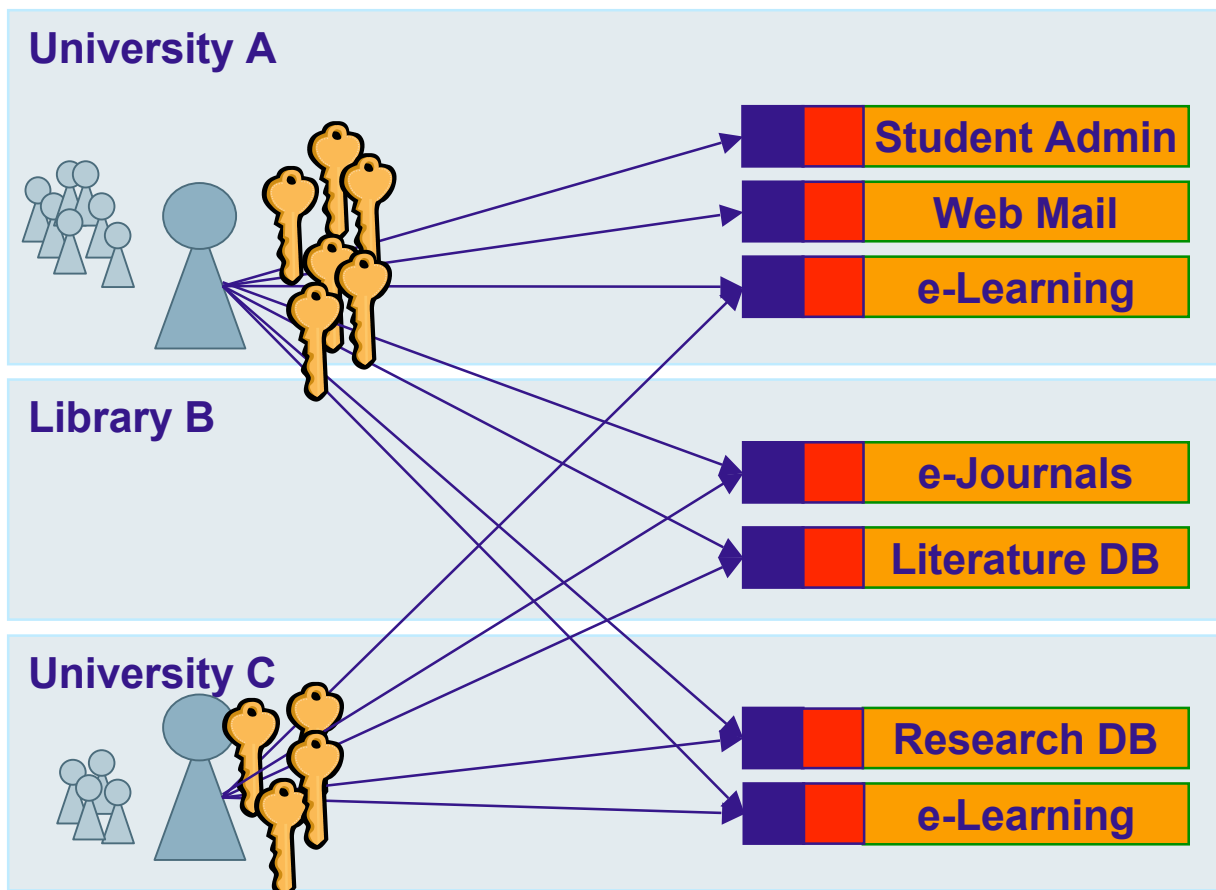

SWITCH

The Swiss Education & Research Network

AAI Introduction

The SWITCHaai Team, <aa@switch.ch>

Without AAI



- Tedious user registration at all resources
- Unreliable and outdated user data at resources
- Different login processes
- Many different passwords
- Many resources not protected due to difficulties
- Often IP-based authorization
- Costly implementation of inter-institutional access

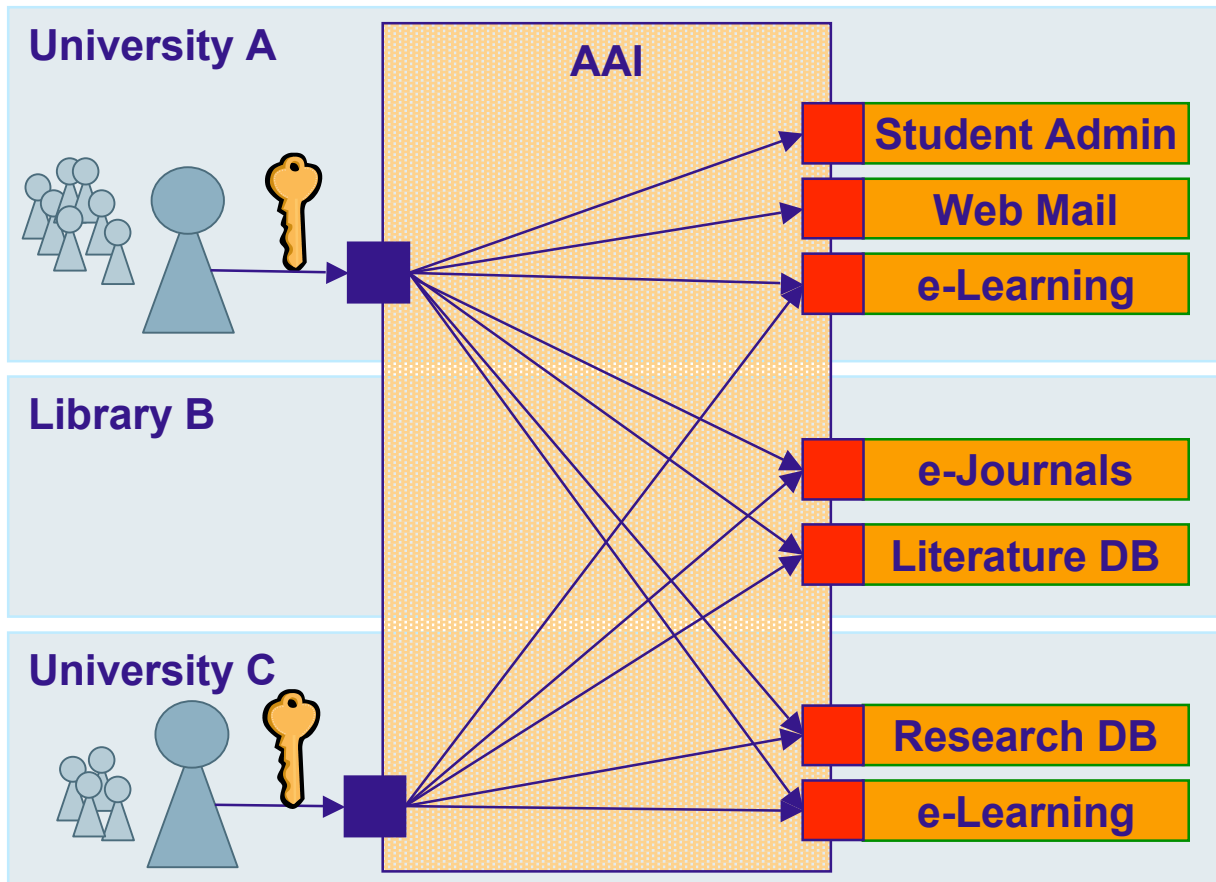
User Administration
Authentication

Authorization

Resource



With AAI



- No user registration and user data maintenance at resource needed
- Single login process for the users
- Many new resources available for the users
- Enlarged user communities for resources
- Authorization independent of location
- Efficient implementation of inter-institutional access

