SWITCH

The Swiss Education & Research Network

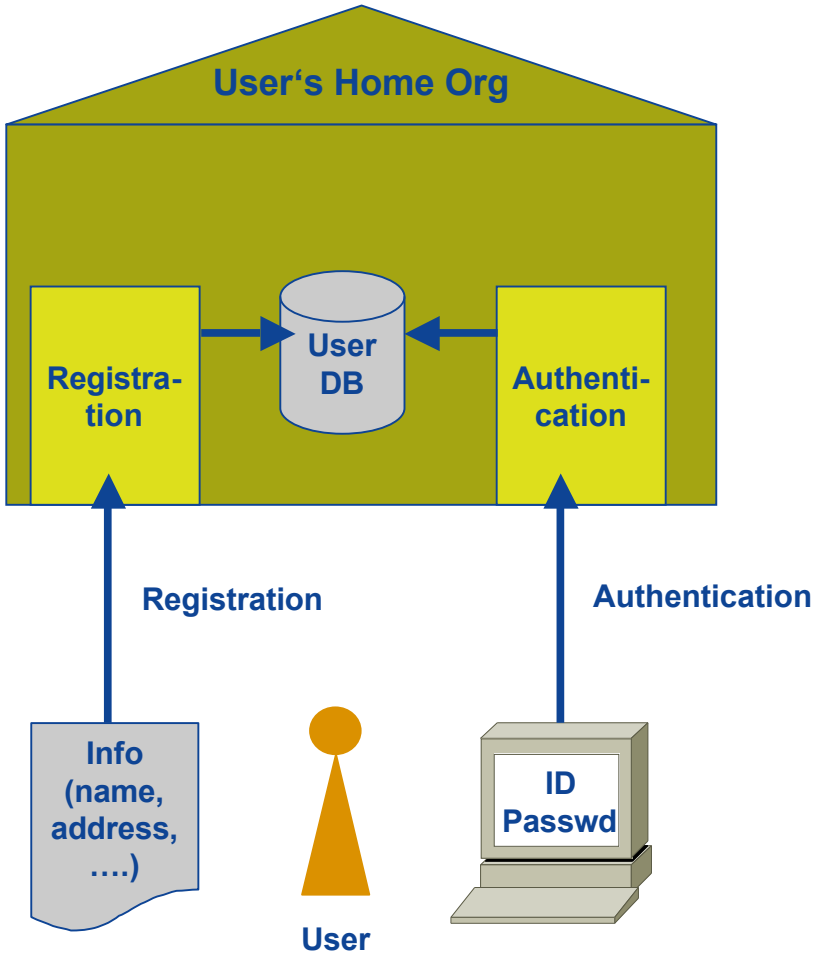
What does it take to participate in the AAI?

Thomas Lenggenhager, SWITCH

December 2, 2002

Preconditions for Home Organizations

SWITCH
The Swiss Education & Research Network



Registration

- A Home Organization must be able to
  - register its users and store information about them in a user directory (database)
  - provide a minimal set of such user attributes to the AAI
- The registration and administration processes have to guarantee that these attributes are kept accurate

Authentication

- A Home Organization has to offer secure authentication over the network to its users
- It is up to the Home Organization which authentication technology it chooses.

The AAI defines only minimal requirements for user registration and authentication, but does not require any specific technology (e.g. smartcard).

