SWITCH

The Swiss Education & Research Network

## Pilot Projects
# Coordination Workshop

| | |
|---|---|
| Date: | 18. February 2003 |
| Time: | 09:30 – 12:30 |
| Place: | University of Bern, Gesellschaftsstrasse 6 |

SWITCH aai

# Agenda

| Agenda | | |
|---|---|---|
| **09:30 - 09:45** | Introduction | Christoph Graf |
| **09:45 – 10:15** | Project News: (DRAFT)<br>• Shibboleth News<br>• Task Force Certification Authority (AAI-TF-CA)<br>• Task Force "Finance" (AAI-TF-FIN)<br>• System and Interface Specification | Rolf Gartmann, Christoph Graf, Thomas Lenggenhager |
| **10:15 – 11:45** | Status of Pilot Projects<br>• Goals<br>• Project Plan<br>• User Community / Attribute Requirements<br>• Dependencies<br>• Required support from SWITCH | Project Leaders |
| **11:45 – 12:15** | • Areas of Cooperation<br>• Letter of Intent<br>• Program Management | Christoph Graf |
| **12:15 – 12:30** | Miscellaneous | All |
| **12:30 – 13:30** | Lunch | All |

# Shibboleth News

- Current version is Shibboleth 0.7 (26. November 2002)
- Next versions expected:
  - 0.8: 1. March 2003
  - 1.0: 9. April 2003 (before Internet2 Spring Meeting)

- New implementation of ARP storage with ‘plug-ins’ probably not finished for 0.8, expected sometime in spring.
- Shibboleth will get support for ‘list of attributes requested by SHAR’.
- Interactive user-involvement before attribute release to come later on.

# Why PKI for AAI?

There are lots of servers talking to each other:

- – Across organisational boundaries
- – Within the Swiss academic community (for the time being)

We want server authentication and traffic encryption

- – Data protection issues
- – Liability issues

-> SSL for encryption and authentication

-> looks like a typical PKI scenario

-> we need to find a suitable CA

# CA Approaches

Global: Trust Verisign like everybody else

- Pro: very simple trust relationship management
- Cons: hassle, cost, blind trust on strangers

Community: Trust a community CA operator

- Pro: very simple trust relationship management, less hassle
- Cons: find someone trustworthy and cheap enough to do it

Local: Trust your local organisational CA operator

- Pro: limited number of trust relationships to manage
- Cons: trust relationships to manage

Individual: self signed certs everywhere (like PGP)

- Pro: easy to set up
- Cons: hassle to manage the trust relationships, NxN problem

# Some (not so) wild Guesswork

We can do better than approach „global“

Mix of „local“ and „community“ looks promising

Not only AAI needs such a service, others will as well

It pays to co-operate, we prefer not to create a solution for AAI only

AAI does not need end user client certs, we think we are not the only ones

# Task Force “AAI-TF-CA”

SWITCH
The Swiss Education & Research Network

## Introduction

AAI, like many other applications, uses SSL for traffic encryption and server authentication. AAI needs therefore a suitable CA and would like to join forces with other projects having similar requirements

| Start | End |
|---|---|
| 1 March 2003 | 30 April 2003 |

## Input

- Preparatory study (www.switch.ch/aai)
- Shibboleth doc (shibboleth.internet2.edu)

## Goals

- Architectural design of a CA, satisfying the needs of the AAI project and other projects with reasonably similar requirements

## Dependencies

## Tasks

- Survey of projects requiring PKI services
- Describe CA requirements of those projects, sketch CA architecture candidates
- Find the best CA architecture candidate
    - satisfying a maximum set of projects (including at least AAI)
    - still providing advantages compared with an AAI-only approach
- Use this candidate to draft an architectural CA design, covering its services and policies.

