



SWITCH

The Swiss Education & Research Network

AAI Attributes, Authorization, System Requirements Resource Registry

The AAI Team <aai@switch.ch>



SWITCH

The Swiss Education & Research Network

Authorization Attributes

Patrik Schnellmann <schnellmann@switch.ch>

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

Attribute	Value
UniqueID	773443@aitest.switch.ch
Given Name	Demouser
Surname	SWITCHaai
Affiliation	staff
Entitlement	http://unil.ch/aai/resources/biblio92 http://ethz.ch/res/12345
Home Organization	aitest.switch.ch
Home Organization Type	others



SWITCH

The Swiss Education & Research Network

Authorization

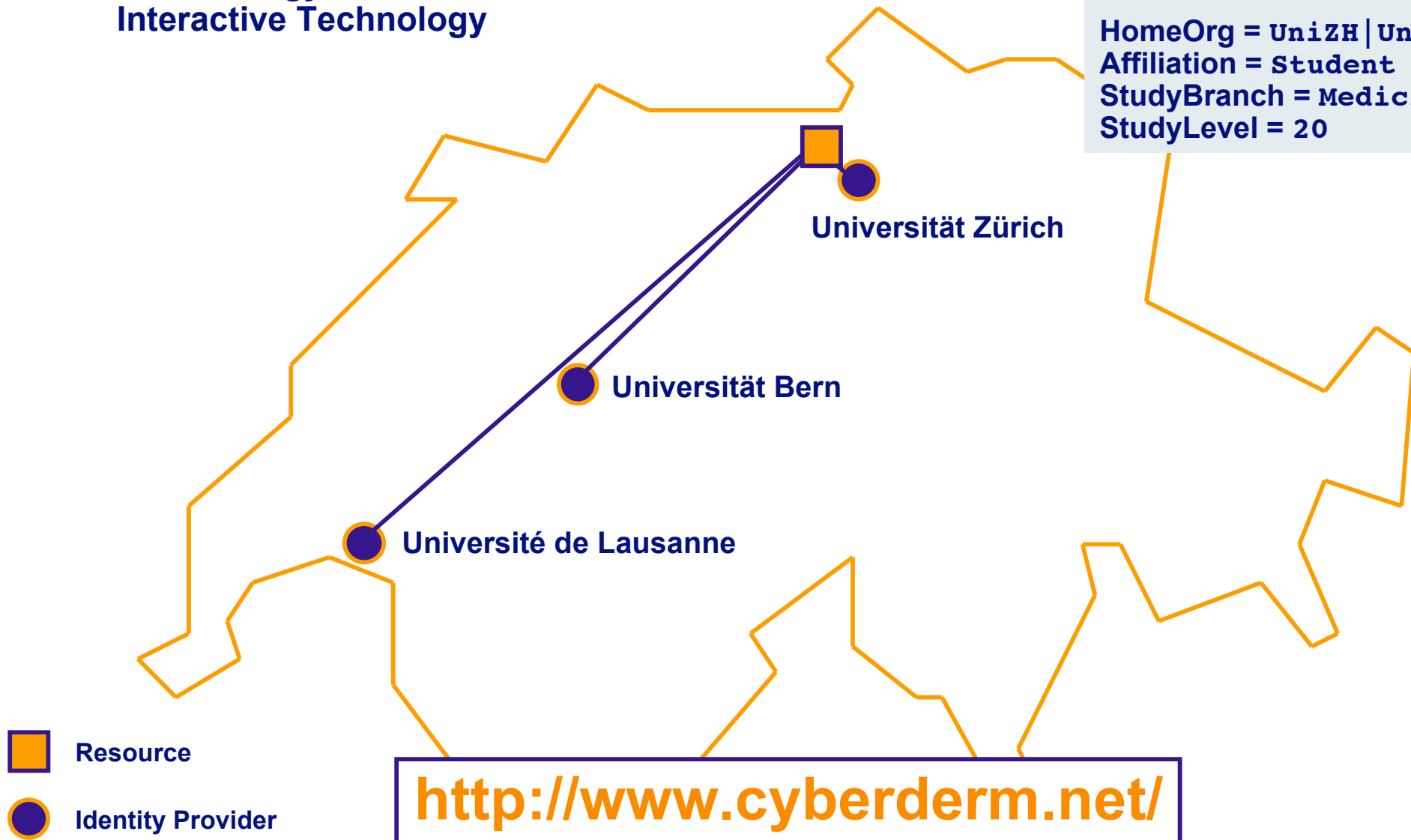
Patrik Schnellmann <schnellmann@switch.ch>

