SWITCH

The Swiss Education & Research Network
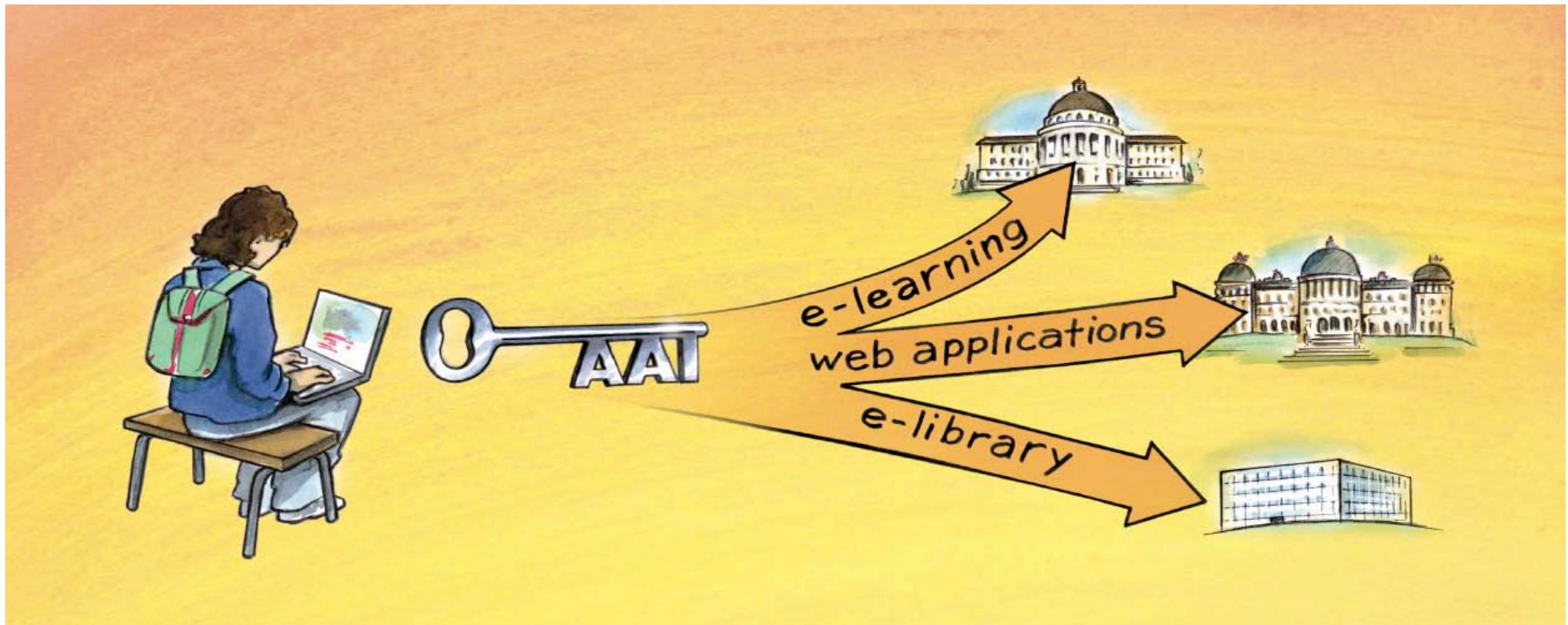
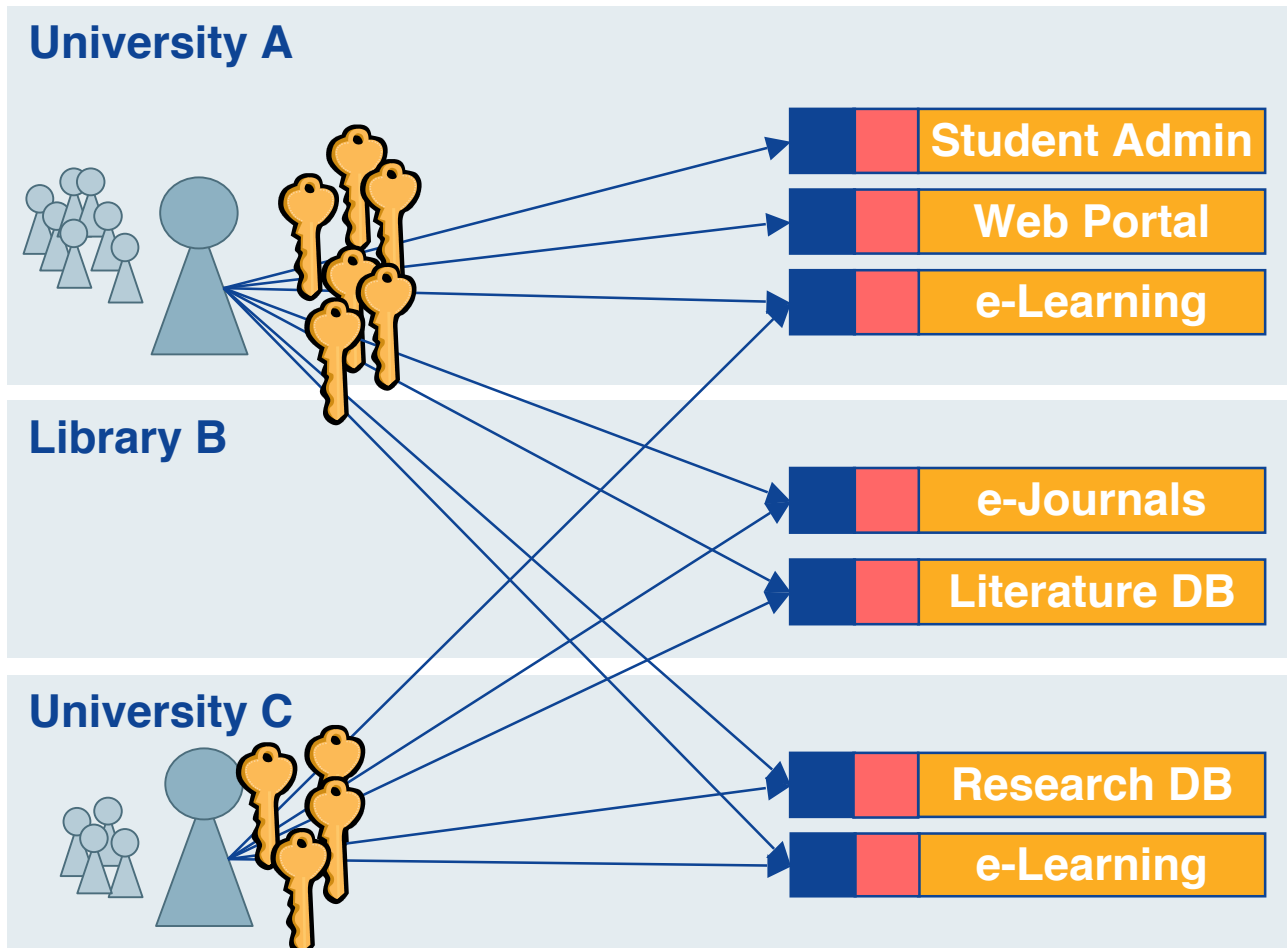# AAI
Introductory Tutorial

