SWITCH

The Swiss Education & Research Network

AAI Attributes, Authoriziation, System Requirements Resource Registry

The AAI Team <aai@switch.ch>

SWITCH

The Swiss Education & Research Network

Authorization Attributes

Patrik Schnellmann <schnellmann@switch.ch>

Authorization 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
Given Name	Demouser
Surname	SWITCHaai
Affiliation	staff
Entitlement	http://unil.ch/aai/resources/biblio92 http://ethz.ch/res/12345
Home Organization	aaitest.switch.ch
Home Organization Type	others

SWITCH

The Swiss Education & Research Network

Authorization

Patrik Schnellmann <schnellmann@switch.ch>

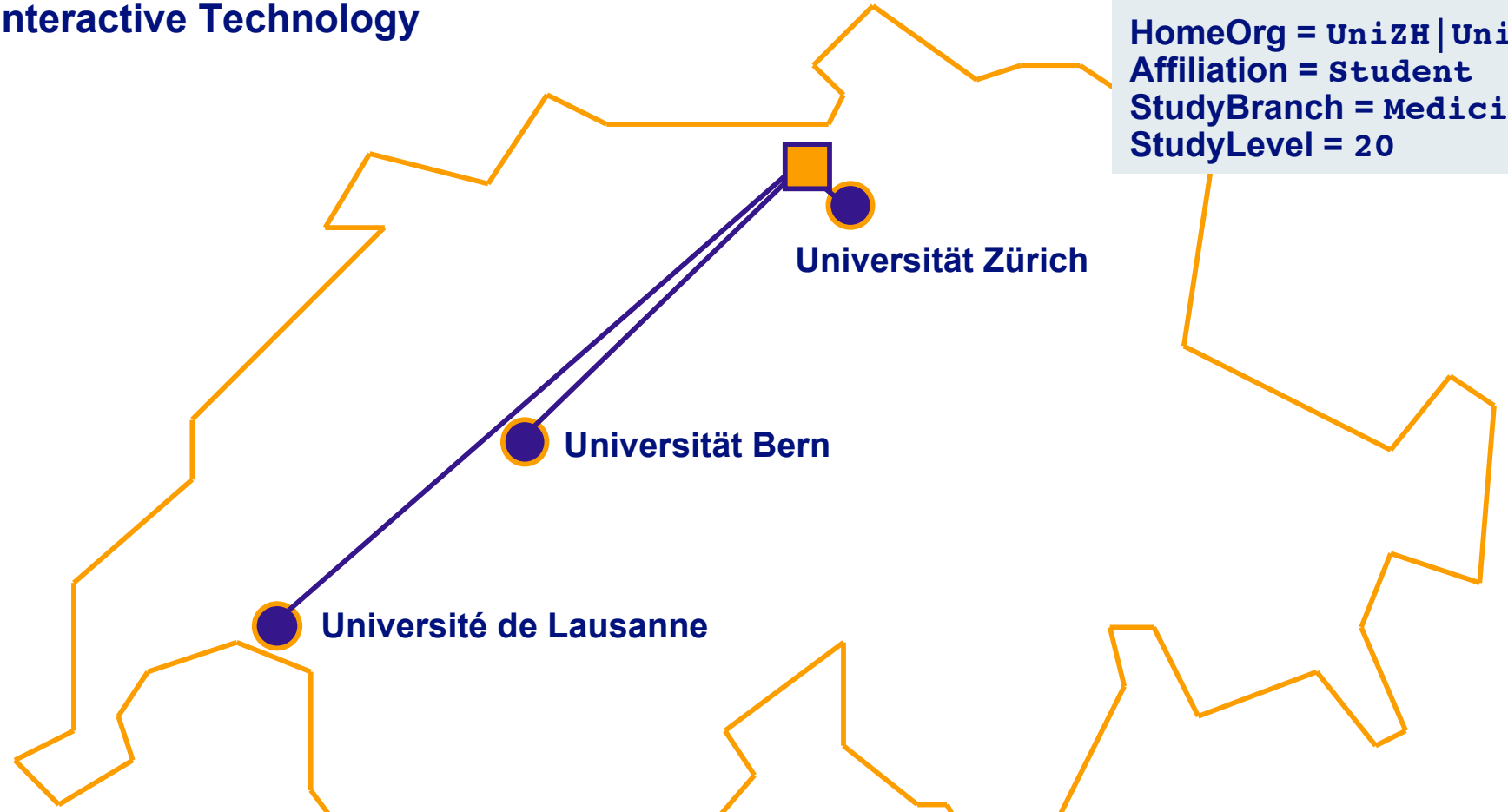
Access Rules using AAI Attributes

SWITCH
The Swiss Education & Research Network

DOIT: Dermatology Online with Interactive Technology

