SWITCH

The Swiss Education & Research Network

AAI
Introductory Tutorial

The SWITCHaai Team, <aai@switch.ch>

Without AAI

University A

Student Admin

Web Mail

e-Learning

Library B

e-Journals

Literature DB

University C

Research DB

e-Learning
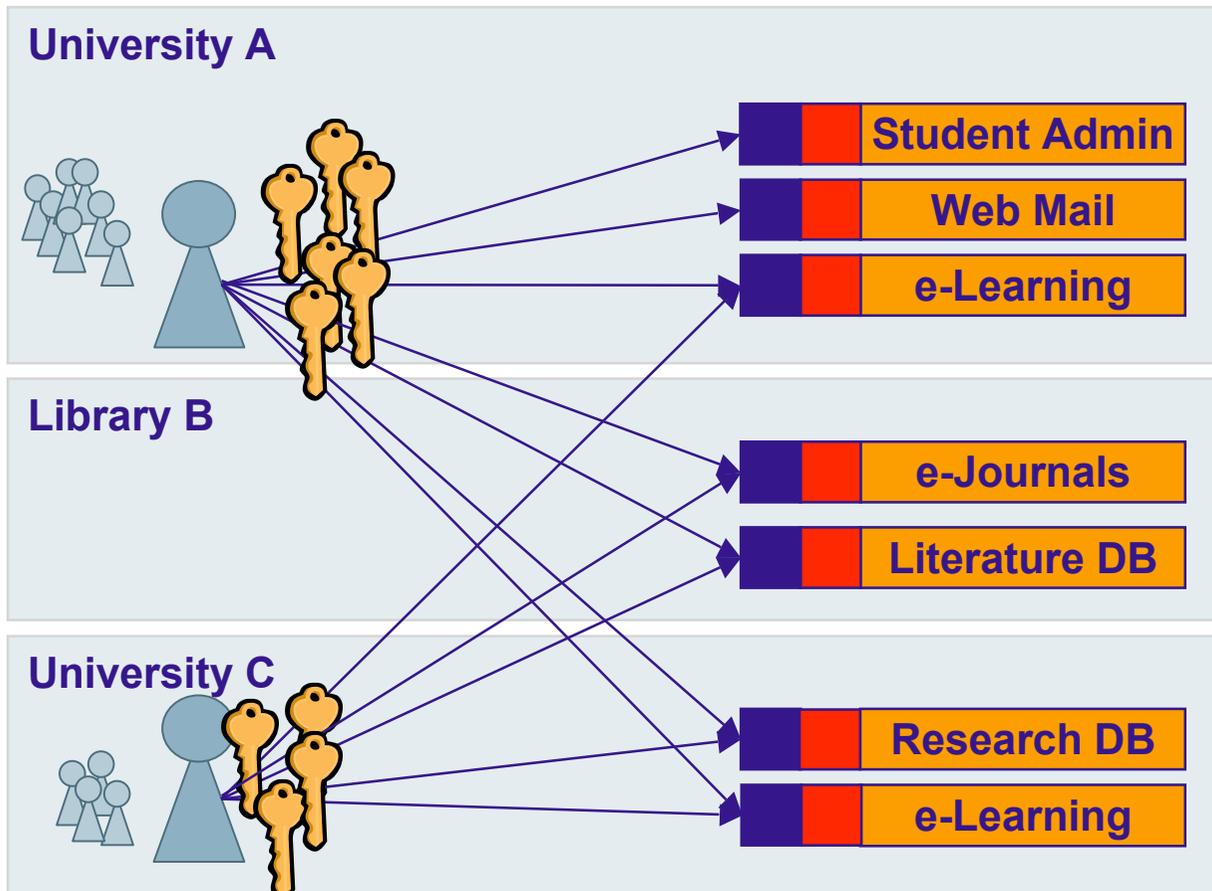
- Tedious user registration at all resources

- Unreliable and outdated user data at resources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	Credentials