Patrik Schnellmann <schnellmann@switch.ch>
Thomas Lenggenhager <lenggenhager@switch.ch>

AAI is the Key!

Authentication and Authorization Infrastructure

AAI = AuthN & AuthZ

Without AAI

University A

Student Admin

Web Portal

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- Unreliable and outdated user data at resources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
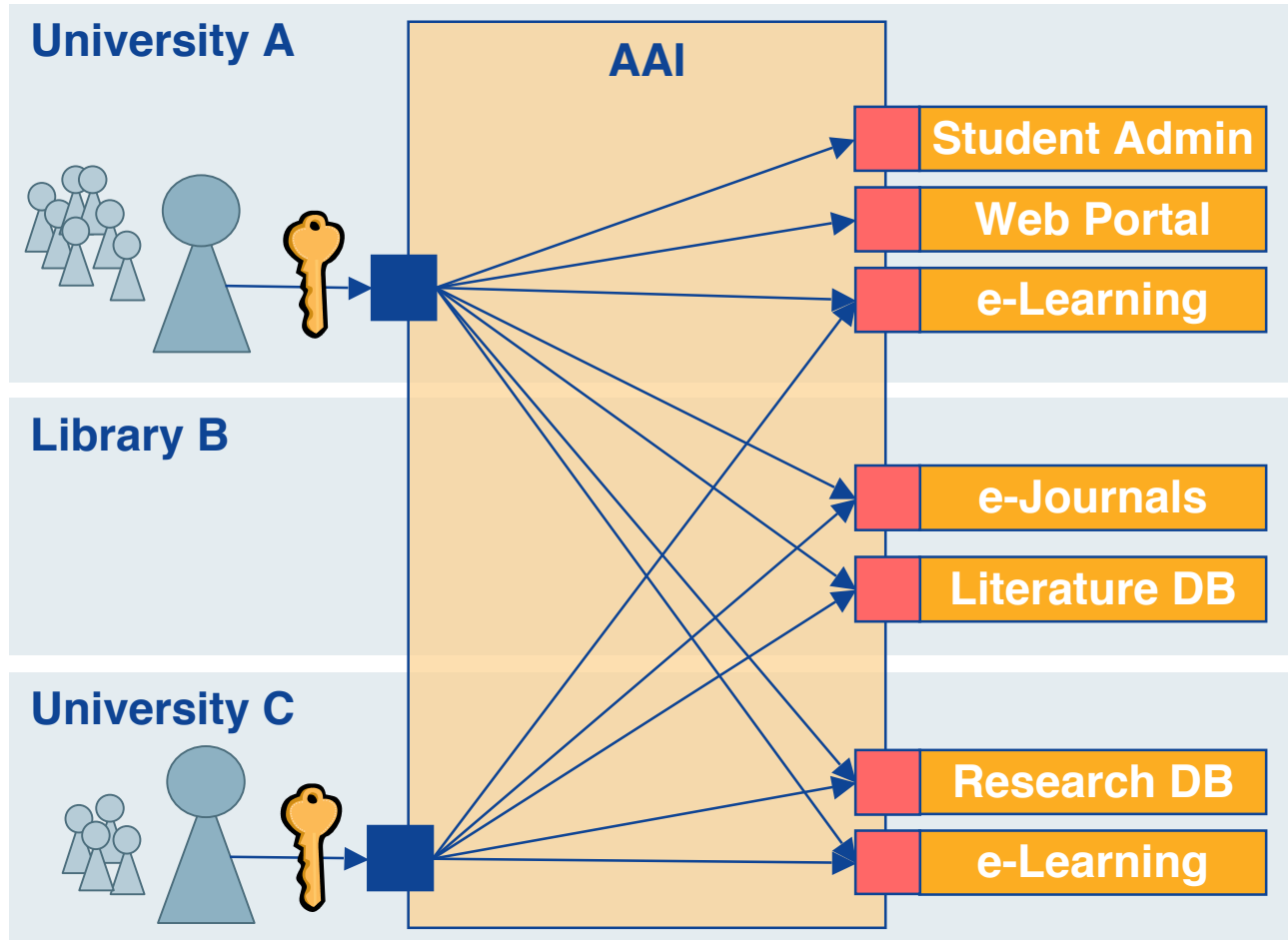- Costly implementation of inter-institutional access

