
SWITCH

The Swiss Education & Research Network

Authentication and Authorization Infrastructure (AAI)

AAI Update

TERENA AACE-Workshop

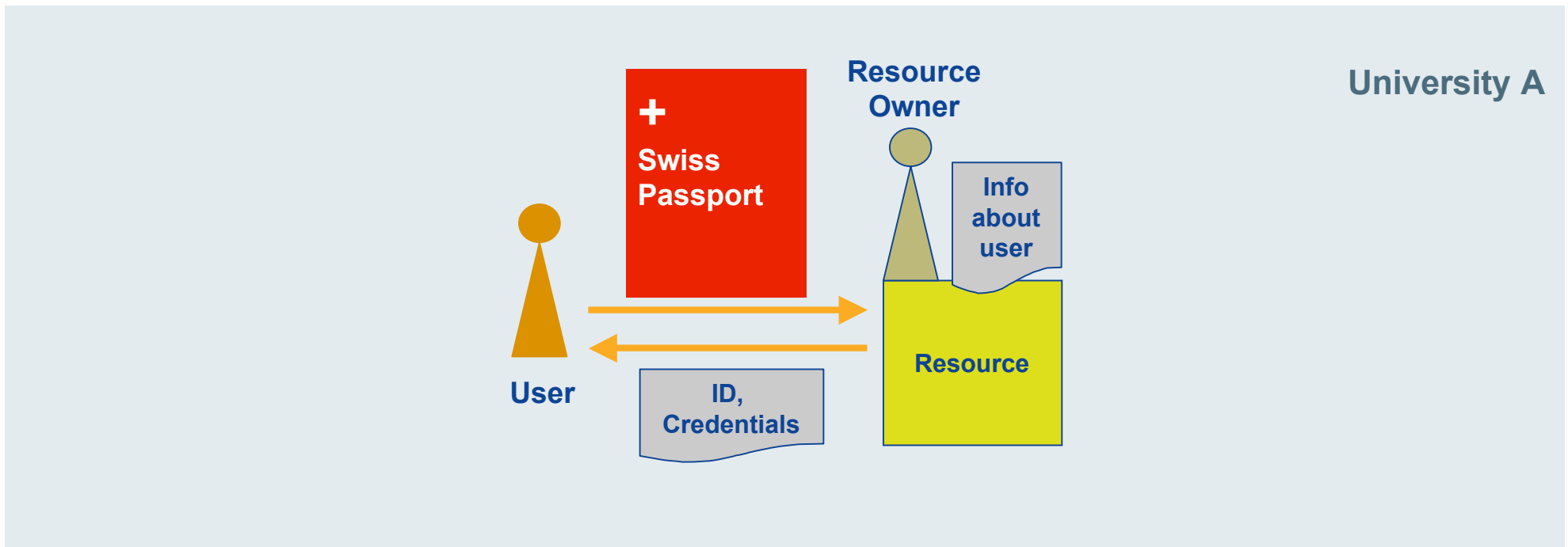
Stockholm

26. November 2002