With AAI

University A

AAI

Student Admin

Web Mail

e-Learning

Library B

e-Journals

Literature DB

University C

Research DB

e-Learning
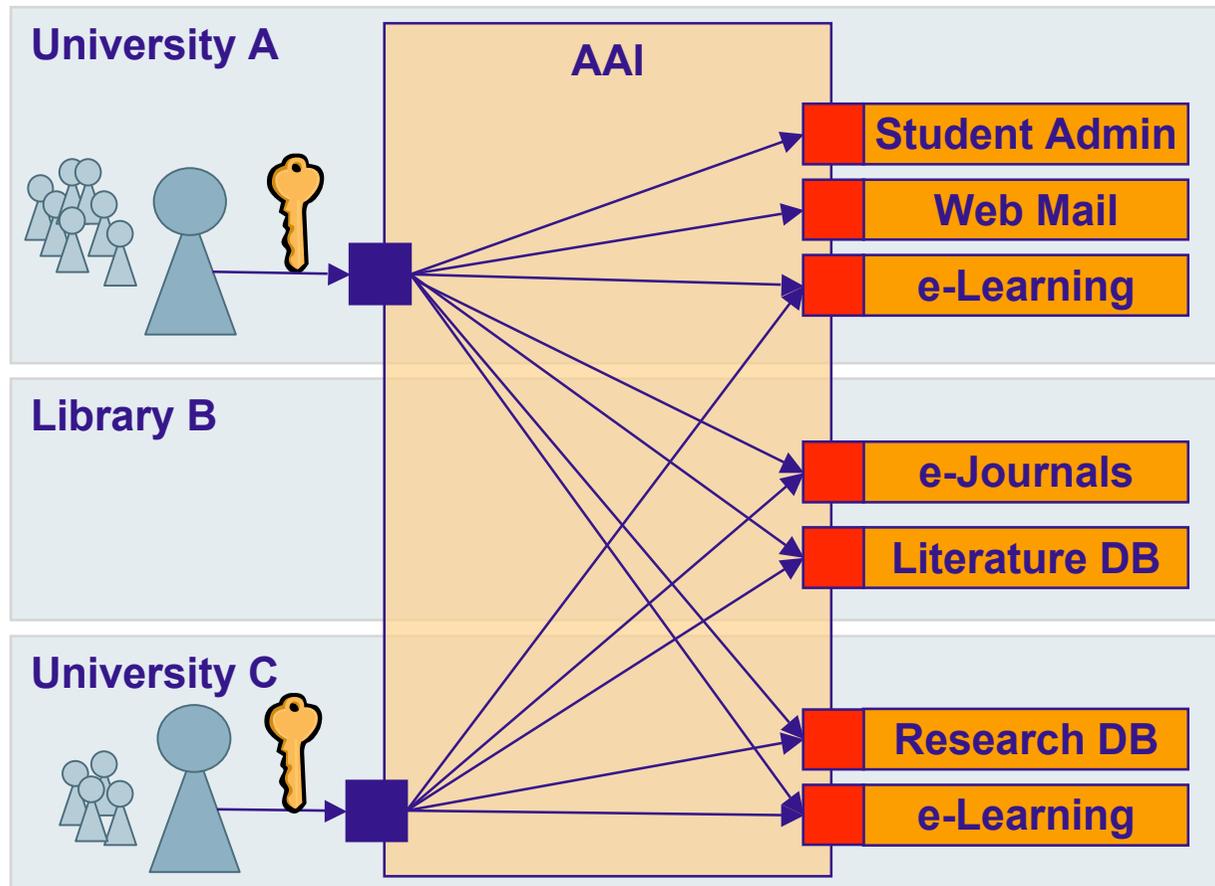
- No user registration and user data maintenance at resource needed

