SWITCH

The Swiss Education & Research Network

AAI Attributes, Authoriziation, System Requirements, SWITCHaai Central Services

The AAI Team, aai@switch.ch

Contents

SWITCH
The Swiss Education & Research Network

- AAI Attributes
- Authorization
- System Requirements
- Virtual Home Organization (VHO)
- WAYF
- Resource Registry

SWITCH

The Swiss Education & Research Network

AAI Attributes

Patrik Schnellmann, schnellmann@switch.ch

SWITCHaai Attributes

SWITCH
The Swiss Education & Research Network

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

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

Example with SWITCHaai Attributes

SWITCH
The Swiss Education & Research Network

Attribute	Value
UniqueID	773443@aaitest.switch.ch
Givenname	Demouser
Surname	SWITCHaai
Affiliation	staff
Entitlement	http://unil.ch/aai/resources/biblio92 http://ethz.ch/res/12345
HomeOrganization	aaitest.switch.ch
HomeOrganizationType	others

SWITCH

The Swiss Education & Research Network

Authorization

Patrik Schnellmann, schnellmann@switch.ch

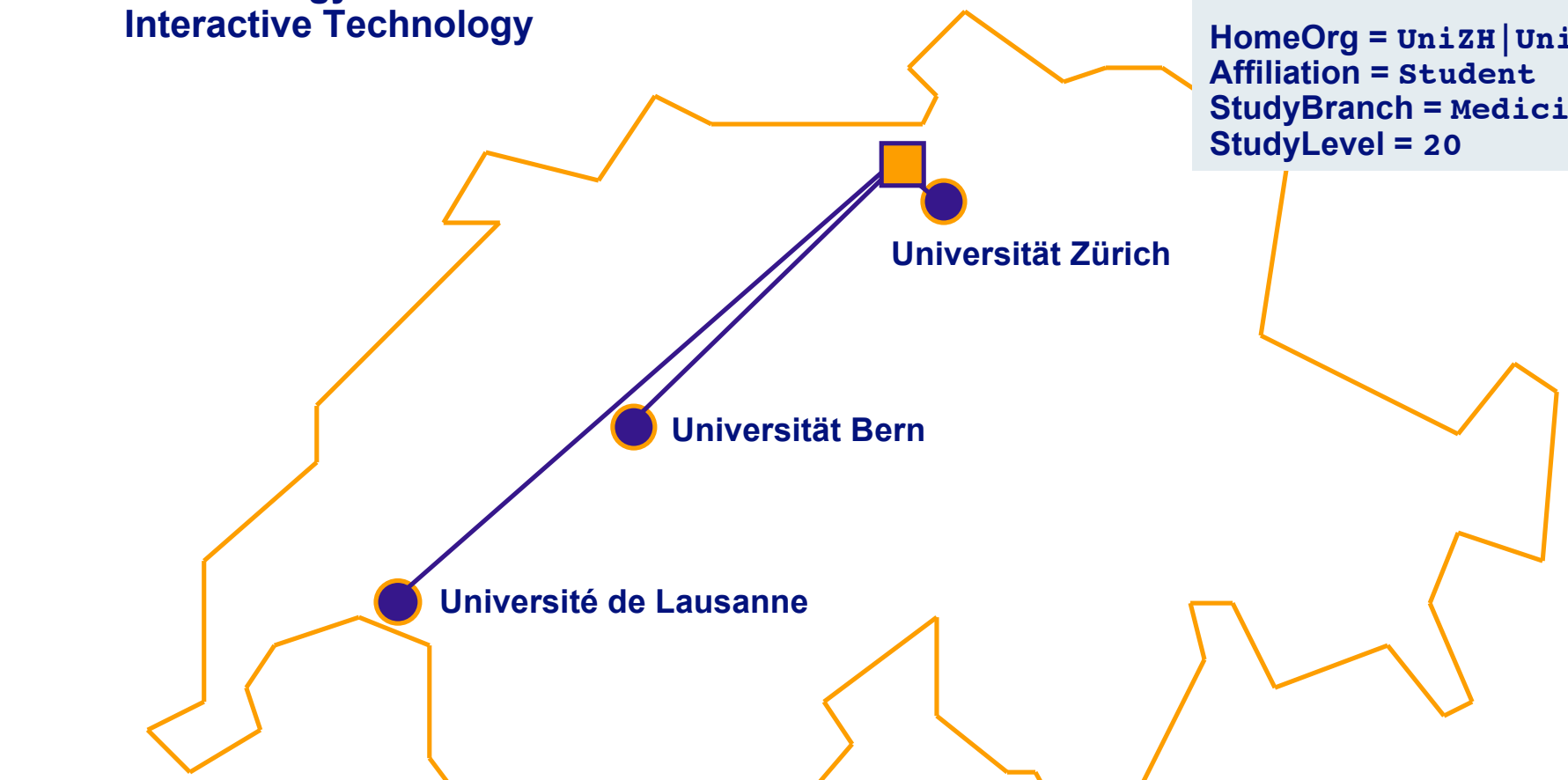
Access Rules using AAI Attributes

SWITCH
The Swiss Education & Research Network

DOIT: Dermatology Online with Interactive Technology

Access Rule

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

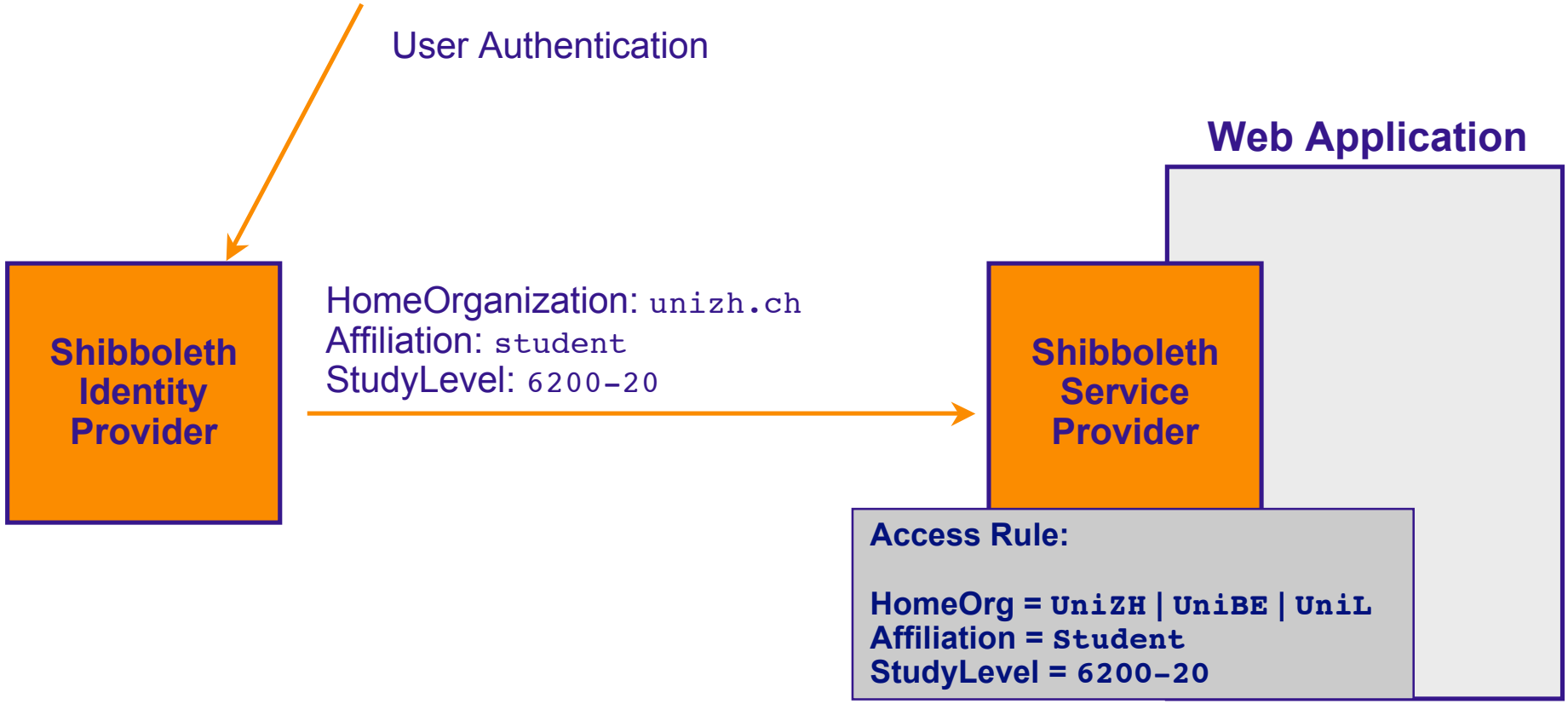


Resource

Identity Provider

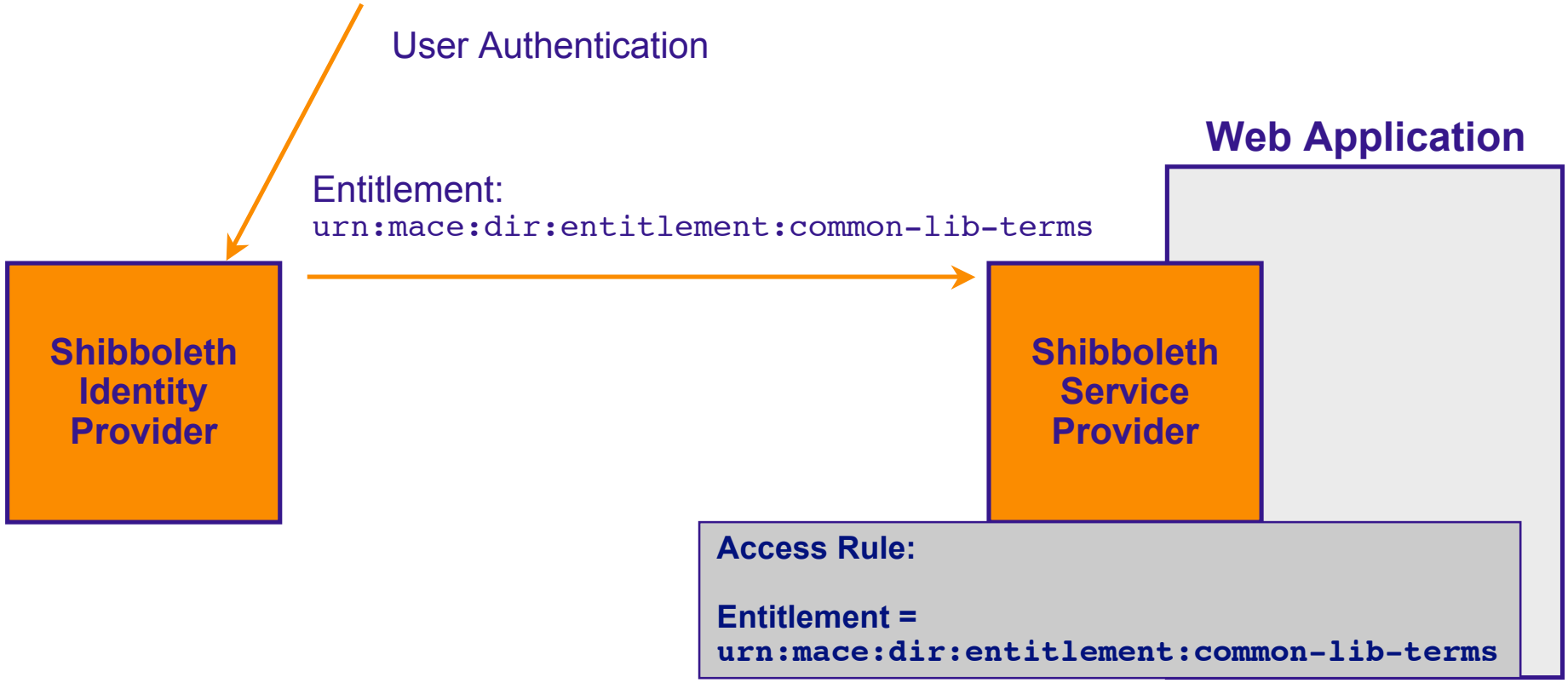
http://www.cyberderm.net/

Authorization I: Group membership

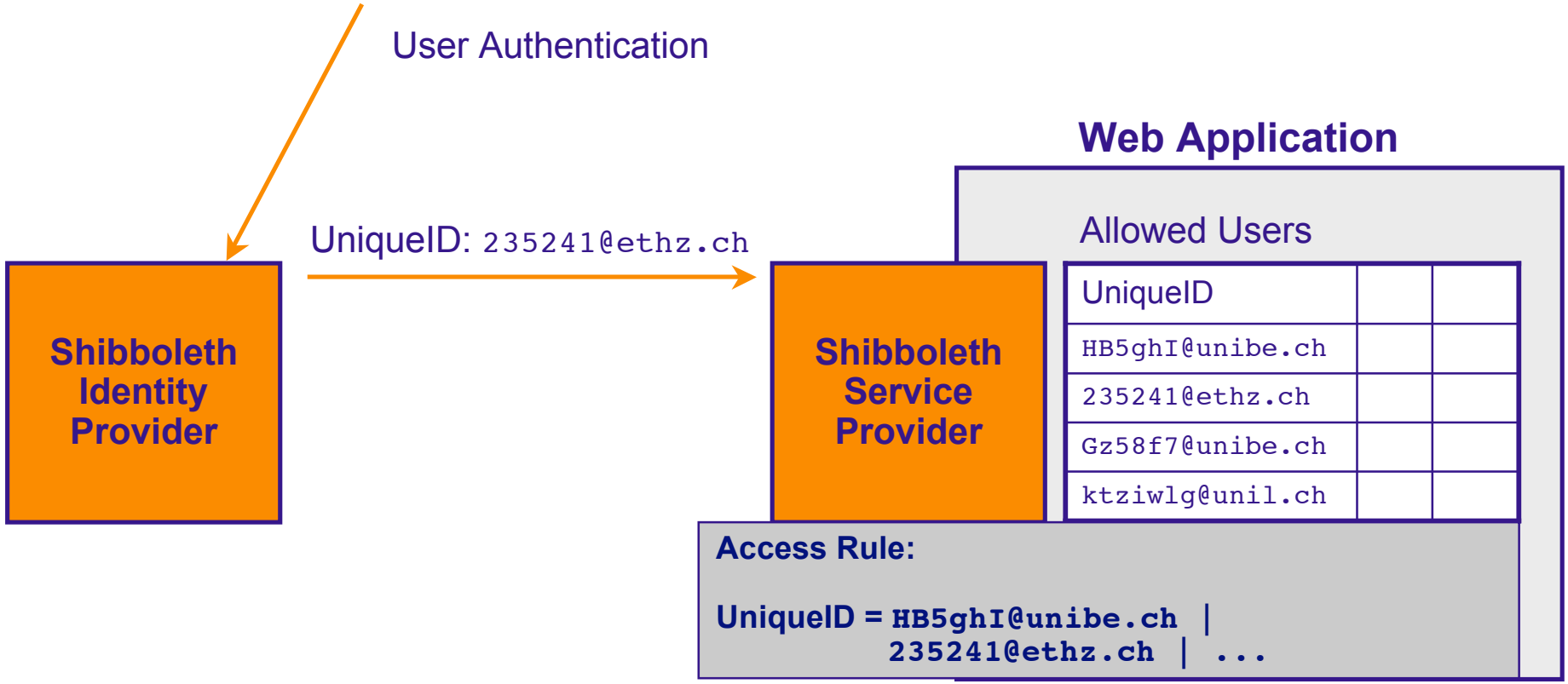


Authorization II: Entitlement

SWITCH
