AAI Tutorial

SWITCH
Serving Swiss Universities

SWITCHaai Team
aai@switch.ch

Berne, 5. May 2009

Agenda

1 What is AAI?

2 Demo

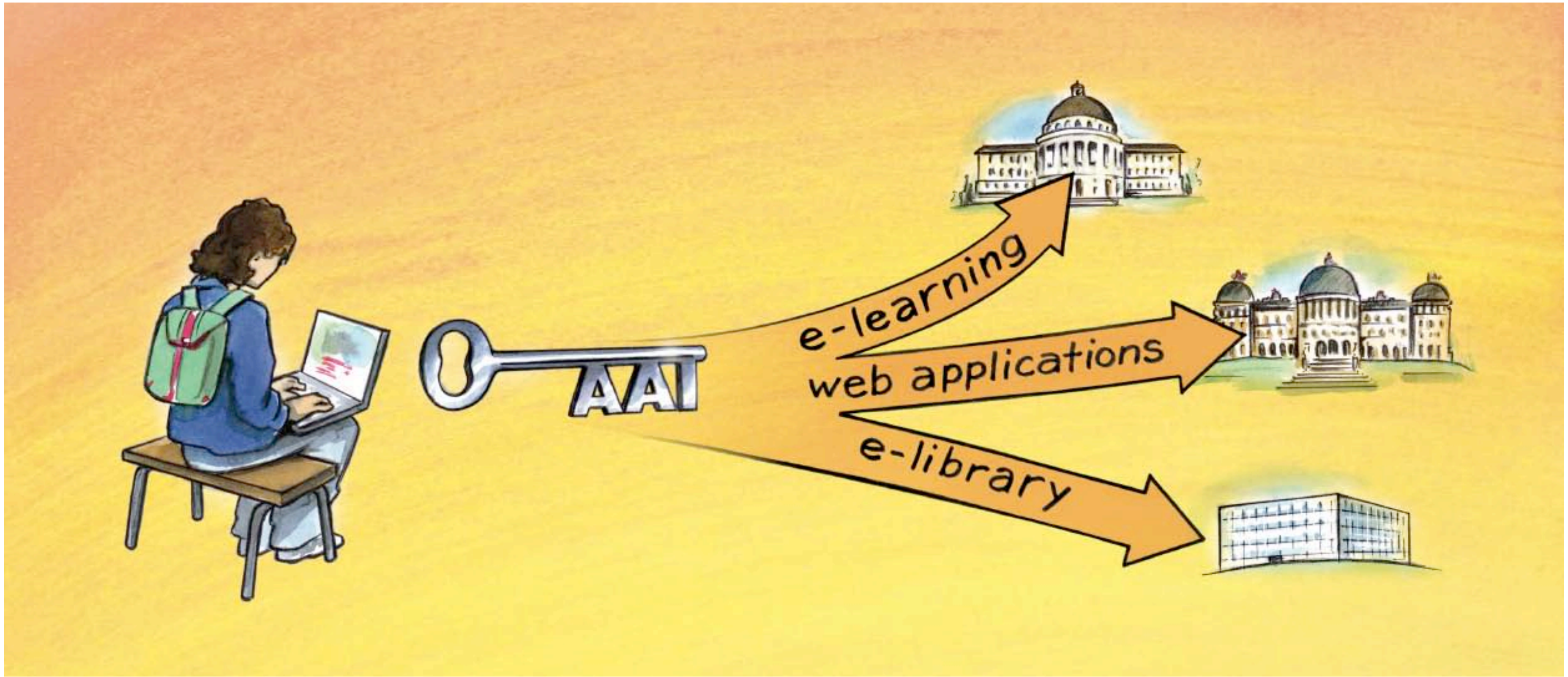
3 The SWITCHaai federation

4 Technical details behind AAI

5 Summary and Q&A

AAI - Key to access them all

AAI = Authentication and Authorization Infrastructure



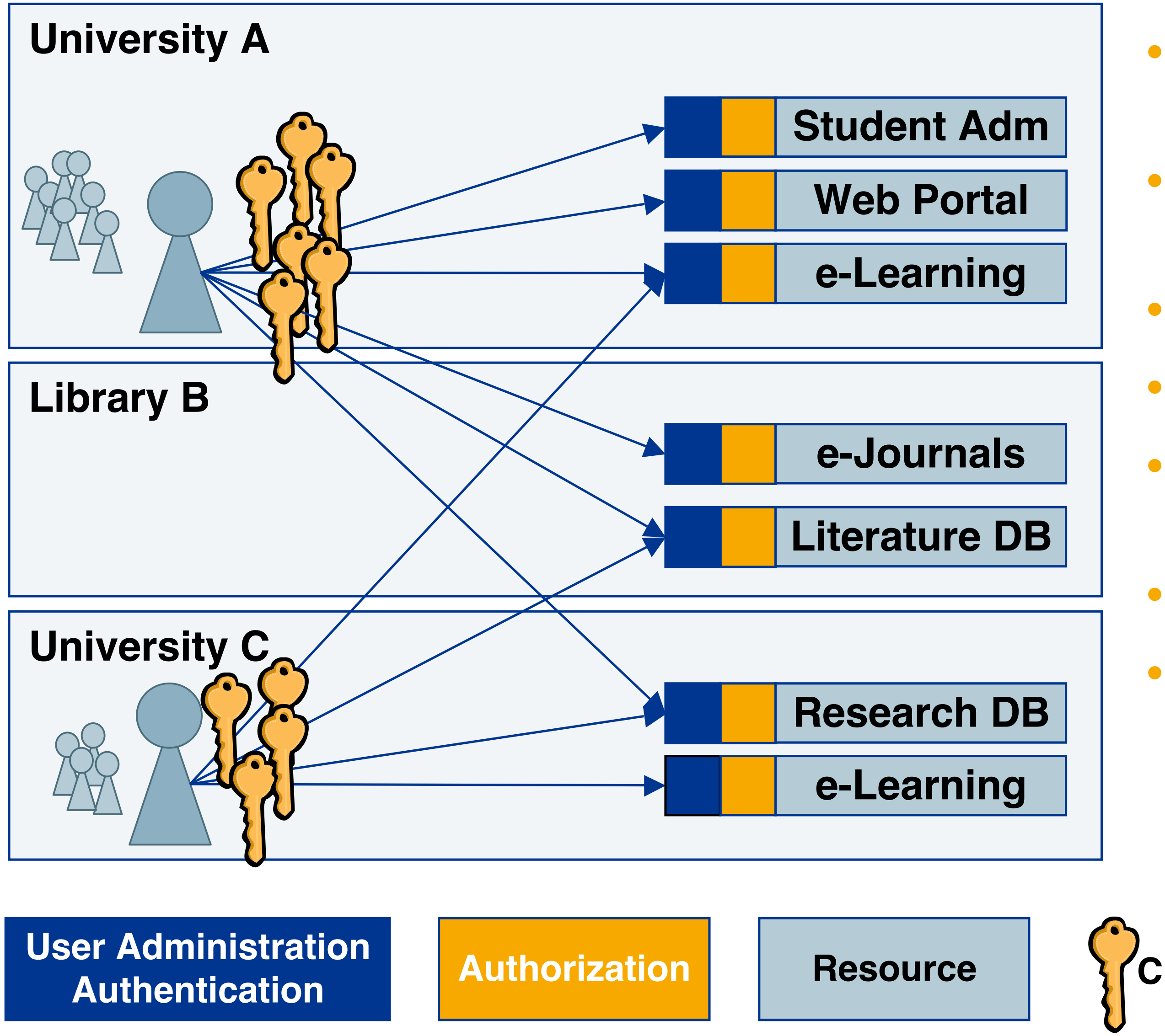
Evolution of Identity Management

- Stone Age:
  Application maintains unique credential and identity information for each user
- Bronze Age:
  Credentials are centralized (e.g. kerberos, LDAP) but applications maintain identity information
- Iron Age:
  Credentials and core identity information is centralized, applications maintain only app-specific user data