- 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

Shibboleth

- ❑ **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/

# 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://dokeos.unige.ch/home

SWITCHaai Building Blocks
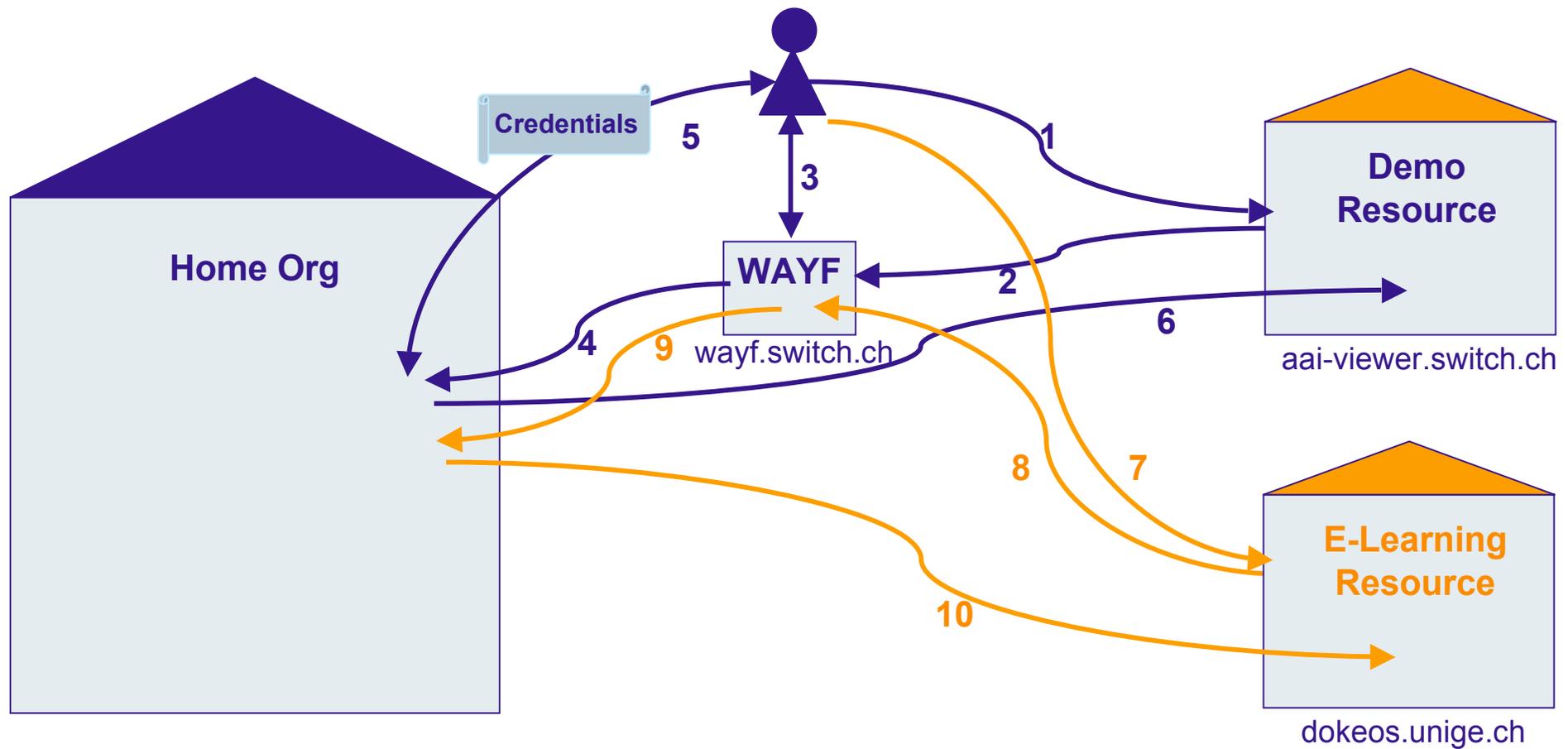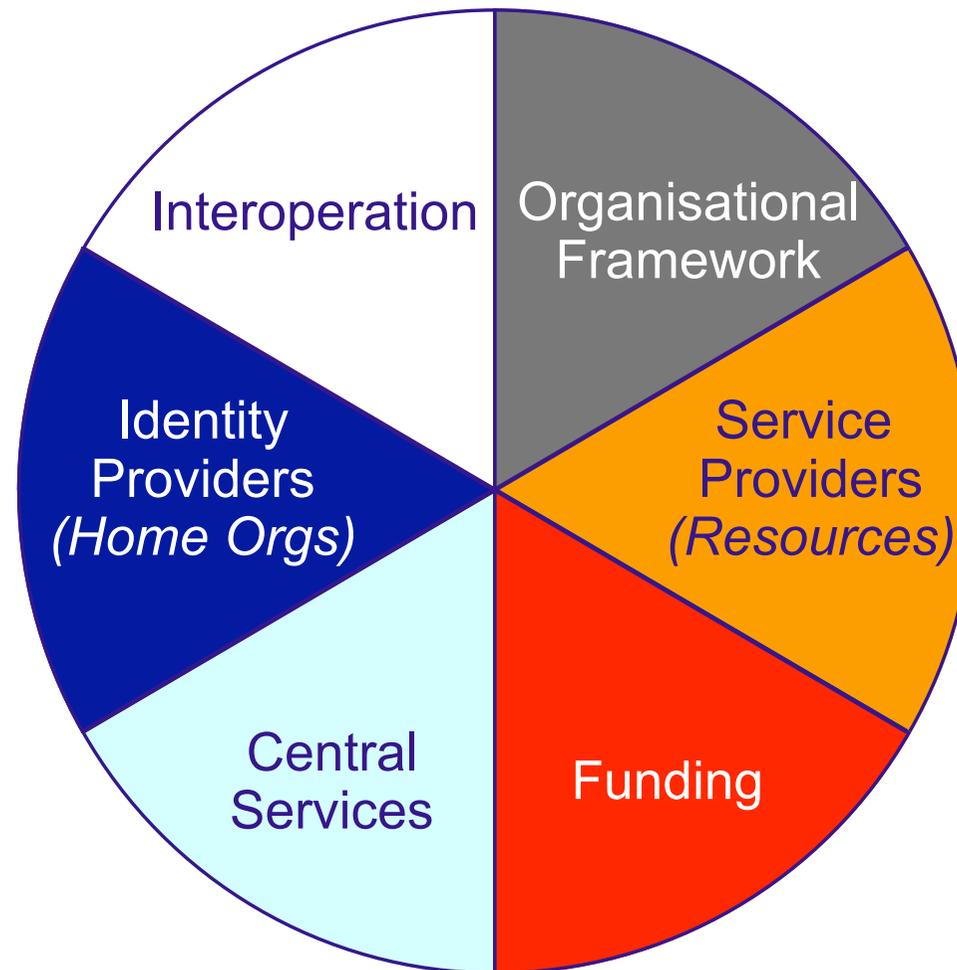
Identity Providers in SWITCHaai