User Administration Authentication

Authorization

Resource

Credentials

With AAI

- 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

University A

Library B

University C

AAI

Student Admin

Web Portal

e-Learning

e-Journals

Literature DB

Research DB

e-Learning

User Administration Authentication

Authorization
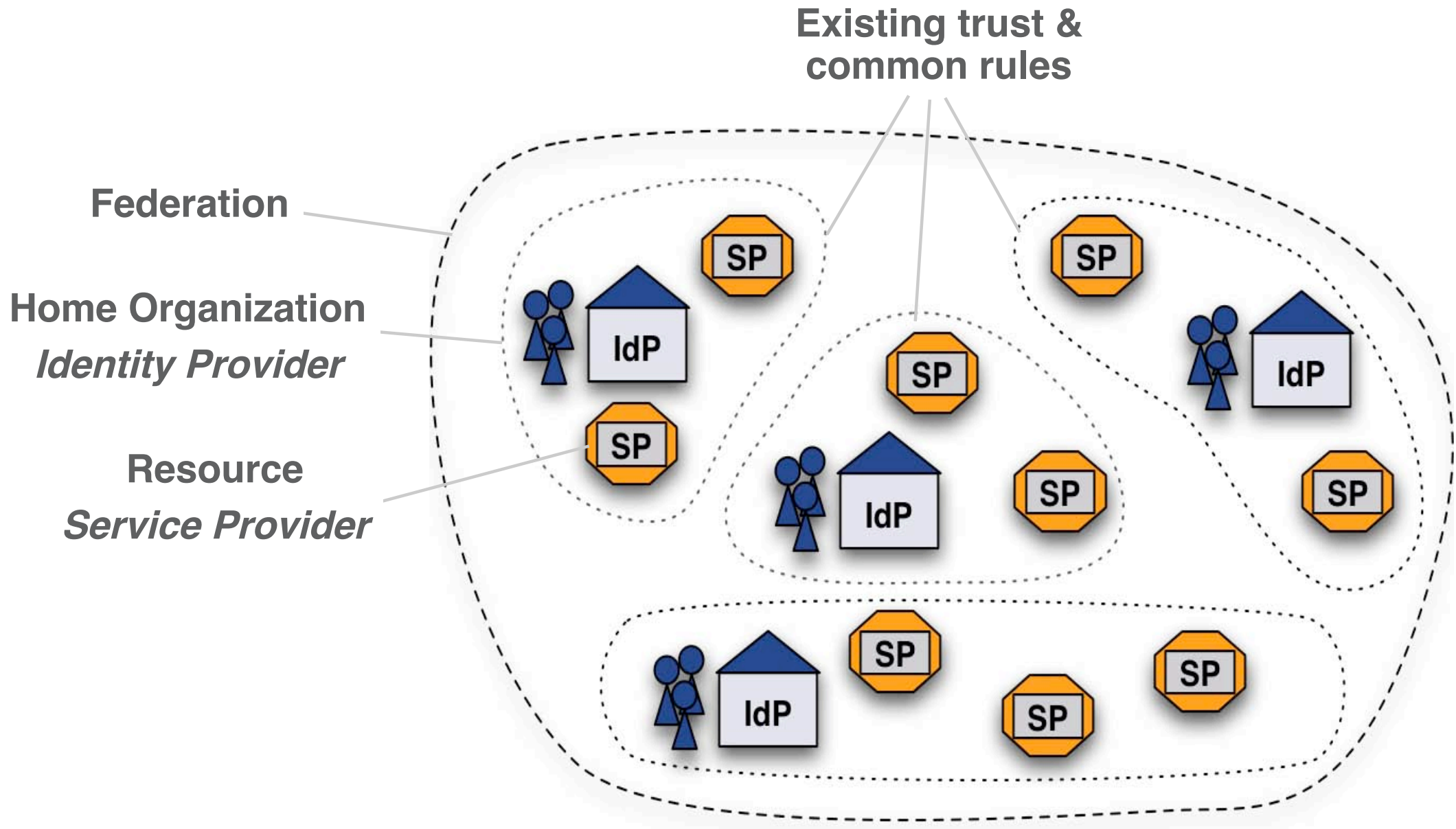
Resource

Credentials

Shibboleth

- **Open Source**
- **Developed by Internet2**
- **Federated approach**
- **Privacy**
- **National deployments in the CH, FI, FR, UK and US**
- **Currently for web resources only**
- **Based on SAML**
- **Liberty Alliance also based on SAML**
- **Growing interest from content providers, e-journal publishers**

http://shibboleth.internet2.edu

What is a Federation?