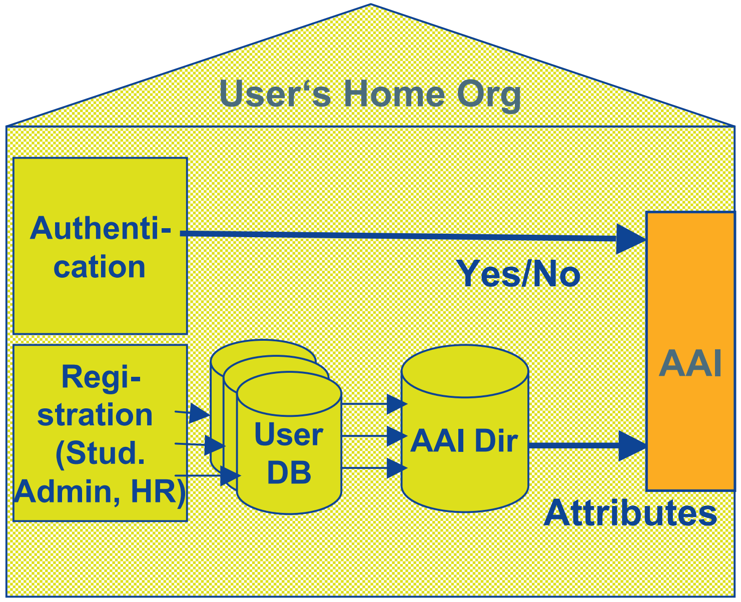
## Members

**You are invited to participate in this task force.**

**Please, subscribe to the AAI-TF-CA mailing list:**

**http://chx400.switch.ch/mailman/listinfo/aai-tf-ca**

# Cost factors for Home Org



## One-time Cost

- AAI Hardware
- AAI Software installation
- Integration of Authentication System
- Adaptation of Registration application
- Integration of User Directories
- Organizational changes (Registration, AAI-Support)
- Data consolidation
- Education (IT, Registration, HR)

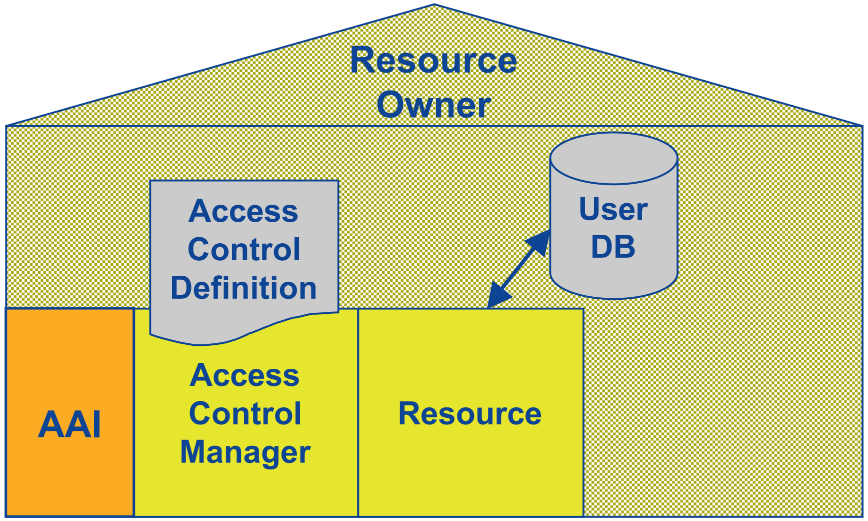
## Repeating cost

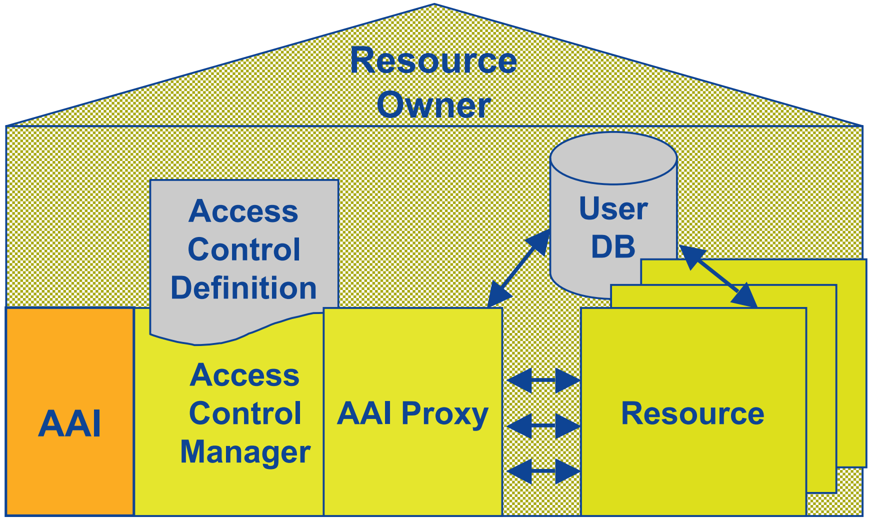
- Hardware and software maintenance fees
- AAI support (manpower)
  - operation
  - 1st, 2nd level support
  - Upgrades, maintenance
  - configuration (Attr release policy, …)
- Additional registration costs per user (if any)

## Assumption

- User Registration and Authentication are implemented (infrastructure, processes)