Rolf Gartmann & Thomas Lenggenhager



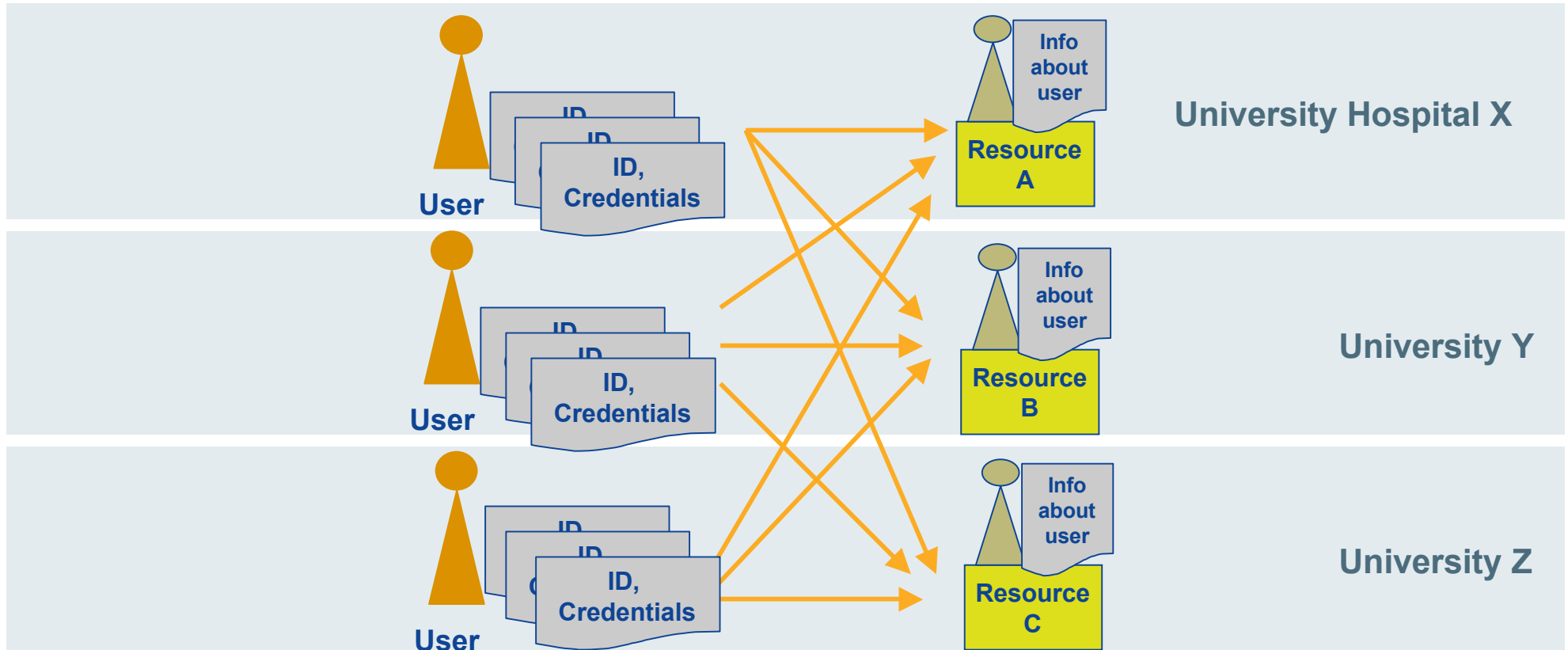
The AA Problem (1)



1 user – 1 resource – 1 organization

⇒ NO PROBLEM

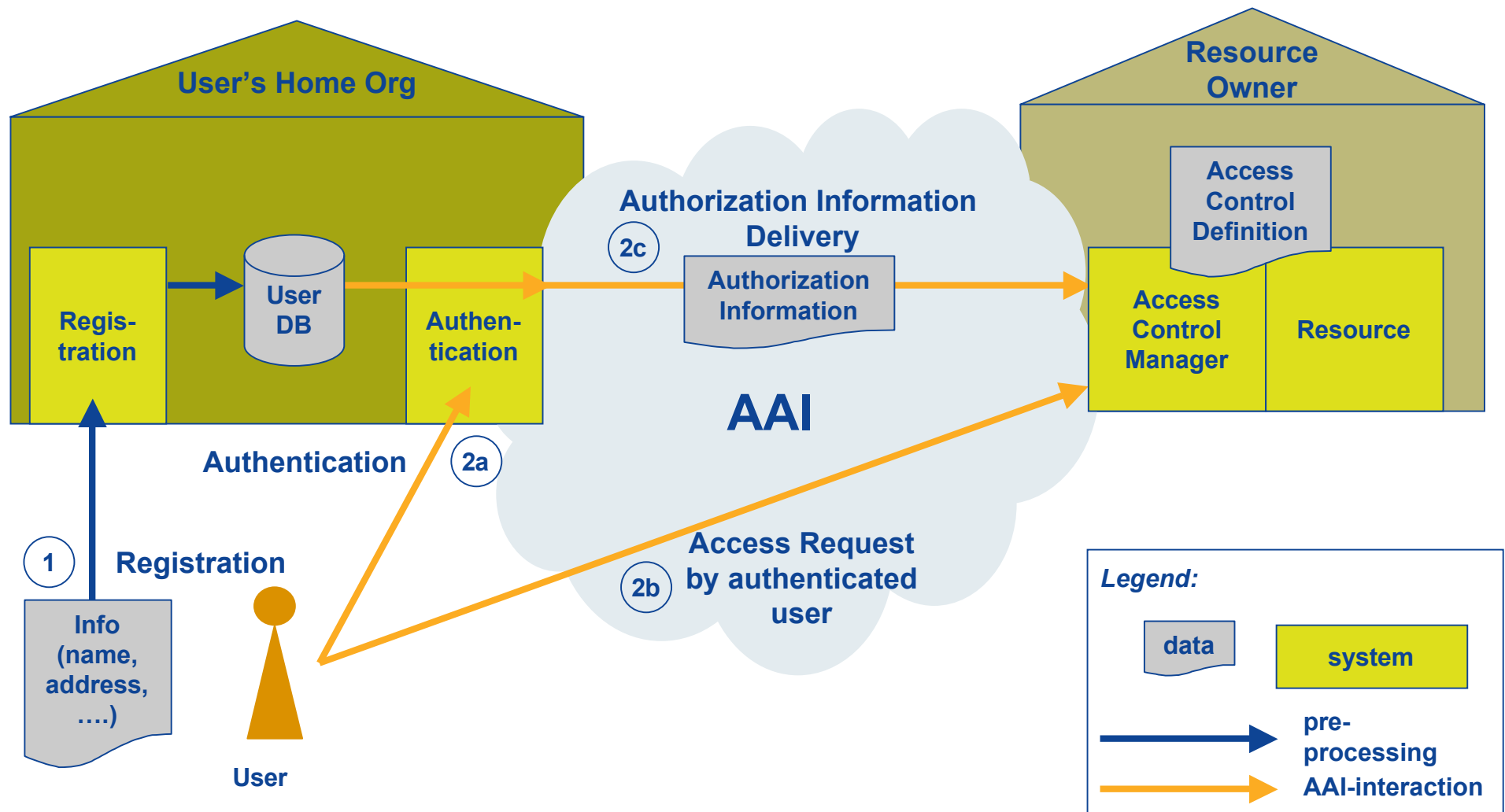
The AA Problem (2)