Existing trust &
common rules

Federation

Home Organization
Identity Provider

Resource
Service Provider

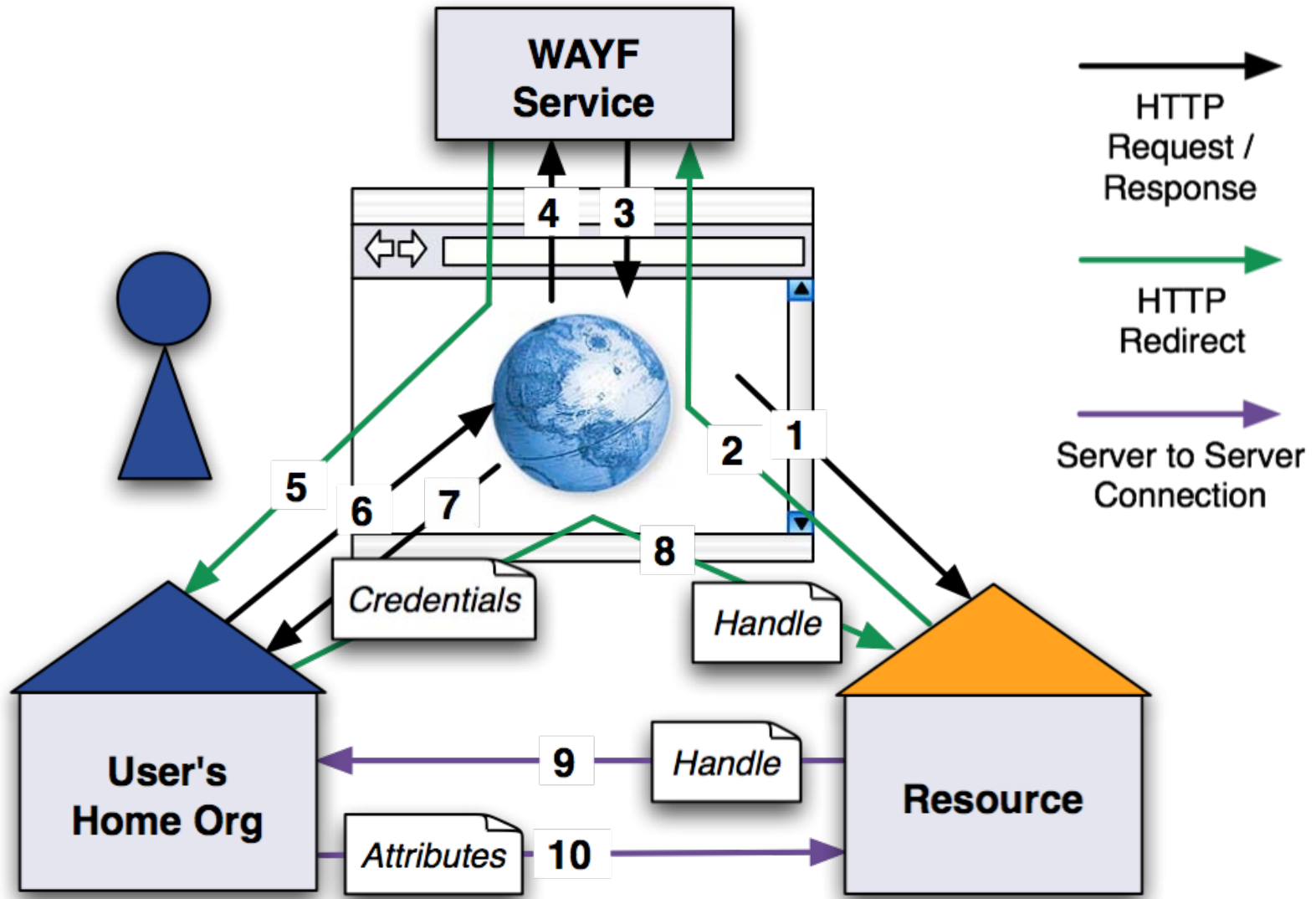# Federated Identity Management

- **Existing digital identity can be used**