Authorization Attributes

SWITCH
The Swiss Education & Research Network

Personal attributes

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

Group membership

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

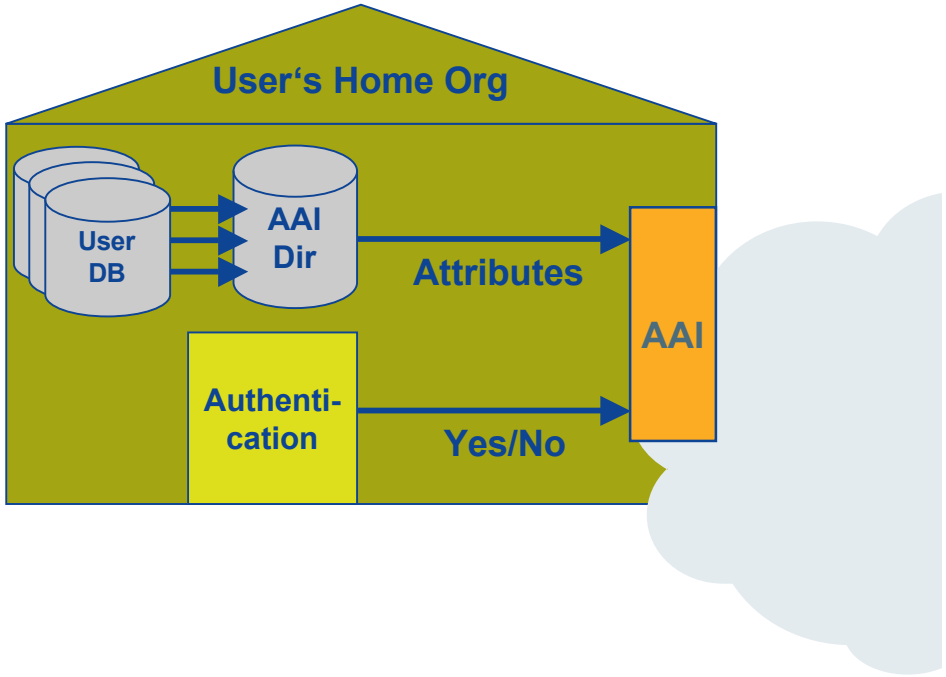
User attributes for AAI

- are based on standards (LDAP: eduPerson, SHIS/SIUS)
- have to be available in real-time
- have to be handled as required by federal and cantonal data protection laws:
  - attributes have to be accurate
  - attributes have to be stored securely
  - attributes should only be transferred to resources with a valid case to use it.
- will be revised in the future in a standard-ized change process, depending on the requirements of Resource Owners and Home Organizations

Version 1.0 of the attribute specification is planned for mid-December and will be published on www.switch.ch/aai. It will include an LDAP schema.

AAI-enabling of Home Organizations

SWITCH
The Swiss Education & Research Network



AAI integration between

- authentication system and AAI
- user DB / directory and AAI

Data consolidation

- Make sure that all the attributes needed are online available in the appropriate AAI format

⇨If necessary, create a specific AAI user directory (read-only, periodically updated from master databases)

The AAI will provide interfaces for the interchange of attributes and authentication information based on LDAP or on a standardized API

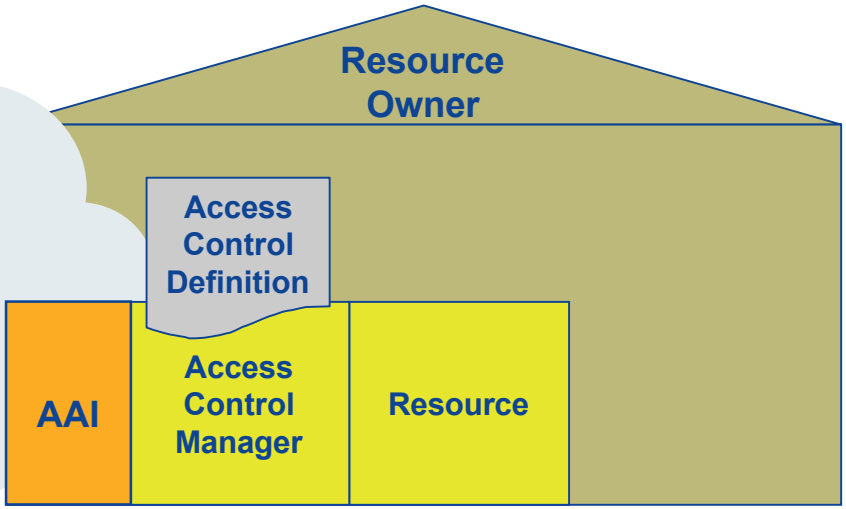
Resource Types (1)

SWITCH
The Swiss Education & Research Network

Type A
- Unpersonalized web resources
- Access control policy based on group membership attributes