Access Rule

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

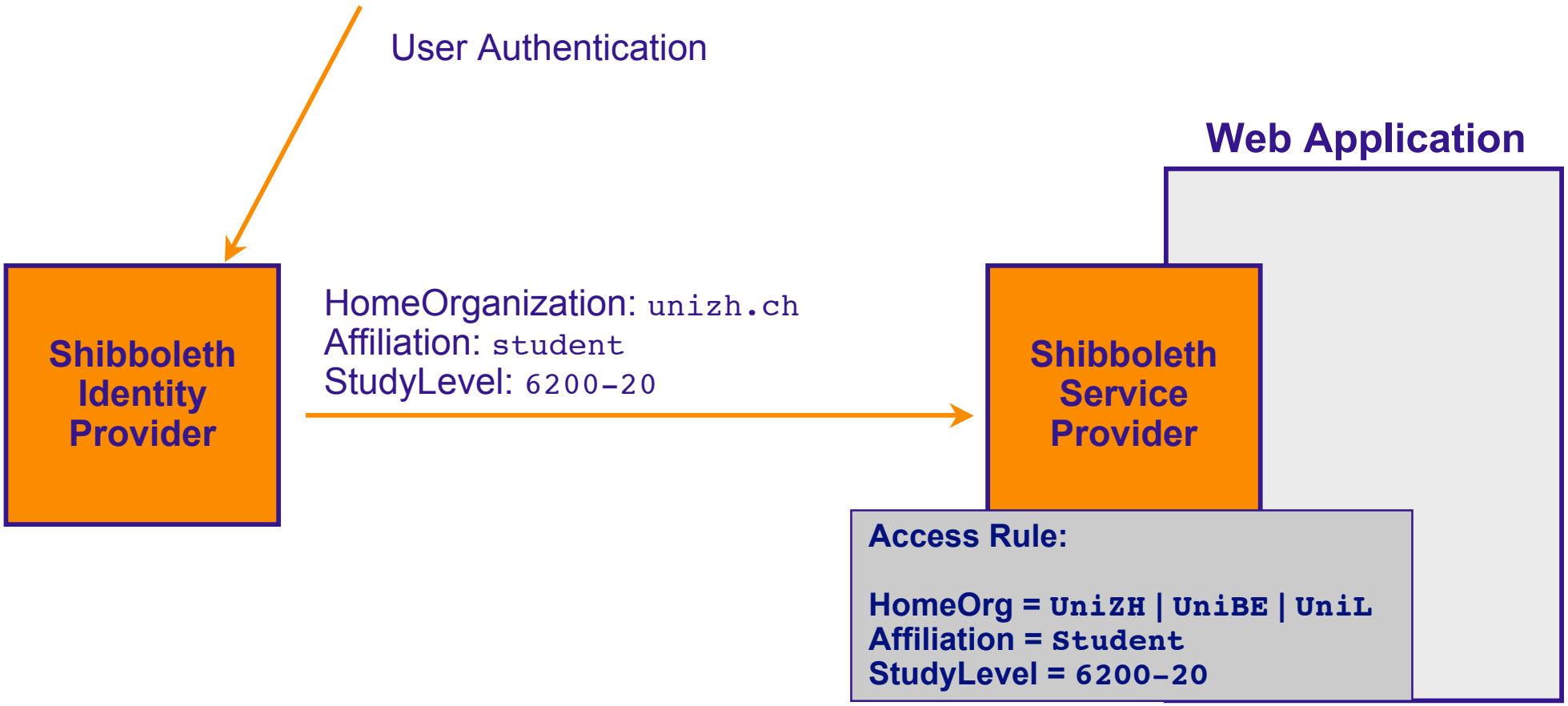


Resource

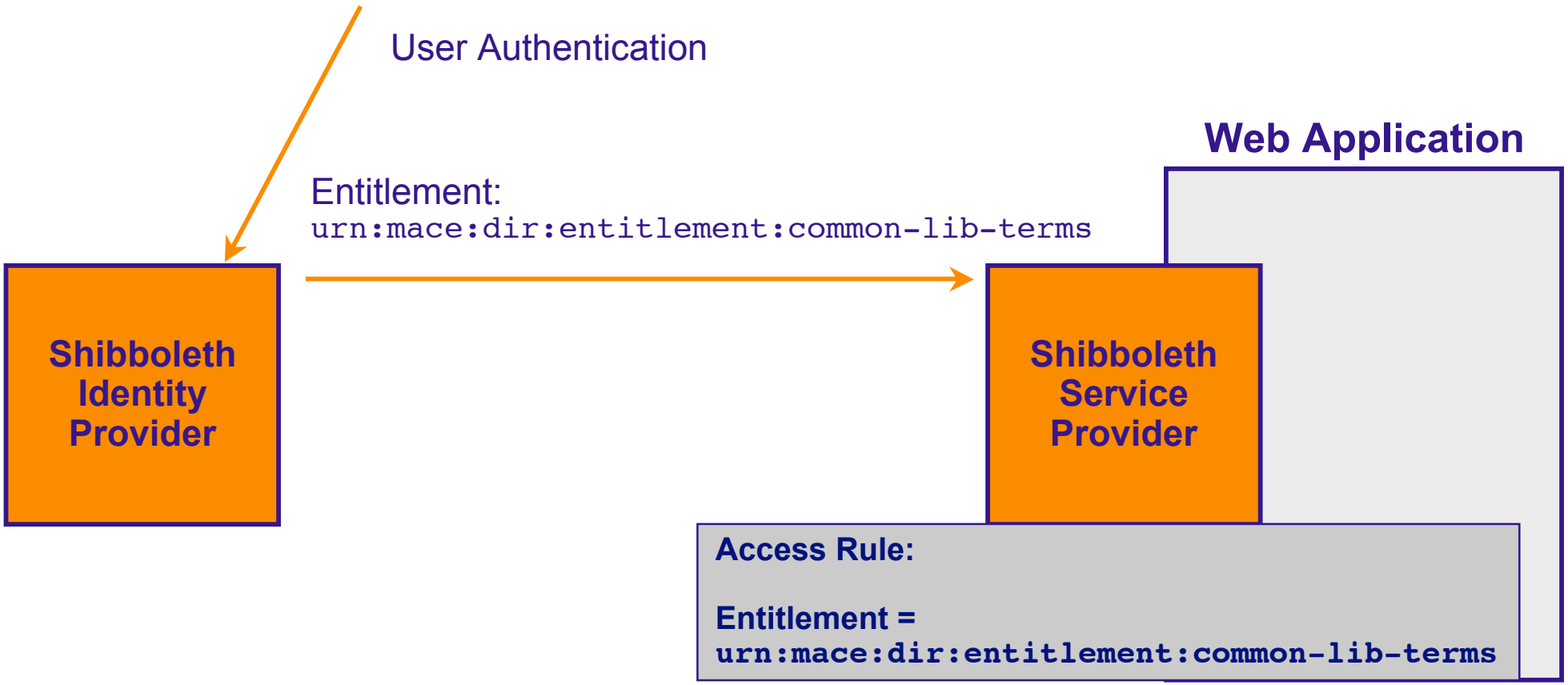
Identity Provider

http://www.cyberderm.net/

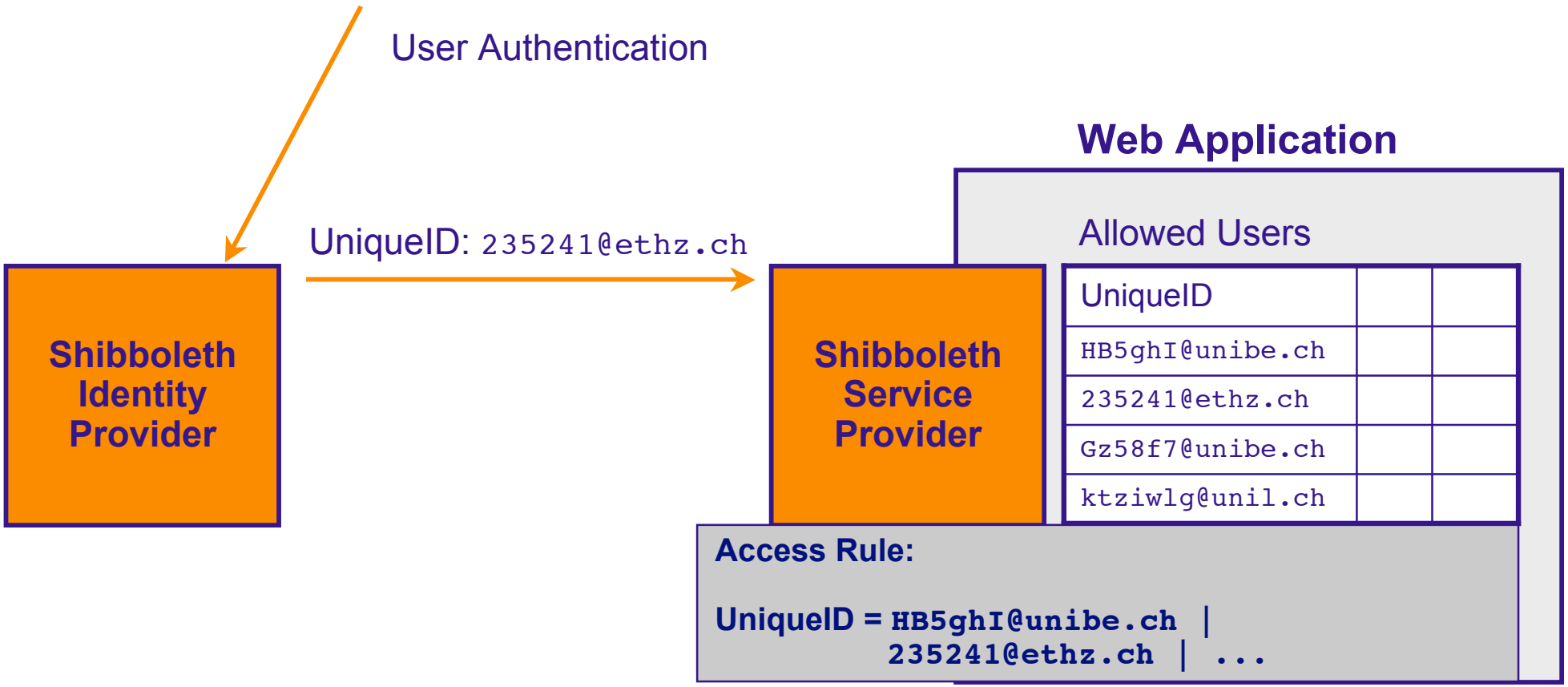
Authorization I: Group membership