# Cost factors for Resource Owners





## One-time Cost

- AAI installation
- Resource integration
- Education
- For AAI Proxies:
  - » AAI Proxy Hardware
  - » AAI Proxy Software implementation and installation

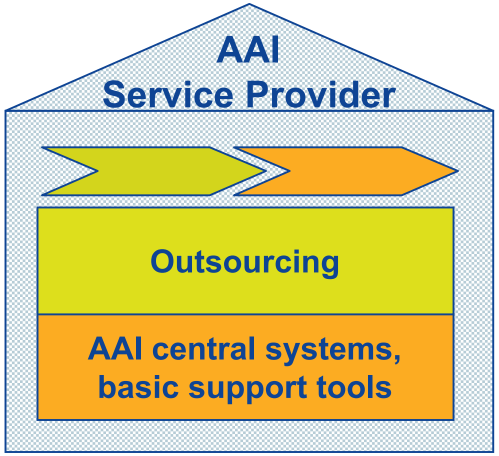
## Repeating cost

- Hardware and software maintenance fees
- AAI support (manpower)
  - » operation
  - » 1st, 2nd level support
  - » Upgrades, maintenace
  - » configuration (Access control, …)

## Assumptions:

- Basic AAI Proxy Software is available (AAI-Pilot)

# Cost factors for Service Provider



## Central AAI Services

## One-time Cost

- Central AAI systems (WAYF, CA/RA, Resource Directory)
  - Hardware
  - Software installation
- Setting up of Competence Center
  - Consulting Services
  - Test Lab

## Repeating cost

- AAI Marketing and Education
- AAI Consulting
  - For Home Orgs
  - For Resource Owners
- AAI Test Lab
- Operation of central AAI systems:
  - Support (manpower)
  - Maintenance fees

## Outsourcing Services

## One-time Cost

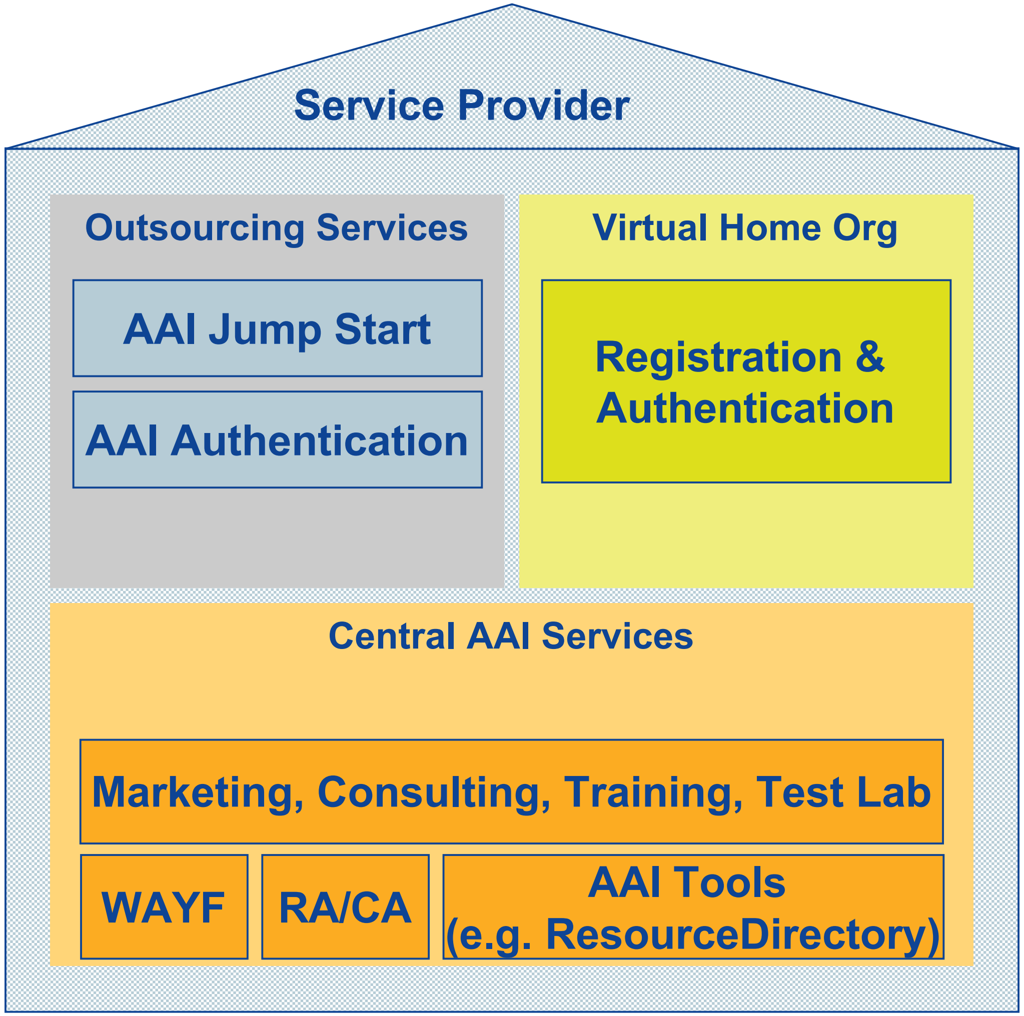
- Implementation of
  - Authentication Service
  - Virtual HomeOrg Service
  - Portal Service?