Access Rules using AAI Attributes

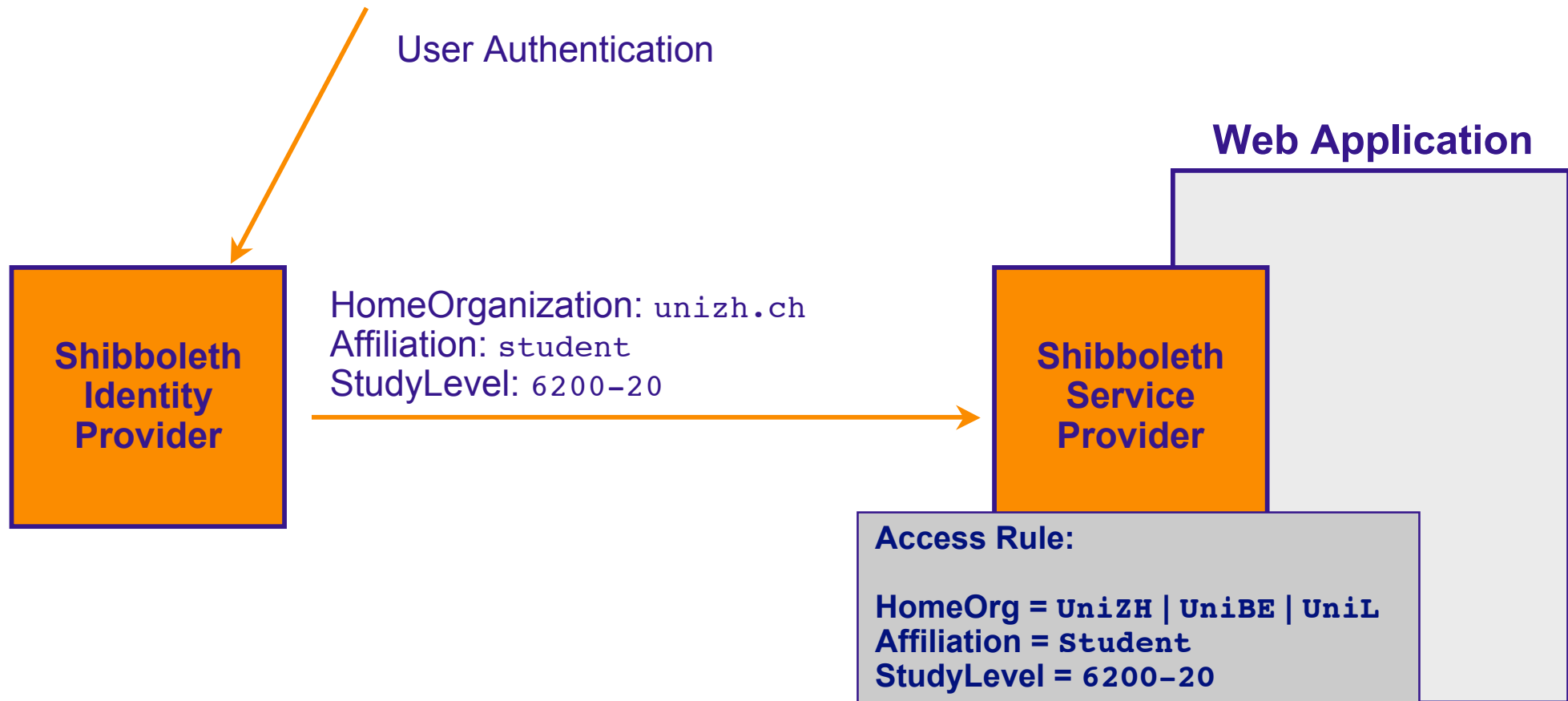
DOIT: Dermatology Online with Interactive Technology