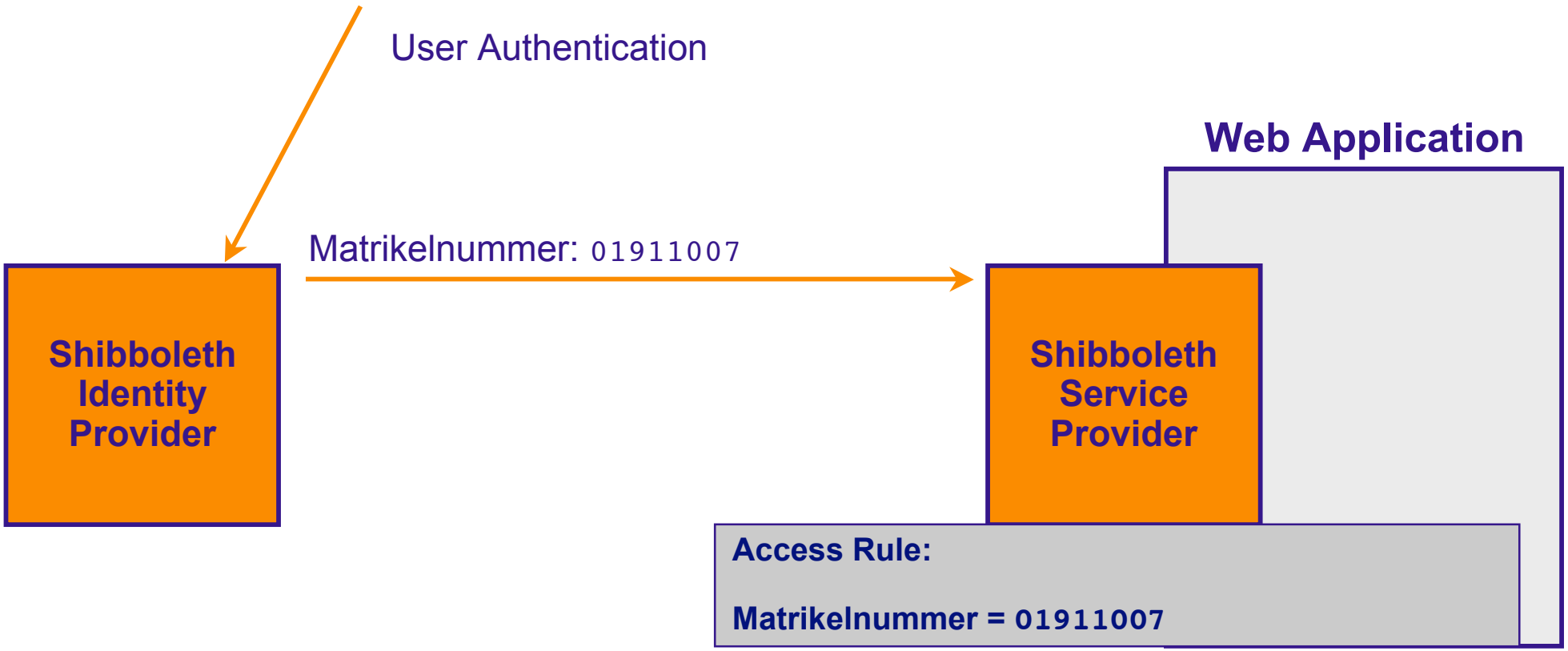
Authorization II: Entitlement



Authorization III: Individual User



Authentication IV: Additional Attributes



SWITCH

The Swiss Education & Research Network

System Requirements

Patrik Schnellmann <schnellmann@switch.ch>