## Repeating cost

- Operation of Outsourcing Services
- Improvement of Outsourcing Services

# SWITCH's Offering

SWITCH
The Swiss Education & Research Network



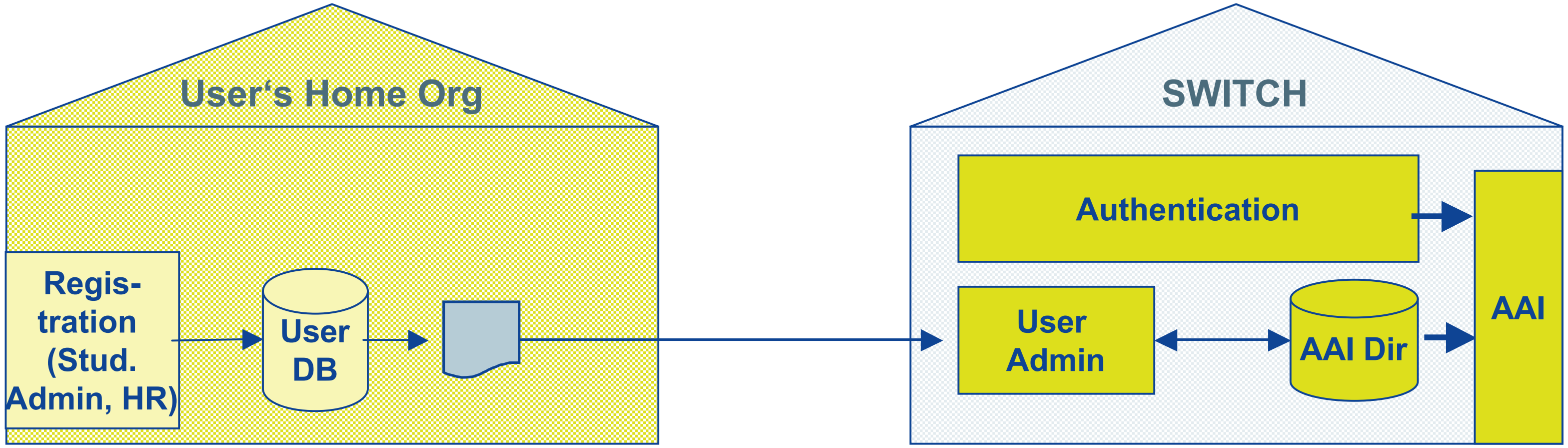
**Central AAI Services**
- Operation of central AAI components
- Center of Competence, Test Lab
- Training and Consulting
- Strategy and Marketing
- Legal Consulting

**Outsourcing Services**
- Outsourcing Services for Home Organizations
  - permanent
  - temporary

**Virtual Home Org**
- Operation of a virtual Home Organization, mainly for people with a legal right to access AAI-protected resources but without formal relationship with a 'real' Home Organization

