AAI – Introductory Tutorial

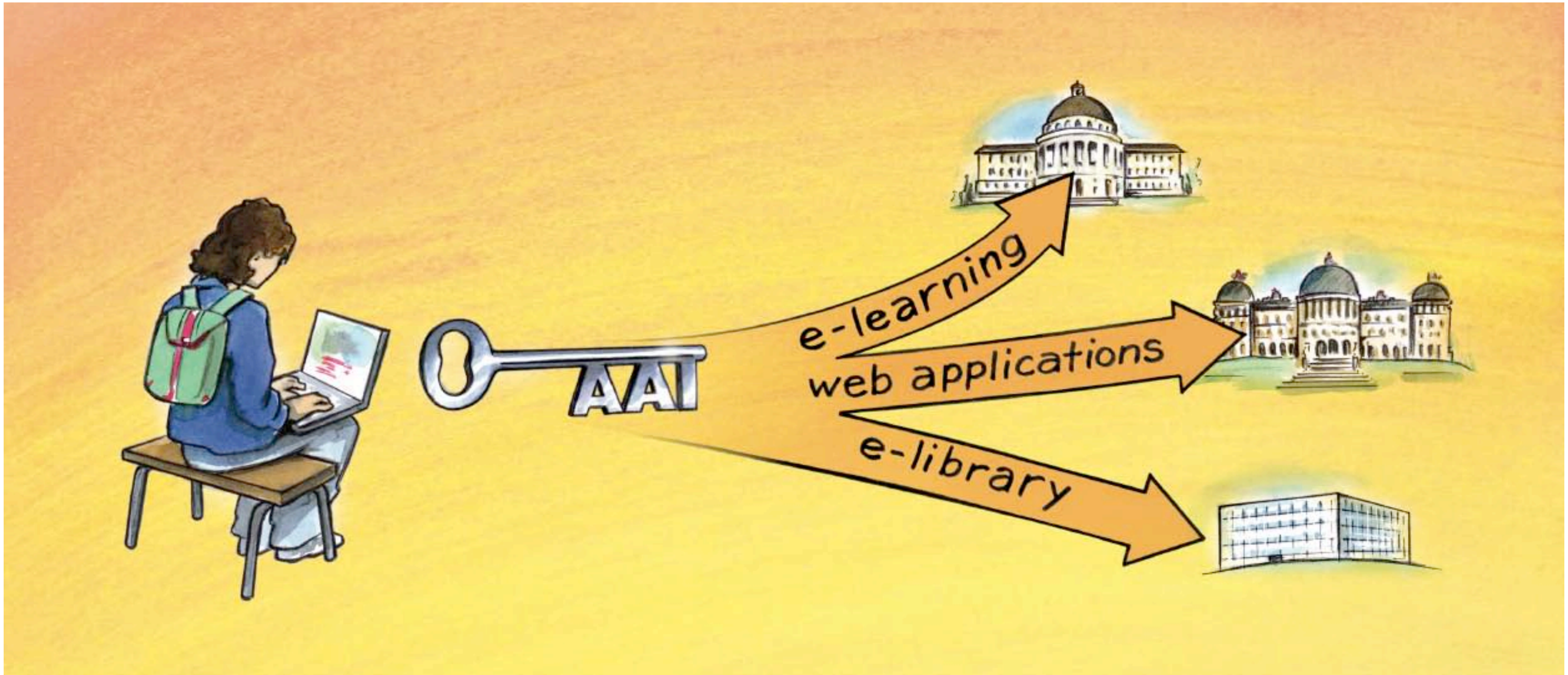
AAI Info-Day - 29. November 2007

Serving Swiss Universities

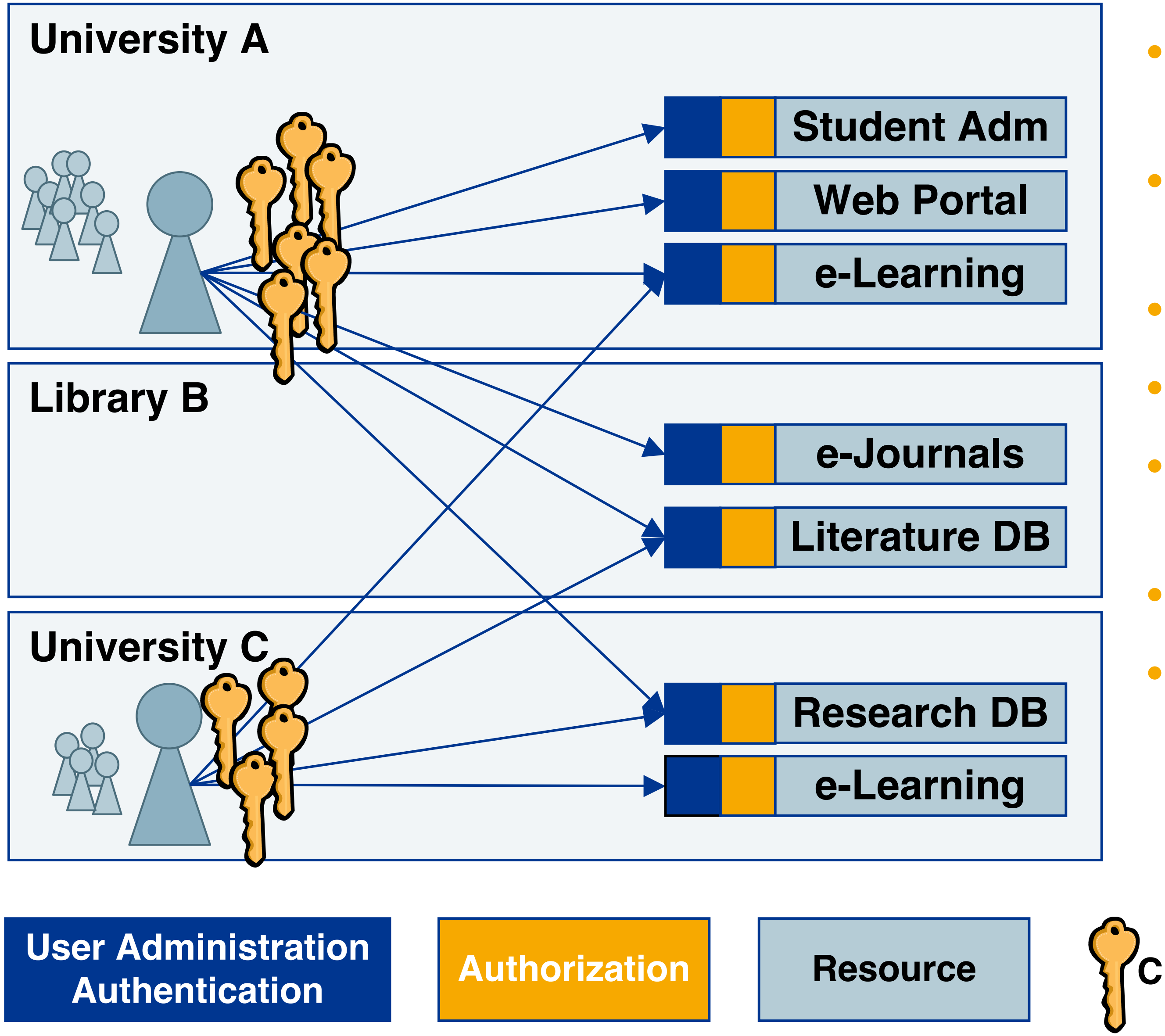
SWITCHaai Team
aai@switch.ch

AAI - Key to access them all

AAI = Authentication and Authorization Infrastructure

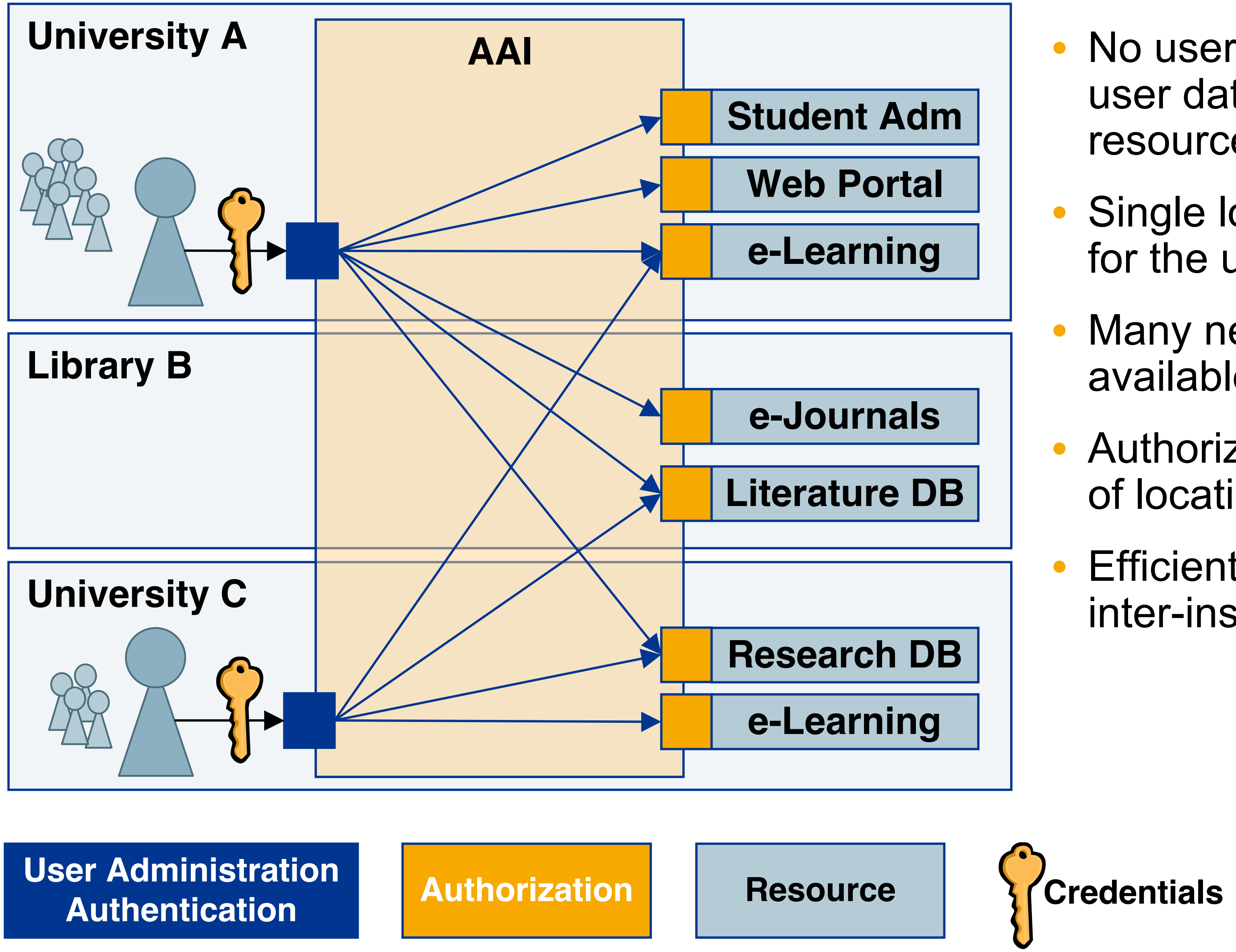


Without AAI



- 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- Unreliable and outdated user data at resources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

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
- Authorization independent of location
- Efficient implementation of inter-institutional access

Shibboleth

- The word **Shibboleth** was used to identify members of a group
- Open Source Software
- Based on SAML (Security Assertion Markup Language), an OASIS Standard
- Mostly used by universities