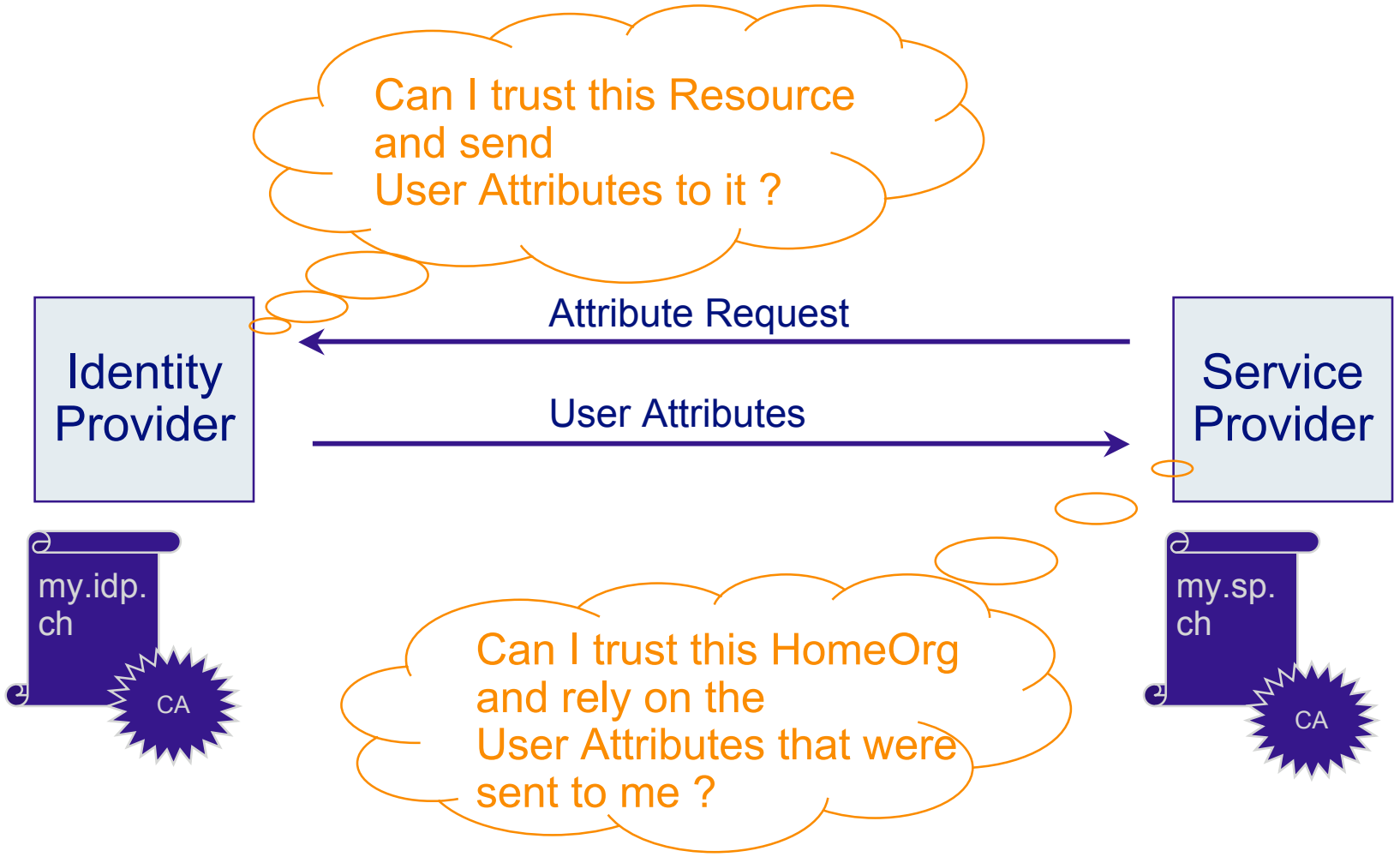
Requirements I - Web Browser

SWITCH
The Swiss Education & Research Network

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

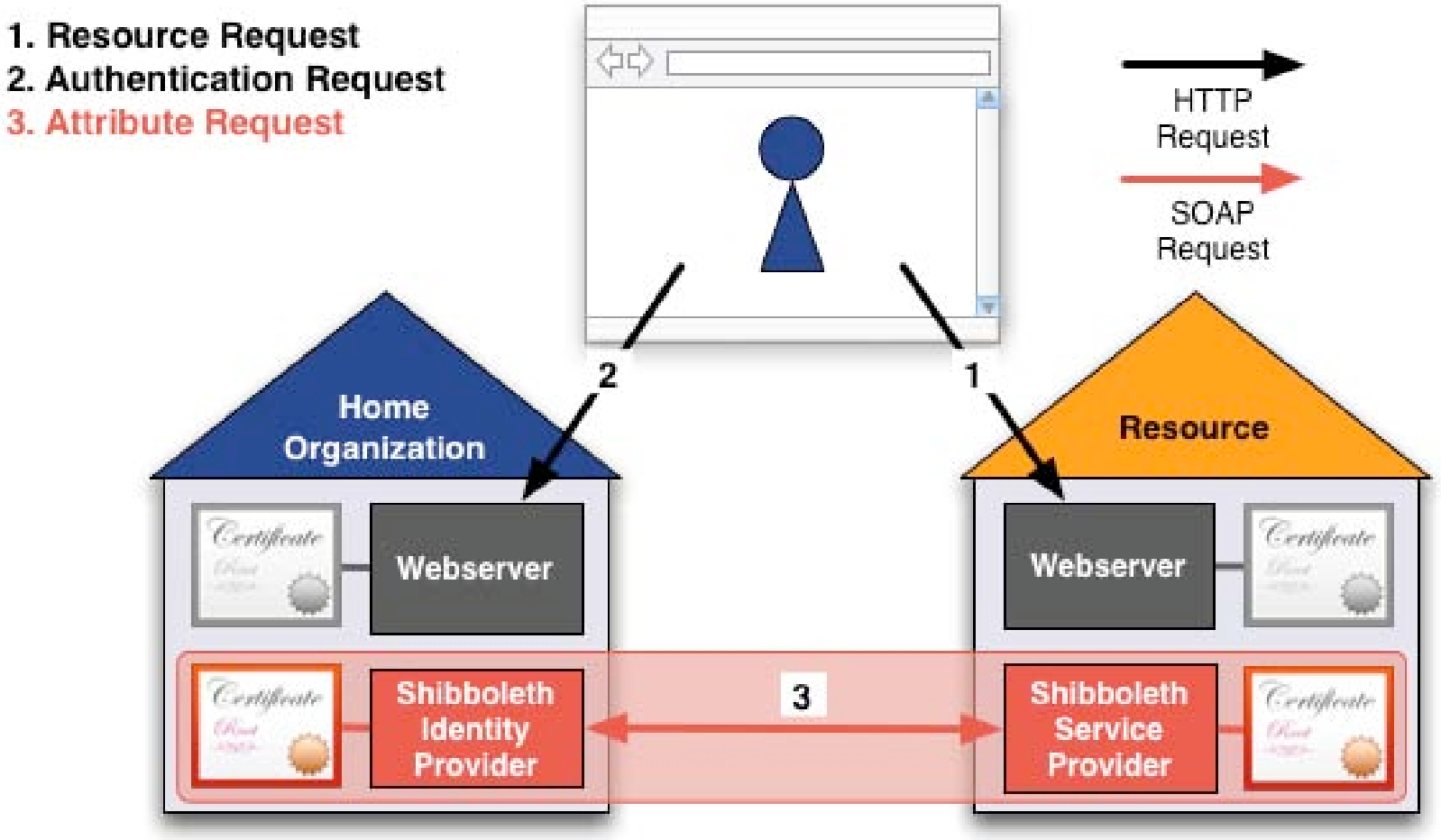
⇨ Basic features of any modern Web Browser