Coverage

**175'000 Users (> 75%)
In Swiss Higher Education**

Legend:
- Operational
- Federation Member

Identity Providers

AAI-enabling your Home Organization

Identity Provider

Authentication System

e.g. JNDI

Web Server

Shibboleth

SSO

Username

User Directory

JDBC
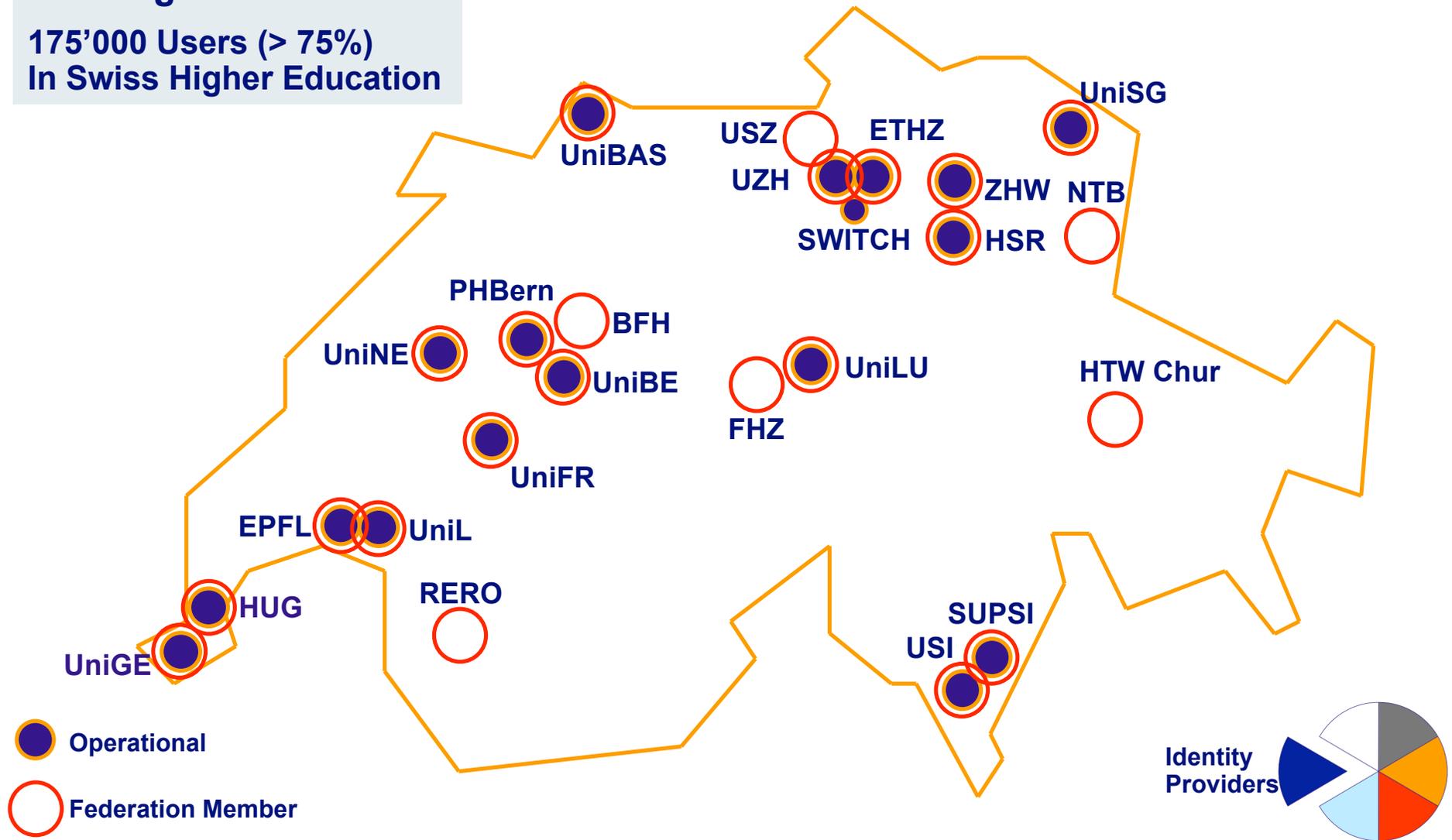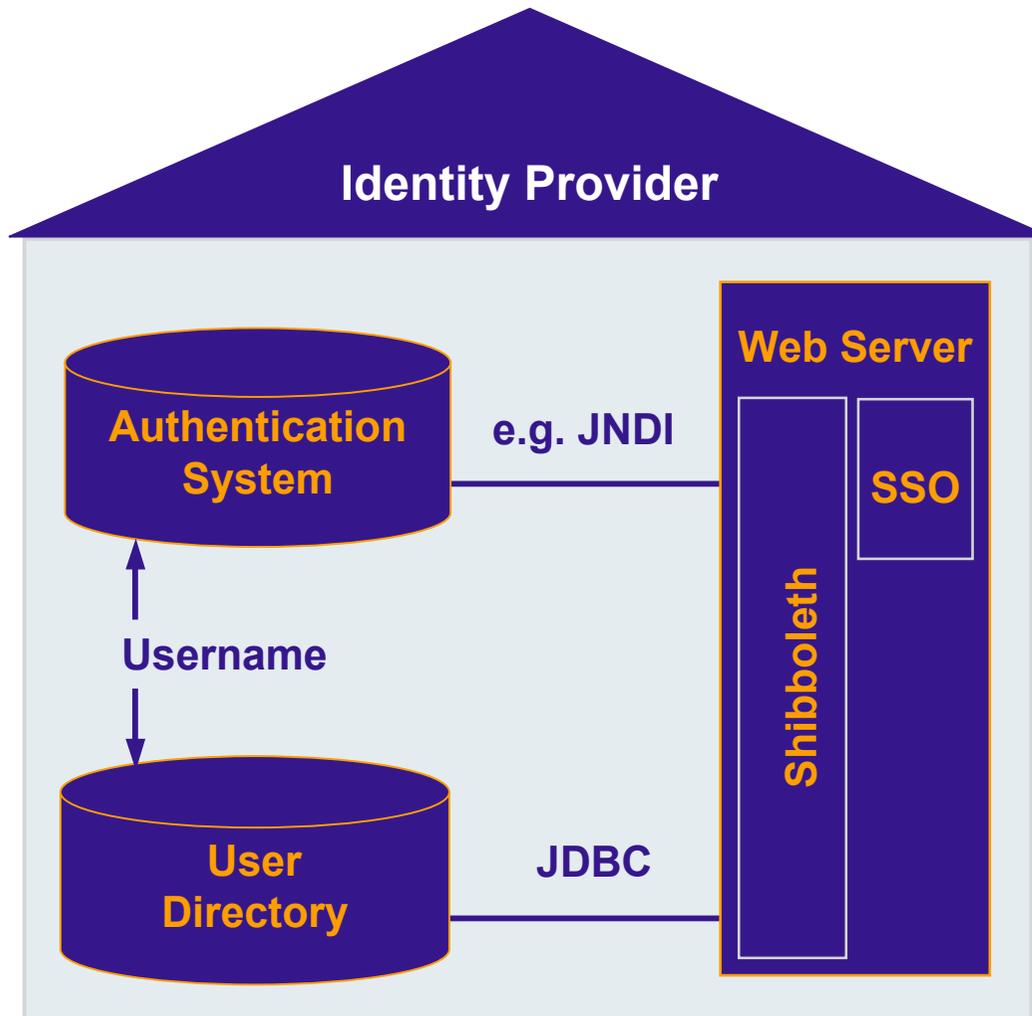
Web Servers
- Tomcat
- Apache + Tomcat
- IIS + Tomcat