The Swiss Education & Research Network

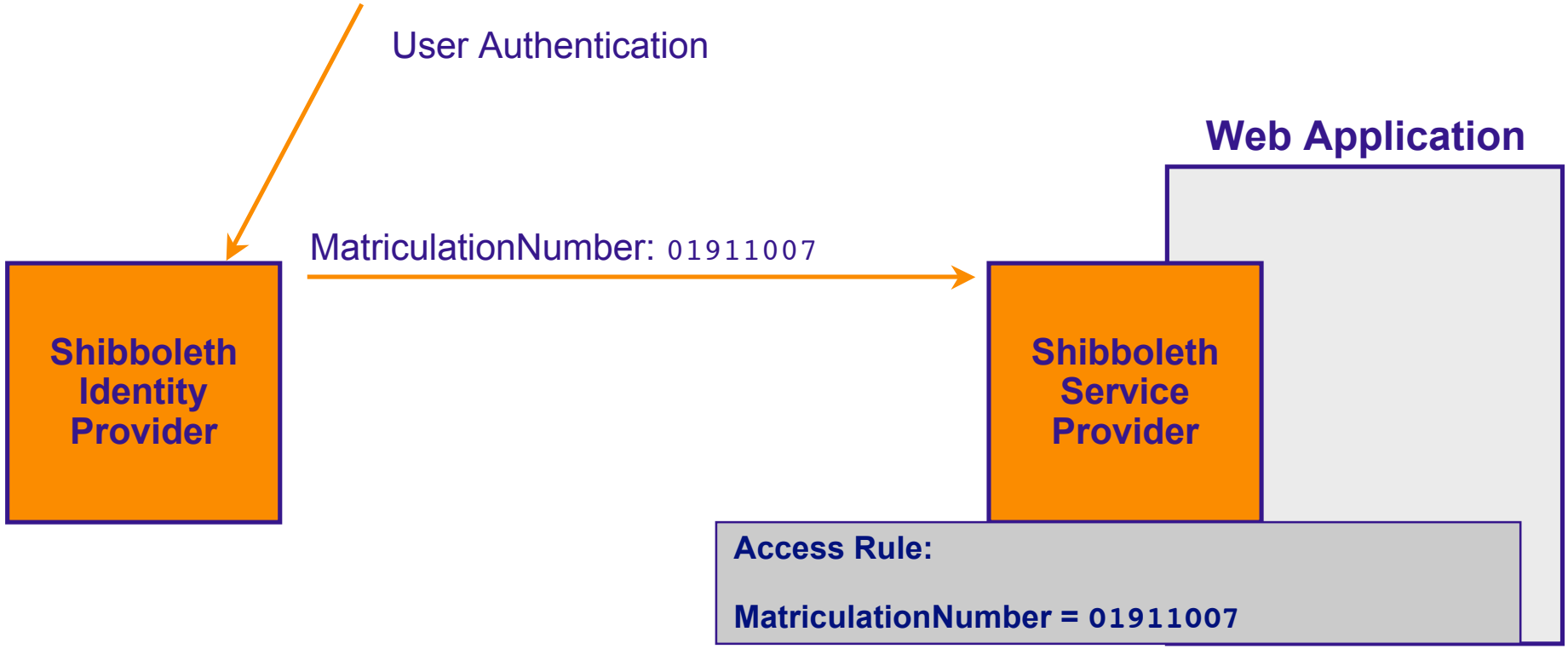


Authorization III: Individual User



Authentication IV: Additional Attributes

SWITCH
The Swiss Education & Research Network



SWITCH

The Swiss Education & Research Network

System Requirements

Patrik Schnellmann, schnellmann@switch.ch

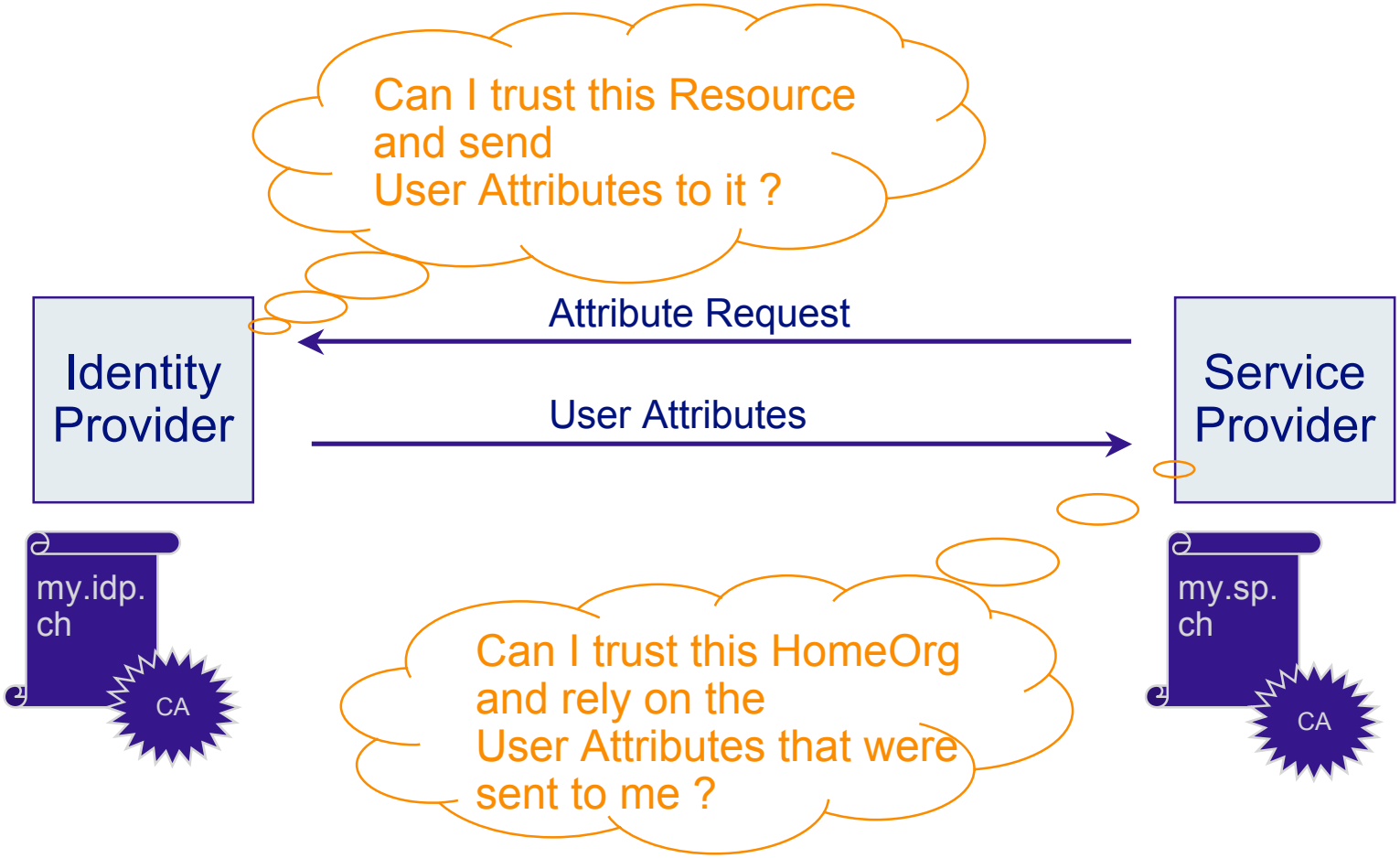
Requirements I - Web Browser

SWITCH
The Swiss Education & Research Network

- Cookies
- Browser redirect
- SSL
- JavaScript (if not available: additional click necessary)