User Administration
Authentication

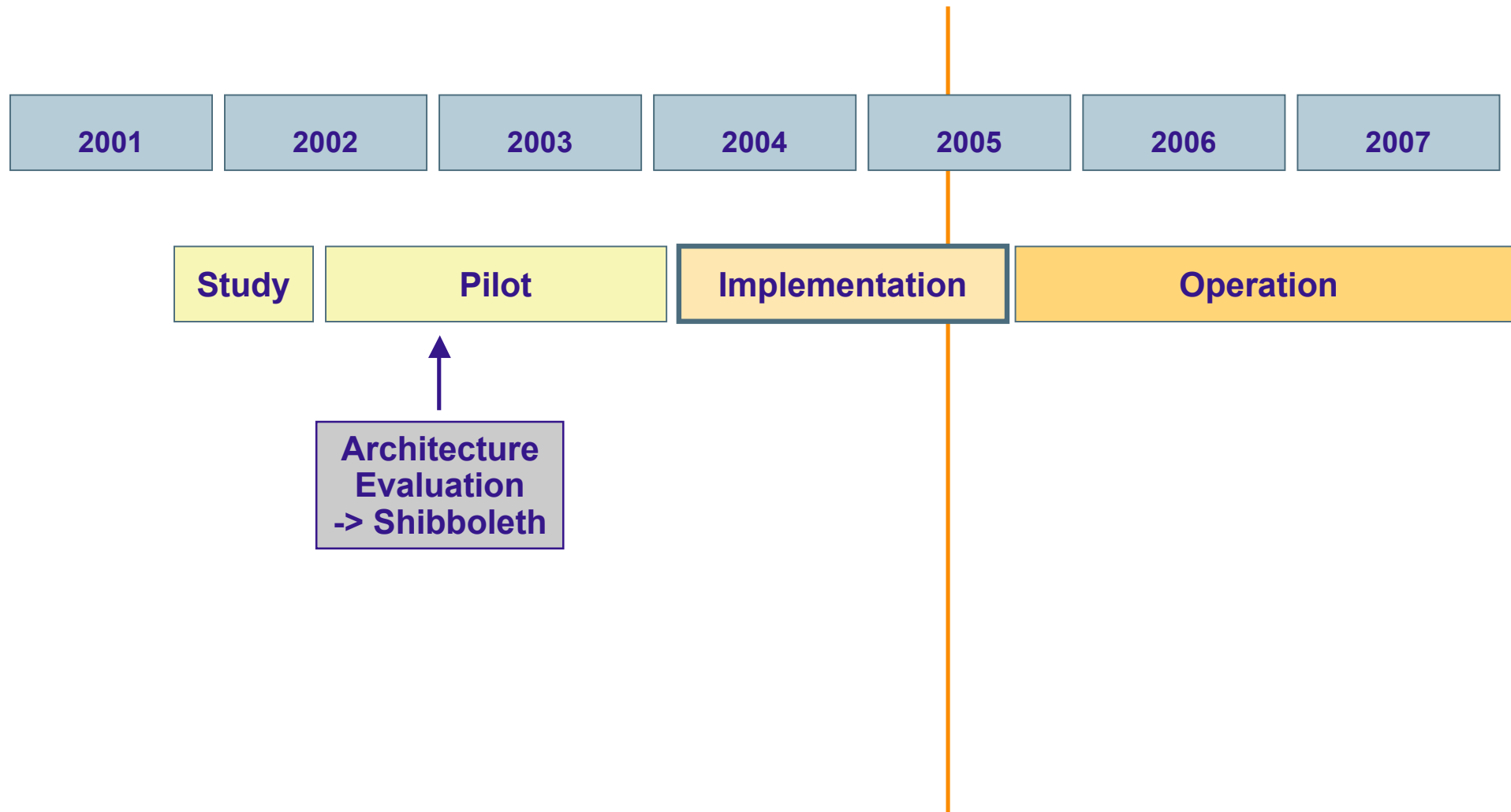
Authorization

Resource



Credentials

SWITCHaai Project Planning



- ❑ **Open Source**
- ❑ **Developed by Internet2**
- ❑ **Federated Approach**
- ❑ **Privacy**
- ❑ **National deployment projects in the US, UK and Finland, growing interest in other European countries**
- ❑ **For web resources only - as a first step**
- ❑ **Based on SAML**
- ❑ **Cooperations with Liberty Alliance**
- ❑ **Cooperations with Content Providers (e-journals)**

<http://shibboleth.internet2.edu/>

Internet Explorer (Windows)

- Click on Certificate
- Open
- Install Certificate
- Defaults OK

Safari (für OS 10.3 Panther)

- Download Certificate
- Doubleclick on File
- X509 Anchors
- Keychain Password = Administrator Password
- Keychain Access -> Quit Keychain Access

<http://www.switch.ch/pki/import.html>

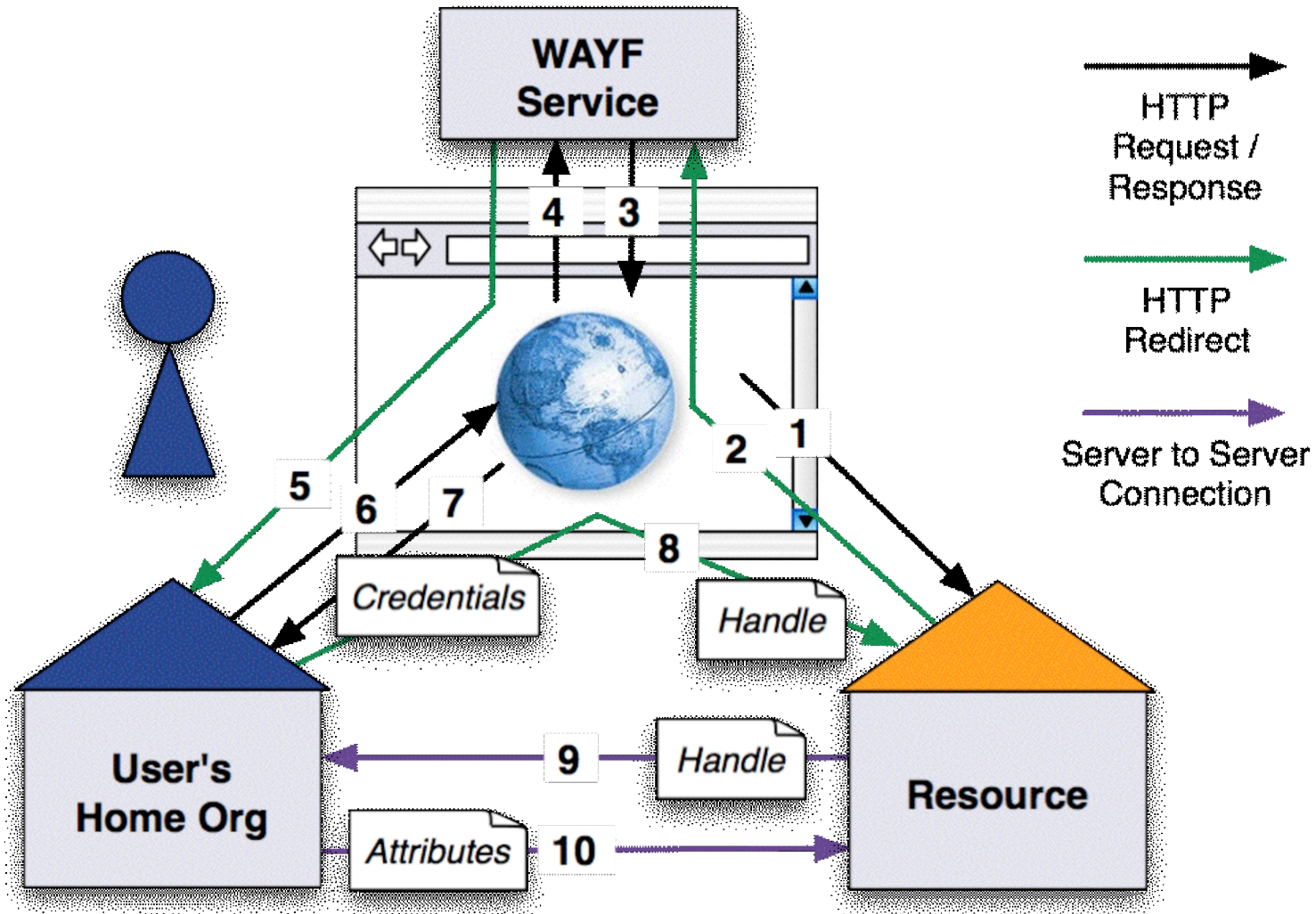
Demo (Try it yourself)