Web Single Sign-On (SSO)
- CAS
- Pubcookie

Authentication Systems / User Directories
- OpenLDAP, Active Directory
- MS SQL, Oracle
- ...

Identity Providers

Authorization Attributes

Personal

Unique Identifier
Surname
Given name

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

Group Membership

Home Organization Name
Home Organization Type
Affiliation (student, staff, …)

Study branch
Study level
Staff category
Group membership
Organization Path
Organizational Unit Path

- Implementation of Attributes
 - **Mandatory**
  - Recommended or optional

- Based on
  - eduPerson Attributes
  - "Schweizerisches Hochschulinformationssystem" (SHIS)
- NO username, password

Interoperation

http://www.switch..ch/aai/docs/AAI_Attr_Specs.pdf
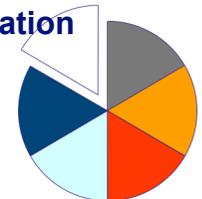
Access Control Example: DOIT

SWITCH
The Swiss Education & Research Network

DOIT: Dermatology Online with Interactive Technology

Access Rule

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

Universität Zürich

Universität Bern

Universtié de Lausanne
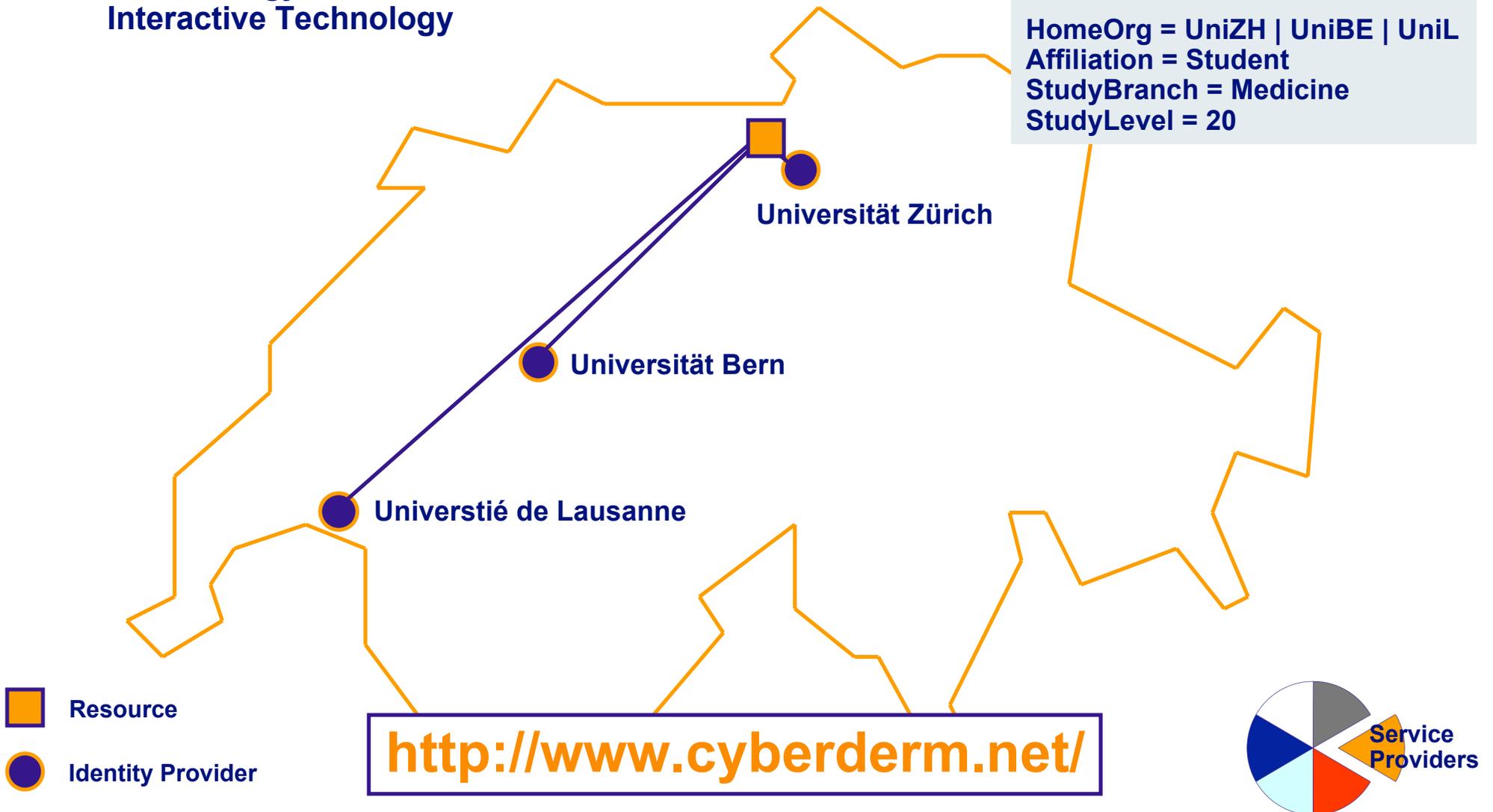
■ Resource

● Identity Provider

http://www.cyberderm.net/

Service Providers

Types of Service Providers

E-Learning

OLAT   **WebCT Vista**

WebCT CE   **VITELS**

DOIT   **dokeos**

Moodle   BSCW   **ILIAS**

Claroline   Blackboard

Libraries

EZproxy

ScienceDirect   JSTOR

VirtualLib   RERO

Aleph

Other Web Apps

eConf-Portal   **Neptun**

CompiCampus   **Sympa**

EVA   **WebSMS**

Silvia

jahia   SAP-CM

uPortal

Lenya   IS-Academia

operational   pilot   project ideas

Commercial

e-academy   Cablecom

Federal Court   eShops

SwissLex   WebLaw

20'000 Active Users
143 Resources

Service
Providers

Shibbolization of Resources

- Static Content (HTML, directories…)

- Web Applications written in script (PHP/ASP/Perl) within Apache/IIS

- Java Web Applications running in Tomcat

- Already Shibbolized Applications

Apache/IIS

shib module

Scripts (PHP/ASP)

mod_jk

shibd

content

Java Applications

Tomcat

http://www.switch.ch/aai/howto/

Service Providers

Java Service Provider Integration

SWITCH
The Swiss Education & Research Network

Today

Web Server	Java AppServer
•Apache	•Tomcat
•IIS	

Shibboleth SP (module)