Access Rule

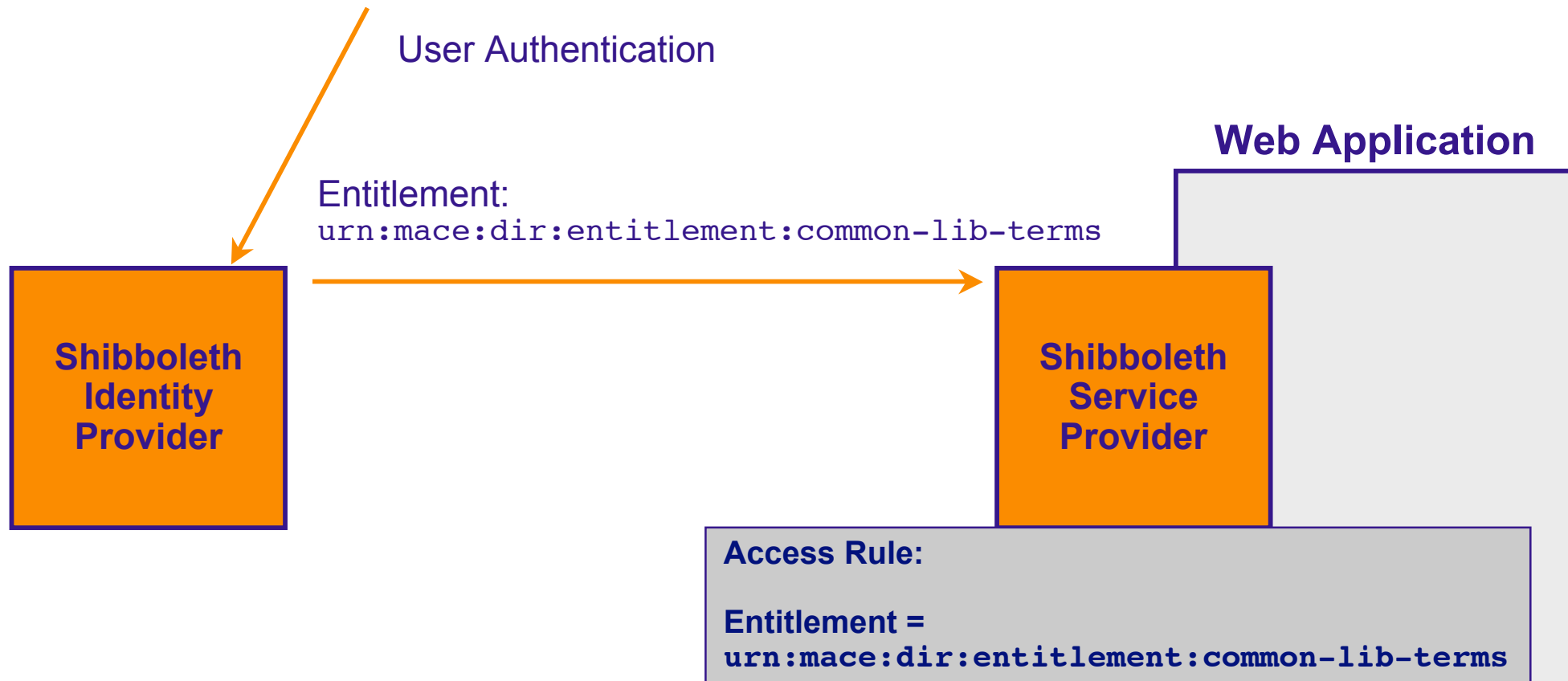
HomeOrg = UniZH | UniBE | UniL
Affiliation = Student
StudyBranch = Medicine
StudyLevel = 20