⇨AAI extensions for web server

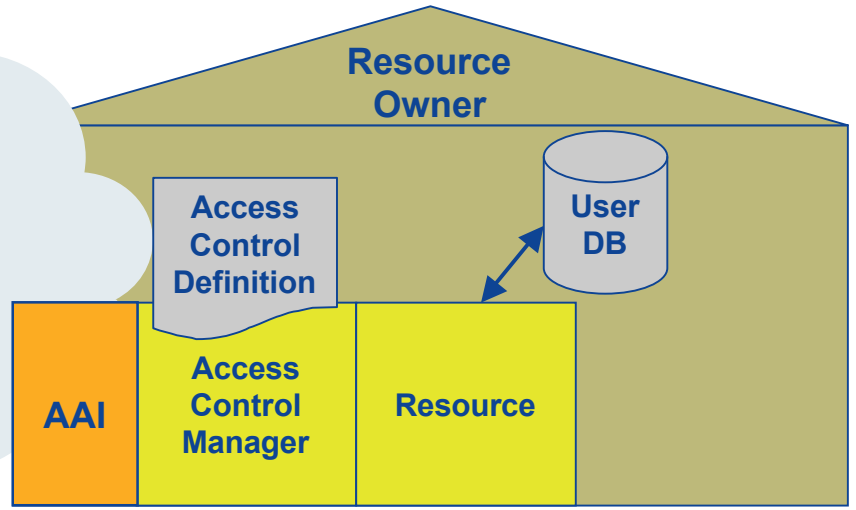
Example
- Intranet web servers



Type B
- Personalized web resources
- Access control policy based on individual and group membership attributes

⇨AAI extensions for web server

Examples
- Discussion forum
- Web mail
- Student administration

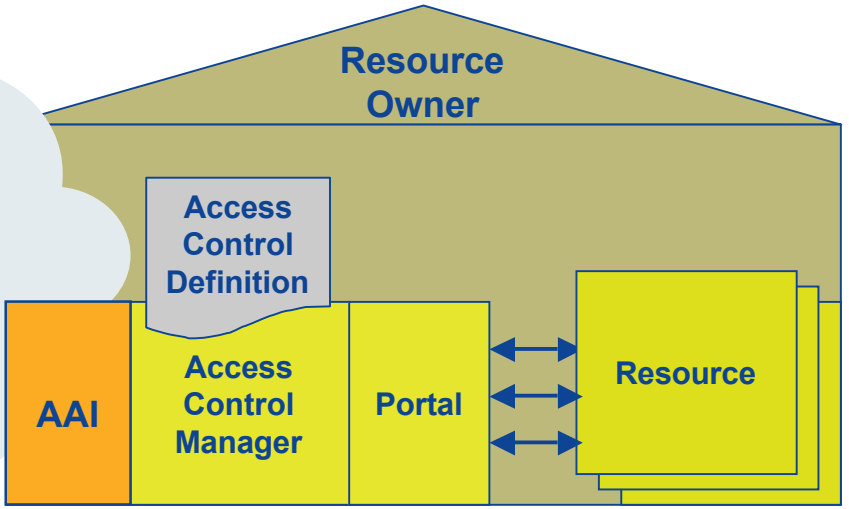


Resource Types (2)

SWITCH
The Swiss Education & Research Network

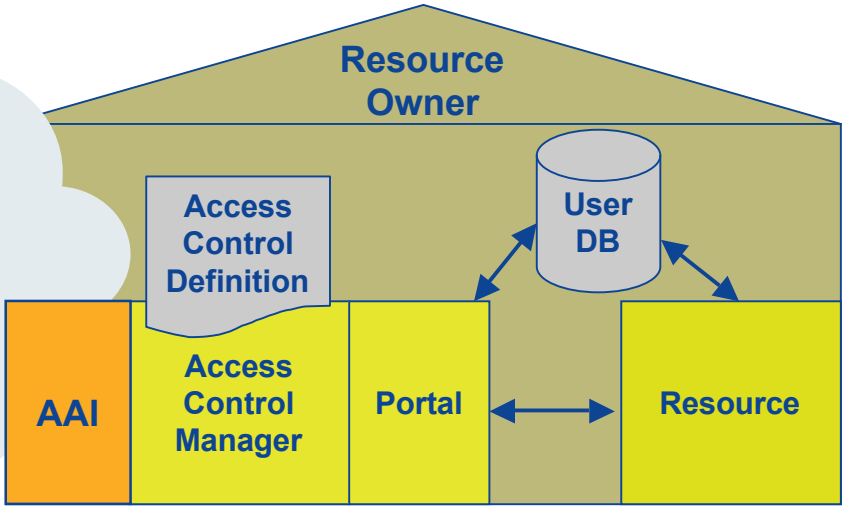
Type C
- Unpersonalized “black box” web resources with proprietary access control
- ⇨AAI portal

Example
- 3rd party content providers (libraries)



Type D
- Personalized “black box” web resources with proprietary access control and user administration
- ⇨AAI portal