http://shibboleth.internet2.edu

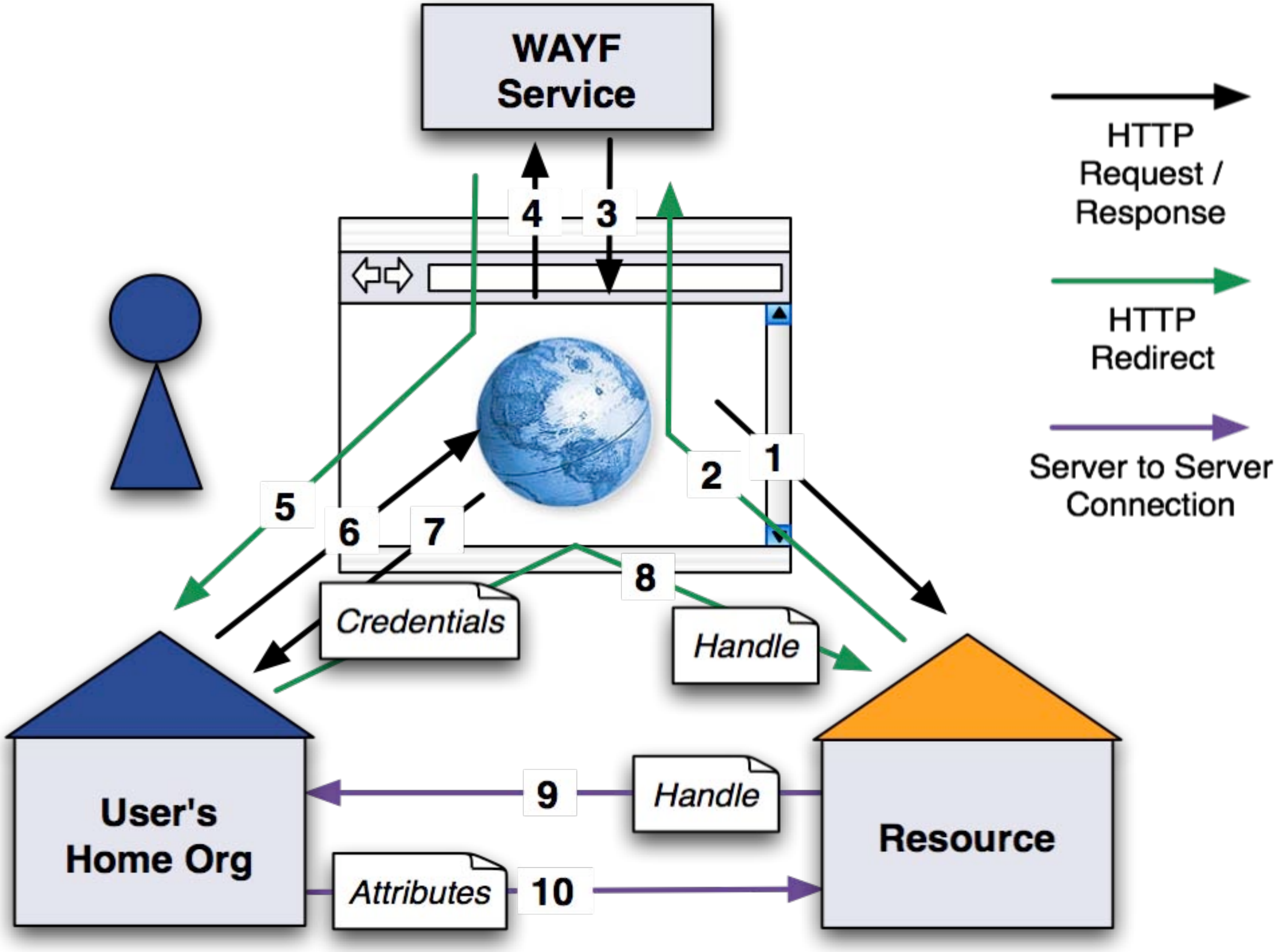
Demo – try it yourself

Go to http://www.switch.ch/aai/demo/