- These solutions assume application are within the same administrative domain

Diamond Age: Federated Identity

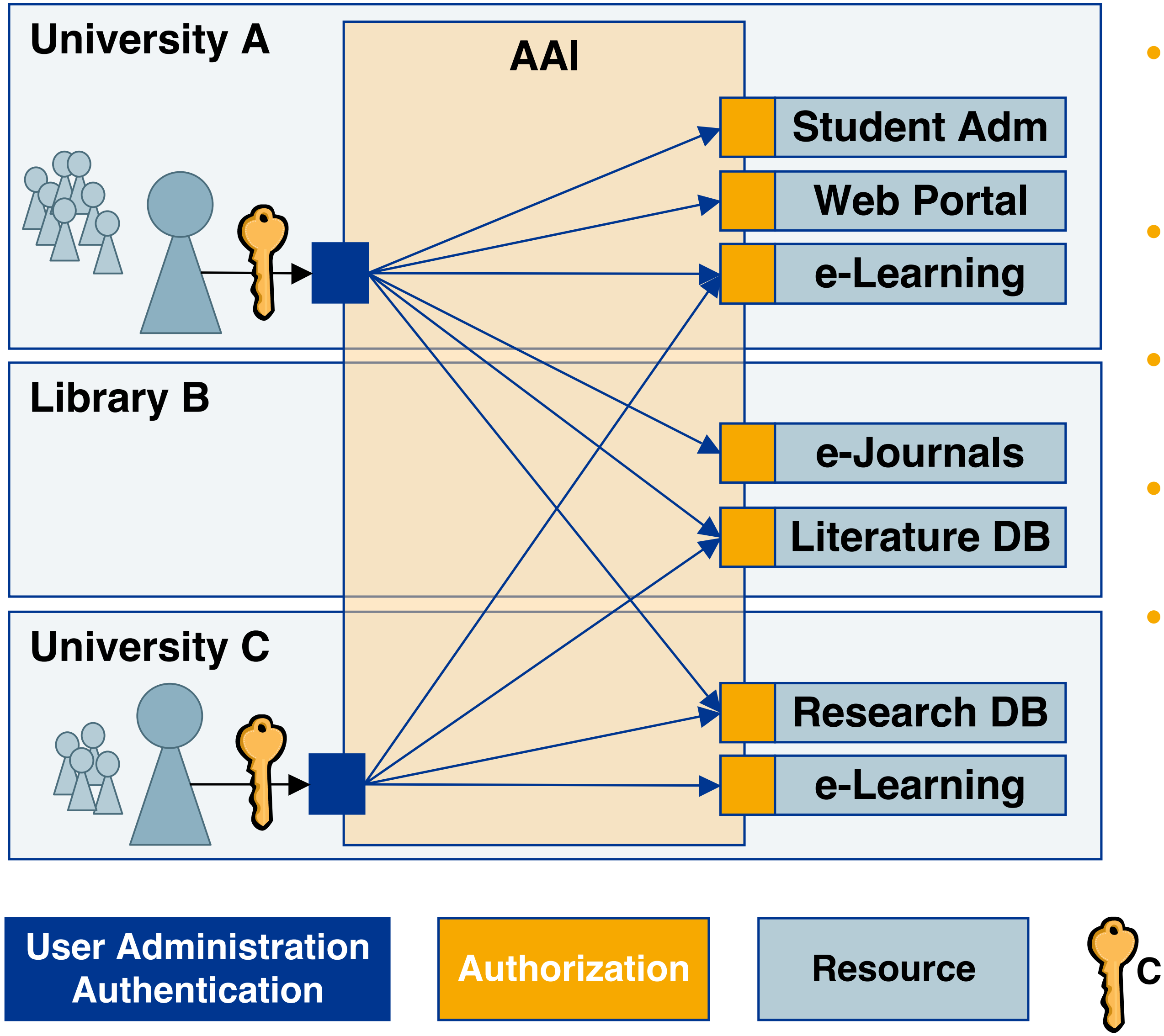
- Federated identity management is the next logical step; sharing information outside your administrative domain.
- The first principle within federated identity management is the active protection of user information.
  - Protect the user's identifier; applications don't necessarily need to know **who** the person is
  - Protect the user's identity information; only give applications what they absolutely need

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- Unreliable and outdated user data at resources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