□ <http://www.switch.ch/aai>

-> Live Demo

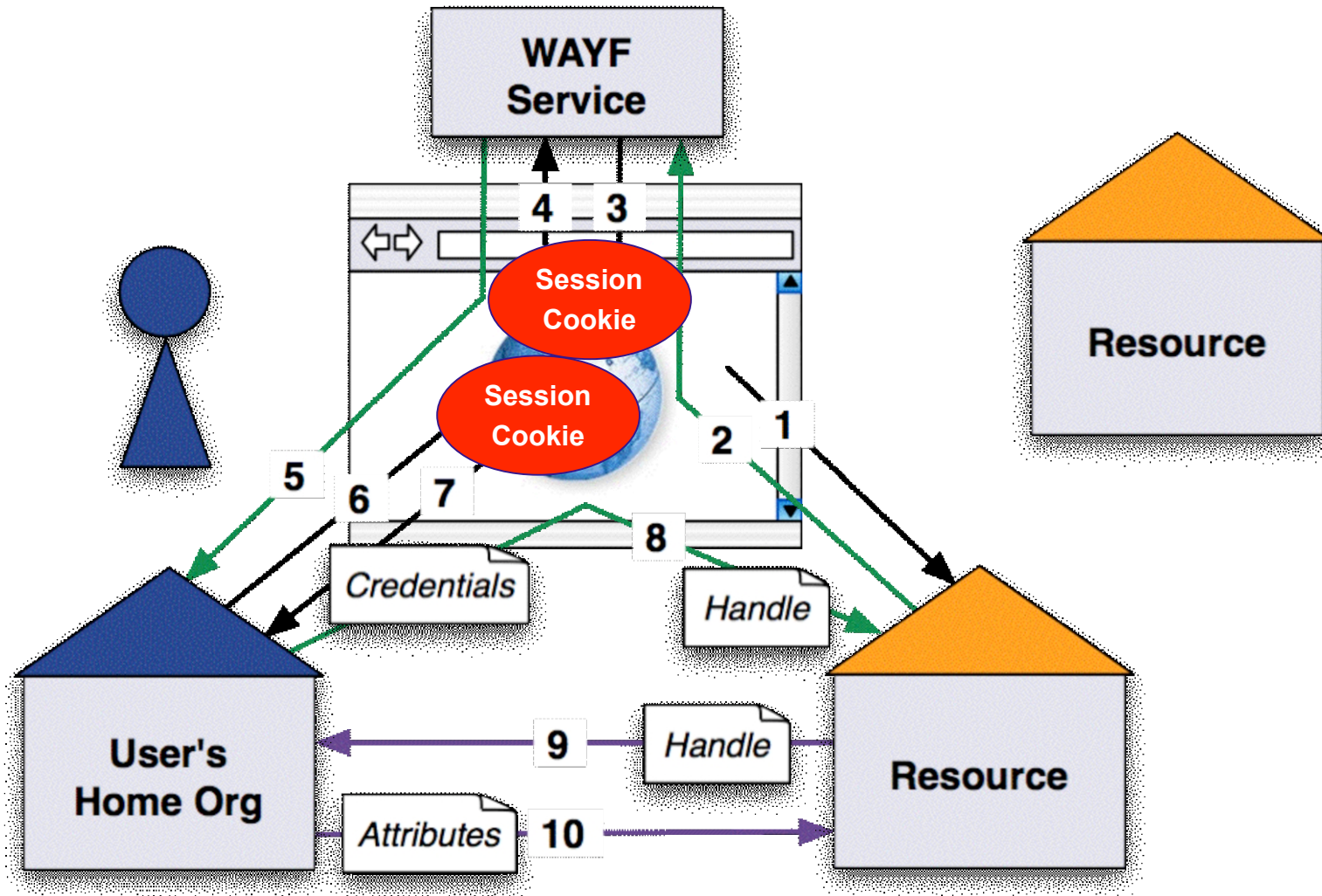
-> demo resource

http://www.switch.ch/aai/demo/demo_live.html



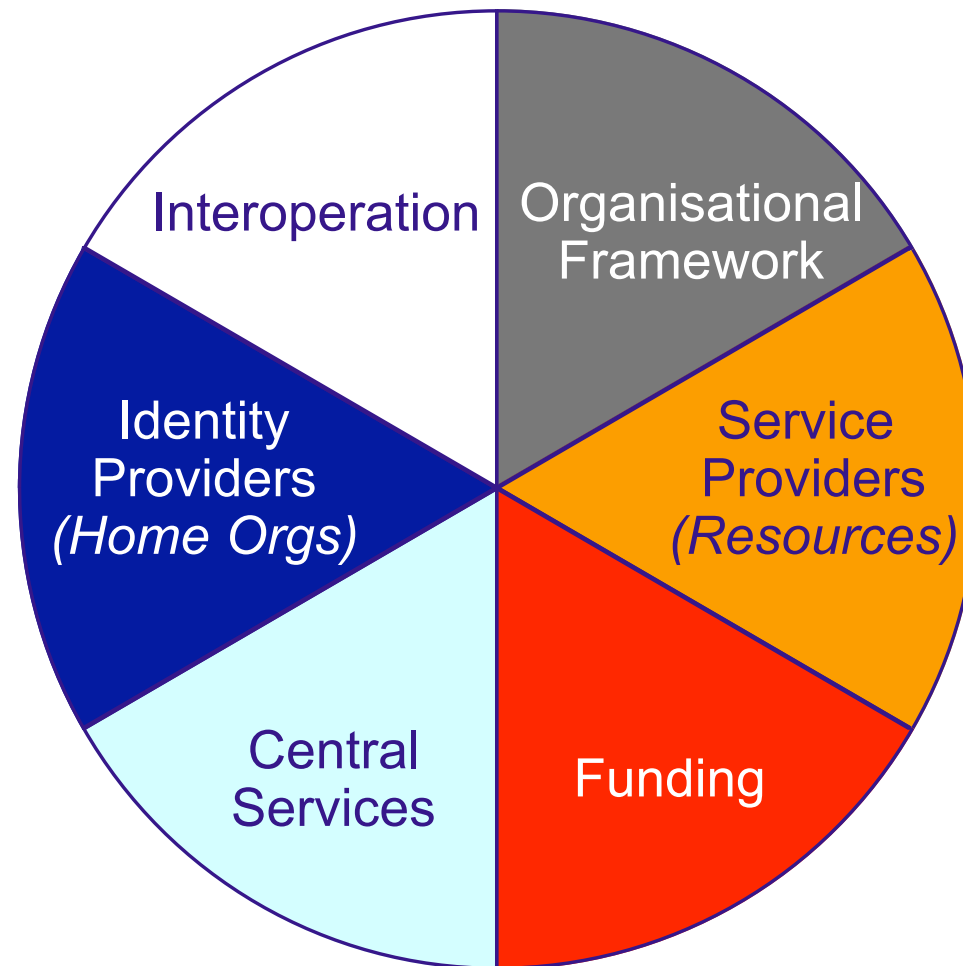
<https://kohala.switch.ch/secure>

Single Sign On





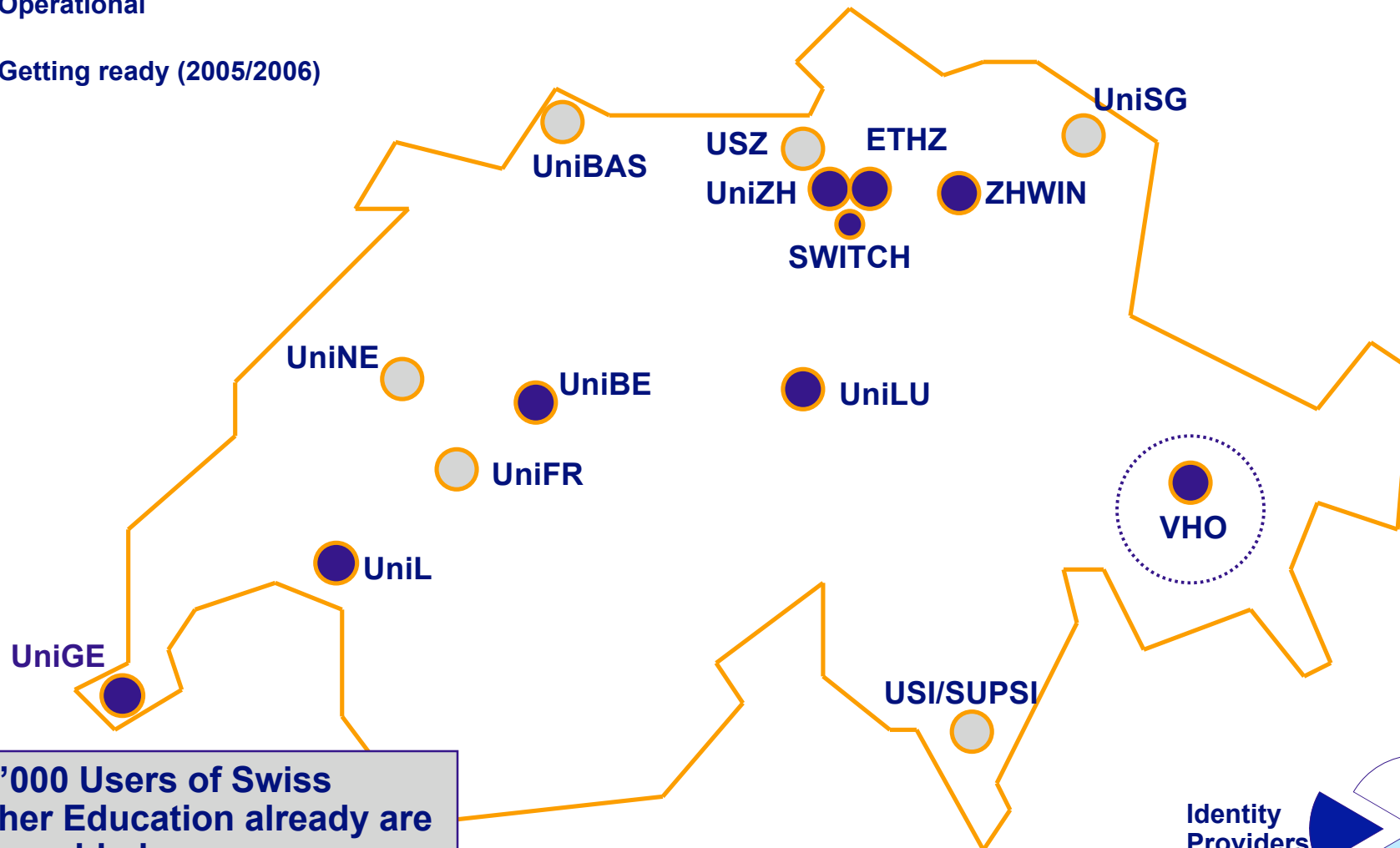
<http://www.computerkurse.ethz.ch/>

SWITCHaai Building Blocks



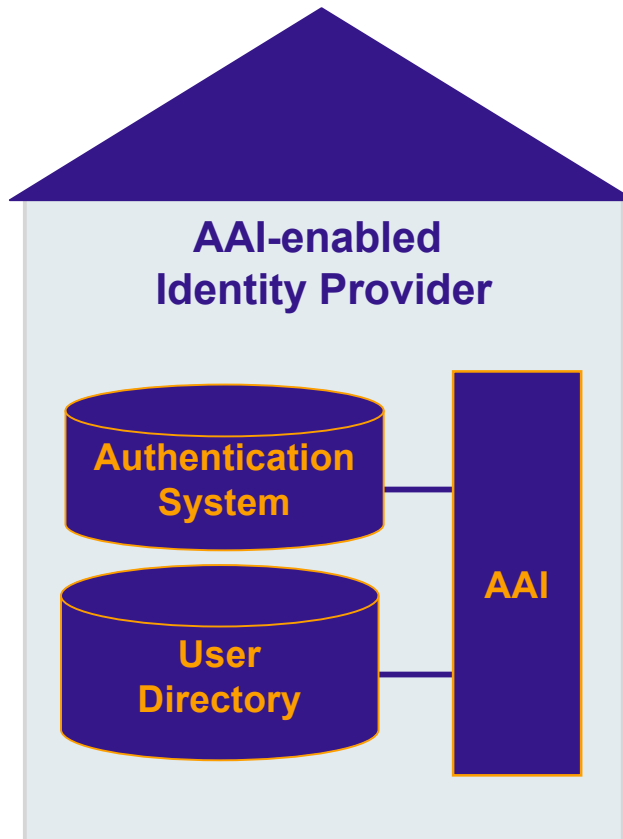
AAI Identity Provider

-  Operational
-  Getting ready (2005/2006)



110'000 Users of Swiss Higher Education already are AAI-enabled (= 50% of all users)