  - **also outside the own home organization**
  - **for authentication**
  - **and authorization**

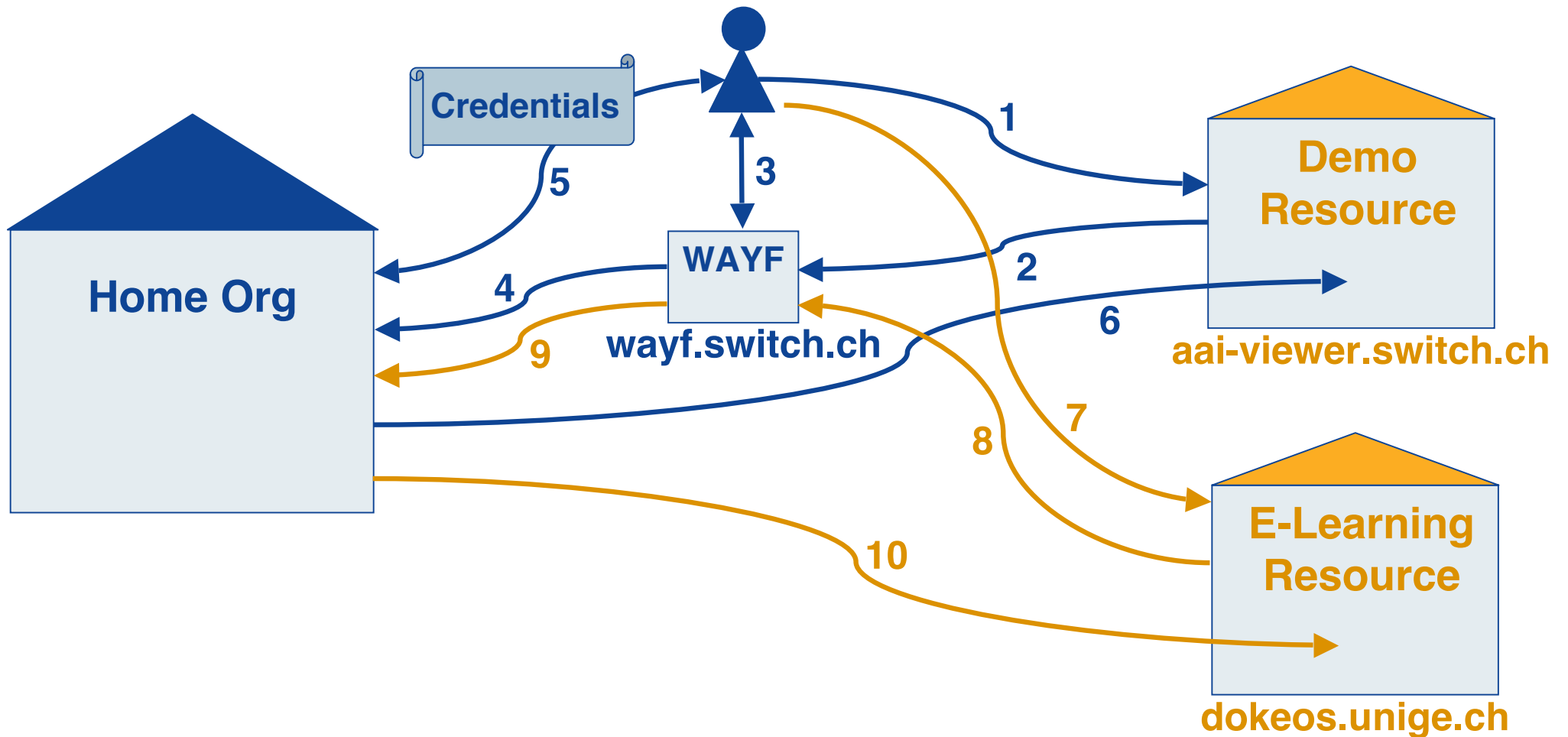- **Service Providers trust the Identity Management at the users Home Organization**