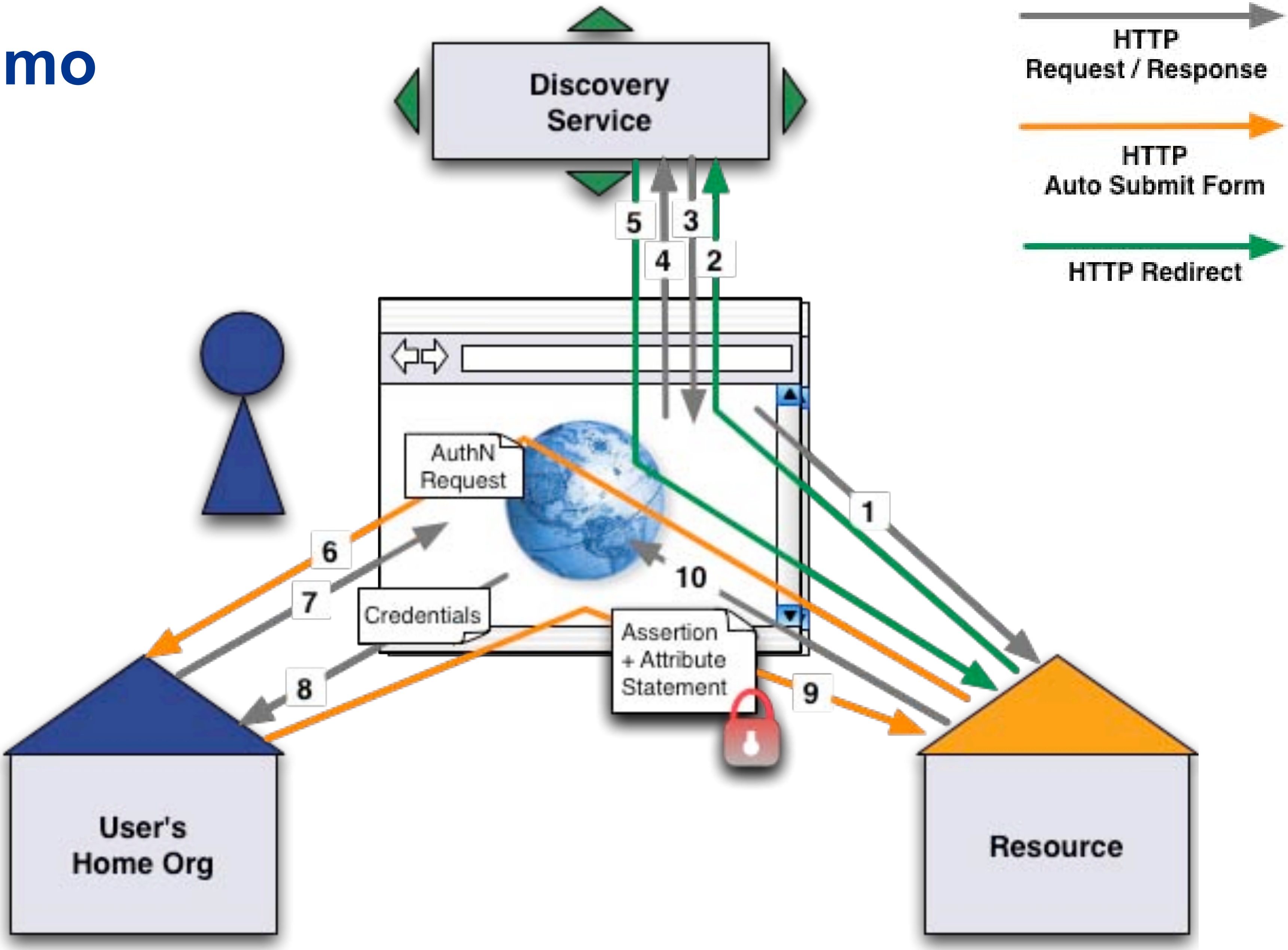


- No user registration and user data maintenance at resource needed
- Single login process for the users
- Many new resources available for the users
- Authorization independent of location
- Efficient implementation of inter-institutional access

Agenda

1. What is AAI?
2. Demo
3. The SWITCHaai federation
4. Technical details behind AAI
5. Summary and Q&A

Demo

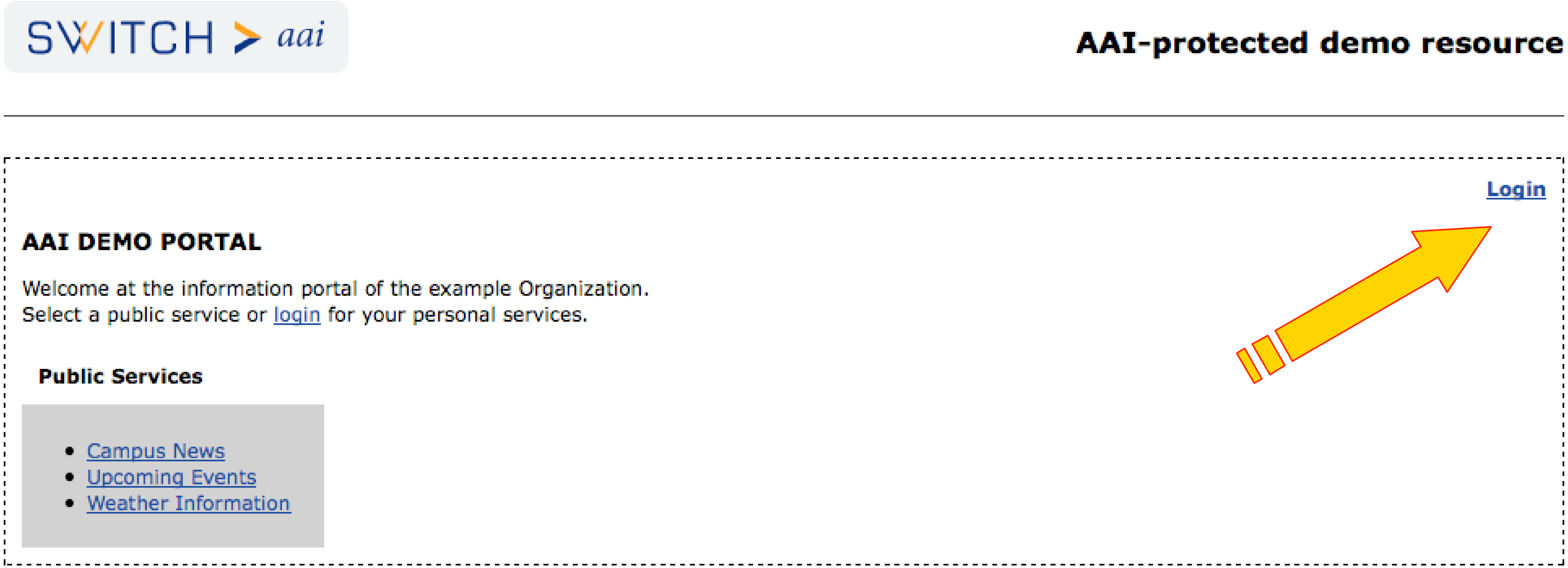


http://www.switch.ch/aai/demo/

Demo – try it yourself

Go to https://aai-demo.switch.ch/portal/

→ Click on „Login” link.