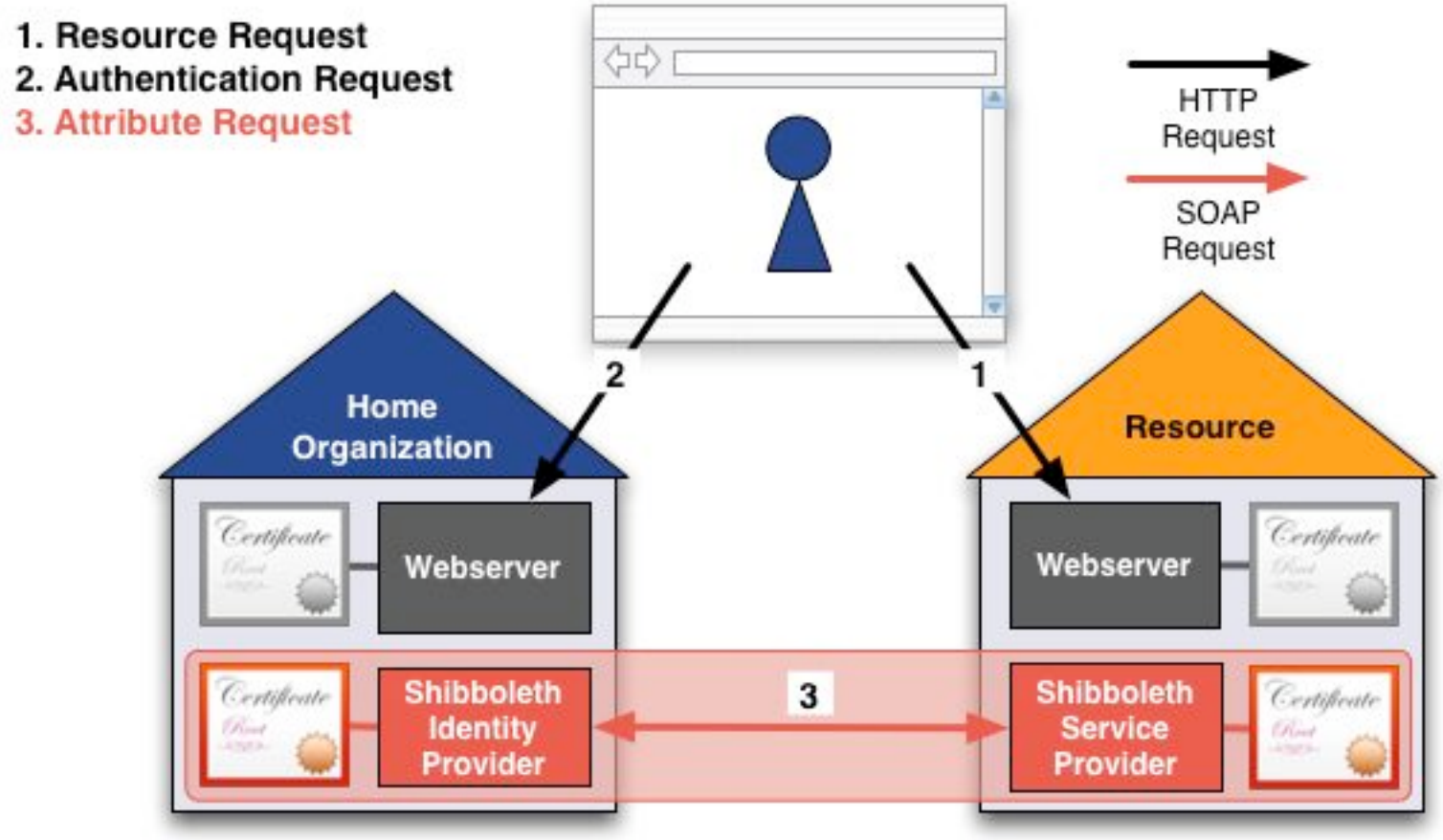
⇨ Basic features of any modern Web Browser

Requirements II - X.509 Certificates



⇨ Mutual authentication of Identity Provider and Service Provider

Requirements III - X.509 Certificates



⇨ Shibboleth and web server may use different X.509 certificates

Requirements IV - X.509 Certificates

SWITCH
The Swiss Education & Research Network

- Currently accepted Certificate Authorities (CAs) in SWITCHaai
  - SWITCHpki: SwissSign, SCS (Cybertrust Educational CA)
  - Thawte: Server CA, Server Premium CA
  - Verisign: Class 3 CA
  - TC TrustCenter: Class 2, Class 3
- Procedure defined to include additional CAs