Demo: Try it yourself

- **http://www.switch.ch/aai/demo**
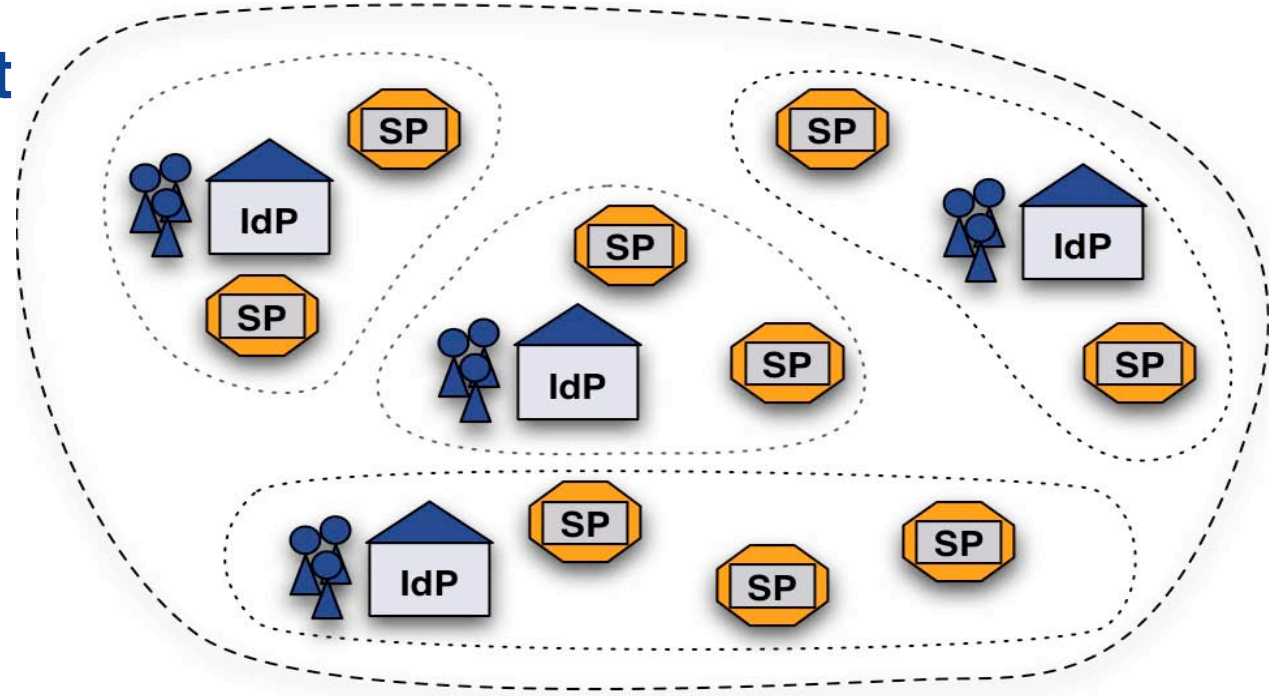
  ➜ **click on «demo resource»**