➔ Click on „demo resource”

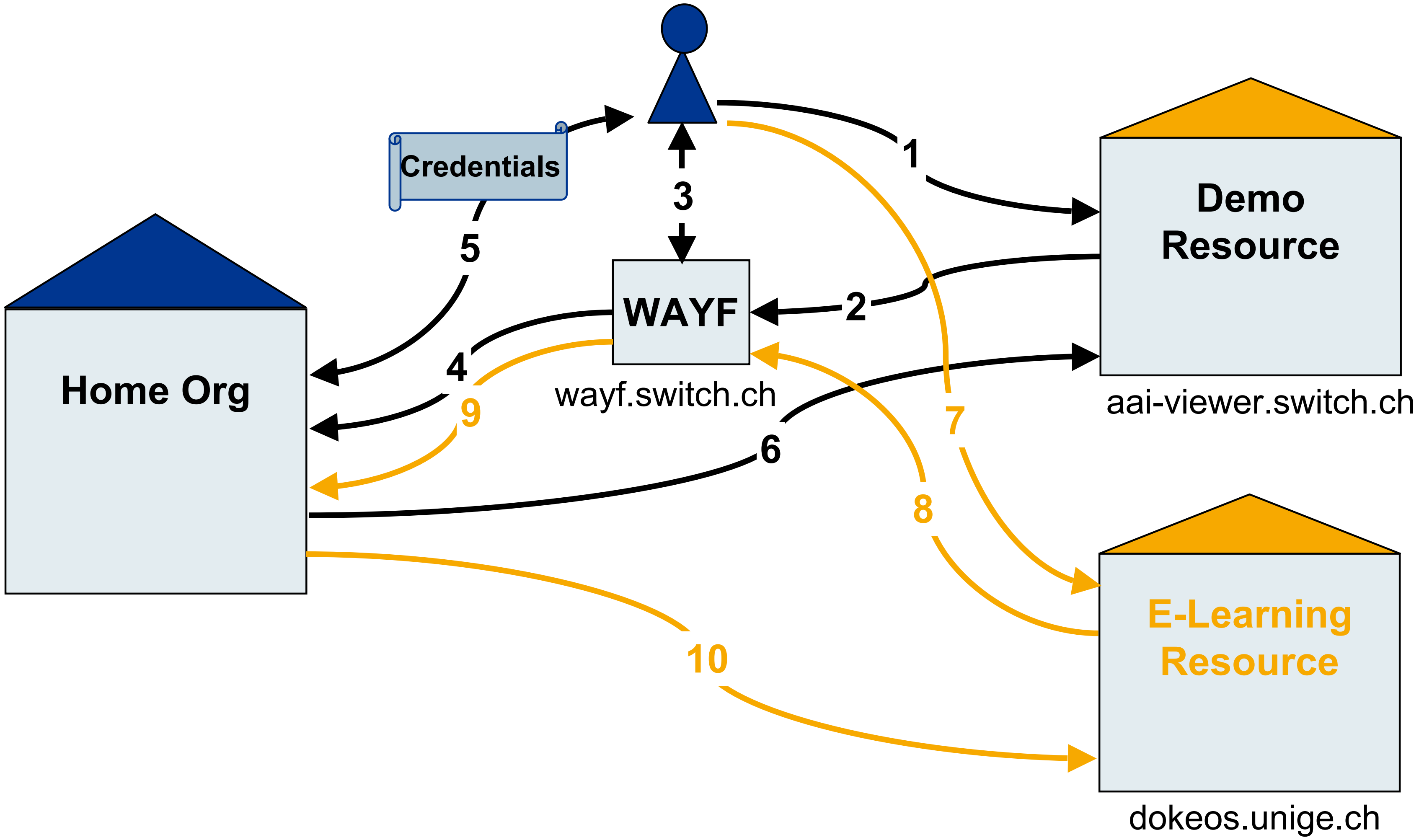
http://www.switch.ch/aai/demo/medium.html