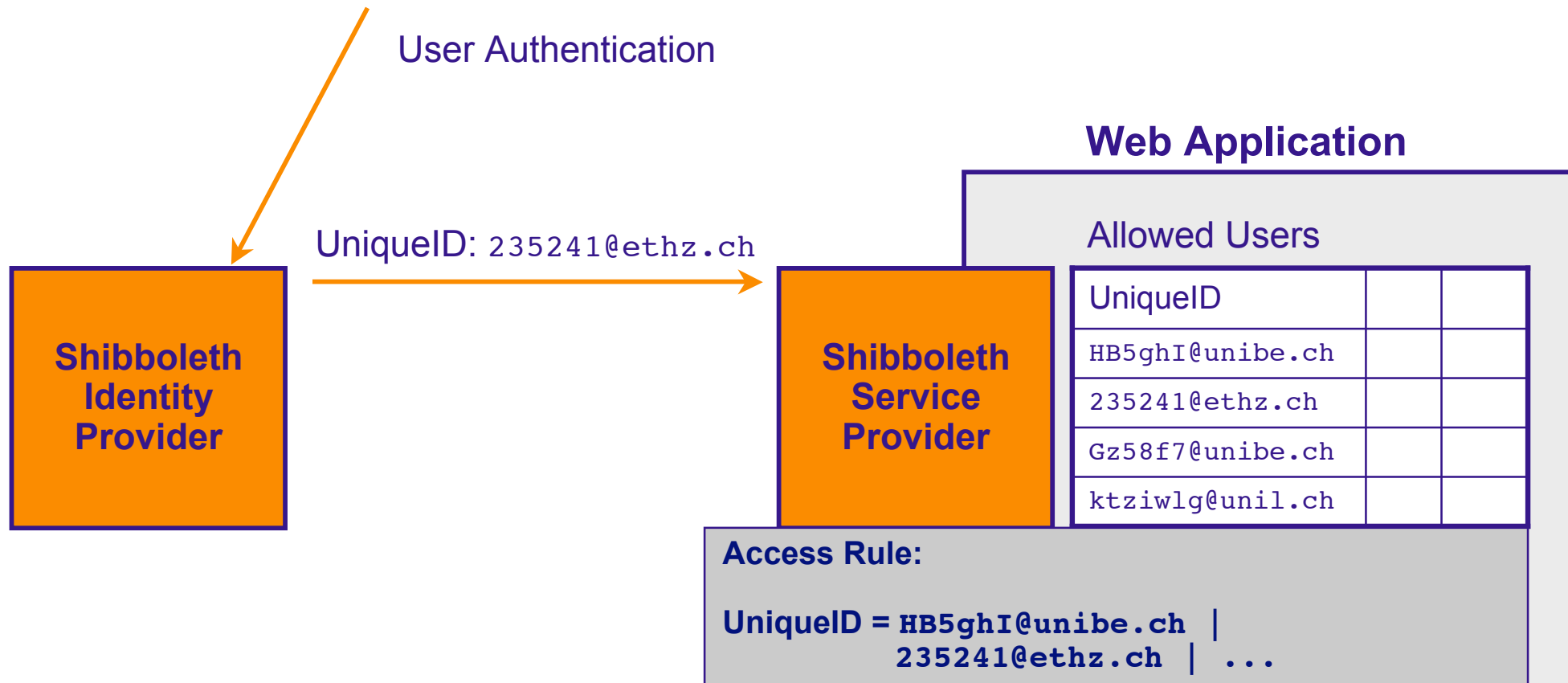
Authorization I: Group membership



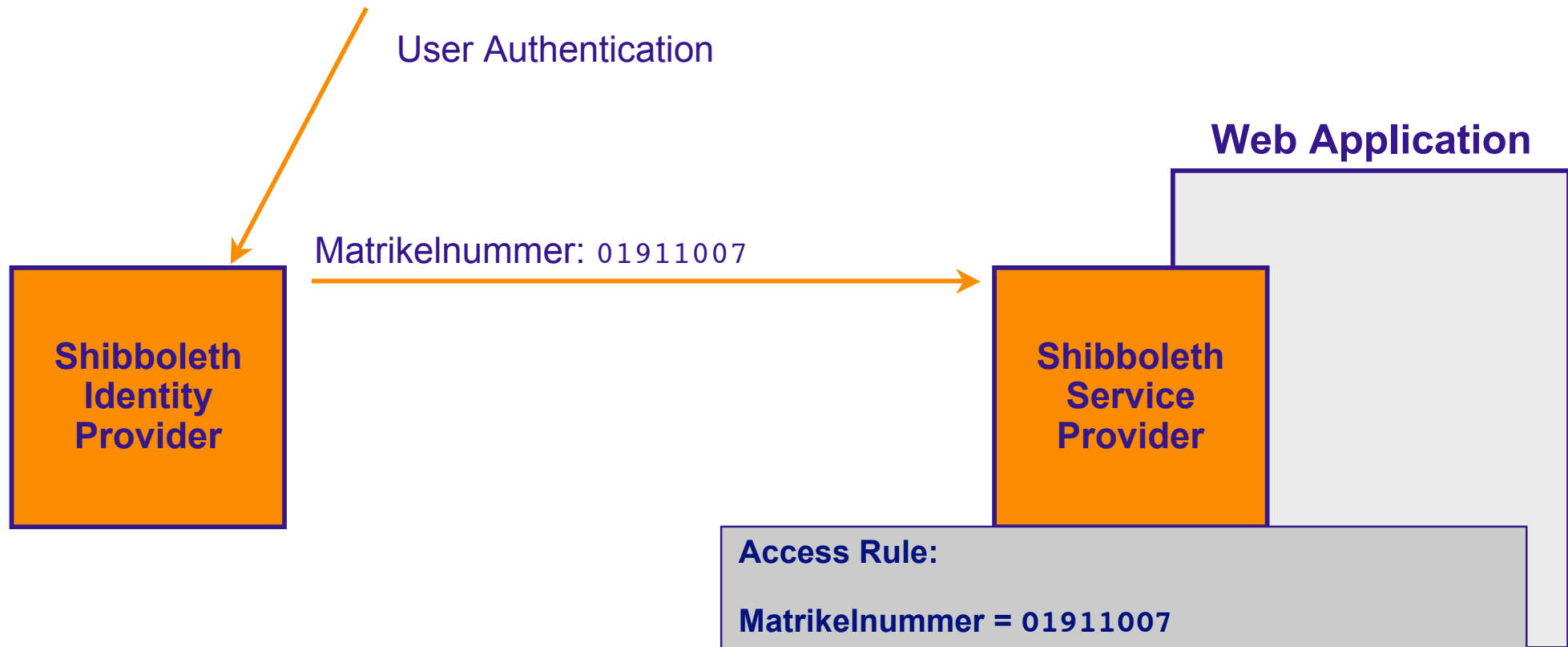
Authorization II: Entitlement



Authorization II: Individual User