- **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



AAI Service Providers (Resources)

e-Learning

OLAT	Vista@SVC
WebCT@ETHZ	VITELS
DOIT	ILIAS
Moodle	BSCW
AD Learn & Co	Blackboard

Libraries

EZproxy
ScienceDirect
...

Other Web Applications

CompiCampus	SMS-Gateway	
Vconf	TWiki	IS-Academia

Commercial Contents

SwissLex
eShops

ca. 50 AAI-enabled hosts,
ca. 10'000 active users

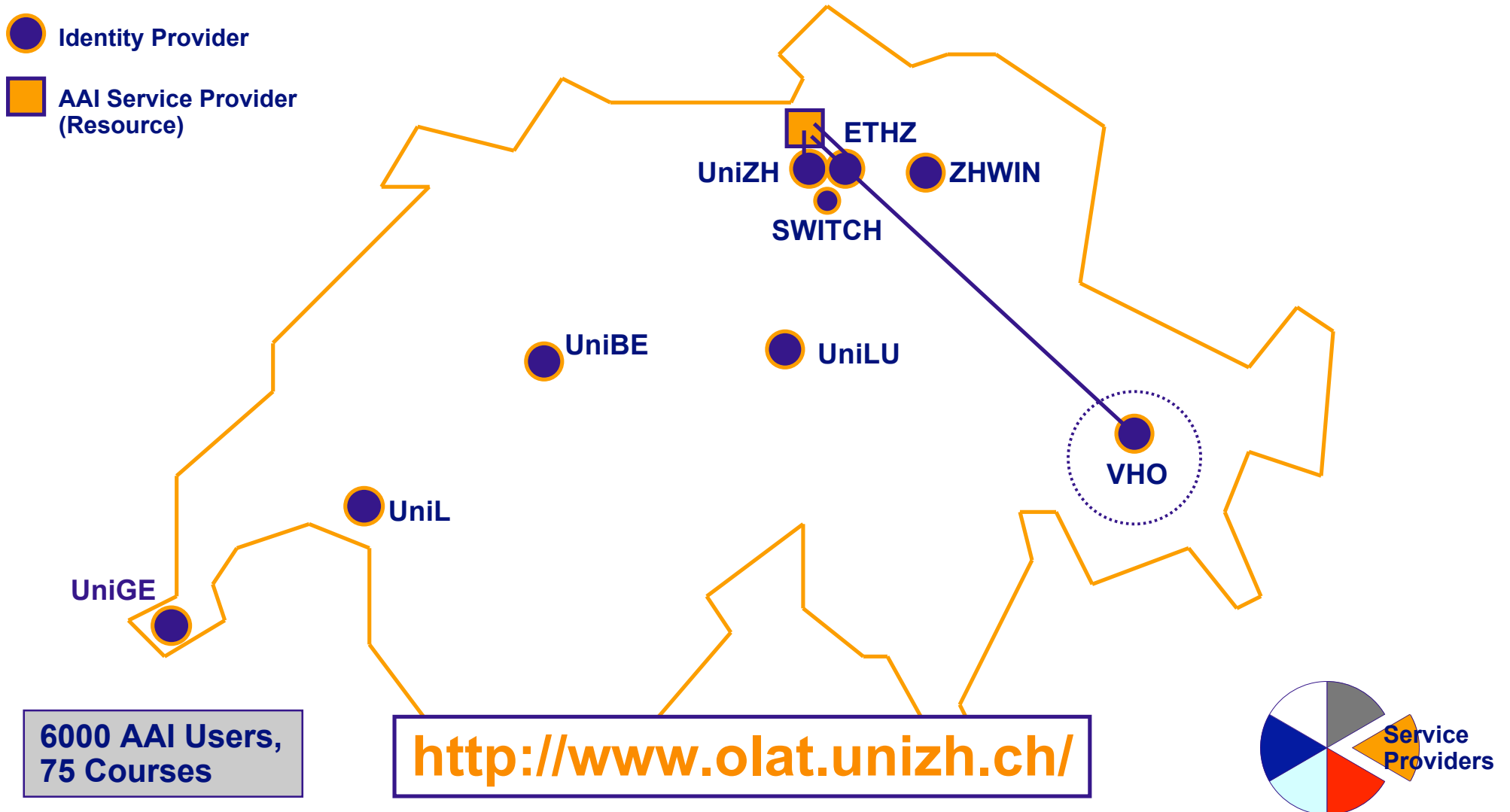


Showcase: OLAT

OLAT: Online Learning and Training (open source e-learning platform of the University of Zurich)



 Identity Provider

 AAI Service Provider (Resource)