AAI-protected demo resource

Login

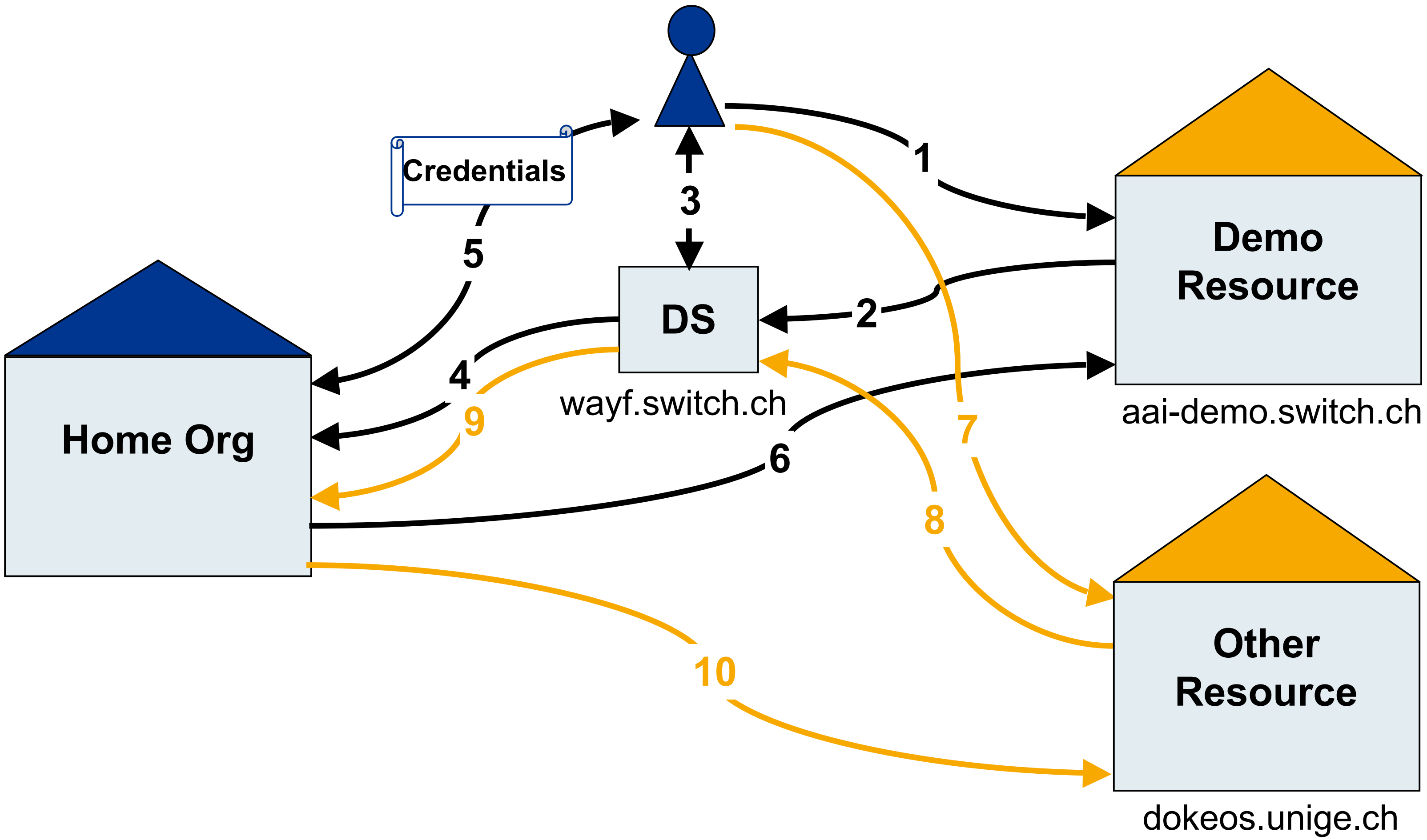
AAI DEMO PORTAL

Welcome at the information portal of the example Organization.
Select a public service or login for your personal services.