Authentication IV: Additional Attributes





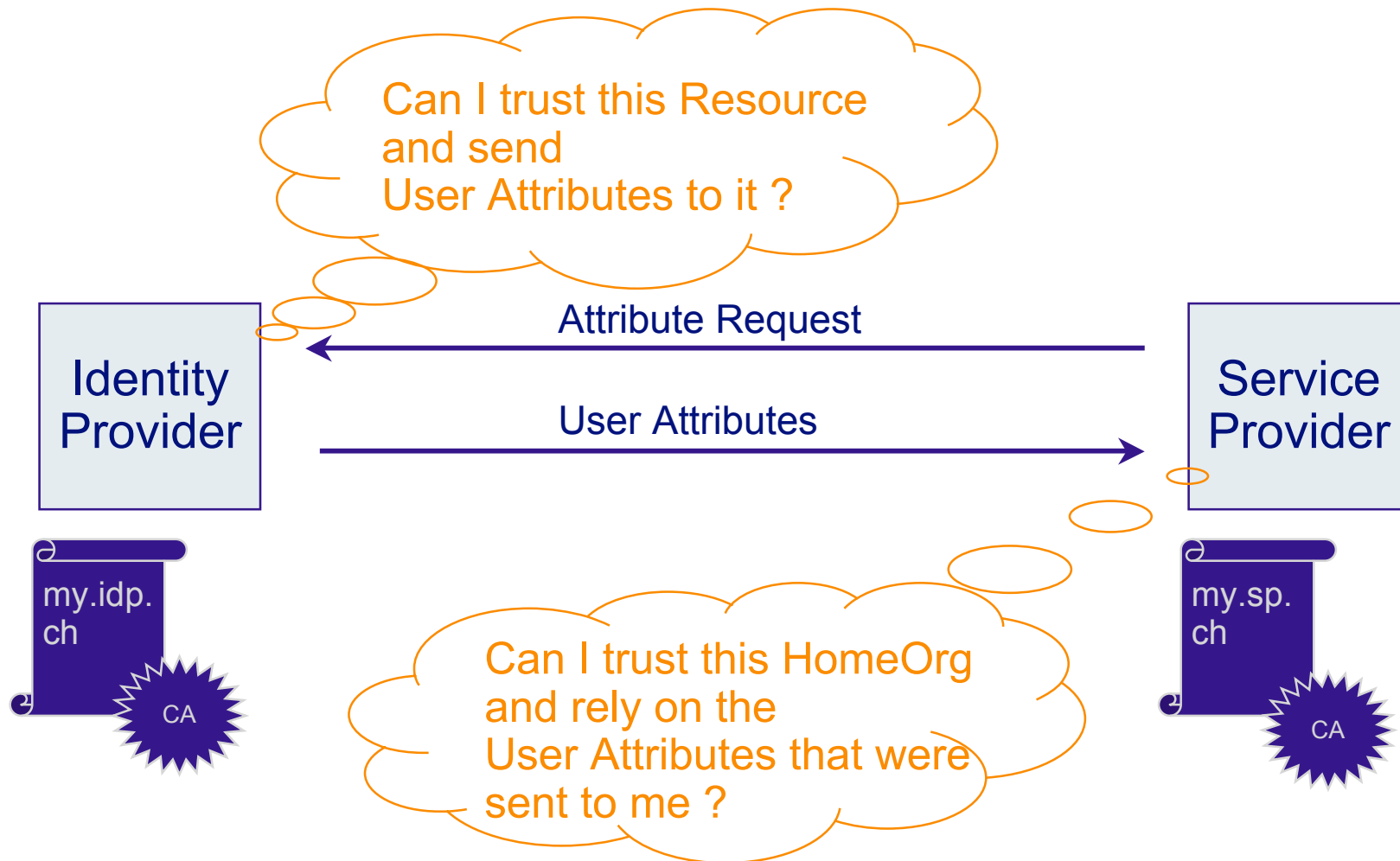
SWITCH

The Swiss Education & Research Network

System Requirements

Patrik Schnellmann <schnellmann@switch.ch>