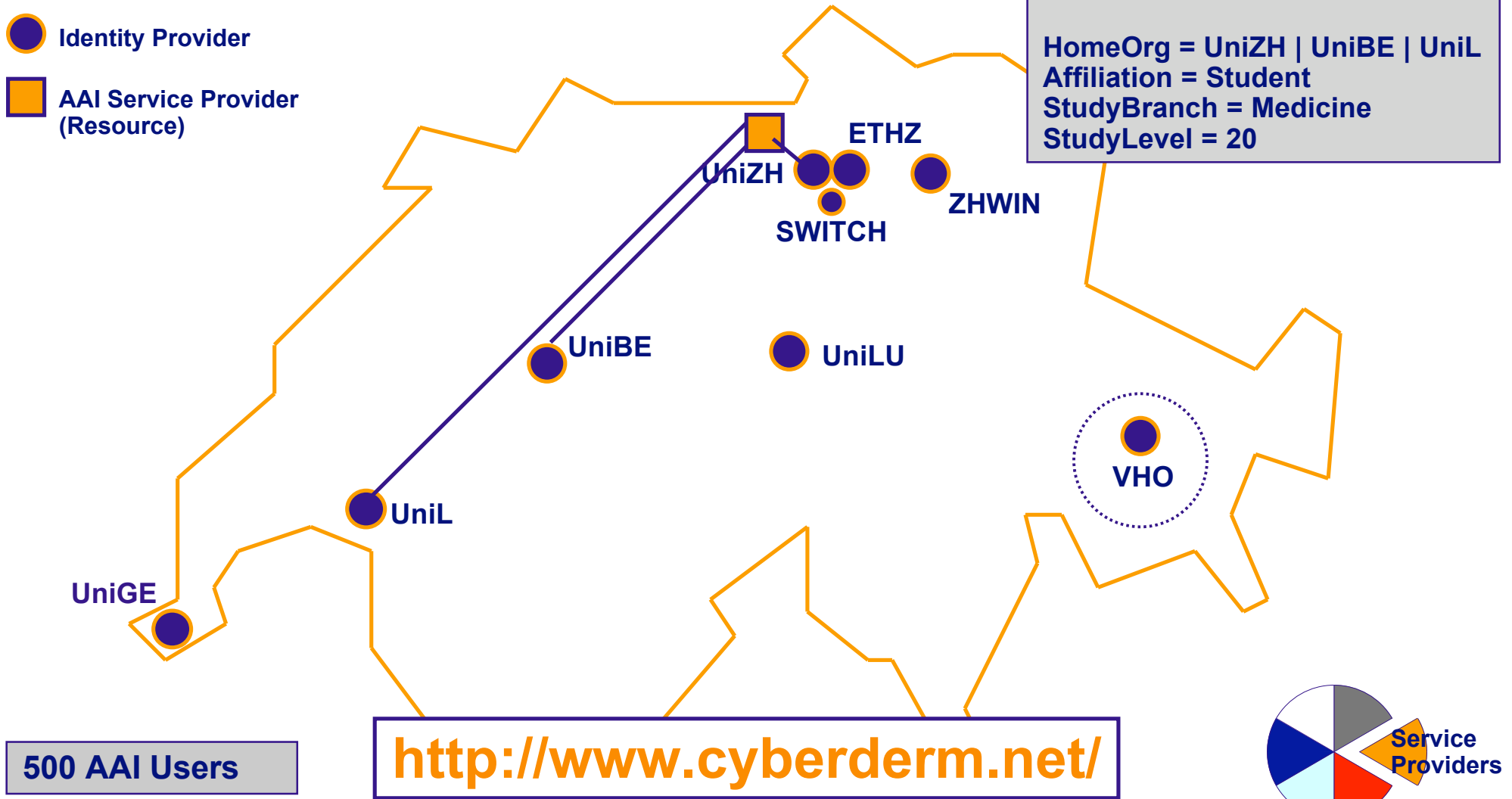


Showcase: DOIT

DOIT: Dermatology Online with Interactive Technology

-  Identity Provider
-  AAI Service Provider (Resource)

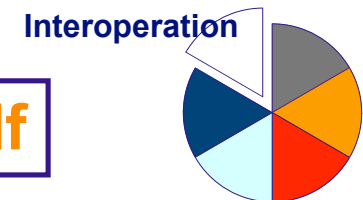
Access Rule:
HomeOrg = UniZH | UniBE | UniL
Affiliation = Student
StudyBranch = Medicine
StudyLevel = 20



Authorization Attributes (1)

- 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
- 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

http://www.switch.ch/aai/docs/AAI_Attr_Specs.pdf



Authorization Attributes (2)

Personal attributes

- **Unique Identifier**
- **Surname**
- **Given name**

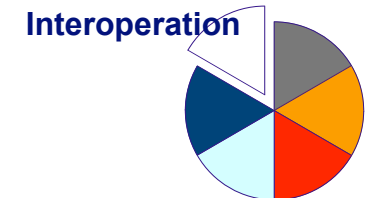
- **E-mail**
- **Address(es)**
- **Phone number(s)**
- **Preferred language**
- **Date of birth**
- **Gender**

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**

- 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

- Based on 'Schweizerisches Hochschulinformationssystem (SHIS/SIUS)'
<http://www.bfs.admin.ch> (Fachbereich Bildung und Wissenschaft)

- Example for Universities

studyBranch1 (8 codes)

4 Exakte + Naturwissenschaften — Sciences exactes + naturelles

studyBranch2 (21 codes)

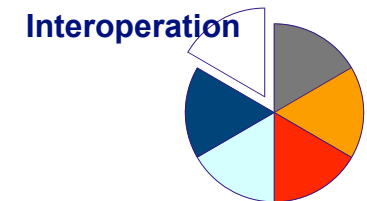
41 Exakte Wissenschaften — Sciences exactes

studyBranch3 (90 codes)

4200 Informatik — Informatique

studyLevel

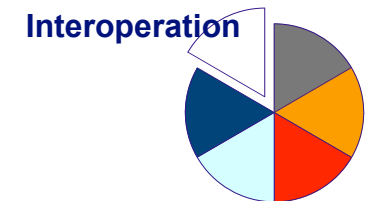
4200-15 Studierende in der Studienphase, die zum Bachelor führt
Etudiants réguliers se trouvant dans une phase d'études
qui les conduit au titre de Bachelor