# AAI Jump Start Service: Description

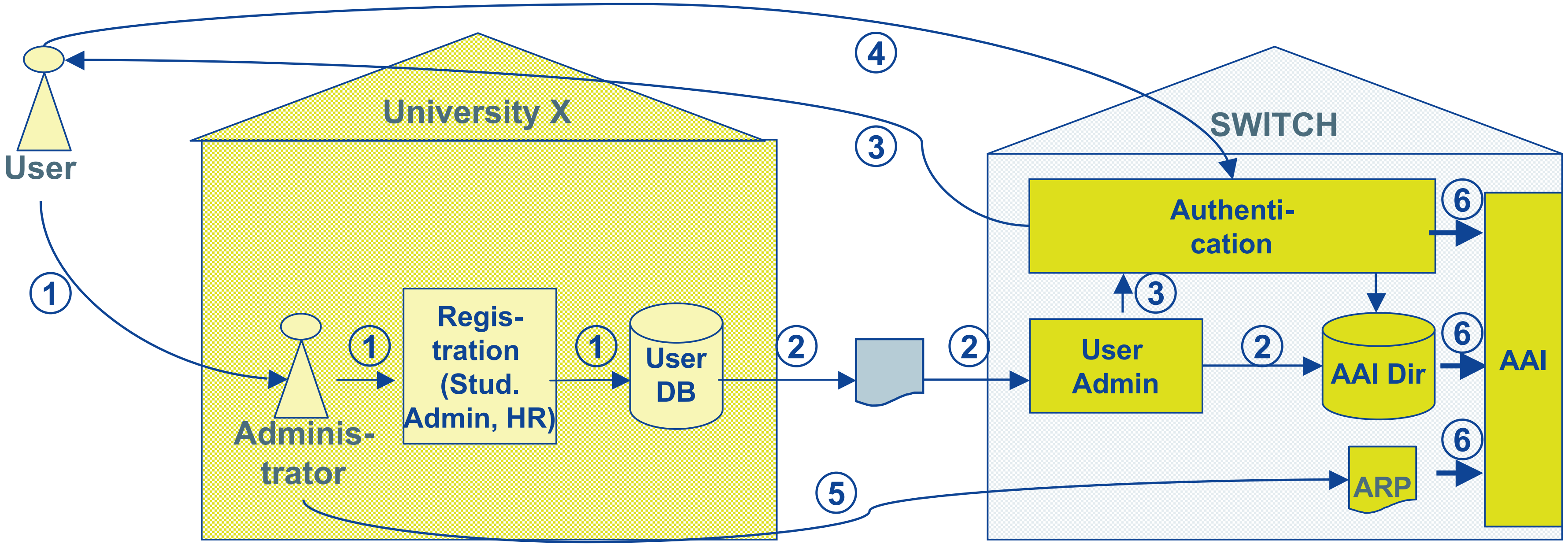
SWITCH
The Swiss Education & Research Network



| AAI Jump Start Service | |
|---|---|
| Customers | Home Organizations |
| Description | • Basic authentication system and AAI attribute directory operated by SWITCH<br>• Web-based user interface for password administration by end user<br>• File-based bulk import of user data provided by Home Org, data conversion into AAI format (optional)<br>• Simple Attribute Release Policy (ARP) |
| Customer’s Responsibility | User registration, correctness of delivered user data |
| SWITCH’s Responsibility | Operation of authentication system, AAI dir, Shibboleth on behalf of a Home Organization, based on SLA |