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

SWITCH

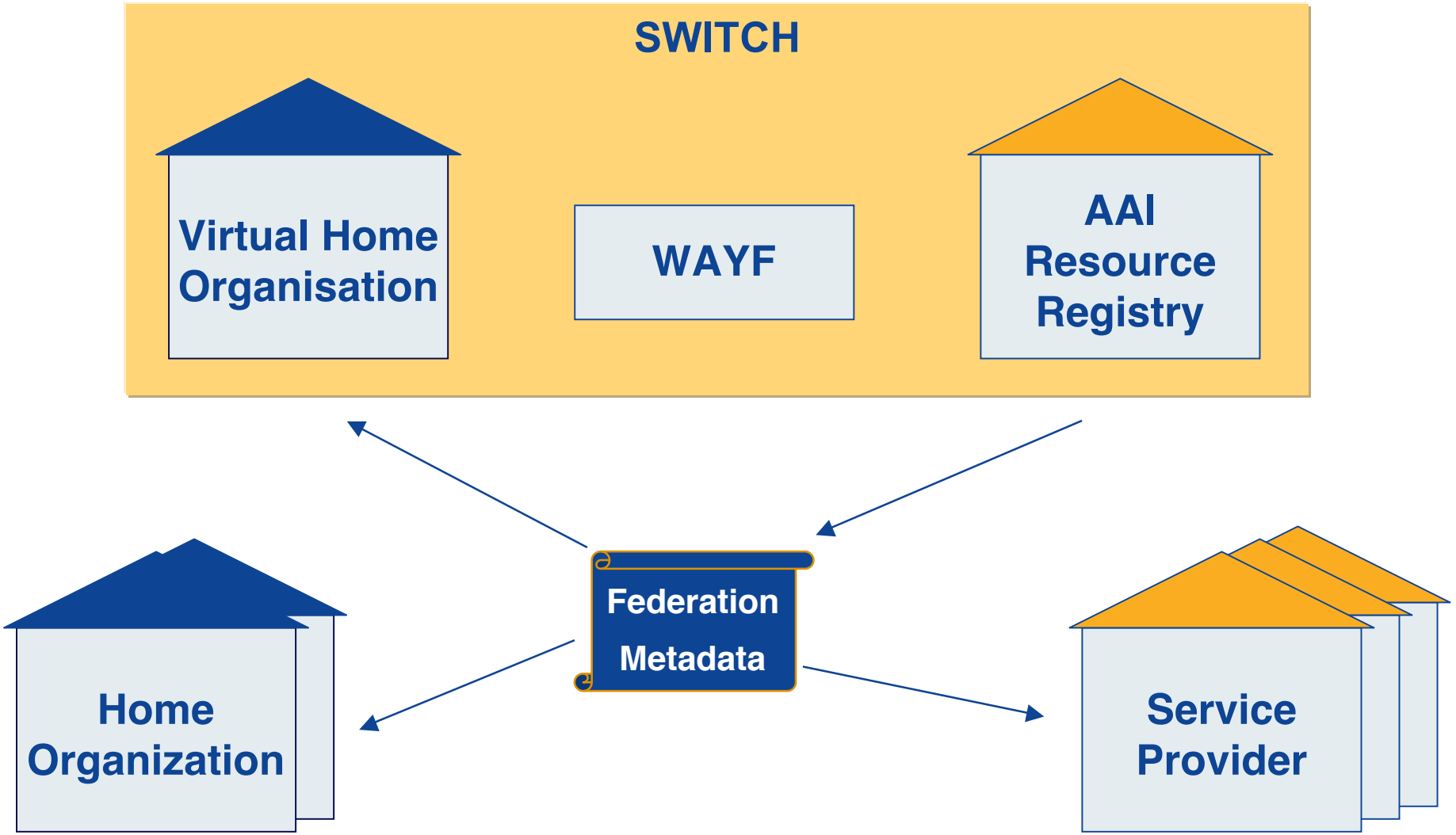
The Swiss Education & Research Network

SWITCHaai
Central Services

Lukas Hämmerle, haemmerle@switch.ch

SWITCHaai Central Services

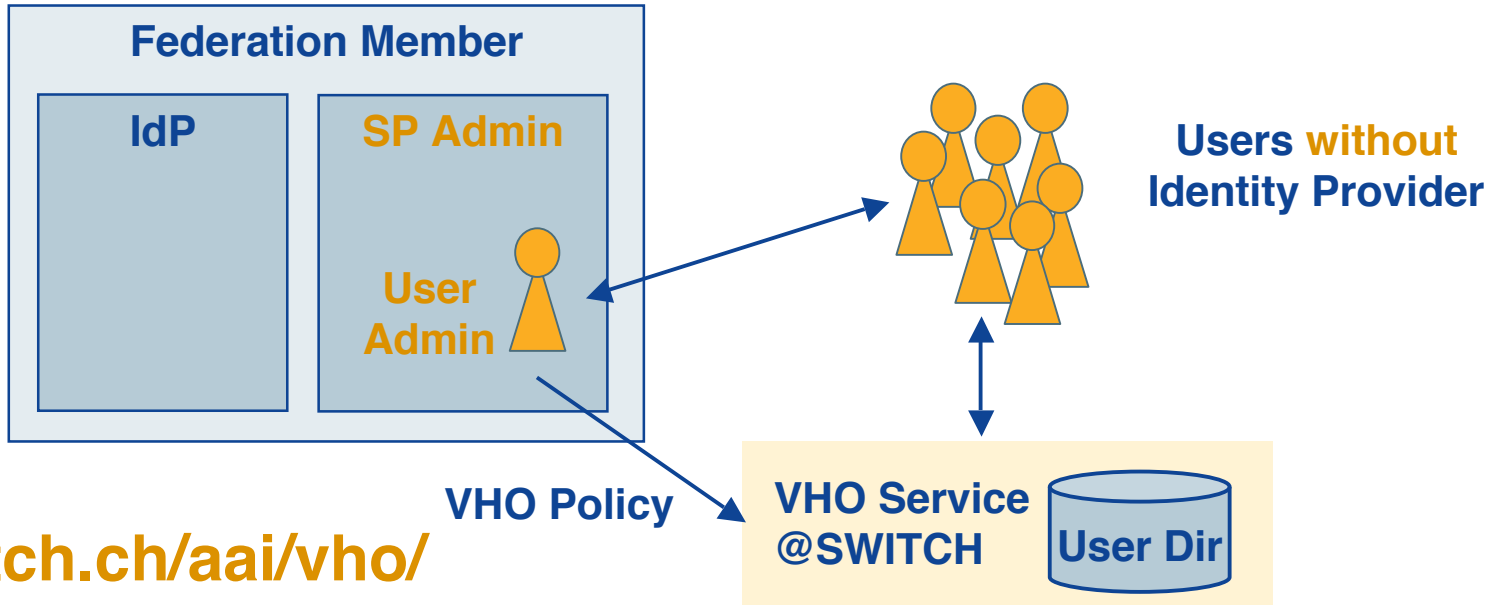
SWITCH
The Swiss Education & Research Network



Virtual Home Organization Service

SWITCH
The Swiss Education & Research Network

- SP can integrate users without an Identity Provider
- SP Admin accepts VHO policy & nominates User Admin
- User Admin allocates «AAI-enabled» accounts for users lacking an IdP
- *A VHO account is only of use for SPs under control of the SP admin. Third parties will not trust these identities.*



