SWITCH
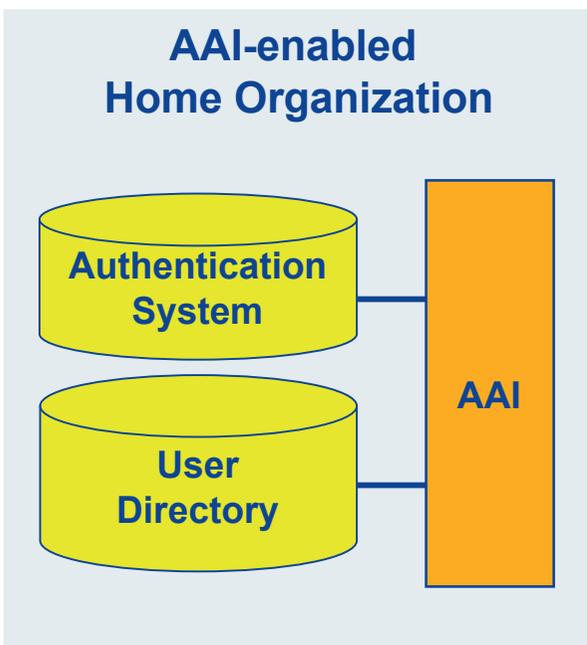
The Swiss Education & Research Network

The AAI Attributes
and
the User Directories

Thomas Lenggenhager, SWITCH

23. März 2004

Directories within a AAI Home Organization

**AAI-enabled
Home Organization**

**Authentication
System**

AAI

**User
Directory**

- **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)**

- **Integration with User Directory via Java APIs**
  - **LDAP via JNDI**
  - **Databases via JDBC**

➔ **Login name is the link between the two parts**

SSO = Single Sign On

Authorization Attributes

SWITCH

- **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)

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**

- 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