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

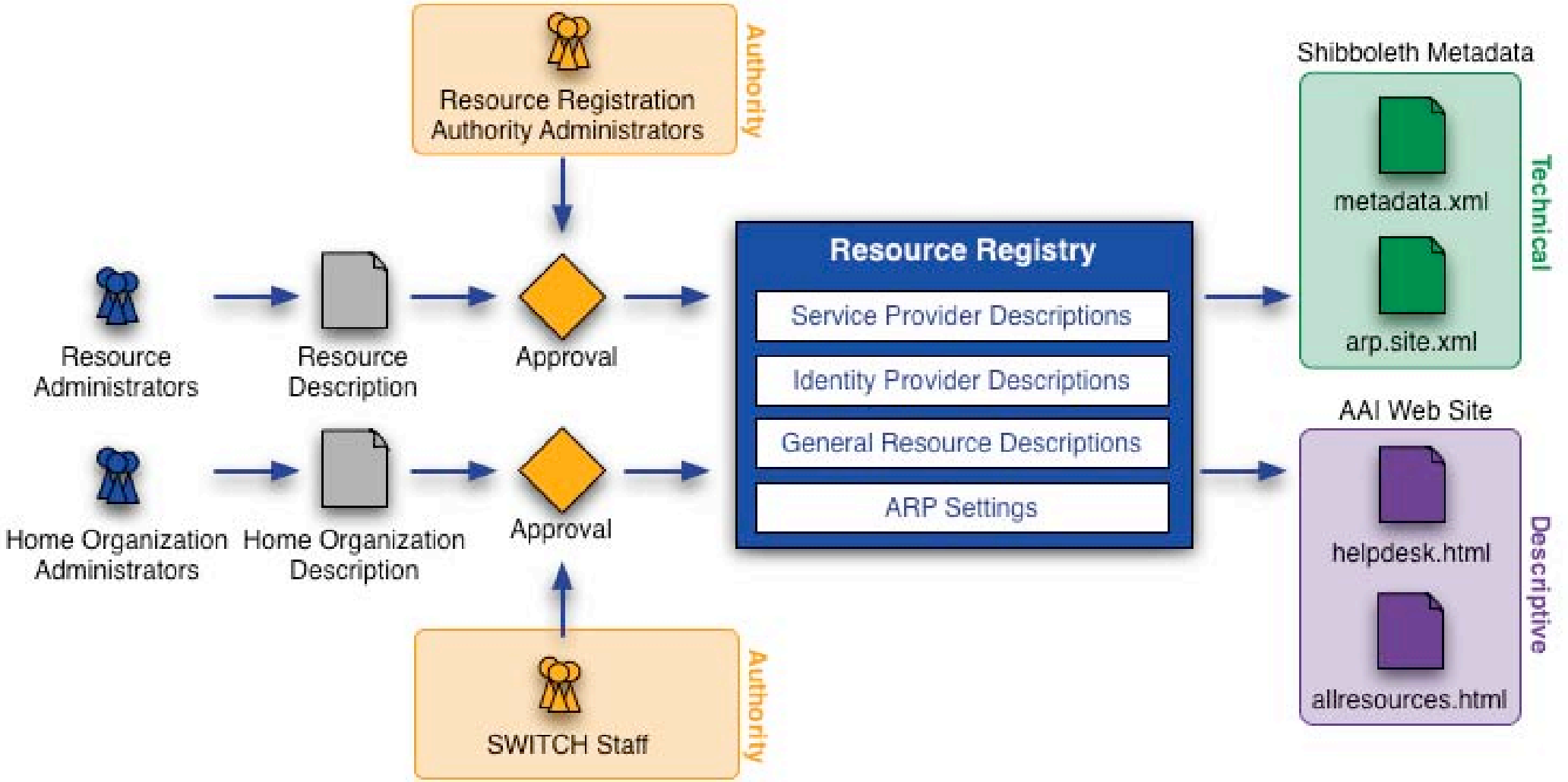
The Swiss Education & Research Network

Resource Registry

Lukas Hämmerle, haemmerle@switch.ch

Resource Registry Processes

SWITCH
The Swiss Education & Research Network



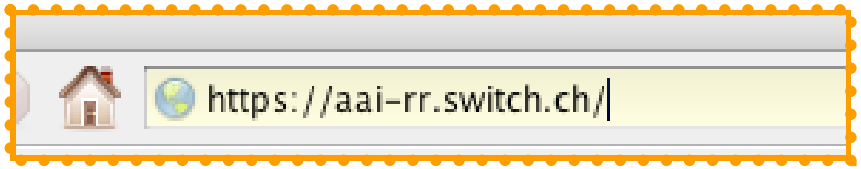
Before an SP/IdP description becomes part of federation metadata, it must be approved by an authority first