Public Services

- Campus News
- Upcoming Events
- Weather Information

Inter-organizational Single Sign On



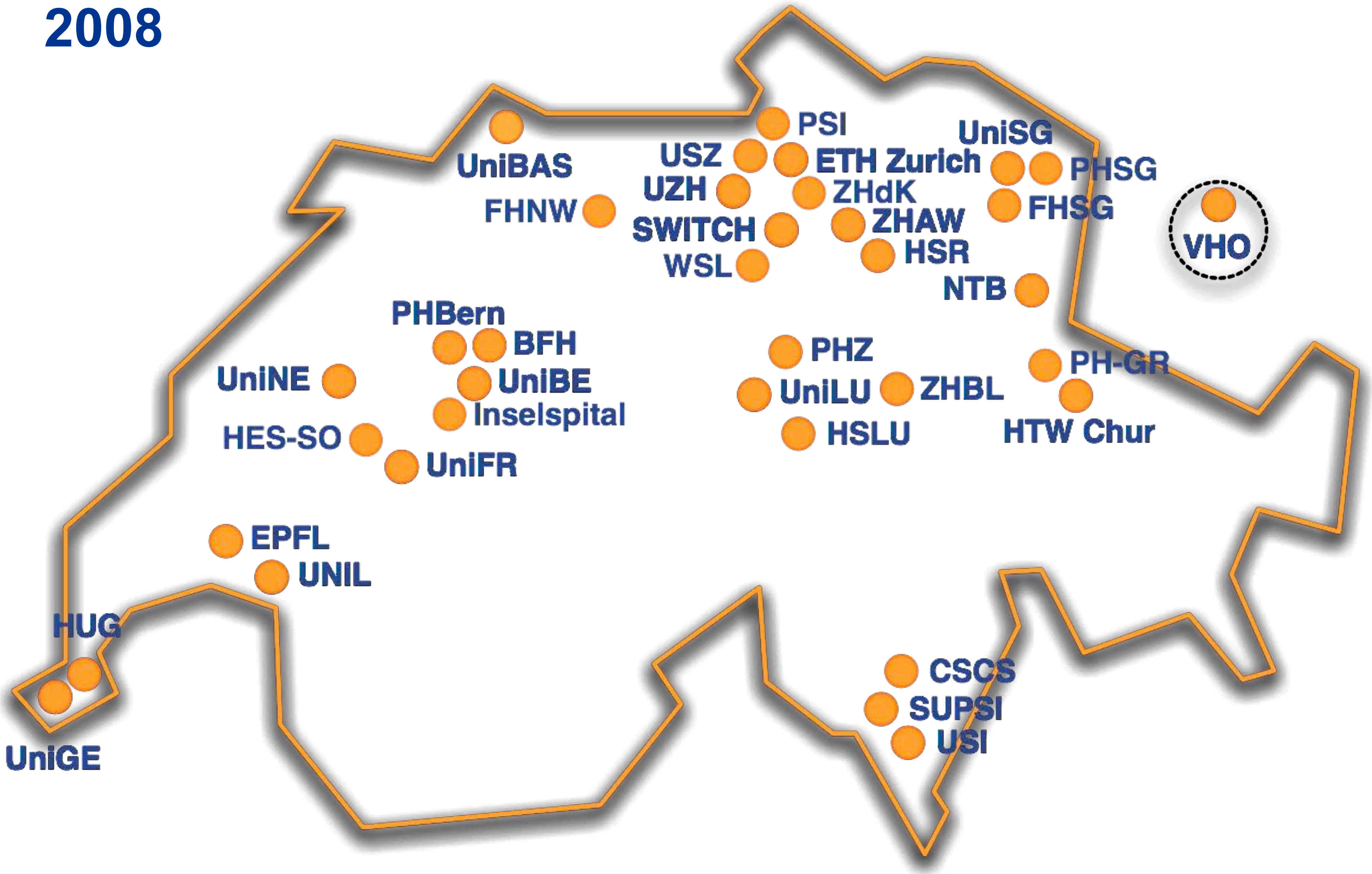
https://dokeos.unige.ch

Agenda

1. What is AAI?
2. Demo
3. The SWITCHaai federation
4. Technical details behind AAI
5. Summary and Q&A

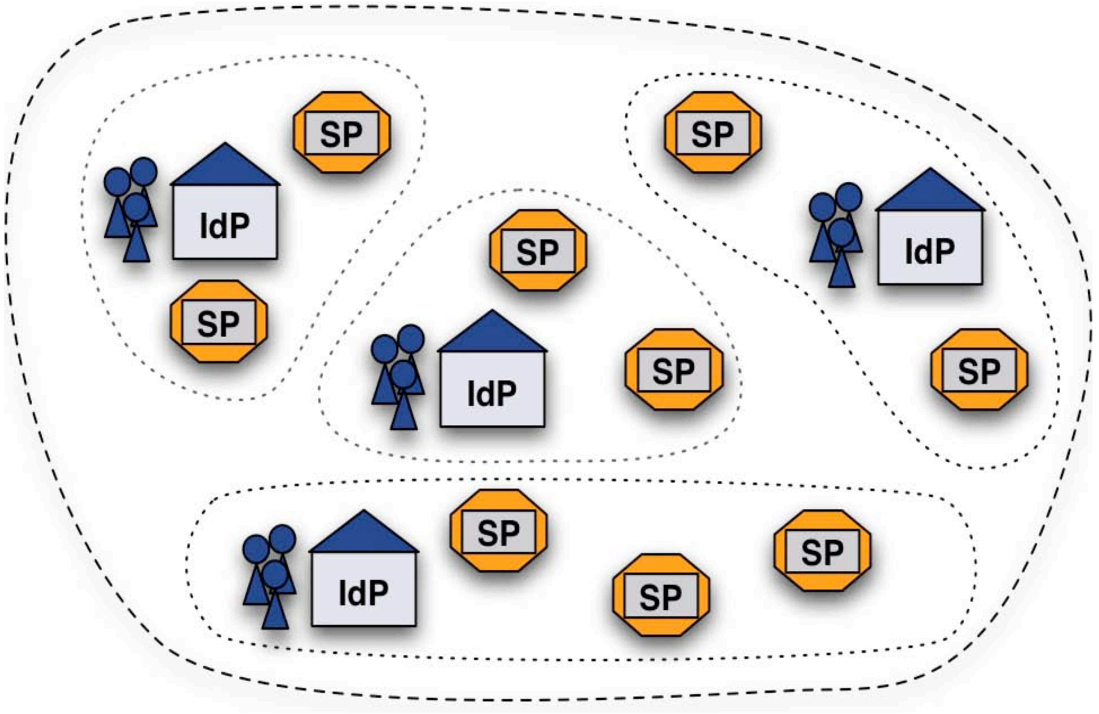
Growth of the SWITCHaai Federation

2008



What is a Federation?

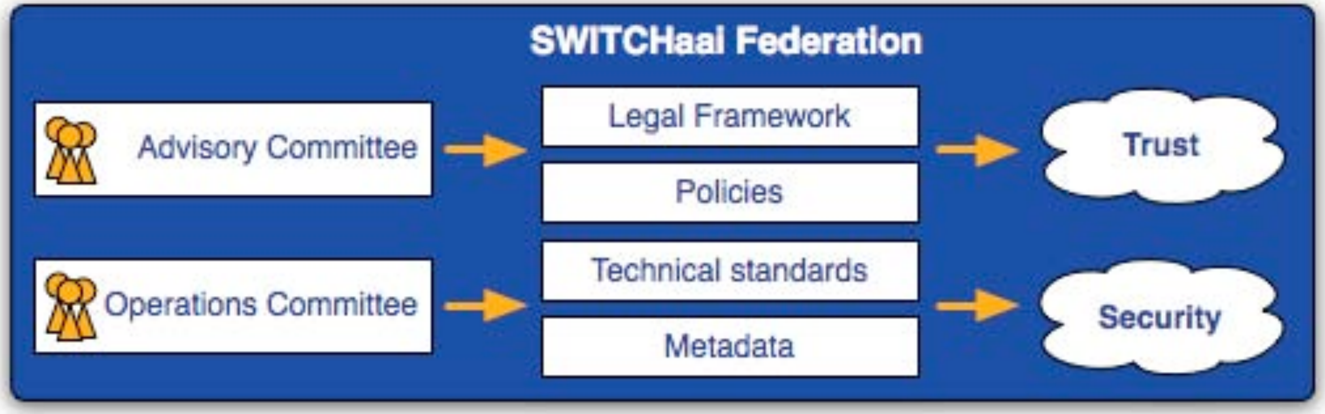
- A set of organizations agreeing on a common set of rules and standards
- **Goal** Cooperate in inter-organizational authentication, authorization and accounting