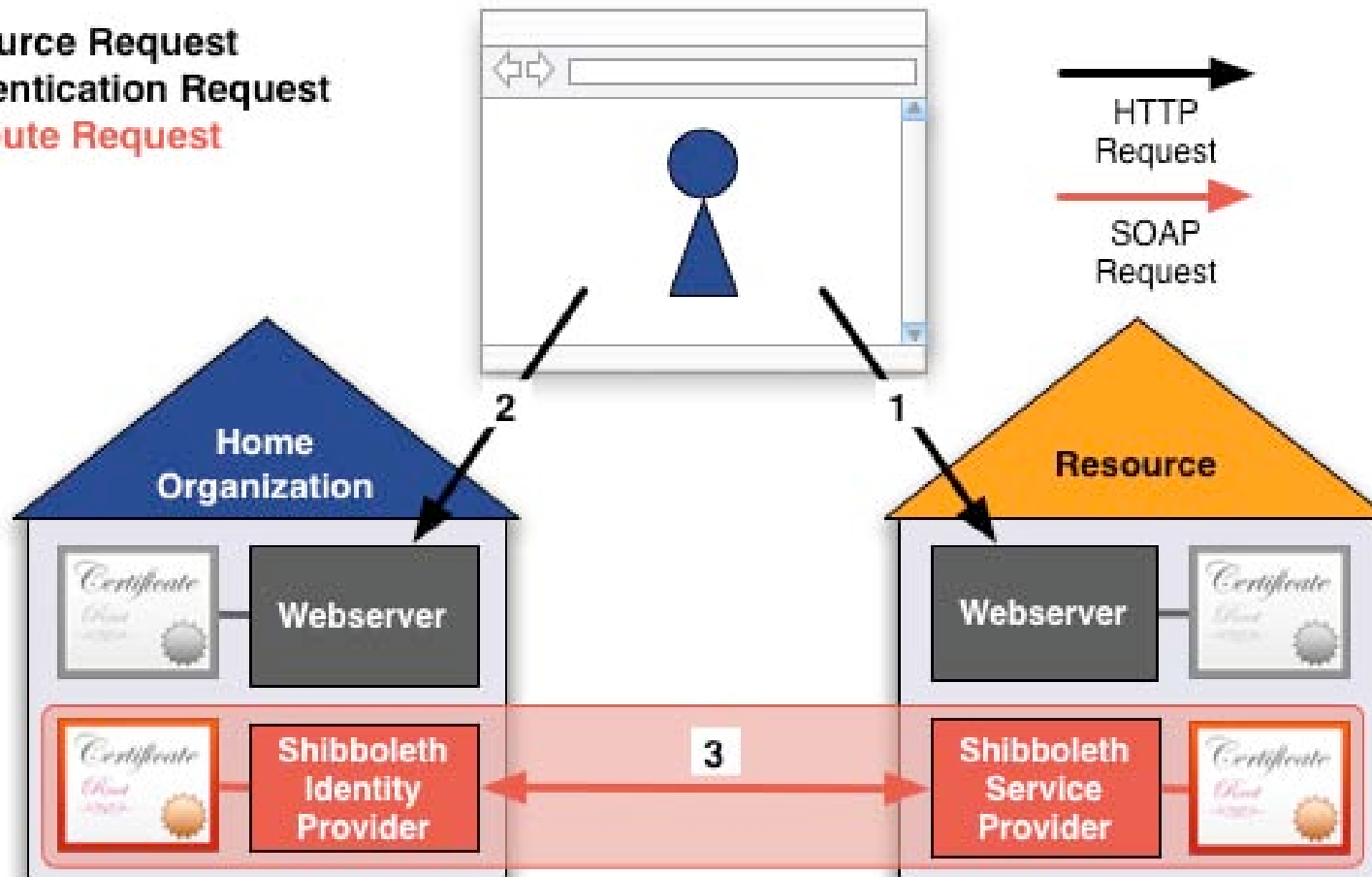
- ❑ Cookies
 - ❑ Browser redirect
 - ❑ SSL
 - ❑ JavaScript (if not available: additional click necessary)
- ⇒ Basic features of any modern Web Browser