# AAI Jump Start Service: Interactions

SWITCH
The Swiss Education & Research Network



1 Registration

2 Transfer of user data

3 Creation and transfer of user credentials

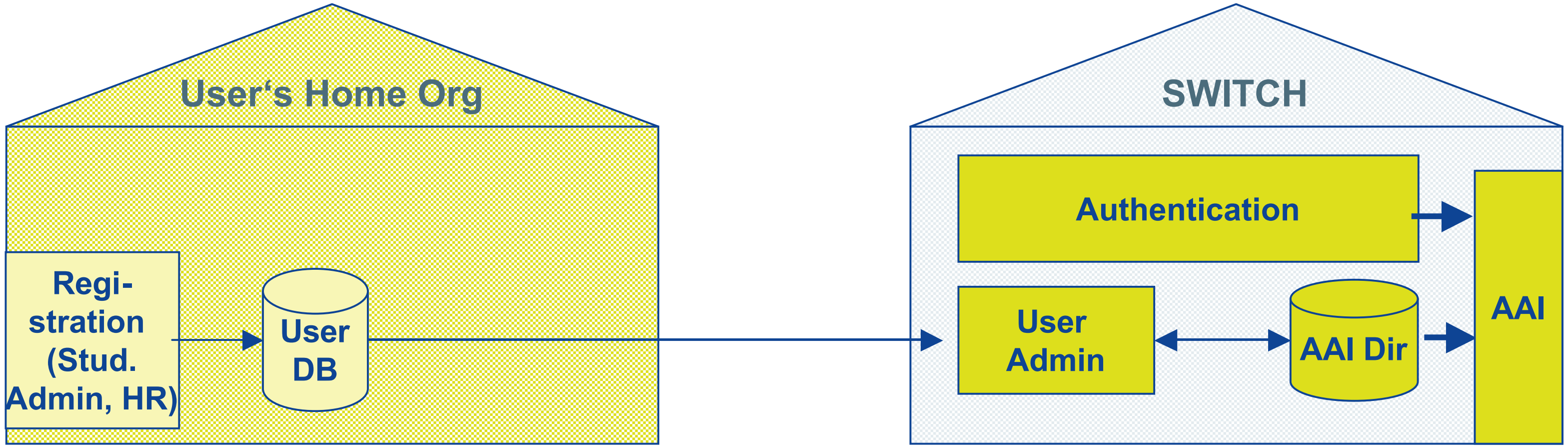
4 Password administration

5 Configuration of Attribute Release Policy (ARP)

6 Shibboleth interactions

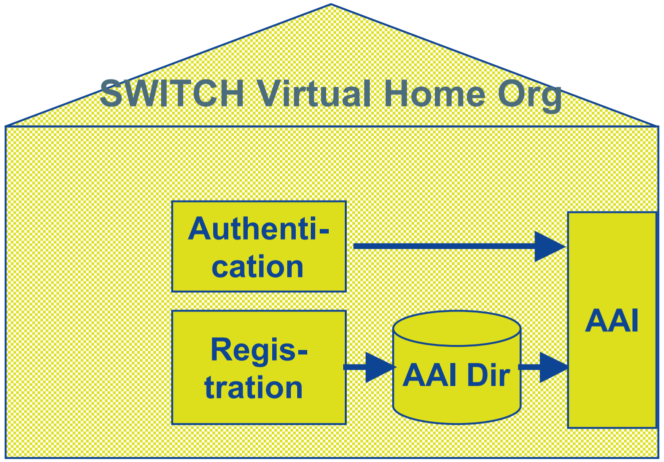
**SWITCH acts on behalf of University X**
**(authorization attribute "Name of Home Organization" = 'X.ch')**

# AAI Authentication Service: Description



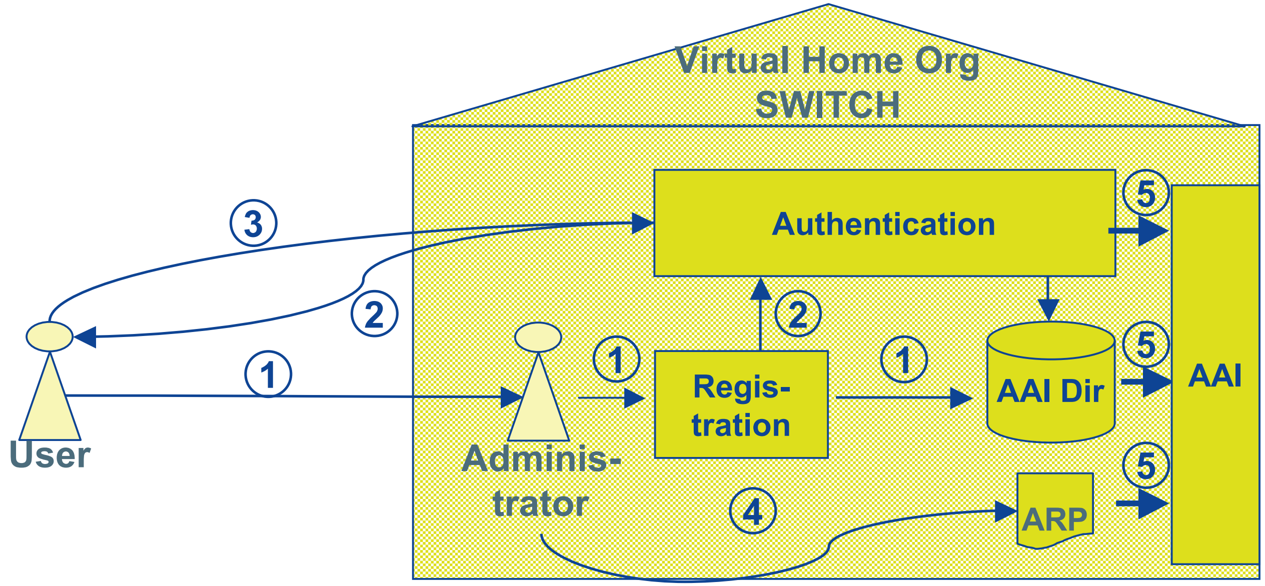
| AAI Authentication Service | |
|---|---|
| Customers | Home Organizations |
| Description | • Authentication system and AAI attribute directory operated by SWITCH<br>• Web-based user interface for Attribute Release Policy configuration by Home Org / by end user<br>• Web-based user interface to authentication system for end users<br>• Real-time coupling between AAI directory and Home Org's user databases, automatic data conversion into AAI format |
| Customer's Responsibility | User registration, correctness of user data |
| SWITCH's Responsibility | Operation of authentication system, AAI dir, Shibboleth on behalf of a Home Organization, based on SLA |

