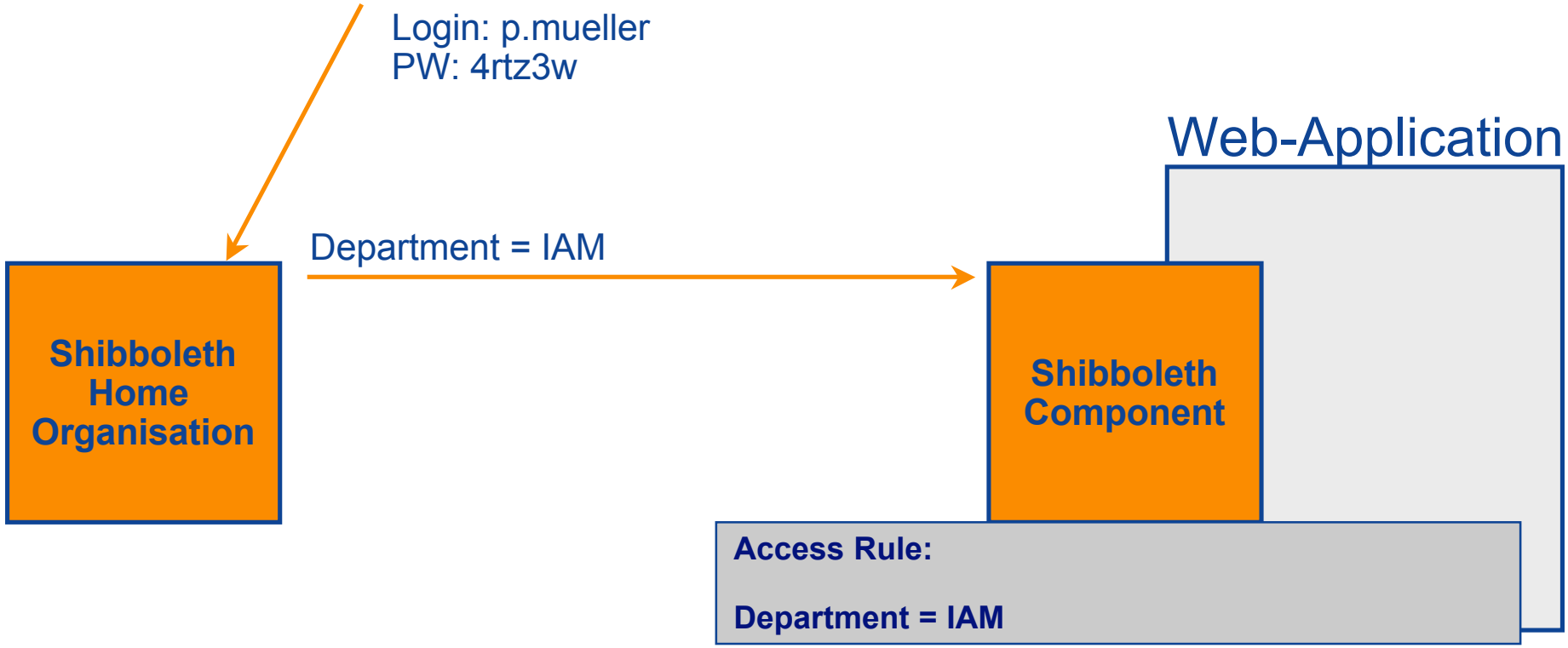
Method 1: SWITCHaai Attributes



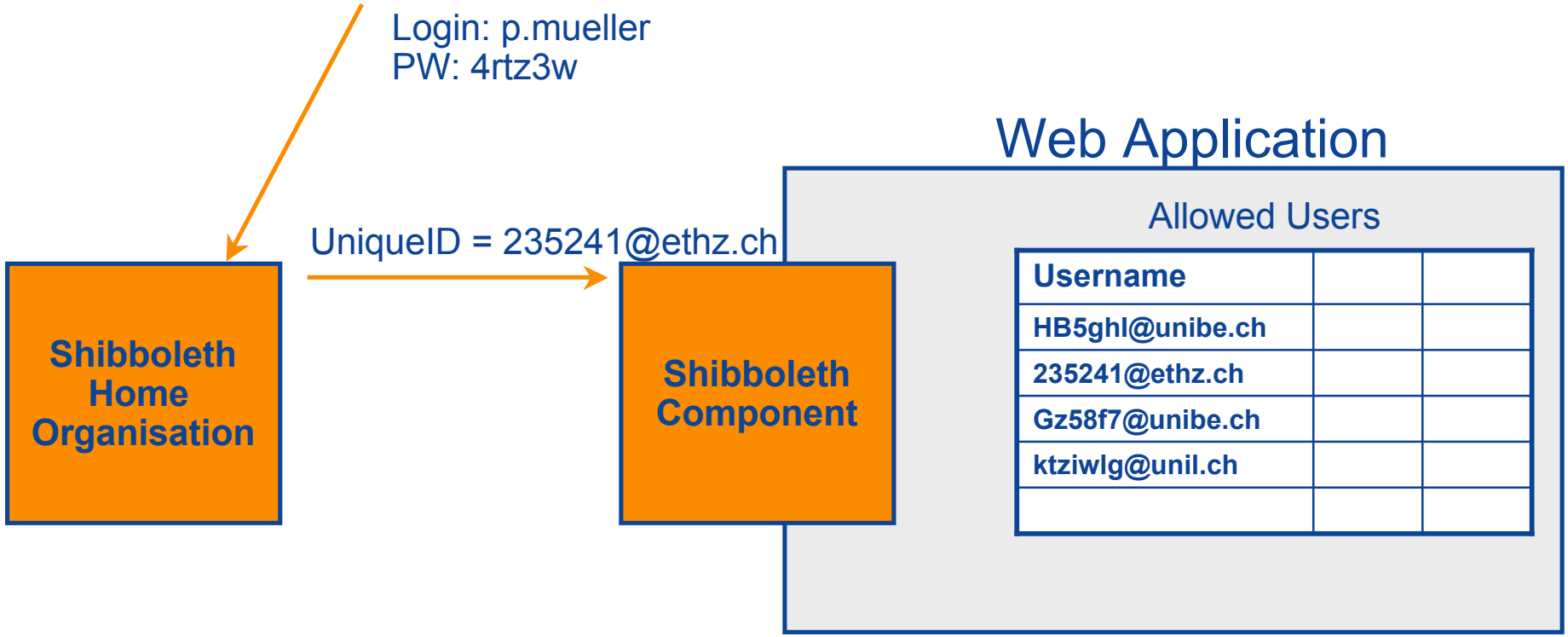
Method 2: Entitlement



Method 3: Definition of additional Attributes



Method 4: Application has it's own Access Control



SWITCH

The Swiss Education & Research Network