mod_jk / JK redirector
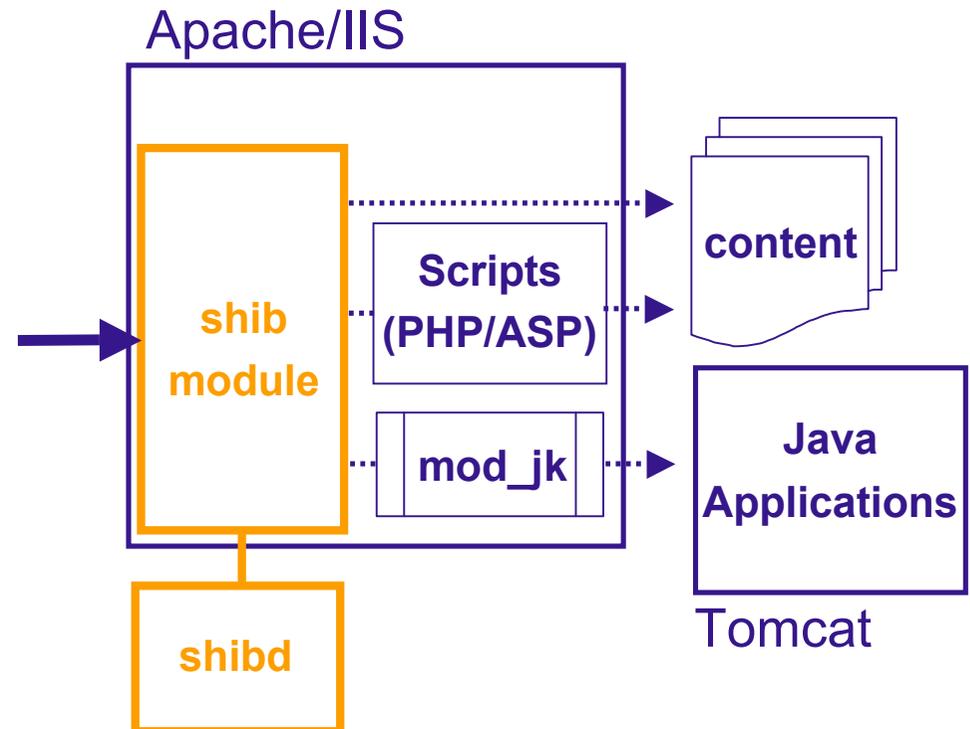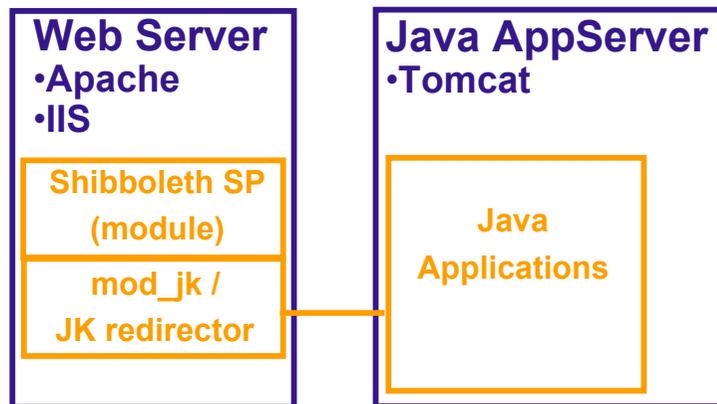
Java Applications

Example: Jahia @ UniL

Soon (Spring 07)

Java AppServer
•Tomcat, …

Shib SP (Java)
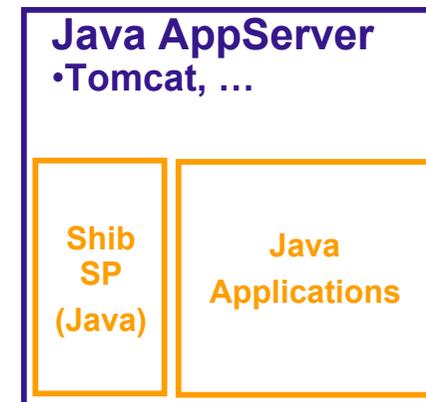
Java Applications

Using Shibboleth 2.0
Java Service Provider

Service Providers

Already Shibbolized Applications

SWITCH
The Swiss Education & Research Network

- ArtSTOR
- Blackboard
- Bodington.org
- CSA
- Darwin Streaming Server
- Digitalbrain PLC
- eAcademy
- EBSCO Publishing
- Elsevier ScienceDirect
- ExLibris - SFX
- Fedora
- Higher Markets
- Hupnet
- ILIAS
- JSTOR

- Moodle
- Napster
- NSDL
- OCLC
- OLAT
- Ovid Technologies Inc.
- Proquest Information and Learning
- Serials Solutions
- SYMPA
- Thomson Gale
- TWiki
- Useful Utilities - EZproxy
- WebAssign
- WebCT

http://shibboleth.internet2.edu/seas.html

Service Providers

Summary

❑ **AAI - Authentication and Authorization Infrastructure**

   ❑ **Secure Single Sign On to web resources**

   ❑ **175'000 AAI users (> 75 % of Swiss higher education)**

   ❑ **Many AAI enabled Resources, mainly in E-Learning**