Demo



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

Inter-organizational Single Sign On

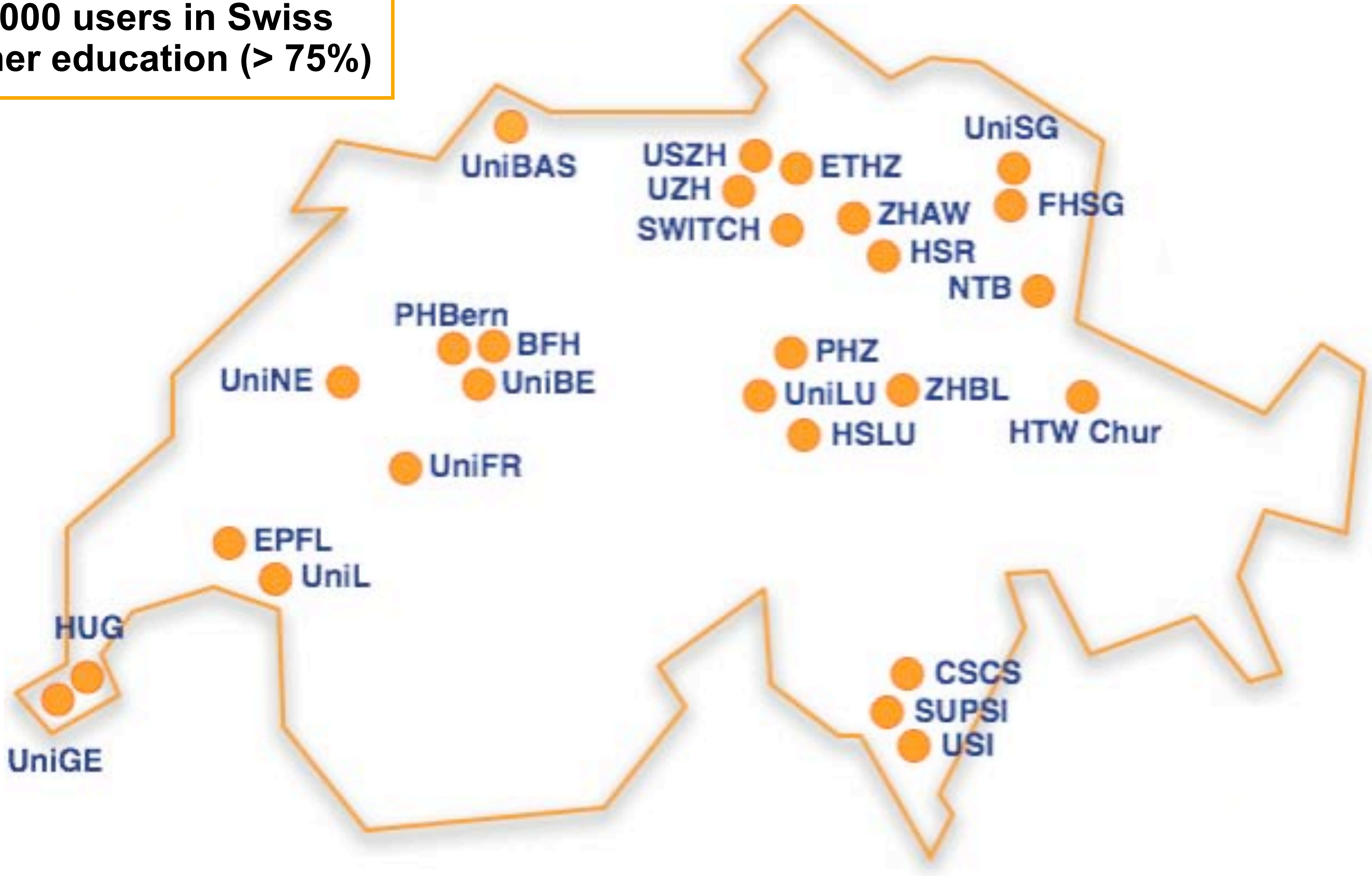


https://dokeos.unige.ch

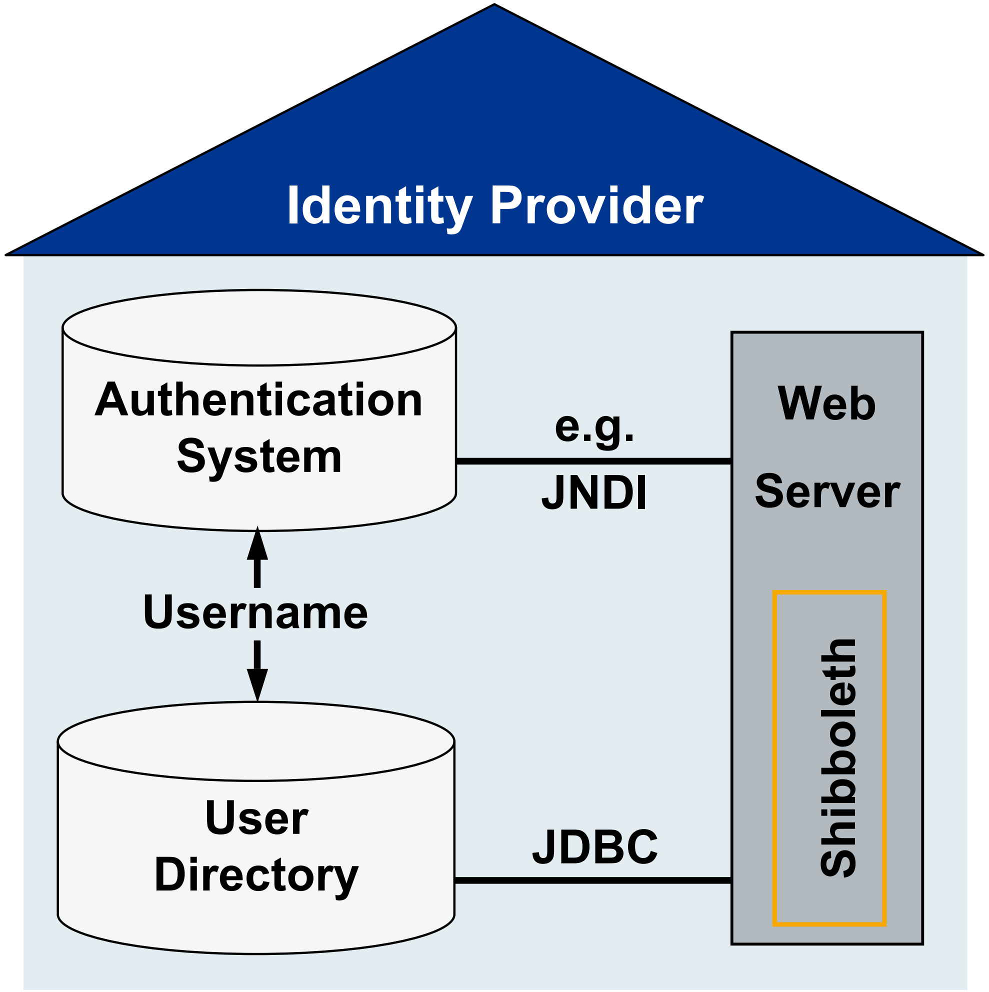
Home Organizations in SWITCHaai

Coverage

195’000 users in Swiss higher education (> 75%)



AAI-enabling a Home Organization



Prerequisites

- Authentication System
- User Directory

The Shibboleth Identity Provider

- Java Web Application
- Runs on Tomcat (optionally with Apache or IIS in front)

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