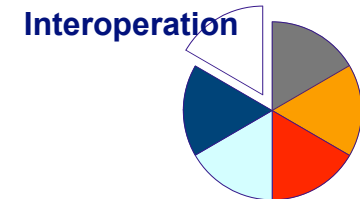
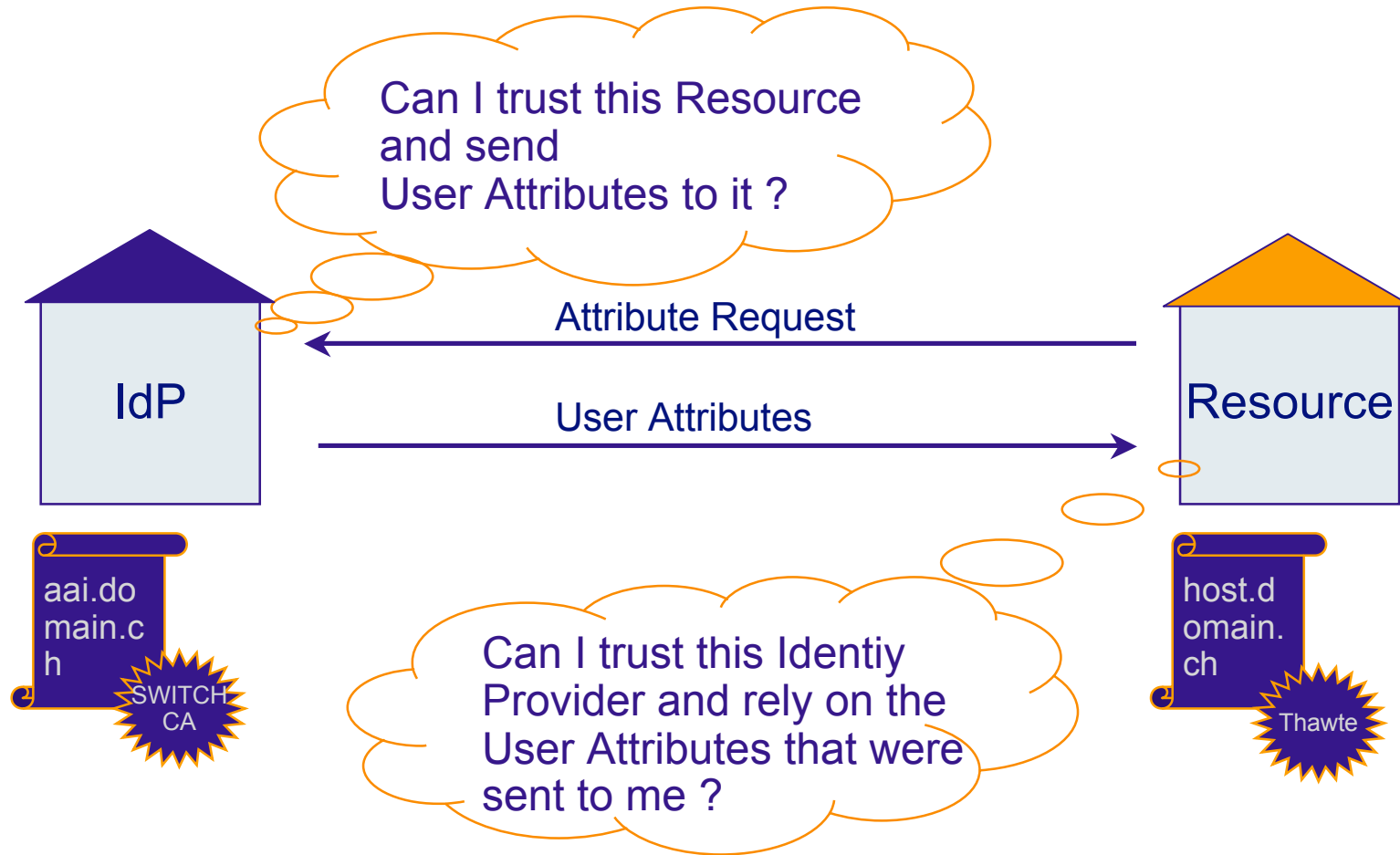
Browser Requirements

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

-> Any „normal“ browser is OK



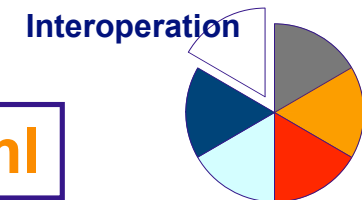
Requirement: Server Certificates



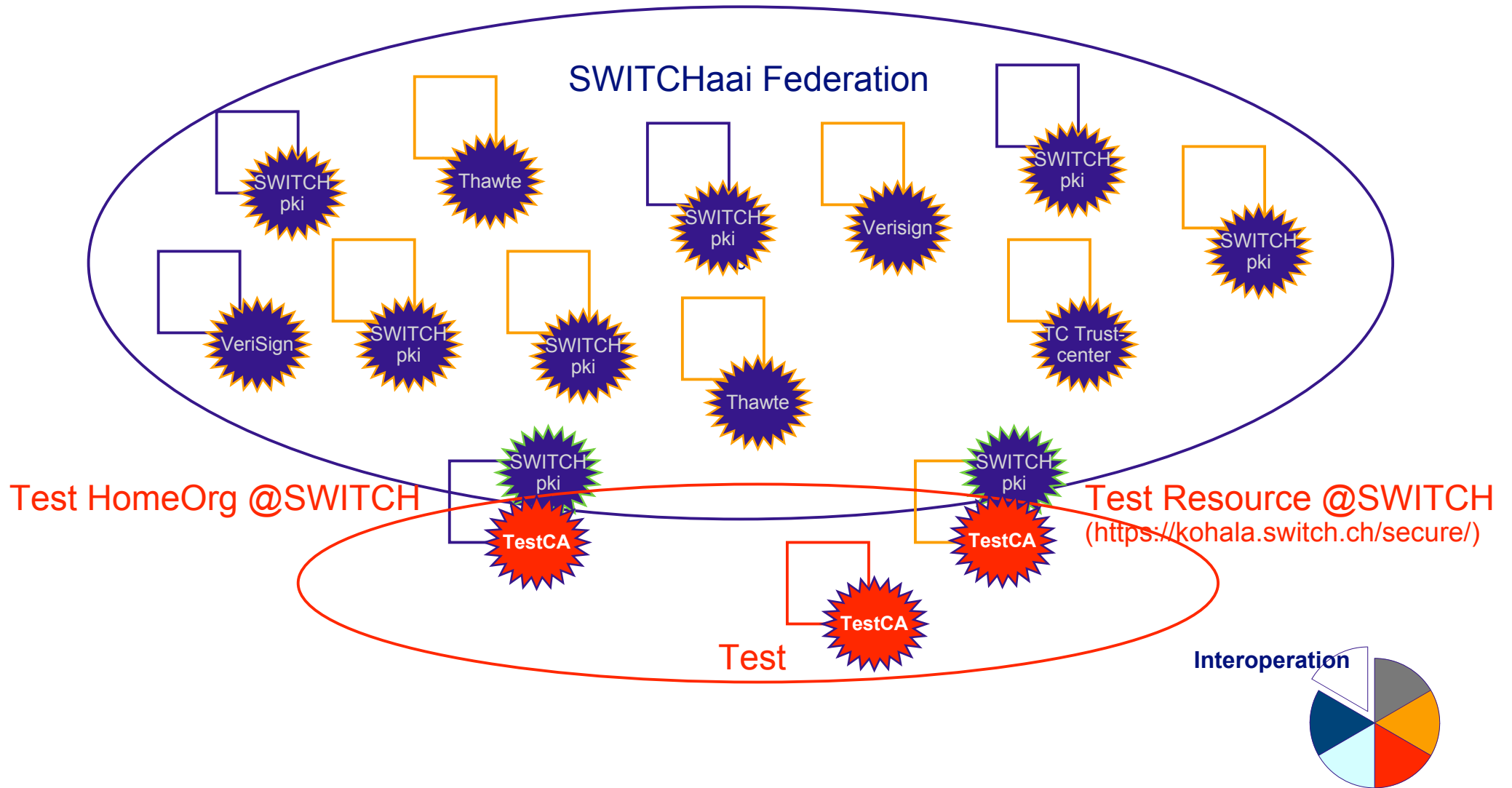
- ❑ **Currently accepted**
 - ❑ SWITCHpki
 - ❑ (One of) Thawte
 - ❑ (One of) VeriSign
 - ❑ (One of TC) Trustcenter

- ❑ **Procedure defined to include additional CAs**

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



Exception: Mere Test-Purposes



International AAI Activities

Shibboleth deployment underway in:

USA (Internet2, InCommon), Finland (HAKA), Switzerland (SWITCH)

Shibboleth related activities in:

United Kingdom (JISC), France (CRU), Australia (AARNet),

University of Amsterdam (NL), KU Leuven (BE), Stockholm University (SE),

Statsbiblioteket Denmark

Compatibility with Shibboleth planned for:

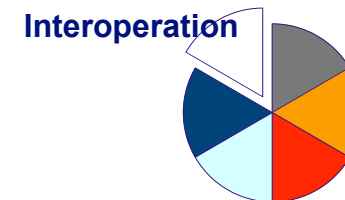
PAPI (RedIRIS, ES), A-Select (SURFnet, NL), Athens