Examples
- E-learning platforms
- Standard applications



Preconditions for Resources

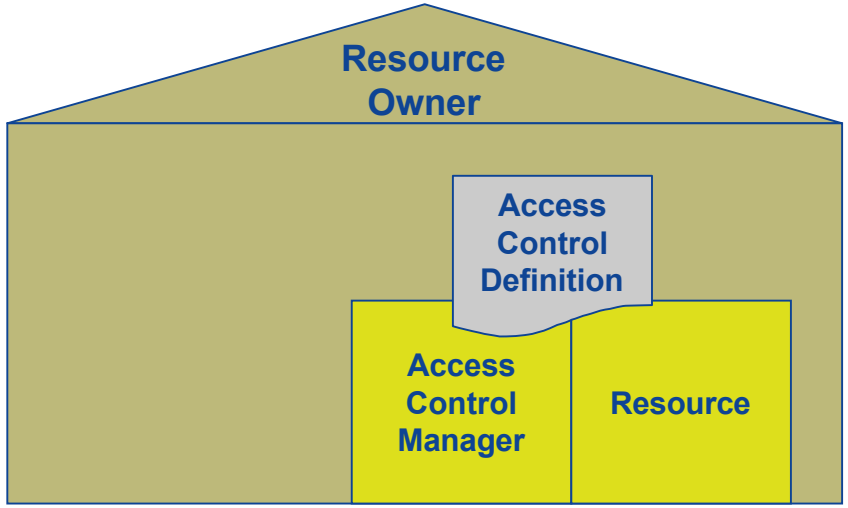
SWITCH
The Swiss Education & Research Network

Access Control

- Access Control Policy can be expressed and implemented as rules based on authorization attributes
- Received attributes have to be appraised as trustworthy
- Resource is of type A-D (detailed technical requirements will follow); if not, technical feasibility has to be verified.

Legal Basis

- A Resource belongs to an Organization which has signed the AAI Policy
- A Resource Owner agrees to handle received attributes as required by the AAI Policy and the Federal and Cantonal Data Protection Law



The AAI project will ensure that common Web Resources can fulfill technical requirements easily and that the necessary legal and organizational framework will be established.

AAI-enabling Resources

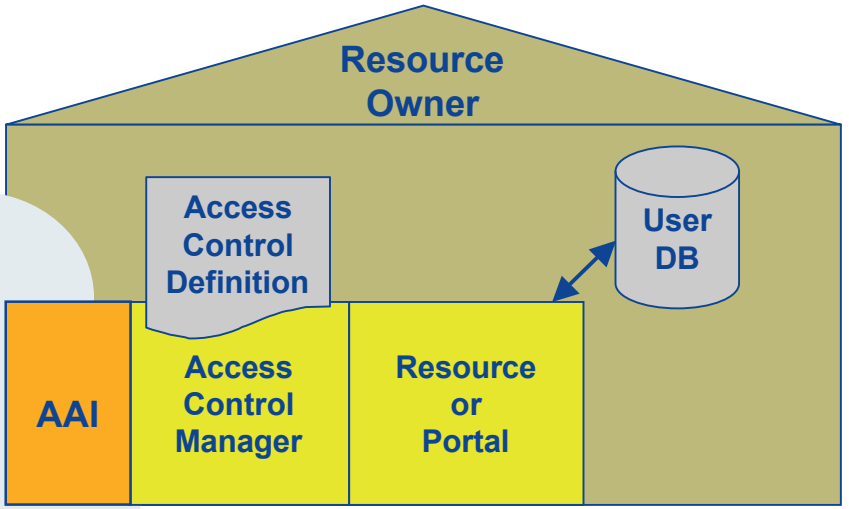
SWITCH
The Swiss Education & Research Network

For Resources of Type A and B

- Install AAI on Resource
- Configure (implement) Access Control Definition
- For personalized resources: implement interaction with User DB