  use Home Organization: AAI Test Home Organization

  use Username: demouser

  use Password: demo

- **with a personal AAI account, use this URL:**

  https://aai-viewer.switch.ch/aai

  and choose your Home Organization

Demo

Single Sign On

SWITCH
The Swiss Education & Research Network

Credentials

Home Org

WAYF
wayf.switch.ch

Demo Resource
aai-viewer.switch.ch

E-Learning Resource
dokeos.unige.ch
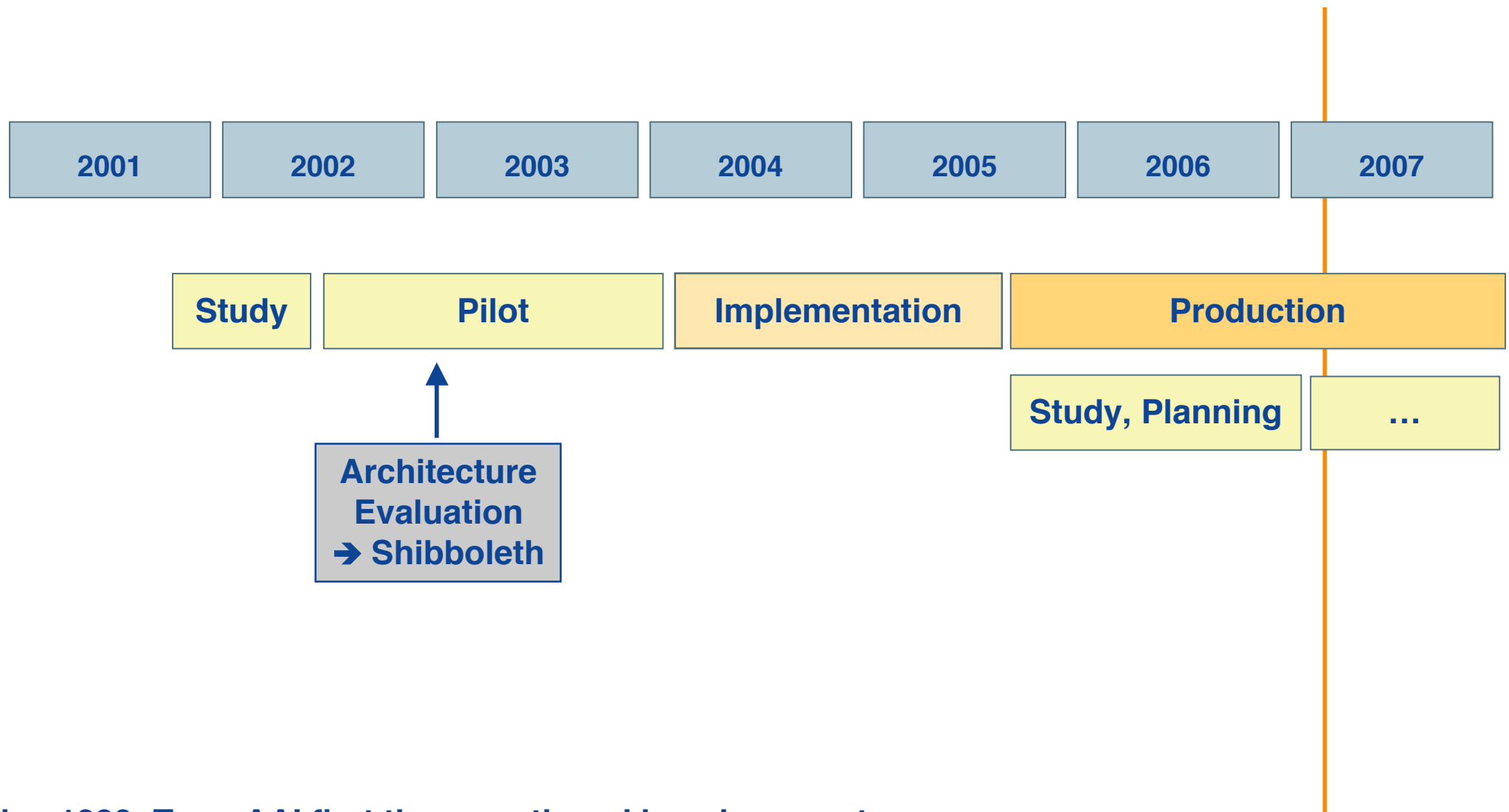
1 2 3 4 5 6 7 8 9 10