⇒ Mutual authentication of Identity Provider and Service Provider

Requirements III - X.509 Certificates

1. Resource Request
2. Authentication Request
3. Attribute Request



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

- ❑ 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/>



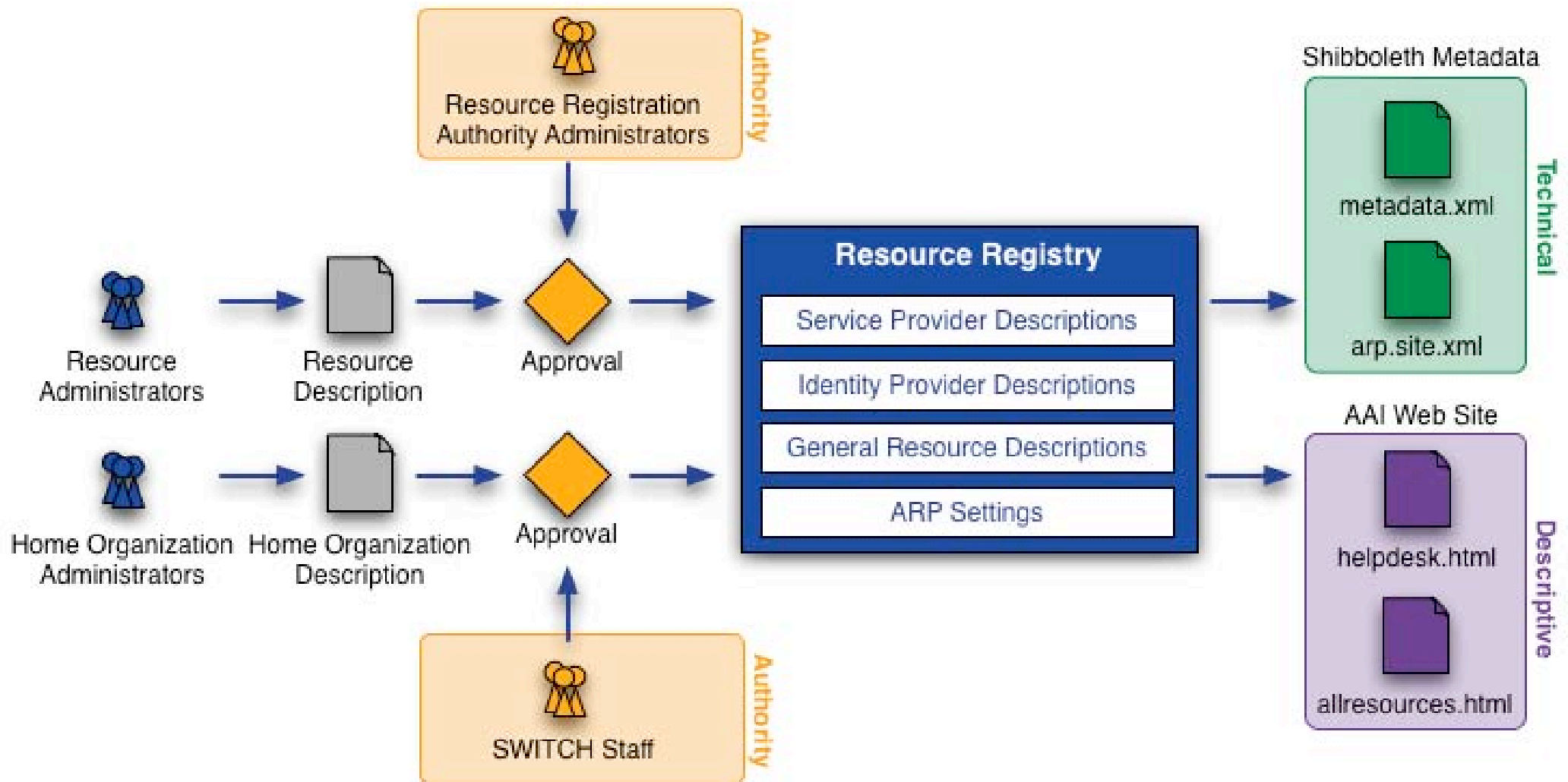
SWITCH

The Swiss Education & Research Network

Resource Registry

Lukas Hämmerle, haemmerle@switch.ch

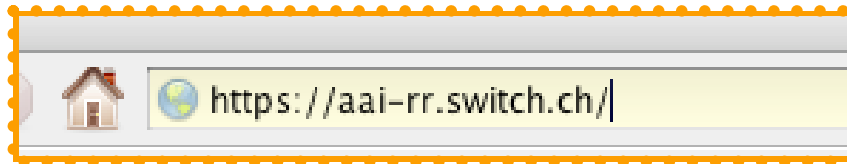
Resource Registry Processes



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

To activate your Service Provider, register your Resource:

① Access the Resource Registry



② Add a new Resource Description





3 Complete the forms

a.)

Edit the Basic Information for new Resource

Basic Resource Information	
Home Organization *	switch.ch (SWITCHaai) <input type="text"/>
	<small>You only can register Resources for Home Organizations which you have Resource Registration Authority administrator for or for Home Organization</small>
Main language	English <input type="text"/>
Main Descriptive Name *	Test Resource
	<small>A name that briefly describes this resource, e.g. "e-Learning Moodle"</small>
Main Description *	This is a test resource <input type="text"/>

b.)

 Basic Resource Information	OK
 Multilingual Descriptions	Incomplete

4 Submit resource description for approval

resource Description after the submission but only until the changes are