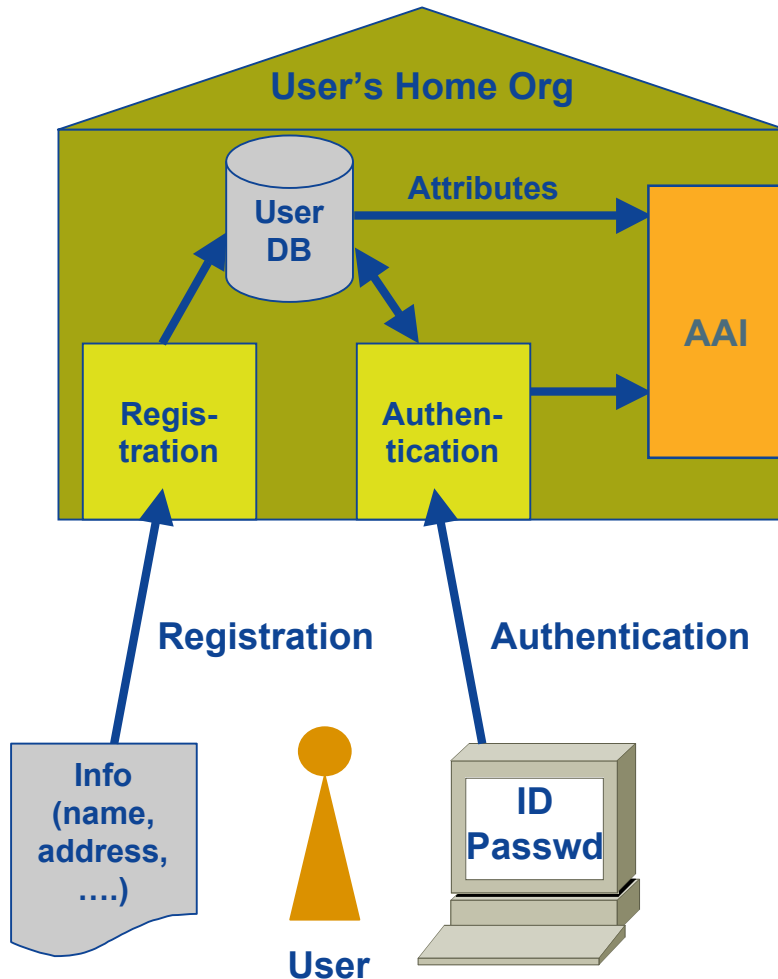


many users – many resources – many organizations

⇒ Big Problem

The AA Model





Preparation

- Registration Process
- Secure Central Authentication System

AAI Integration with

- local authentication system
- user DB / directory

Personal attributes

- Unique Identifier (anonymous)
- Surname
- Given name
- Date of birth
- Gender
- E-mail
- Address
- Phone