https://dokeos.unige.ch/home
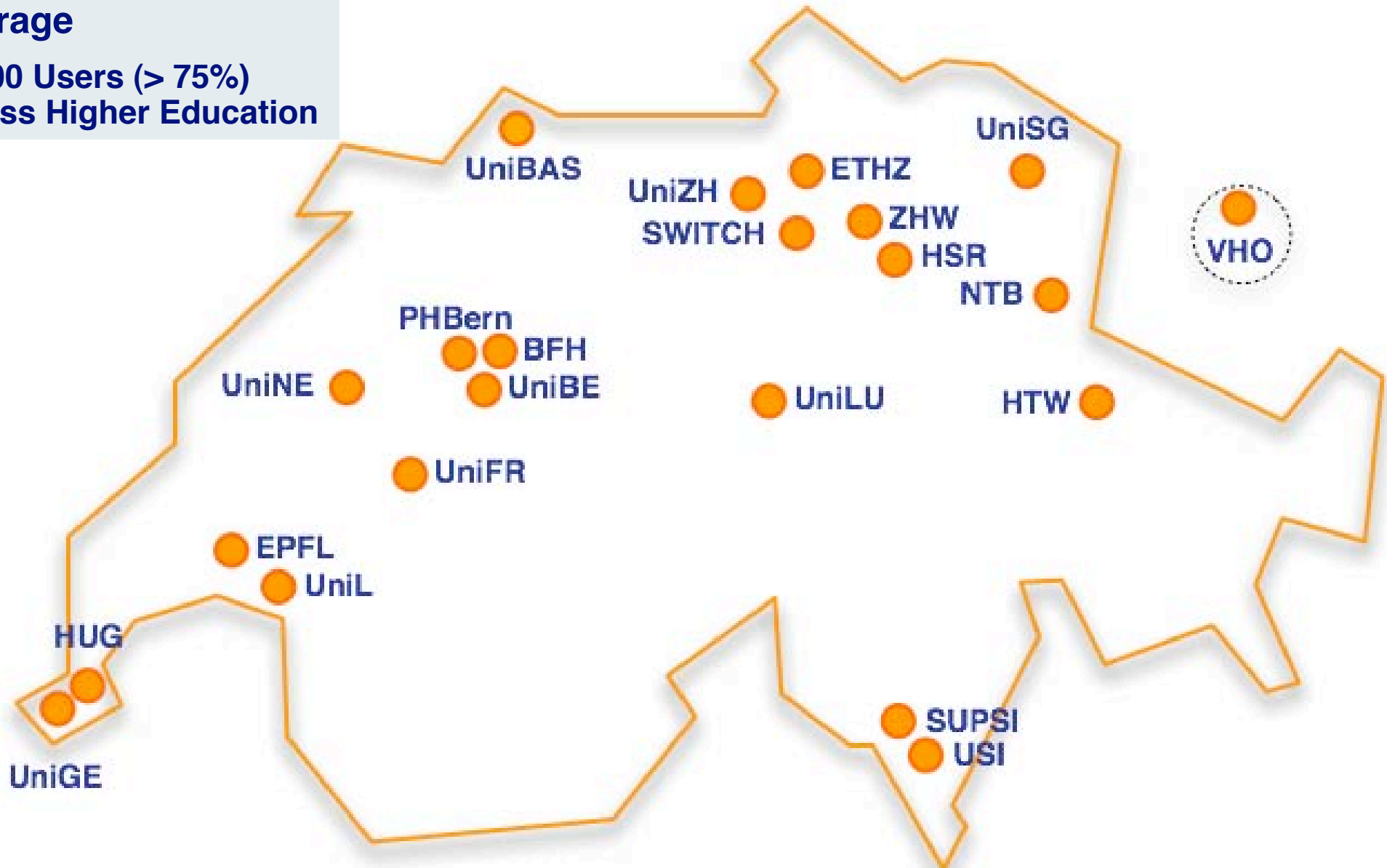
SWITCHaai Project Timeline

Nov 1999: Term AAI first time mentioned in a document
Nov 2000: AAI Workshop

Identity Providers in SWITCHaai

Coverage

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

Service Providers in SWITCHaai

SWITCH
The Swiss Education & Research Network

E-Learning

OLAT Moodle WebCT CE
WebCT Vista VITELS
Dokeos
ADlearn DOOR
DOIT CASUS ILIAS
Claroline Blackboard

Libraries

EZproxy JSTOR
ScienceDirect
VirtualLib DigiTool RERO
EBSCO Aleph

Other Web Applications

eConf Portal SLCS
BSCW
Compicampus OpenCMS
EVA WebSMS Plone
Jahia TWiki Sympa
Lenya uPortal IS-Academia

Commercial & other Partners

MSDNAA Neptun Store
Federal Court
SwissLex

operational
in pilot ideas

>170 Resources

The Federations available

Federation Metadata

- **Metadata is fundamental for a federation!**

- **Security**

  - **Info on certificates and entityID,
    to know with whom to exchange data**

- **Data protection and privacy**

  - **Attribute Release Policy (at the IdP)**

- **Metadata has to be current and in sync,
  no reliable interoperability otherwise**

  - **bilateral data exchange scales badly**

➔ **The resource registry is the tool for metadata management**

Why Server Certificates?