Submit this Resource Description for Approval

that is appended to the e-Mail which is sent to the Resource Registrar

5 Resource Registration Authority administrator (RRA) checks and approves resource description

AAI: Your resource creation request was approved



6 Description becomes part of the federation metadata and propagates to IdPs within max 24 hours.

```
<!-- local test resource -->
```

```
<EntityDescriptor entityID="https://macps.switch.ch/shibboleth">
```

```
<SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc
```

```
<KeyDescriptor use="signing">
```

```
<ds:KeyInfo>
```

Output of Resource Registry

- **metadata.xml**, see <http://www.switch.ch/aai/metadata>
- **arp.site.xml** for Identity Providers
- **Helpdesk webpage** shows helpdesk contacts for your SP



users from institution(m)

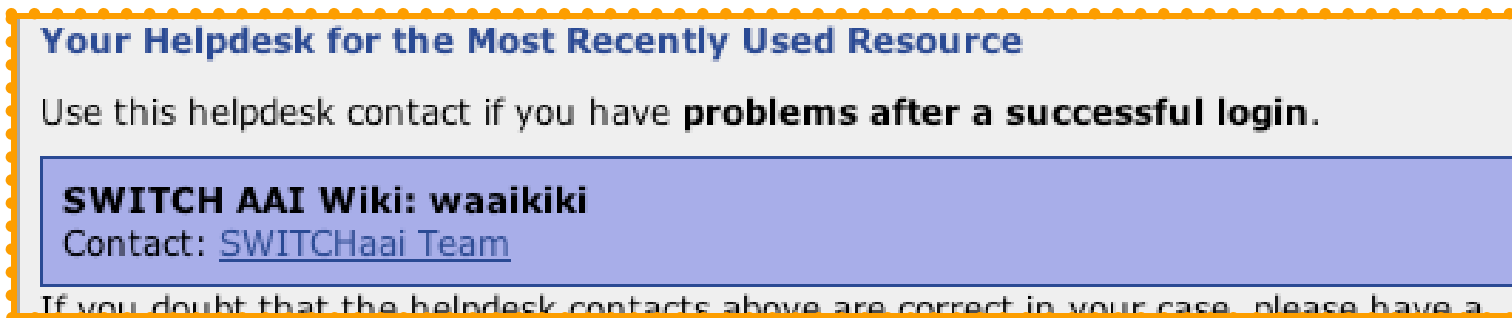
SWITCH AAI Wiki: waaikiki

No Helpdesk web page specified

- ▶ [Show contact persons](#)
- ▶ [Show requested attributes](#)
- ▶ [Show intended audience](#)

See 1 SWITCH AAI Wiki: waaikiki

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



Your Helpdesk for the Most Recently Used Resource

Use this helpdesk contact if you have **problems after a successful login**.

SWITCH AAI Wiki: waaikiki
Contact: [SWITCHaai Team](#)

If you doubt that the helpdesk contacts above are correct in your case, please have a