Group membership

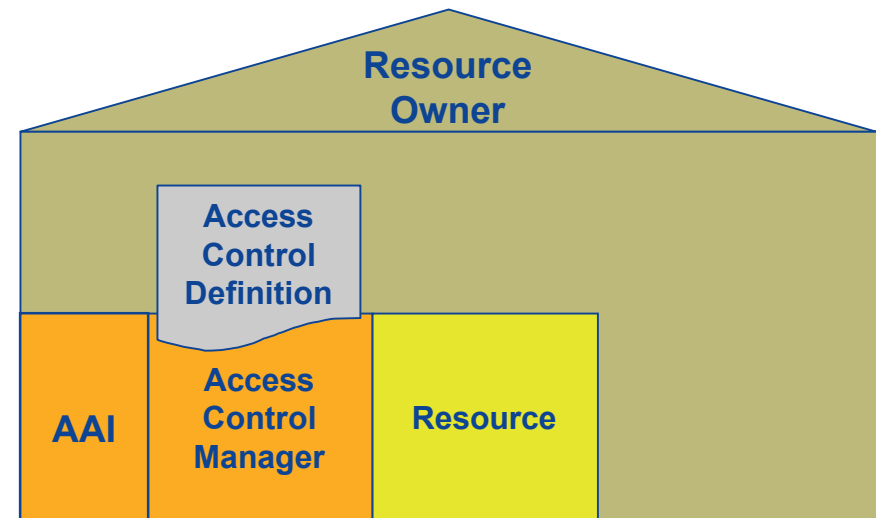
- Name of Home Organization
- Type of Home Organization
- Affiliation
- Study branch
- Study level
- Staff category

User attributes for AAI

- based on
 - eduPerson
 - definition for Swiss university statistics
- mandatory / recommended / optional
- handling according to data protection laws
- future extensions according to needs

Resource stores no user specific information beyond sessions

Access control policy based on group membership attributes
⇒ AAI plug-in for web server