Terena TF-EMC² – Task Force European Middleware Coordination and Collaboration

<http://www.terena.nl/tech/task-forces/tf-emc2/>

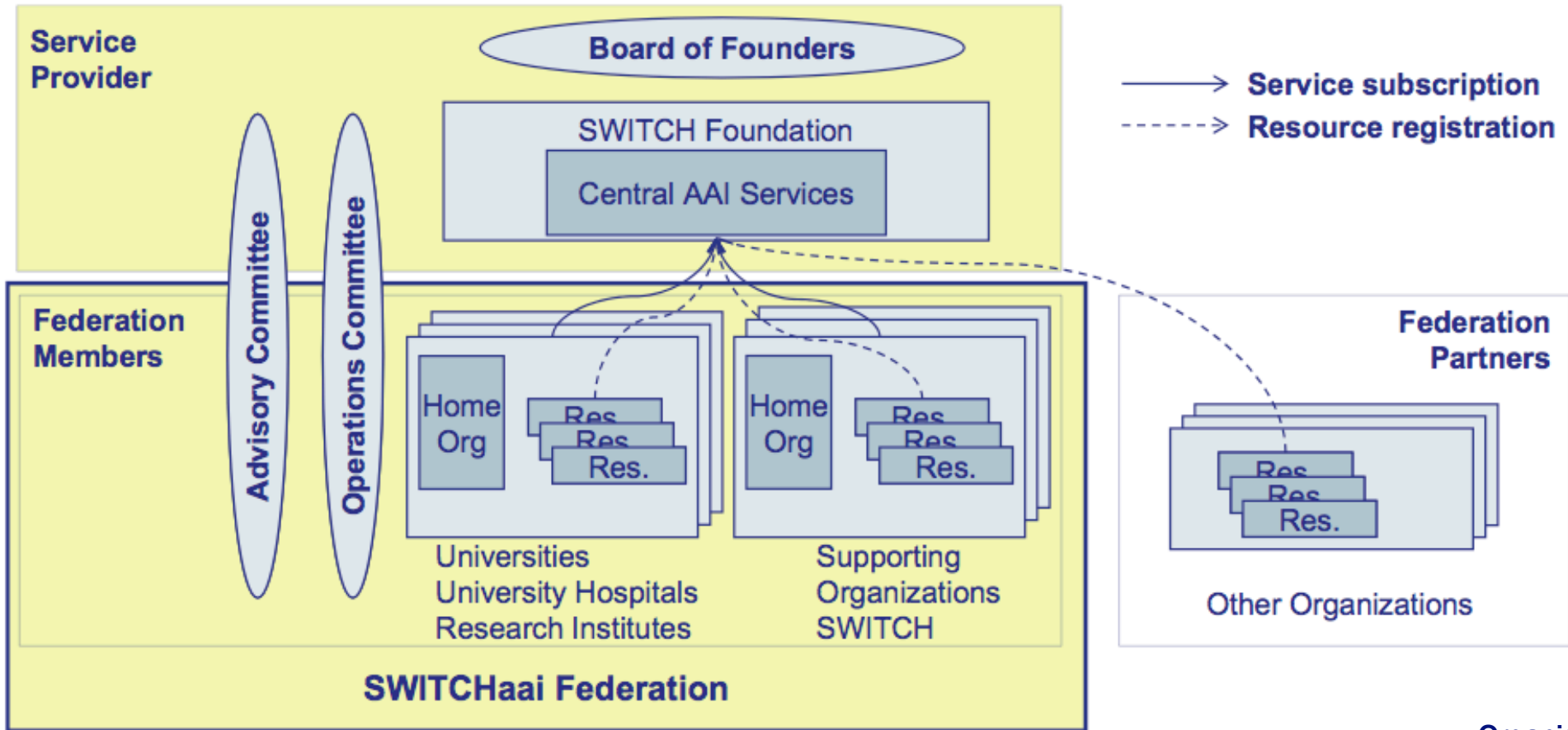
GN2 – JRA5 – Ubiquity (Mobility) and Roaming Access to Services

Define, prototype and build a roaming infrastructure and an AAI



Cotswolds Group - Federations Coordination (Europe, US)

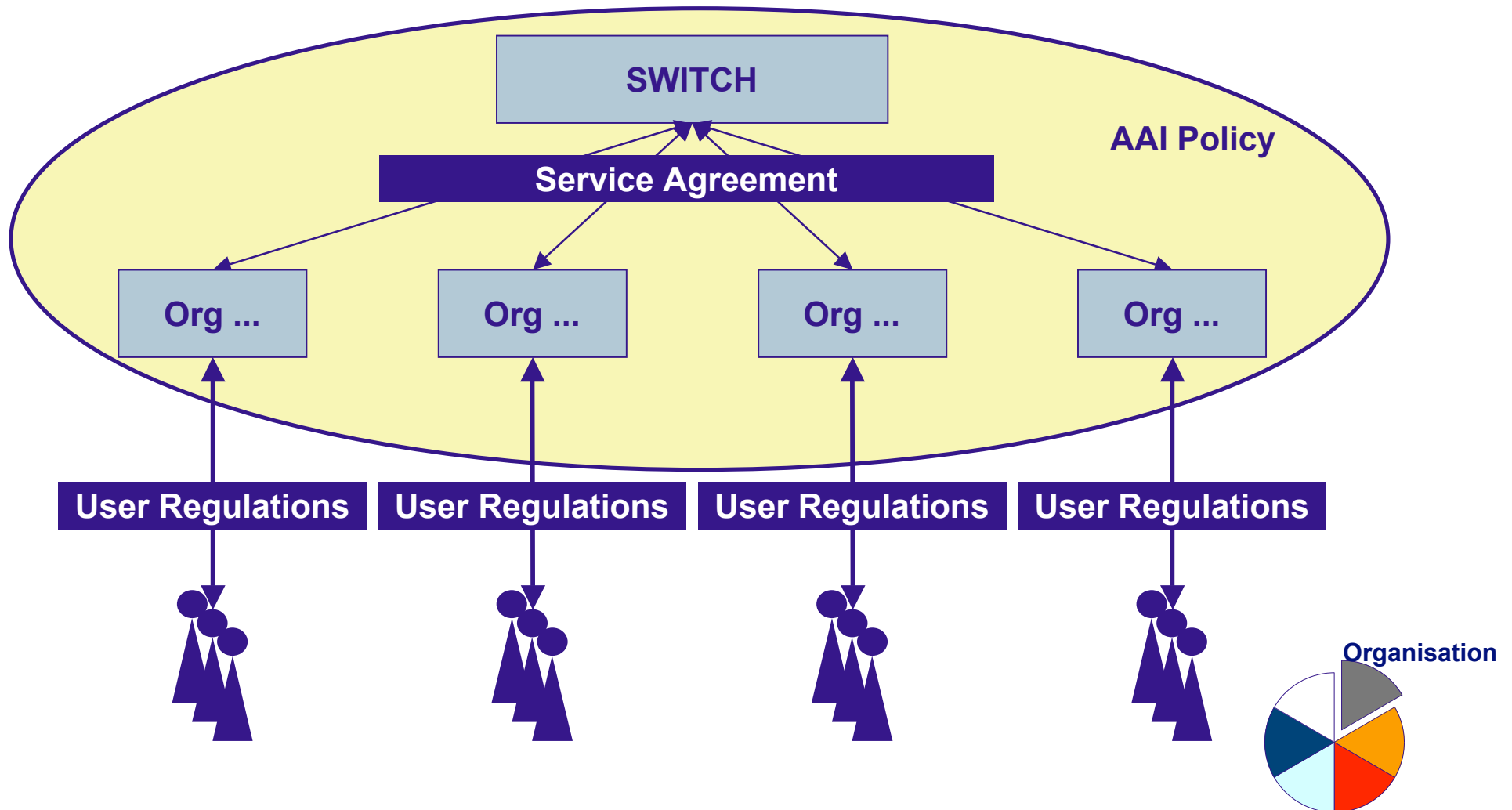
Organisational Framework



SWITCH acts as SWITCHai Federation Service Provider
 Federation membership based on signed service agreements