SWITCHaai Attributes

Personal

Unique Identifier

Surname

Given name

E-mail

User ID

Matriculation number

Employee number

Address(es)

Phone number(s)

Preferred lang.

Date of birth

Gender

Group Membership

Home Organization Name

Home Organization Type

Affiliation

Study branch

Study level

Staff category

Group membership

Organization Path

Organizational Unit Path

Implementation of Attributes

- Mandatory
- Recommended or optional

Based on

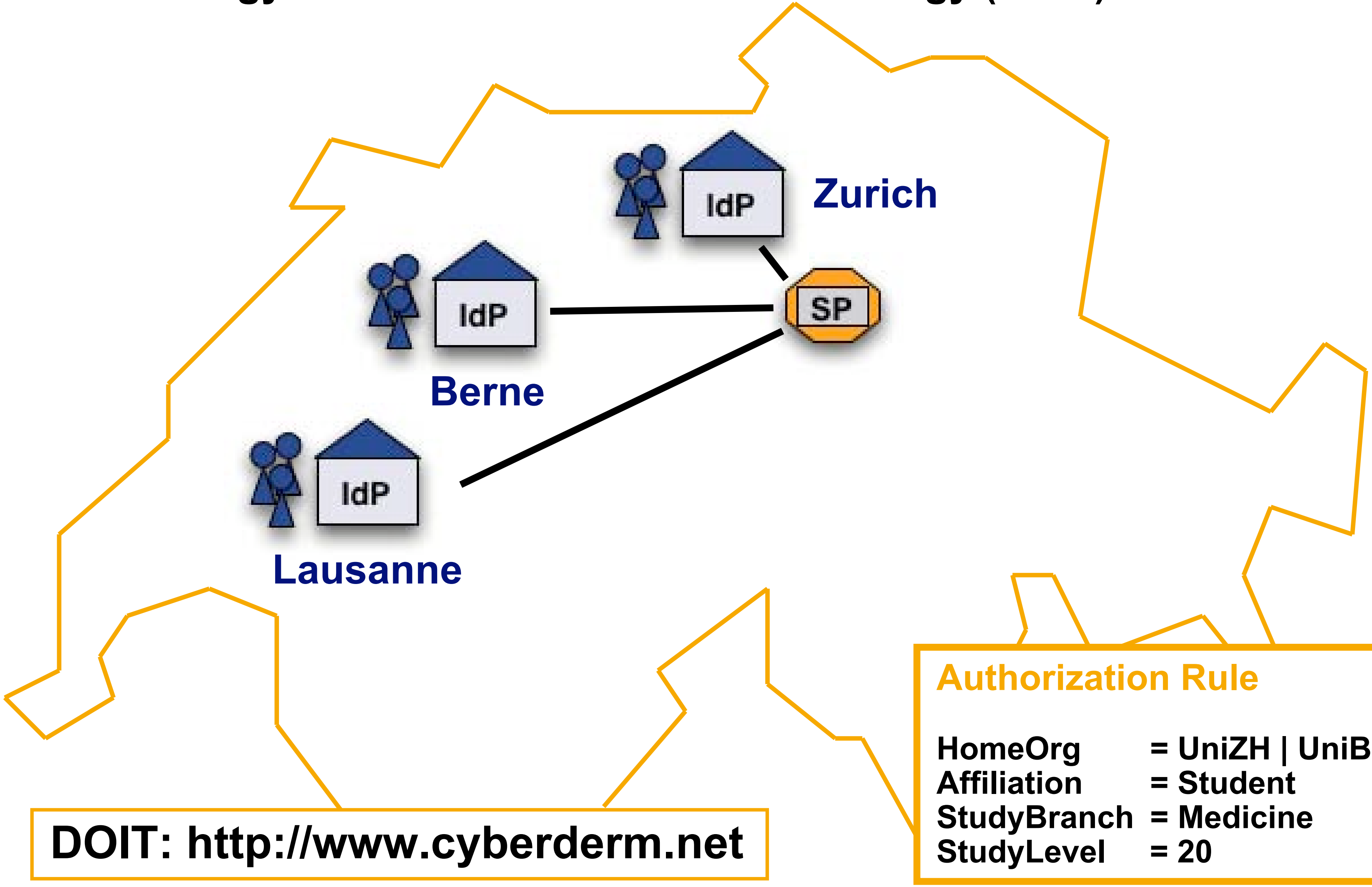
- eduPerson Attributes
- "Schweizerisches Hochschulinformations-system" (SHIS)