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

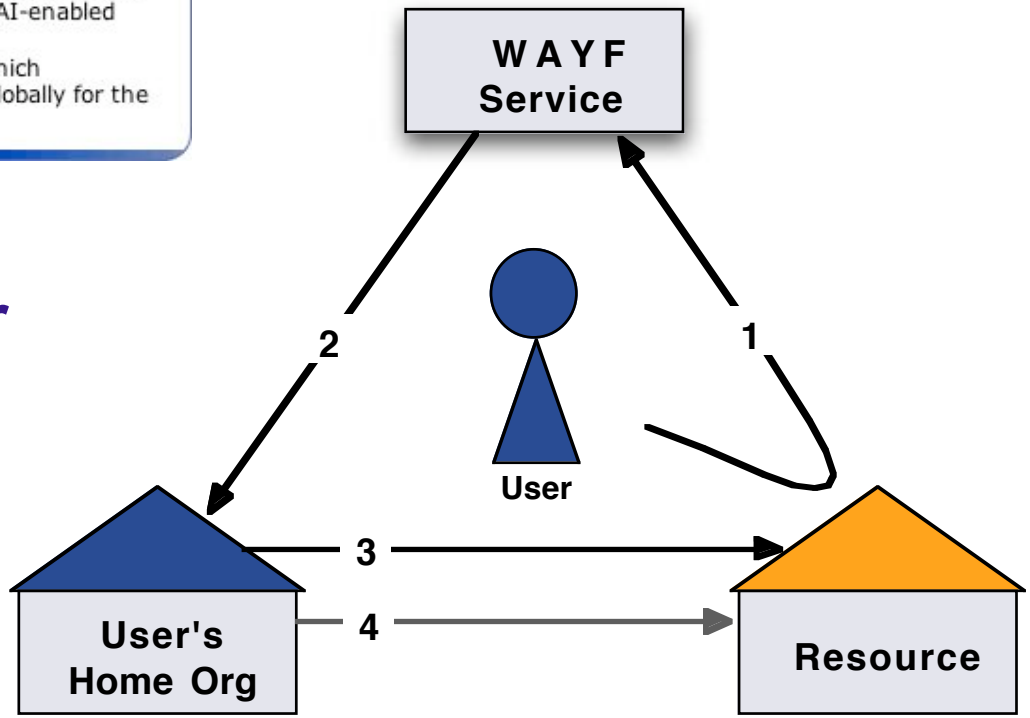
IdP Discovery Service (WAYF)

SWITCH
The Swiss Education & Research Network

Facts about WAYF:

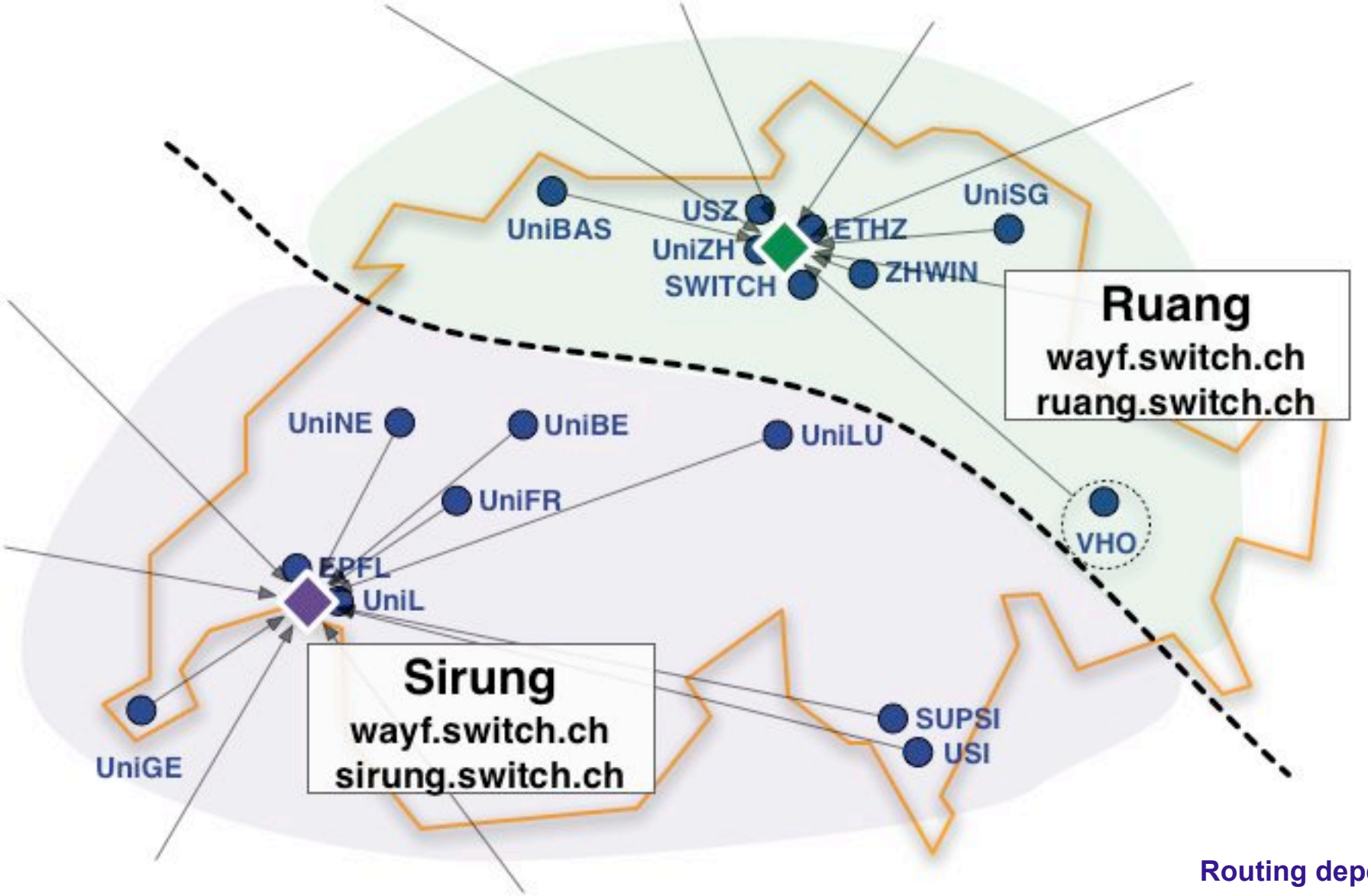
- Stateless requests
- Two requests per visit
  1. (Show drop-down list)
  2. Redirect User to IdP