Le tour de Resource Registry I

SWITCH
The Swiss Education & Research Network

To activate your Service Provider, register your Resource:

1 Access the Resource Registry



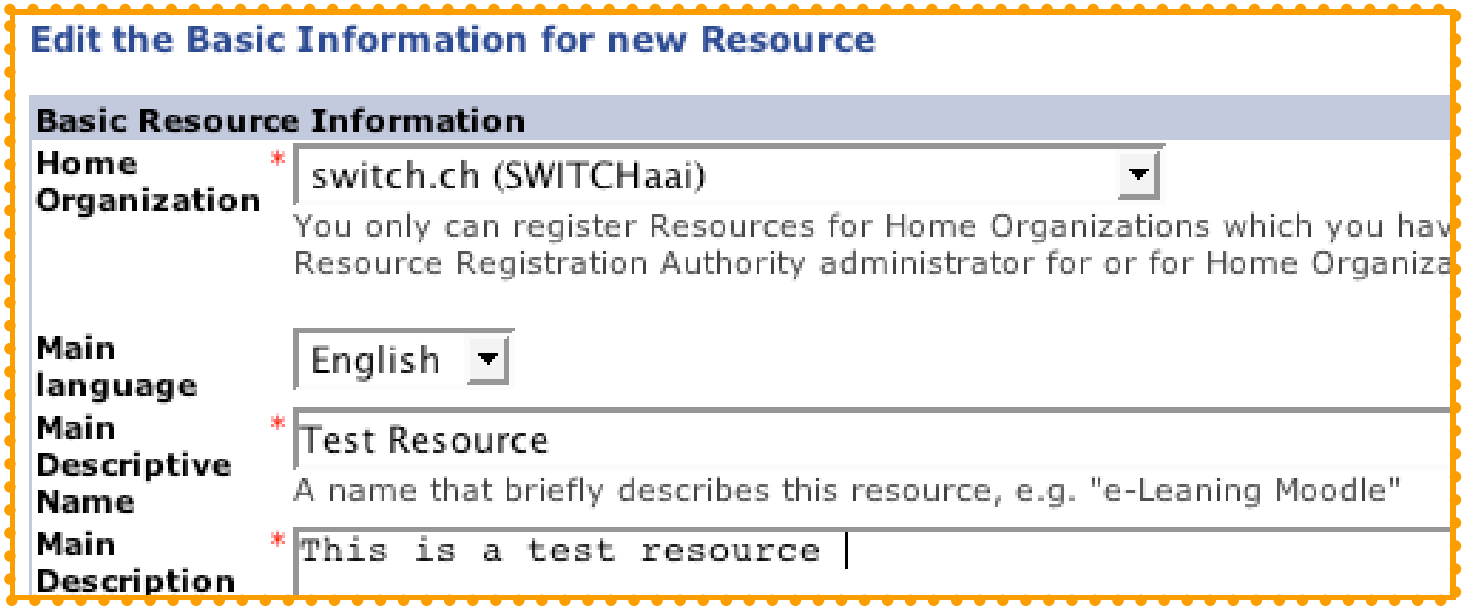
2 Add a new Resource Description

Le tour de Resource Registry II

SWITCH
The Swiss Education & Research Network

3 Complete the forms

a.)

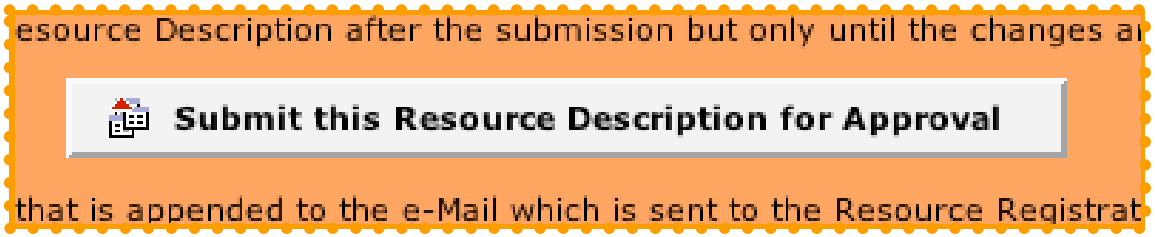


b.)

Le tour de Resource Registry III

SWITCH
The Swiss Education & Research Network

4 Submit resource description for approval



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

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

SWITCH
The Swiss Education & Research Network

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

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