For Resources of Type C and D

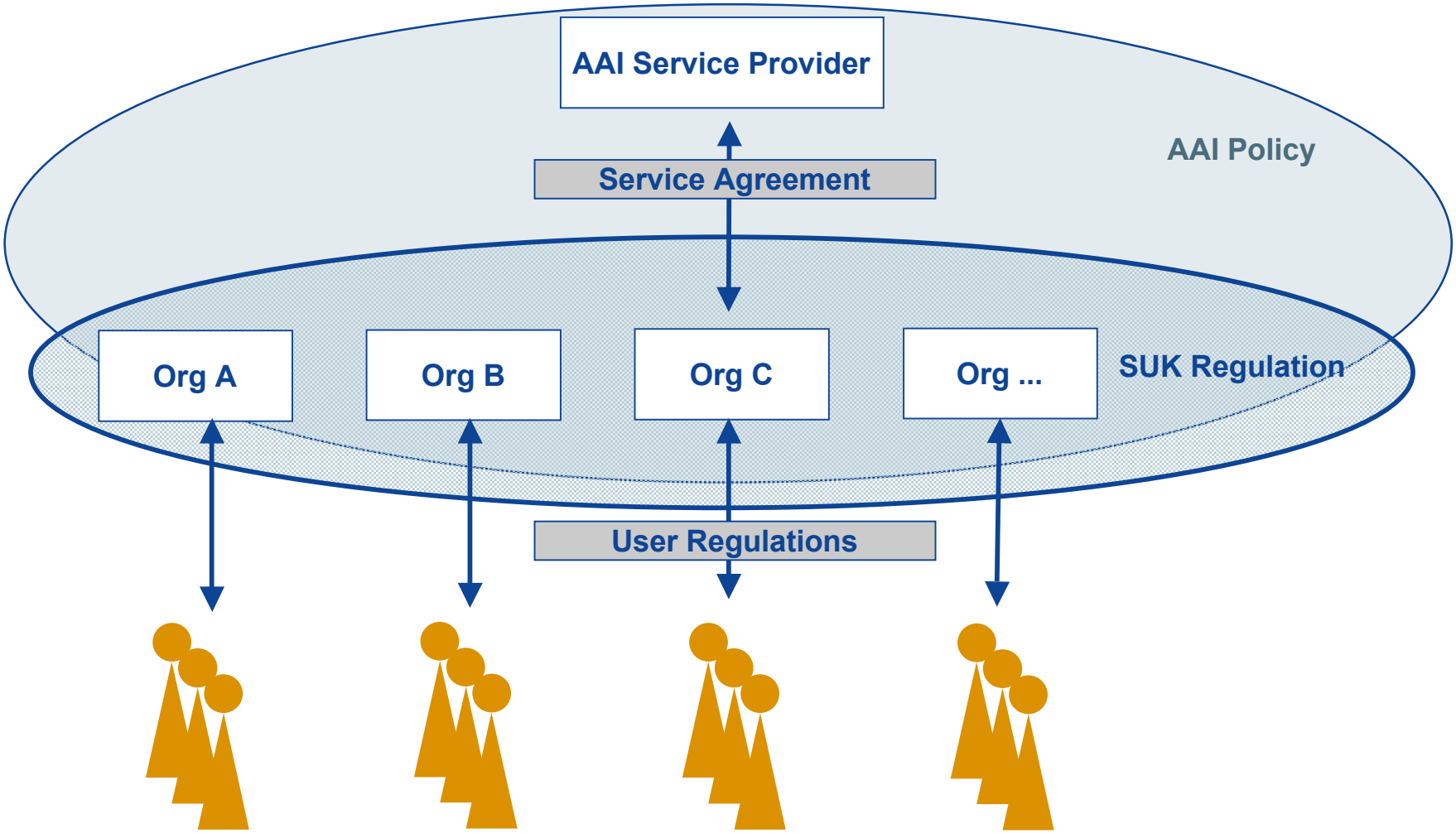
- Implement Portal
- Install AAI on Portal
- Configure (implement) Access Control Definition on Portal
- For personalized resources: implement interaction with User DB



During the AAI pilot phase, reusable sample solutions for widely-used resource types and sample Portals will be implemented.

The Legal Basis of an AAI (1)

SWITCH
The Swiss Education & Research Network



The Legal Basis of an AAI (2)

SWITCH
The Swiss Education & Research Network

SUK Regulation	The SUK regulation will establish the legal basis which regulates data protection issues as well as the liability among the Organizations.
AAI Policy	Based on the SUK decision, the AAI Policy will define a common set of guidelines which describes the rules of good conduct that AAI Service Provider, Home Organizations and Resource Owners agree to.
Service Agreement	The relationship between the Organizations and the Service Provider(s), e.g. SWITCH, will be defined within a Service Agreement.
User Regulation	The relationship between User and Organization has to be set up in the acceptable use policy (AUP), in particular for data protection reasons. The AAI report contains a sample clause which may be inserted in the Home Organizations User Regulations and which should be signed by the user.

SUK / CUS = Schweizerische Universitätskonferenz / Conference Universitaire Suisse