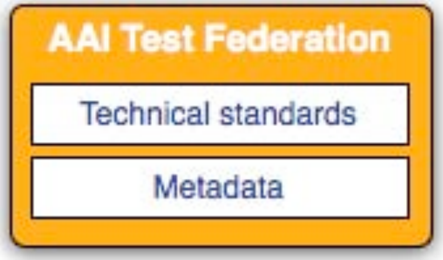


Common trust

- Legal
- Technical

SWITCHaai: An Example Federation





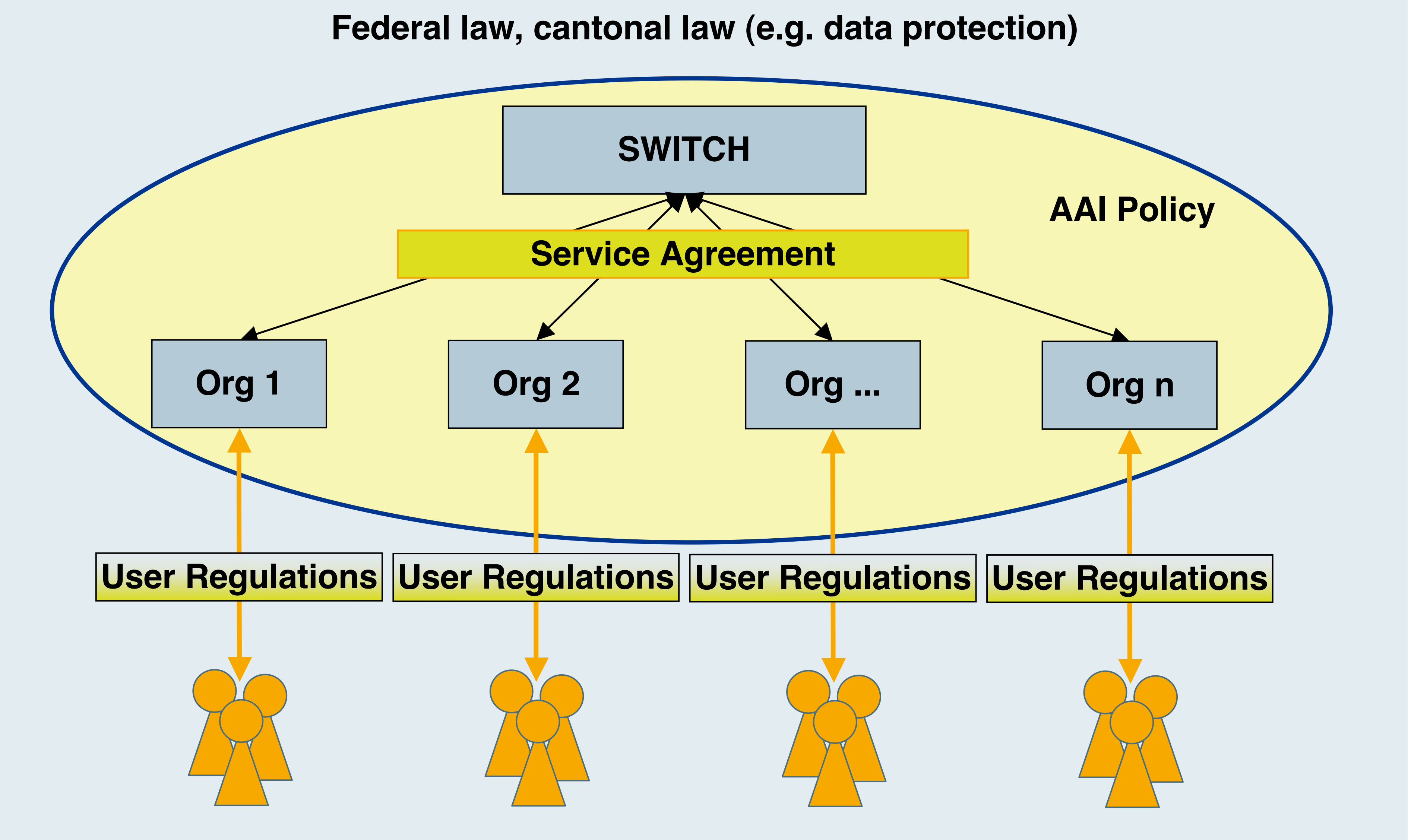
- Controlled by two bodies:
  - **Advisory Committee** deals with policies and legal framework
  - **Operations Committee** deals with technical/operational issues
- Defines two classes of members:
  - **Federation Member:** organization directly services by SWITCH
  - **Federation Partner:** organization sponsored by a member

http://switch.ch/aai/about/federation/

SWITCHaai: An Example Federation

- Rules, Policies, & Agreements
  - **AAI Policy:** concepts and rules for all entities in the federation
  - **Service Agreement:** legal contract between SWITCH and federation member
  - **Federation Partner Agreement**: legal contract between SWITCH and federation partner
  - **CA Acceptance Policy:** policy about CAs and certificates accepted by the federation
  - **AAI Attribute Specification:** minimum set of required and optional attributes supported by federation entities

SWITCHaai: An Example Federation



SWITCHaai: Provided services

- Rules, policies, and agreements
- Documentation: installation/migrations guides, howtos
- Call-in helpdesk and support mailing list
- Centralized Services:
  - Discovery Service
  - Resource Registry (metadata management)
  - Virtual Home Organization
  - Group Management Tool
  - Attribute Viewer
- Test federation
- Some application integration support
- uApprove shibboleth plugin
- Training → http://www.switch.ch/aai/events/installfest-2009/

Agenda

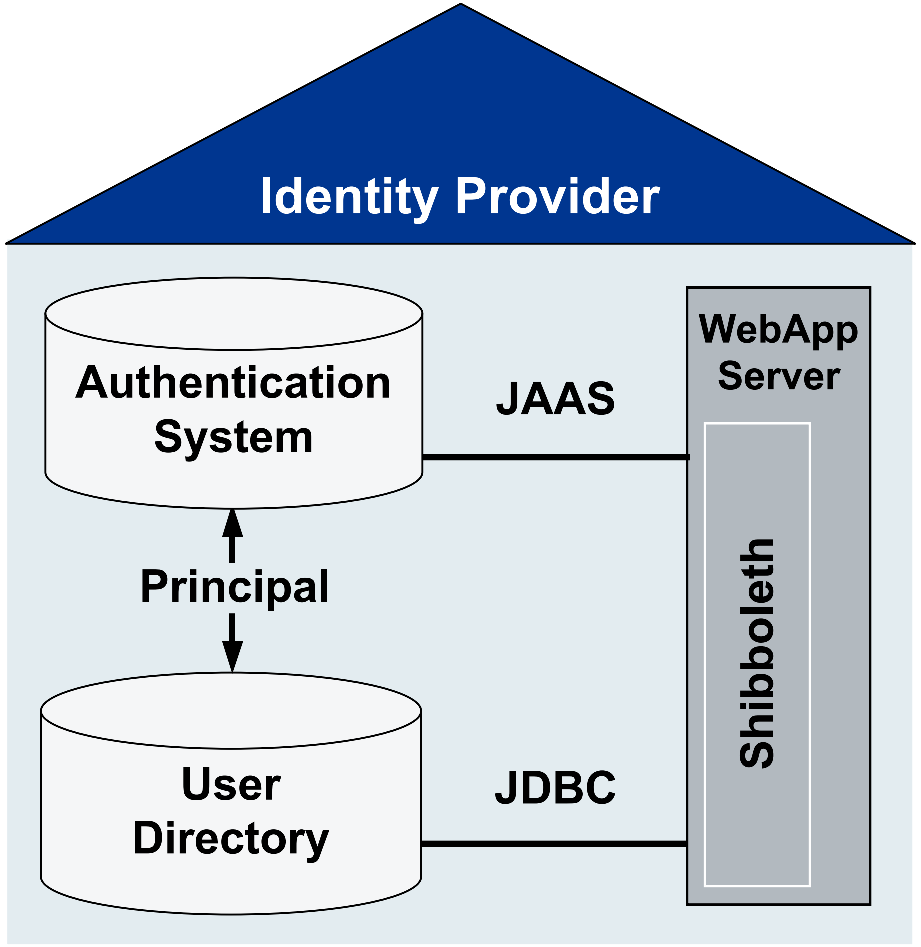
1. What is AAI?
2. Demo
3. The SWITCHaai federation
4. Technical details behind AAI
5. Summary and Q&A