# AAI Virtual Home Organization: Description



| AAI Virtual Home Organization Service | |
|---|---|
| Customers | Individuals not registered with a Home Organization (i.e. no student, no staff) |
| Description | • Complete Home Org Service provided by SWITCH<br>• user registration<br>• user authentication<br>• user attribute delivery |
| Customer's Responsibility | t.b.d. (end user regulation) |
| SWITCH's Responsibility | Fulfills AAI Policy (Home Org part) |

# AAI Virtual Home Organizations: Interactions

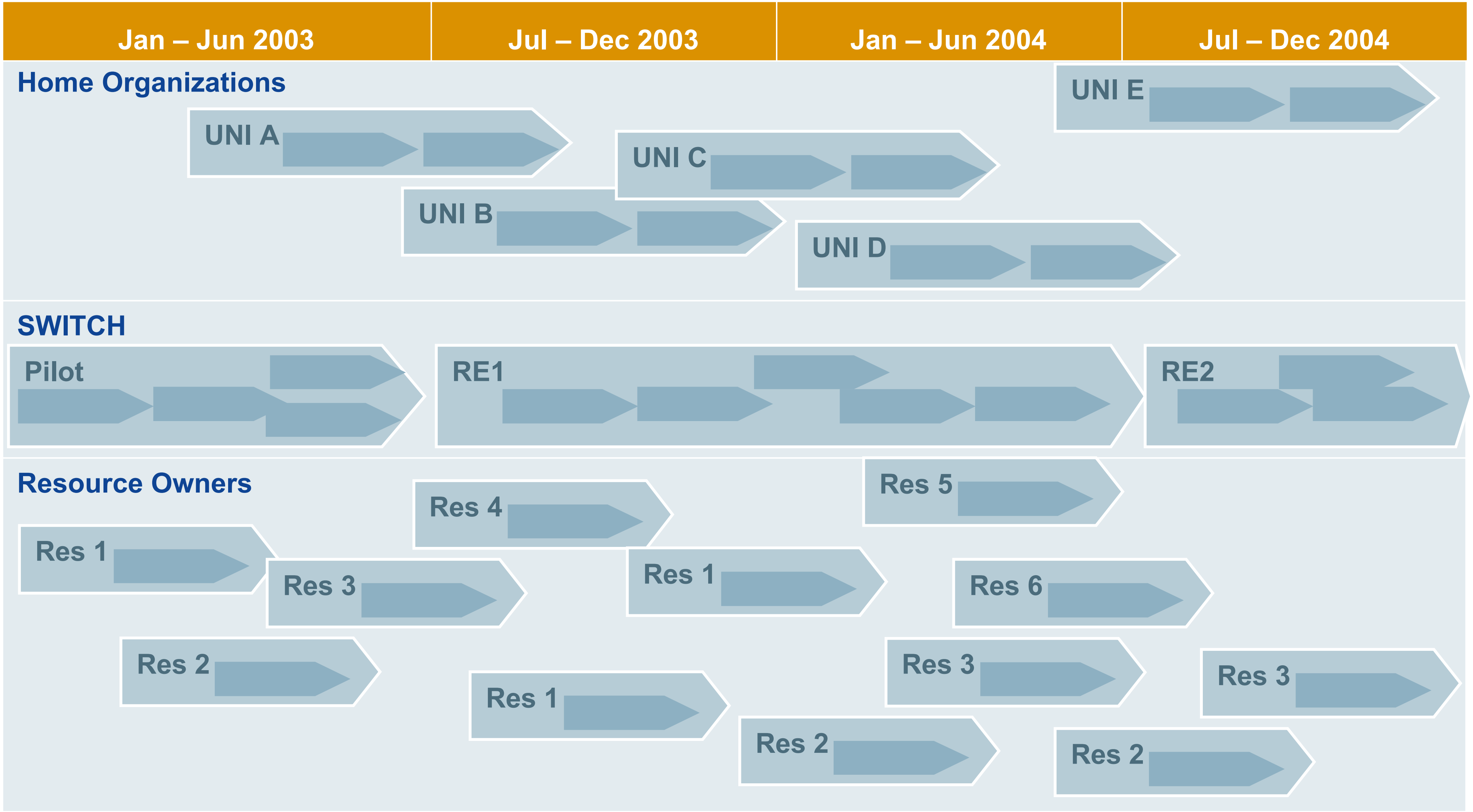


1. Registration
2. Creation and transfer of user credentials
3. Password administration
4. Configuration of Attribute Release Policy (ARP)
5. Shibboleth interactions