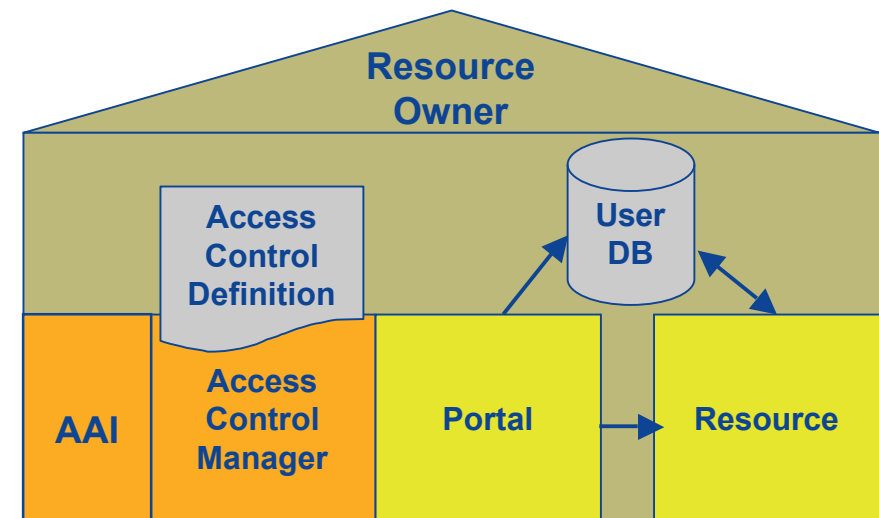


Examples

- content providers, libraries
- non-public web content
- Intranet

Resource stores additional non-AAI attributes per user

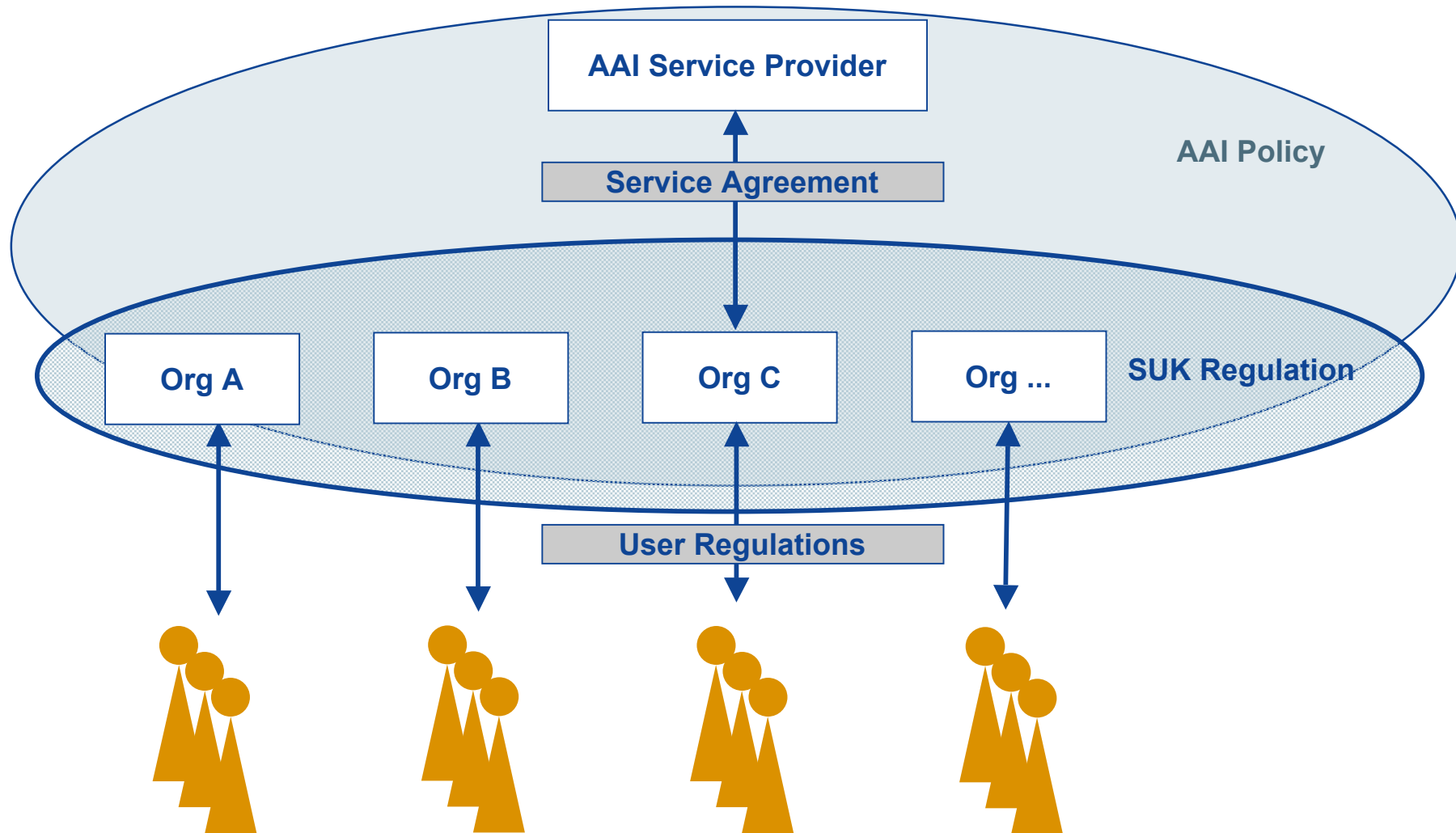
Access control policy based on group membership and / or personal attributes