⇨ NO password

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

Attribute Based Authorization Example

Dermatology Online with Interactive Technology (DOIT)



Authorization Rule

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

DOIT: http://www.cyberderm.net

Service Providers in SWITCHaai

E-Learning

OLAT **Moodle** **WebCT CE**

WebCT Vista **Dokeos** **VITELS**

ADlearn **DOOR**

DOIT **CASUS** **ILIAS**

Claroline Blackboard

Libraries

EZproxy JSTOR

ScienceDirect Ovid

VirtualLib **DigiTool** RERO

EBSCO Aleph

Other Web Applications

eConf Portal **BSCW** **EVA** **SLCS**

Compicampus **Plone** **VASH**

OpenCMS **WebSMS** **Sympa**

ESN Fedora **TWiki** **Blue Coat**

Jahia Lenya uPortal IS-Academia

Commercial & other Partners

MSDNAA **Neptun Store**

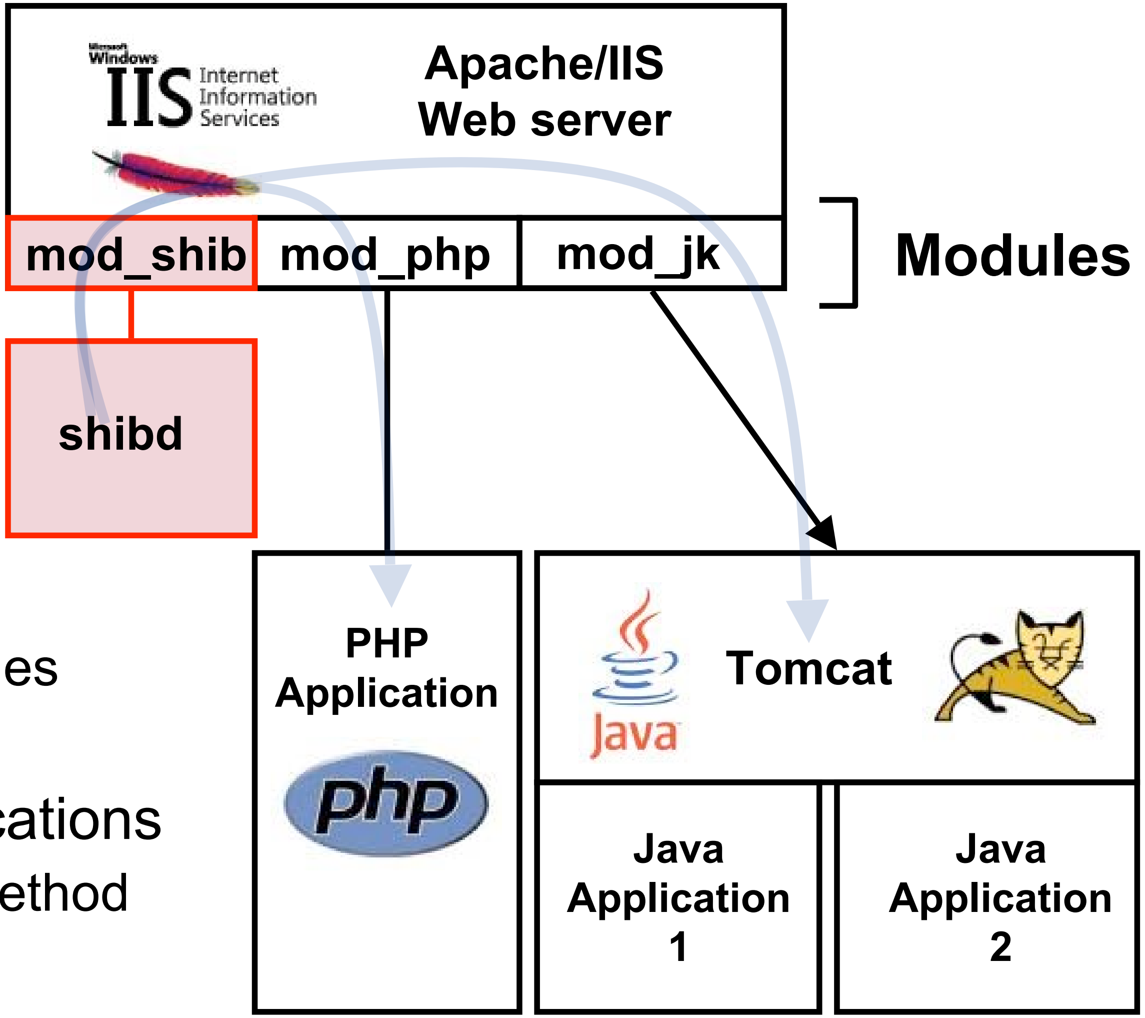
Swiss Federal Court

operational
in pilot ideas

>210 Resources

Shibboleth Service Provider for Apache/IIS

- Runs on: Linux, Solaris, Windows, Mac OS X, FreeBSD, …
- Protects static content and web applications
- **shibd** fetches attributes and propagates them
- Can authorize users with
  - Apache directives
  - Shibboleth XML Access rules
- Provides attributes to applications
  - Alternative authorization method



Already Shibbolized Applications

- American Chemical Society
- ArtSTOR
- Atypon
- CSA
- Digitalbrain PLC
- EBSCO Publishing
- Elsevier ScienceDirect