Shibboleth - The Software

- Open Source
- Word **Shibboleth** was used to identify members of a group
- Based on Security Assertion Markup Language (SAML)
- Internationally used by universities

https://shibboleth.internet2.edu

AAI-enabling a Home Organization



Prerequisite

- Authentication System
- User Directory

Shibboleth is a Java WebApp

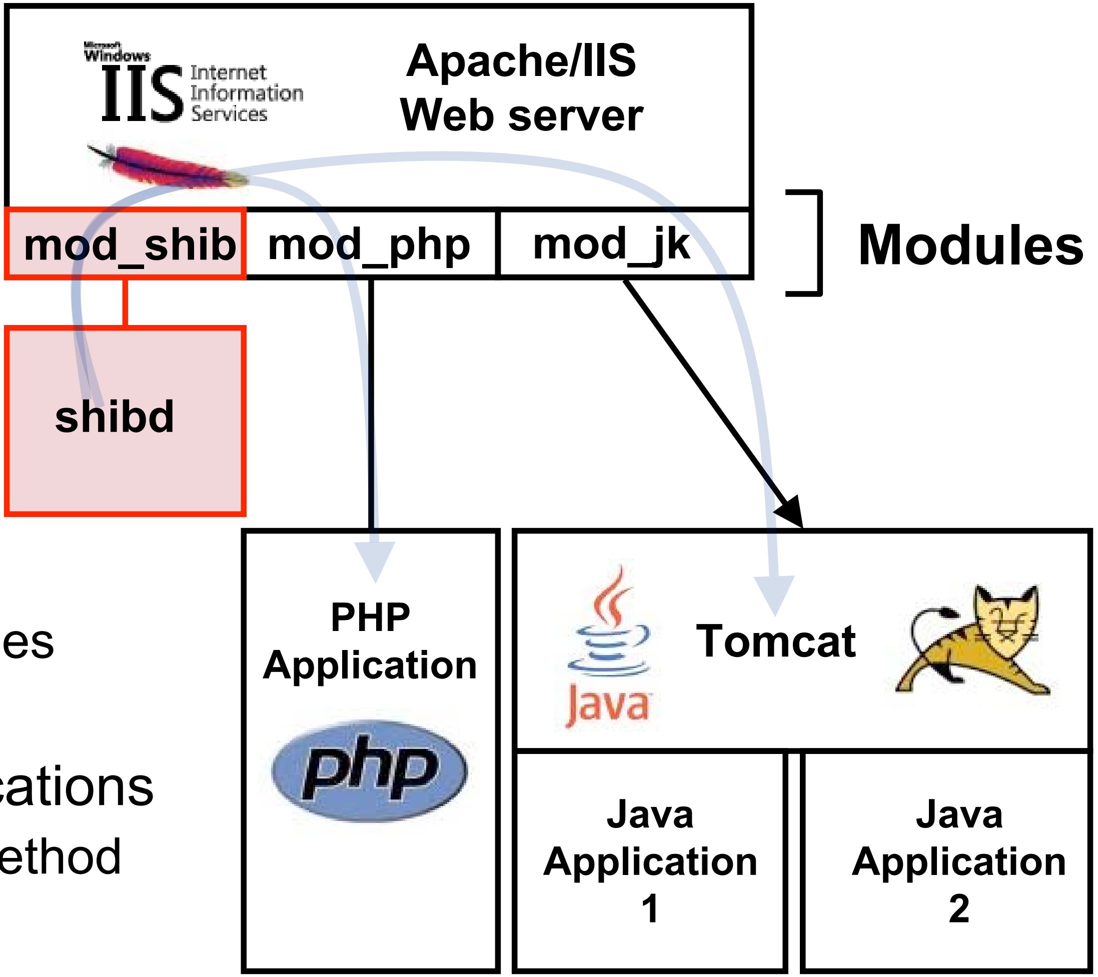
Web Servers supported

- Tomcat/JBoss
- Apache + Tomcat/JBoss
- IIS + Tomcat/JBoss

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

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



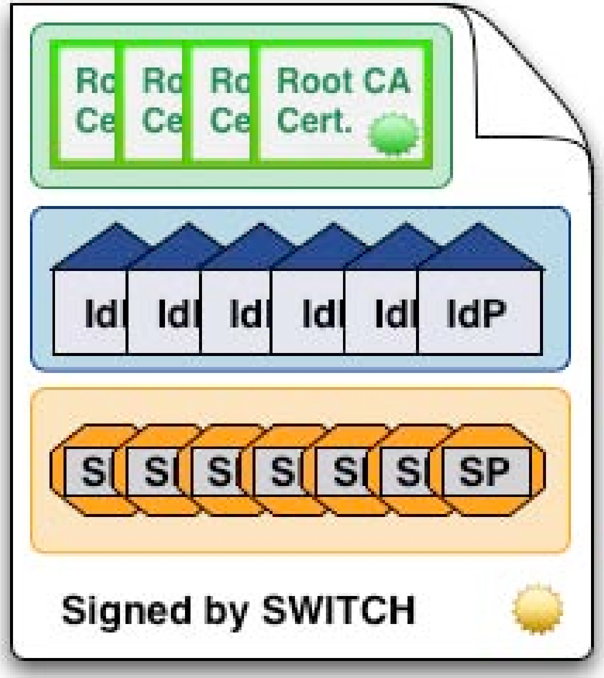
Federation Metadata

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

- Accepted Root CA certificates
- Description of Identity Providers (incl. embedded certificates)
- Description of Service Providers (incl. embedded certificates)