⇨ **The WAYF guides the user to his Identity Provider**



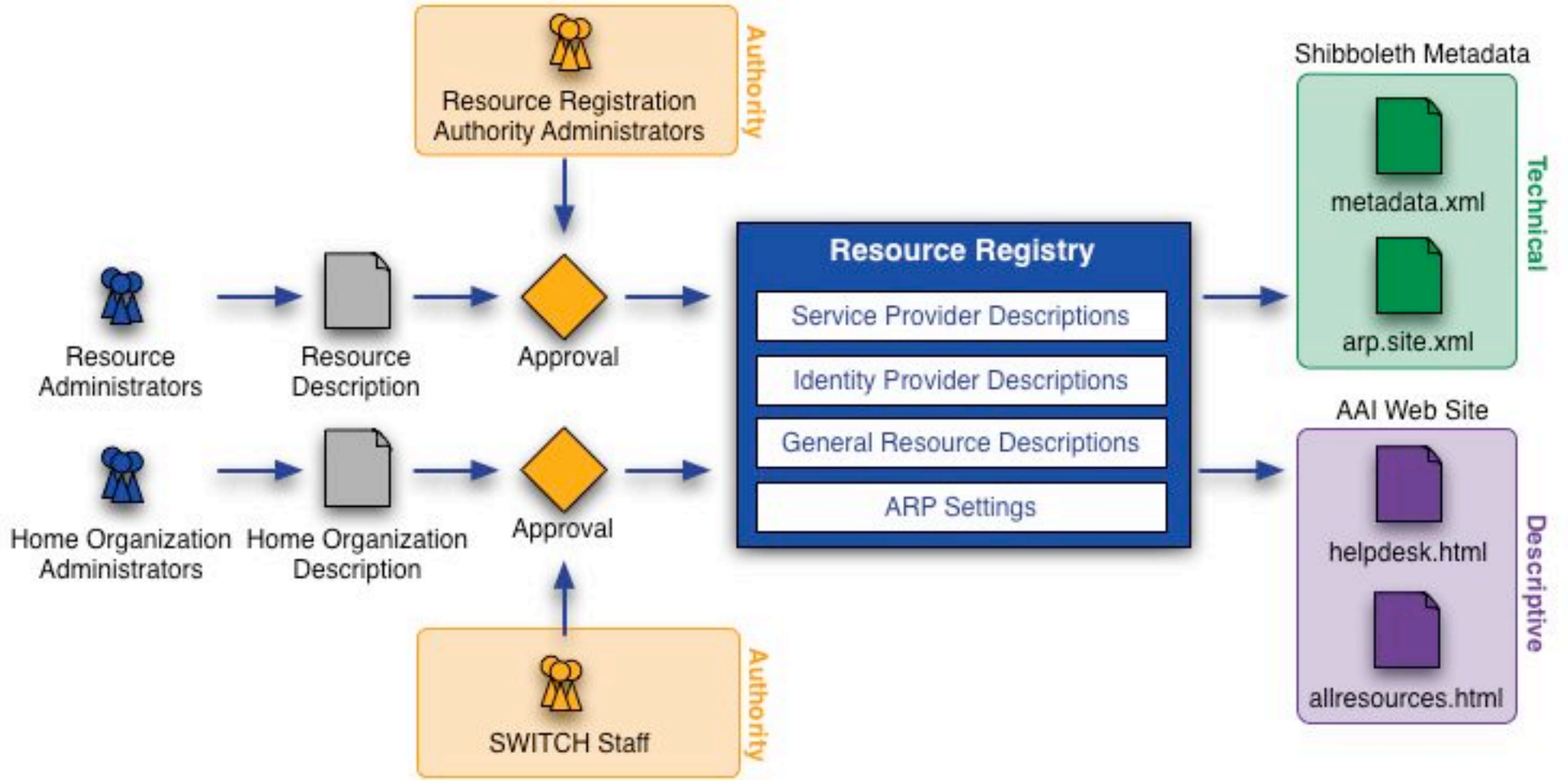
SWITCH Federation WAYF Service

SWITCH
The Swiss Education & Research Network



Routing dependent

Resource Registry Processes



Before an SP/IdP description becomes part of federation metadata, it must be approved by an authority first

The SP and the Resource Registry

SWITCH
The Swiss Education & Research Network

- Make use of the its features

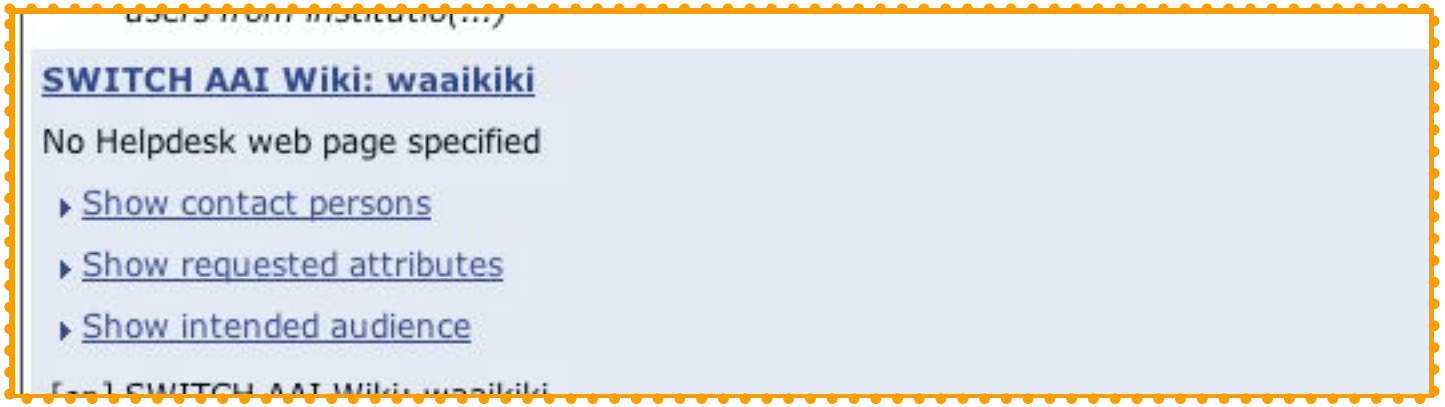
- Provide descriptions in multiple languages
- Attribute Requirements
  - Which attributes does your application really need?
  - Which attributes are just desired?
  - Explain why, use the description
- Intended Audience
  - For which IdPs is your SP relevant?

https://aai-rr.switch.ch

Output of Resource Registry

SWITCH
The Swiss Education & Research Network

- **Metadata**, see **http://www.switch.ch/aai/metadata/**
- **Configuration files** for IdPs (ARP) and SPs (shibboleth.xml, …)
- **Helpdesk webpage** shows helpdesk contacts for your SP



- **Public Resource list**, see **http://www.switch.ch/aai/participants/**