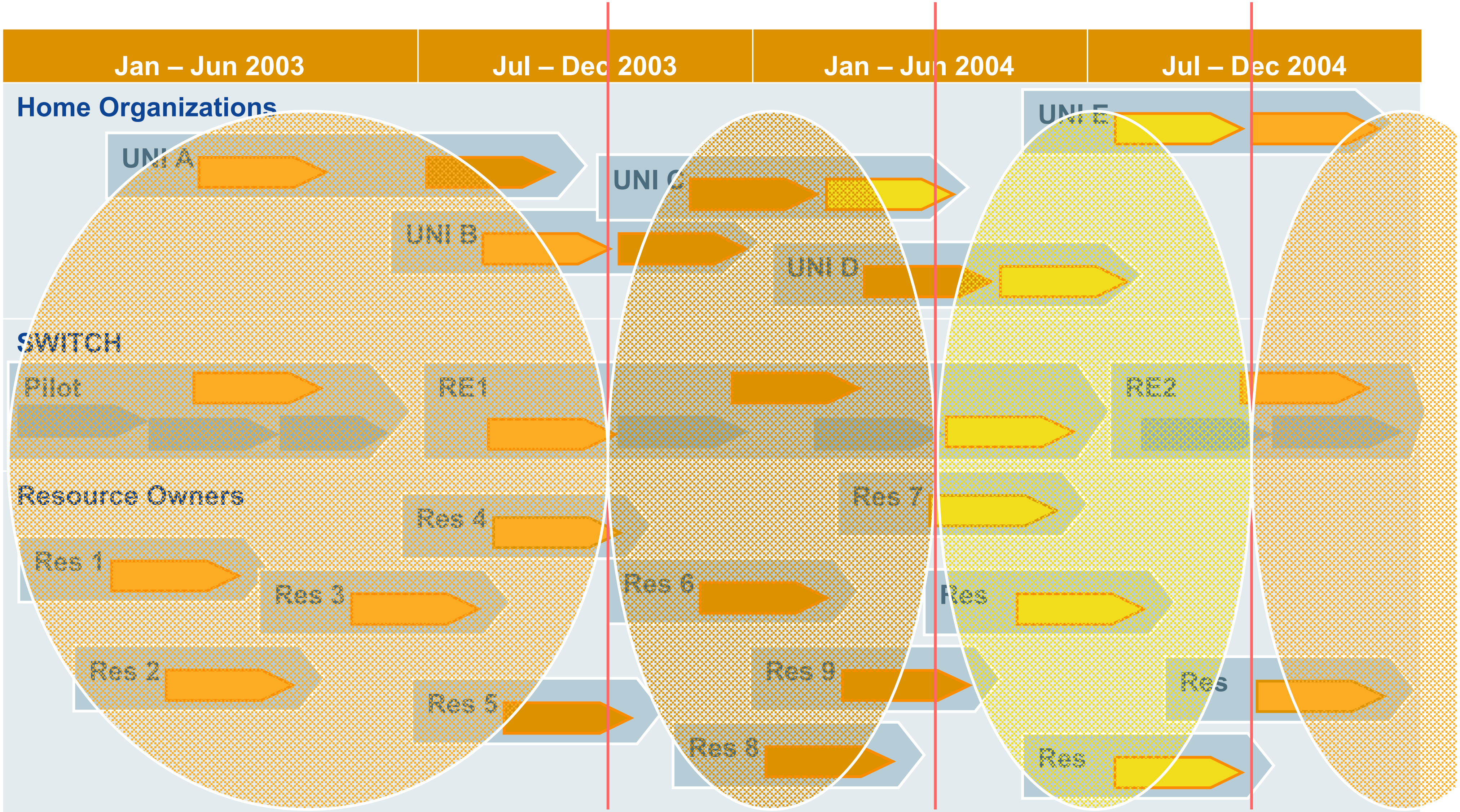
**SWITCH acts as a Home Organization**
**(authorization attribute "Name of Home Organization" = 'SWITCH.ch')**

# AAI Program Management

SWITCH
The Swiss Education & Research Network



# AAI Program Management


Jan – Jun 2003
Jul – Dec 2003
Jan – Jun 2004
Jul – Dec 2004
Home Organizations
UNI A
UNI B
UNI C
UNI D
UNI E
SWITCH
Pilot
RE1
RE2
Resource Owners
Res 1
Res 2
Res 3
Res 4
Res 5
Res 6
Res 7
Res 8
Res 9
Res
Res
Res