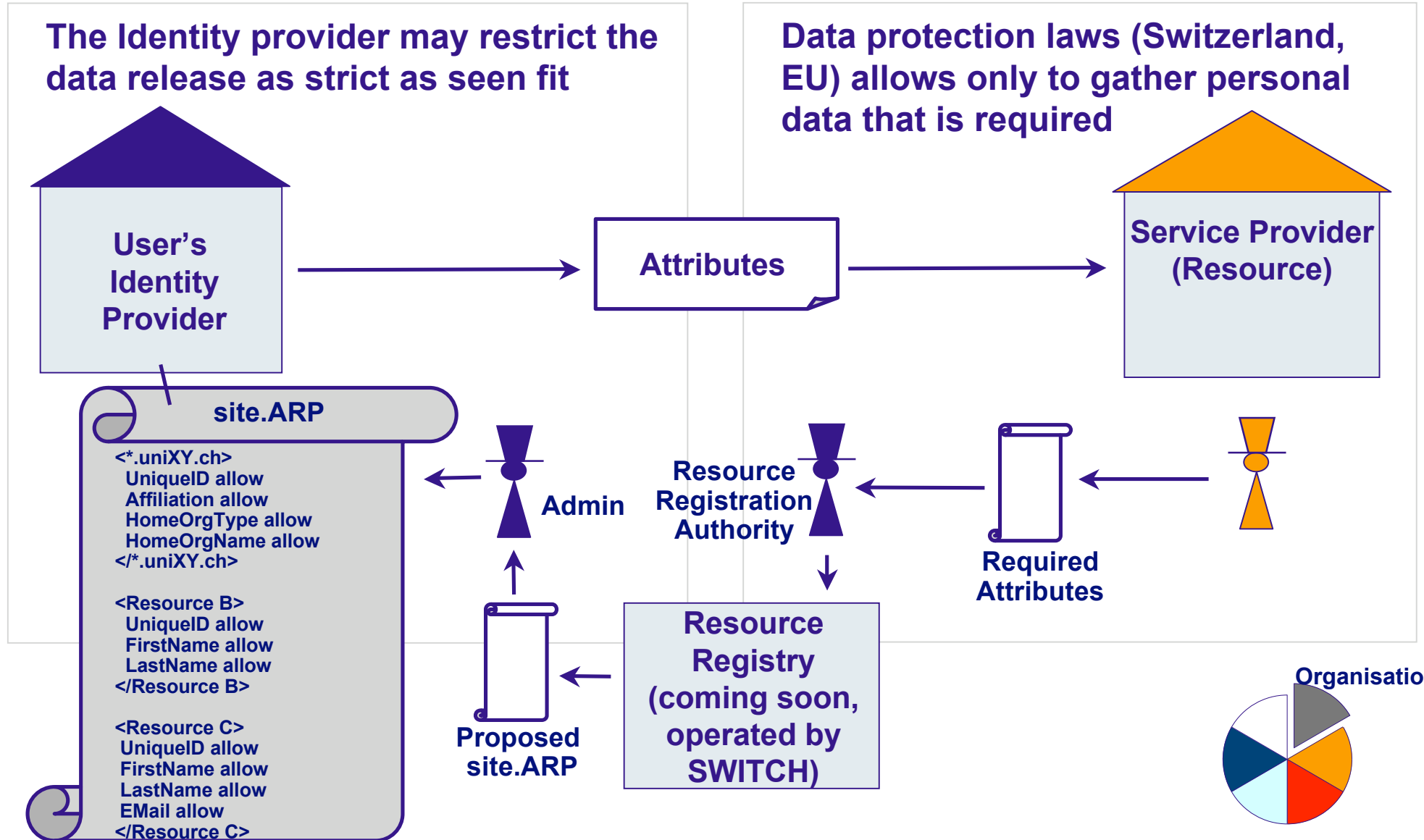
Federal and Cantonal Law (e.g. Data Protection Law)



Data Protection

The Identity provider may restrict the data release as strict as seen fit

Data protection laws (Switzerland, EU) allows only to gather personal data that is required



Resource Registry will be a database (June/July 2005)

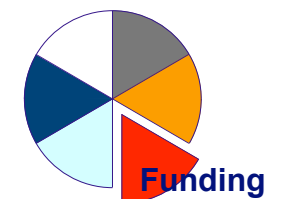
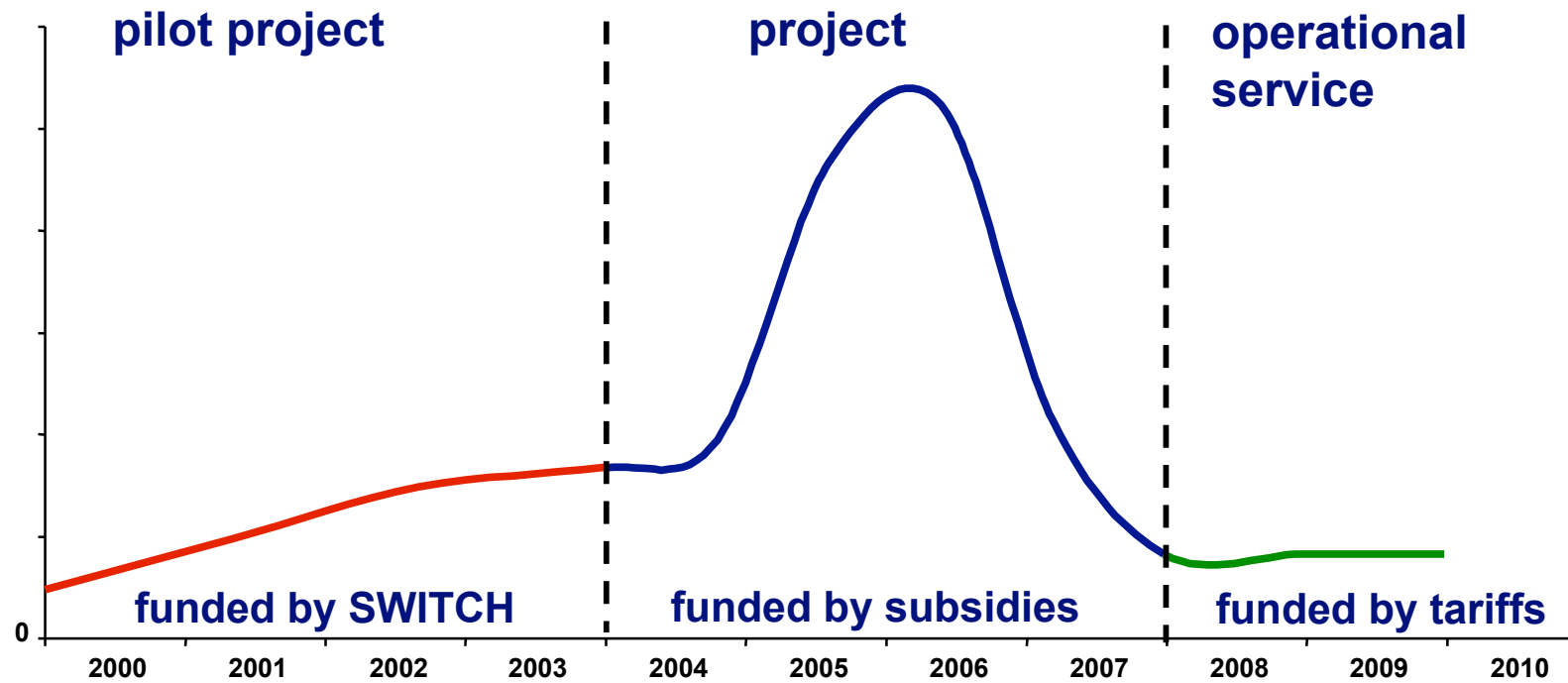
- for the scope of the SWITCHaai Federation
- to ensure that Resource Owners are aware of the AAI Policy
 - Resource Registration Authority (per Home Org) has to accept new Resources
- to generate configuration info required
- More detailed info to come.

It will contain

- info about Shibboleth protected Resources
 - configuration info
 - required for `sites.xml` at Identity Providers
 - attribute requirements of Service Providers (required and desired attributes)
 - required for data protection conformant attribute release (`arp.xml`)
- info about Home Organizations
 - configuration info
 - required for `sites.xml` at Service Providers

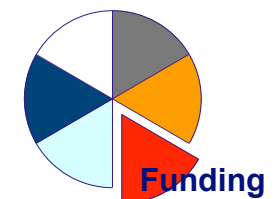


funding / costs



Funded projects

Uni BAS	HomeOrg, EVA, WebCT, DocEx, div. SVC-Projekte
Uni BE	Vorstudien, AAA Plattform, Grid
Uni FR	HomeOrg, Datenschutz-Tool, Aufbau AAI-Knowhow und -Helpdesk
Uni GE	Dokeos, CDSWare, Plone, Mediabase, uPortal, ExLibris SFX
Uni L	jahia, Sylvia, e-Learning
Uni LU	Blackboard
Uni NE	HomeOrg, IS-Academia (als Target)
Uni SG	HomeOrg, IBM LMS, Serviceportal, Forschungsplattform, Ausbau Vconf*
USI	HomeOrg, Moodle
Uni ZH	AAI Versions-Upgrades, SAP-CM, Lenya, Swiss Bio Grid, System X



- ❑ **Strategy & Marketing**
- ❑ **International Contacts**
- ❑ **Support, Consulting, Training**
- ❑ **Providing Federation-specific Files and Configuration Guides**
- ❑ **Operating WAYF (Where Are You From Server)**
- ❑ **Test-HomeOrg and Test-Resource**
- ❑ **Tools (AAIportal, AAIproxy)**
- ❑ **Virtual Home Organization**
- ❑ **Jump Start Service**



Q & A

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

aai@switch.ch