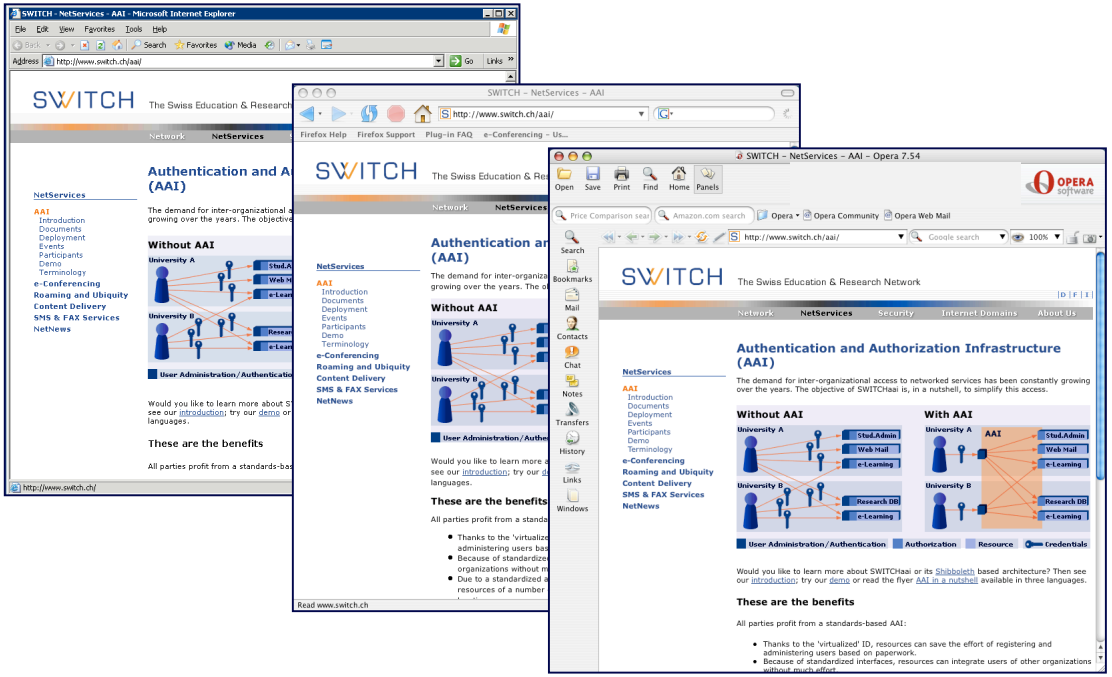
System Requirements

Ueli Kienholz, <kienholz@switch.ch>

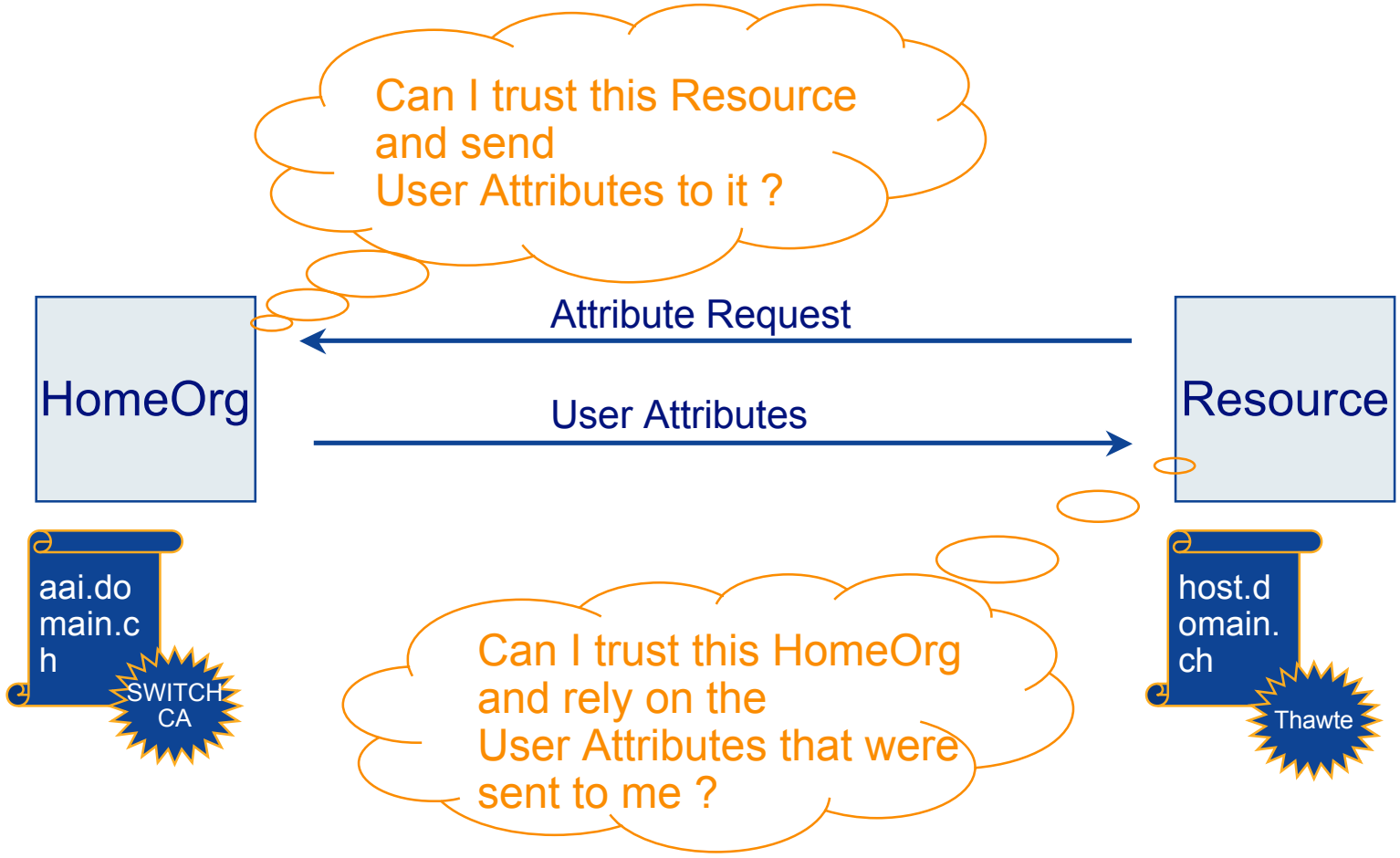
2005 © SWITCH

Browser Requirements

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



Requirement: Server Certificates



CA Acceptance Policy