SWITCHaai Metadata is signed by SWITCH

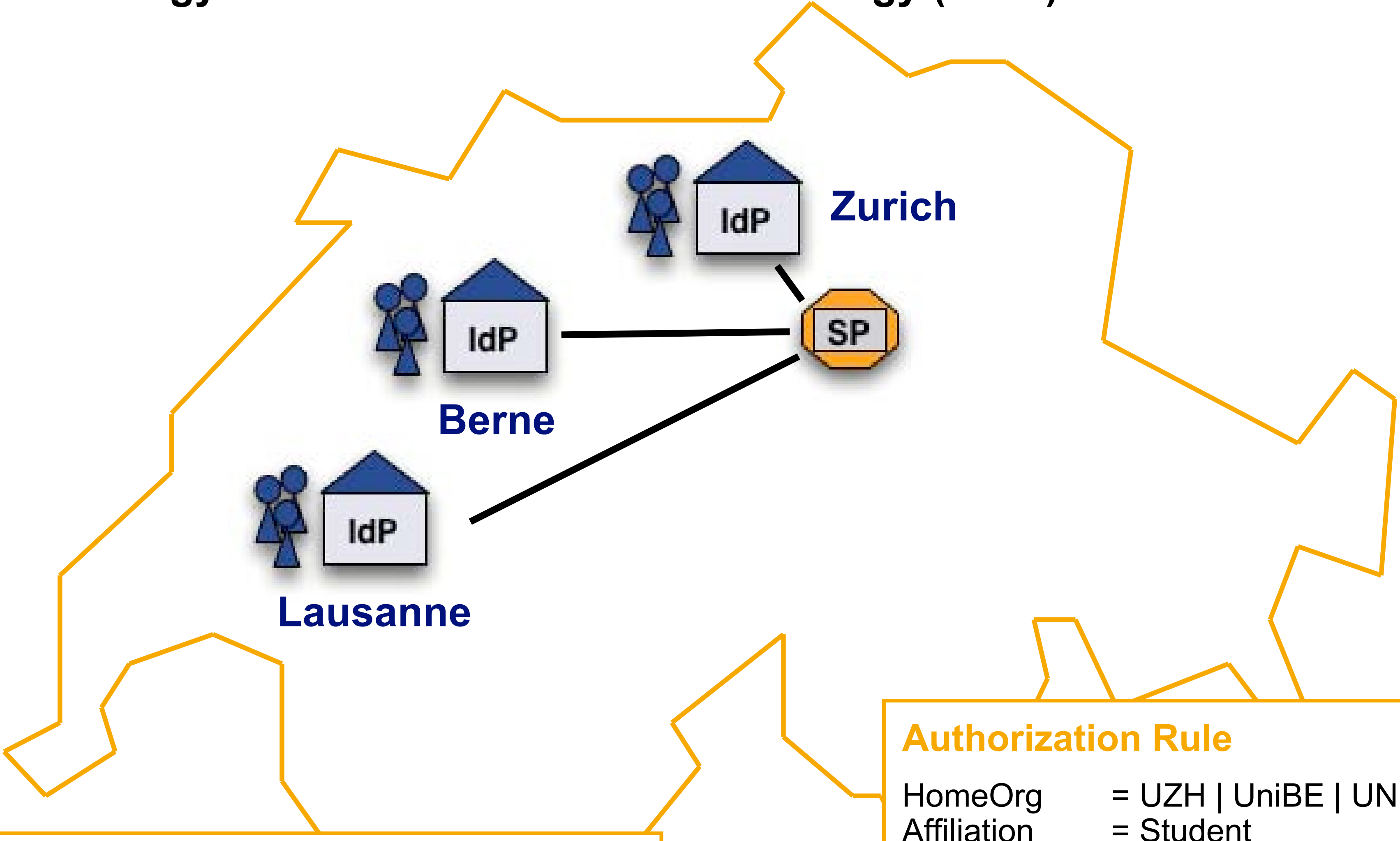
http://www.switch.ch/aai/metadata



Metadata technically describes the federation!

Attribute Based Authorization Example

Dermatology Online with Interactive Technology (DOIT)



DOIT: http://www.cyberderm.net

Authorization Rule

HomeOrg	= UZH | UniBE | UNIL
Affiliation	= Student
StudyBranch	= Medicine
StudyLevel	= 20

SWITCHaai Attributes

Personal

Unique Identifier

Surname

Given name

E-mail

User ID

Matriculation number

Employee number

Address(es)

Phone number(s)

Preferred language

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

Already Shibbolized Applications

Information Providers:	Learning Management Systems:	Other Systems:
• American Chemical Society • ArtSTOR • Atypon • CSA • Digitalbrain PLC • EBSCO Publishing • Elsevier ScienceDirect • ExLibris • H.W. Wilson • JSTOR • The Literary Encyclopedia • Metapress • NSDL • OCLC • Ovid Technologies Inc. • Project MUSE • Proquest Information and Learning • Serials Solutions • SCRAN • Schweizerisches Bundesgericht • Thomson Gale • Thomson Reuters • Useful Utilities - EZproxy	• Blackboard • CLIX • Fronter • ILIAS • INSTRUCT • Moodle • OLAT • Sakai • WebAssign • WebCT	• Bodington.org • Condor • Confluence Wiki • Darwin Streaming Server • Drupal • DSpace • eAcademy • Fedora Repository • Google Apps/Email • GridSphere • GridShib • Higher Markets • Horde • Hupnet • JISCmail • LionShare • Media Wiki • Microsoft • MyProxy • Napster • PHEAA • Sharepoint® from Microsoft • SYMPA • Symplicity • TurnItIn • TWiki • uPortal • WordPress • Zope + Plone\

https://spaces.internet2.edu/display/SHIB2/ShibEnabled

Agenda

1 What is AAI?

2 Demo

3 The SWITCHaai federation

4 Technical details behind AAI

5 Summary and Q&A

AAI - Essential Facts

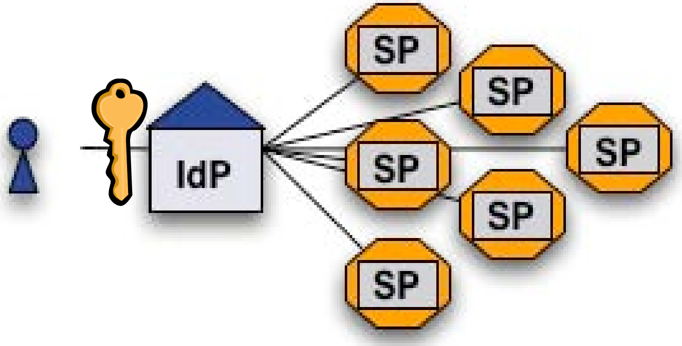
AAI makes life easier for everybody

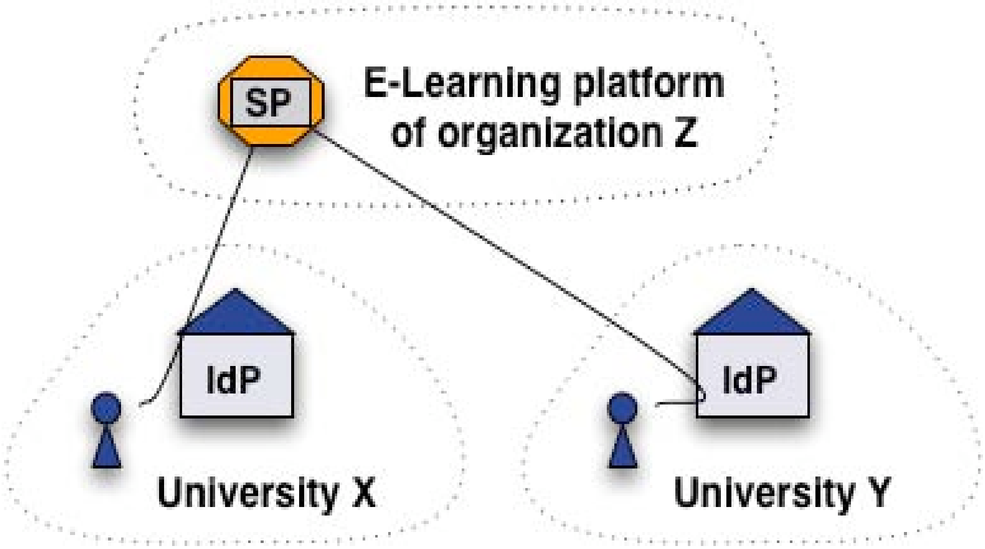
Users have a single account for all their services

Authentication only at user’s home organization

User data is maintained only once

Collaboration between multiple organizations is simplified





Questions ?

Q & A

http://www.switch.ch/aai

aai@switch.ch

SWITCHaai 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-announce Mailinglist
  - http://lists.switch.ch/mailman/listinfo/aai-announce
- The AAI Demo
  - http://www.switch.ch/aai/demo