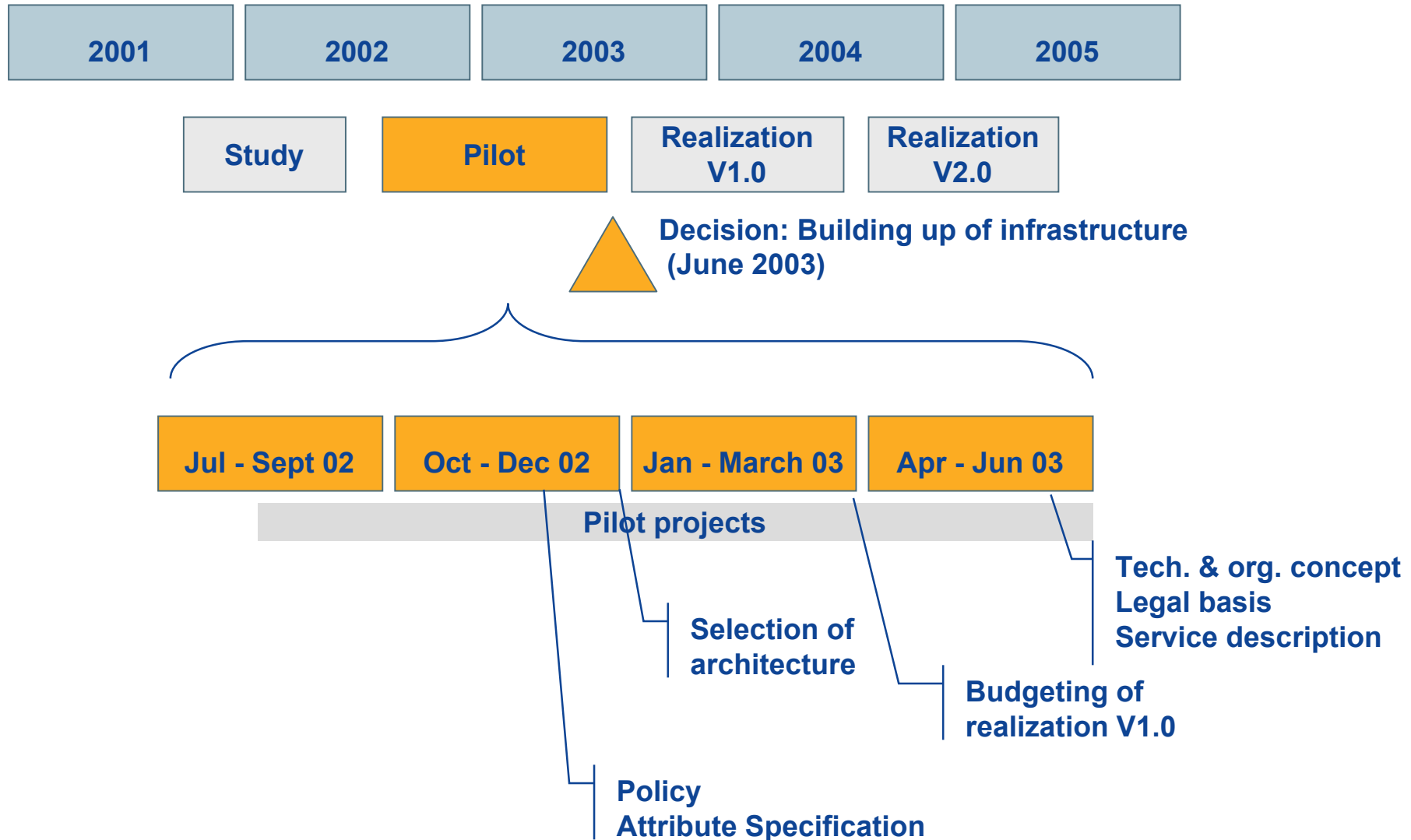
Examples

- e-learning platform
- student administration
- groupware, web mail

Legal Basis of an AAI



Project Planning: Roadmap



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

- AAI Report of the Preparatory Phase
July 2002, 72 pages, English
- AAI Folder
non technical introduction to the topic
Sept. 2002, 4 pages, English, French, German, Italian

Contact aai@switch.ch

AAI Pilot Phase

- **Get a feeling for the architectures:**
(PAPI, Tequila:Rolf Gartmann, Shibboleth:Ueli Kienholz)
- **Reference installations**
- **Build up a Center of Competence**
- **VHO-T / Resources / Forum as a personalized resource**
- **VMware Instances as test platform (Linux based)**

PAPI 1.1.0 - Open Issues

- Well suited at an enterprise level
- Group based assertions about users (and not Attribute based)
- Transmitted information to Resources
- Different assertions about users to different PoA's not solved in this version (no Attribute Policy)
- Most authorization is done at the AS (and not at the PoA as needed in our environment)
- N x M dependency (AS, PoA's)
- Personalized Resources
- Some issues should change in the next version

Shibb Alpha 2.5/Beta 1

Open Issues

- It IS Alpha Code
- Tricky to install
- Not ready for Pilot Projects
- Uncertain Roadmap (1.0 Release has been postponed)
- Not yet deployed (beside Alpha Pilots)
- Interesting Resources Provider already involved (e.g WebCT)
- supported/driven by Internet2

Tequila 1.0

- T'es qui là ? (Are you the one, which is here ?)
- Based on GASPARE (EPFL, enterprise level)
- Designed for a federated environment
- Small development team
- No deployment so far
- Simple, lightweight solution
- 'home made'
- Server side: Perl
- Client side: Perl, Java, 'raw interface'

Tequila Architecture