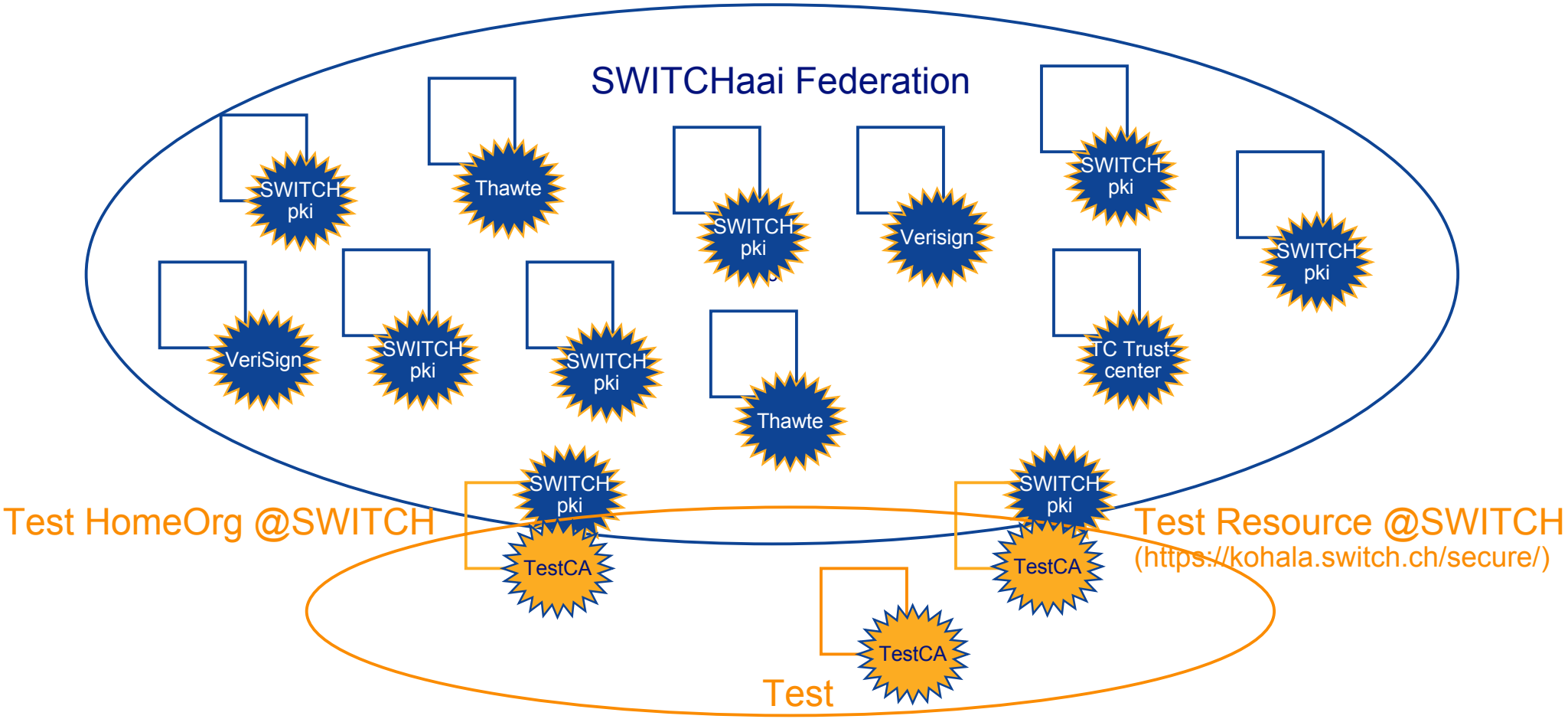
SWITCH
The Swiss Education & Research Network

- Currently accepted
  - SWITCHpki
  - (One of) Thawte
  - (One of) VeriSign
  - (One of TC) Trustcenter
- Procedure defined to include additional CAs

http://www.switch.ch/aai/ca-acceptance-policy.html

Exception: Mere Test-Purposes

SWITCH
The Swiss Education & Research Network



Questions ?

SWITCH
The Swiss Education & Research Network

Q & A

http://www.switch.ch/aai

aai@switch.ch

Exception 2:
SSL connection from Browser

SWITCH
The Swiss Education & Research Network