- ExLibris
- JSTOR
- The Literary Encyclopedia
- NSDL
- OCLC
- Ovid Technologies Inc.
- Project MUSE
- Proquest Information and Learning
- Serials Solutions
- SCRAN
- Thomson Gale
- Thomson ISI/Scientific
- Useful Utilities - EZproxy

- Blackboard
- ILIAS
- Moodle
- OLAT
- Sakai
- WebAssign
- WebCT

- Bodington.org
- Condor
- Confluence Wiki
- Darwin Streaming Server
- DSpace

- eAcademy
- Fedora
- GridSphere
- GridShib
- Higher Markets
- Horde
- Hupnet
- JISCmail
- LionShare
- Media Wiki
- MyProxy
- Napster
- PHEAA
- Sharepoint® from Microsoft
- SYMPA
- Symplicity
- TurnItIn
- TWiki
- uPOrtal
- Zope + Plone

https://wiki.internet2.edu/confluence/display/seas/Home

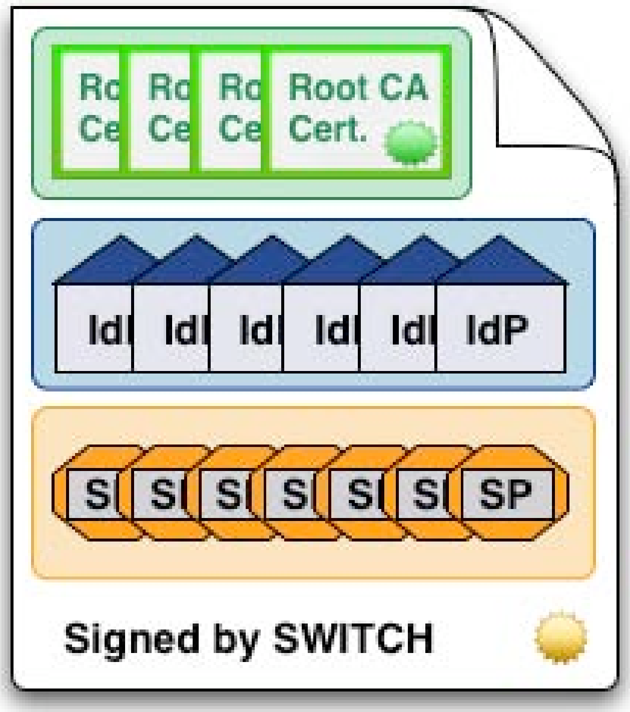
Federation Metadata

XML File (e.g. metadata.switchaai.xml) that contains list of:

- Accepted Root CA certificates
- Description of Identity Providers
- Description of Service Providers

SWITCHaai Metadata is signed

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



Metadata technically describes federation!

AAI Link Collection

- How to join SWITCHaai?
  - http://www.switch.ch/aai/join
- AAI Support Information
  - http://www.switch.ch/aai/support
  - or ask aai@switch.ch
- AAI related tools, e.g.
  - Resource Registry
  - Group Management Tool
  - Virtual Home Organization (VHO)
  - http://www.switch.ch/aai/support/tools
- The AAI Demo
  - http://www.switch.ch/aai/demo