Embedded WAYF

A slightly new approach to the discovery problem

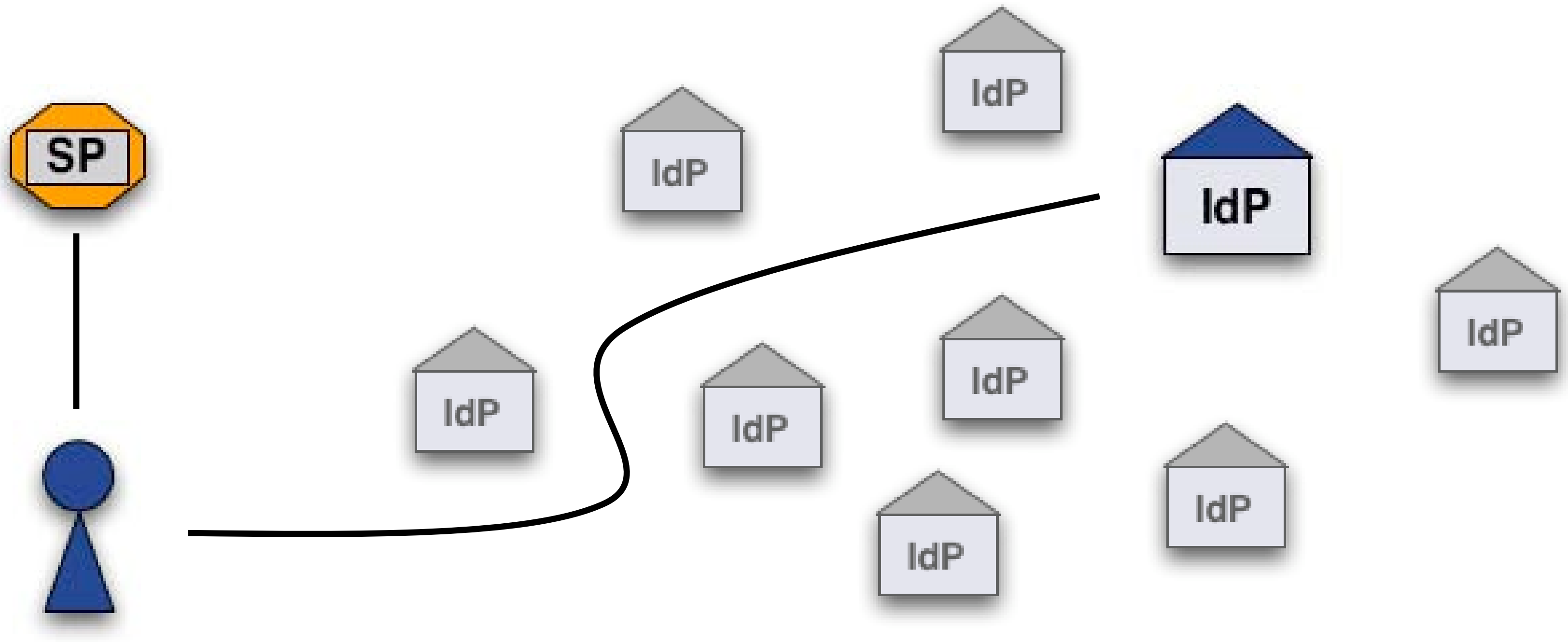
SWITCH

Serving Swiss Universities

Lukas Hämmerle
lukas.haemmerle@switch.ch

The Problem

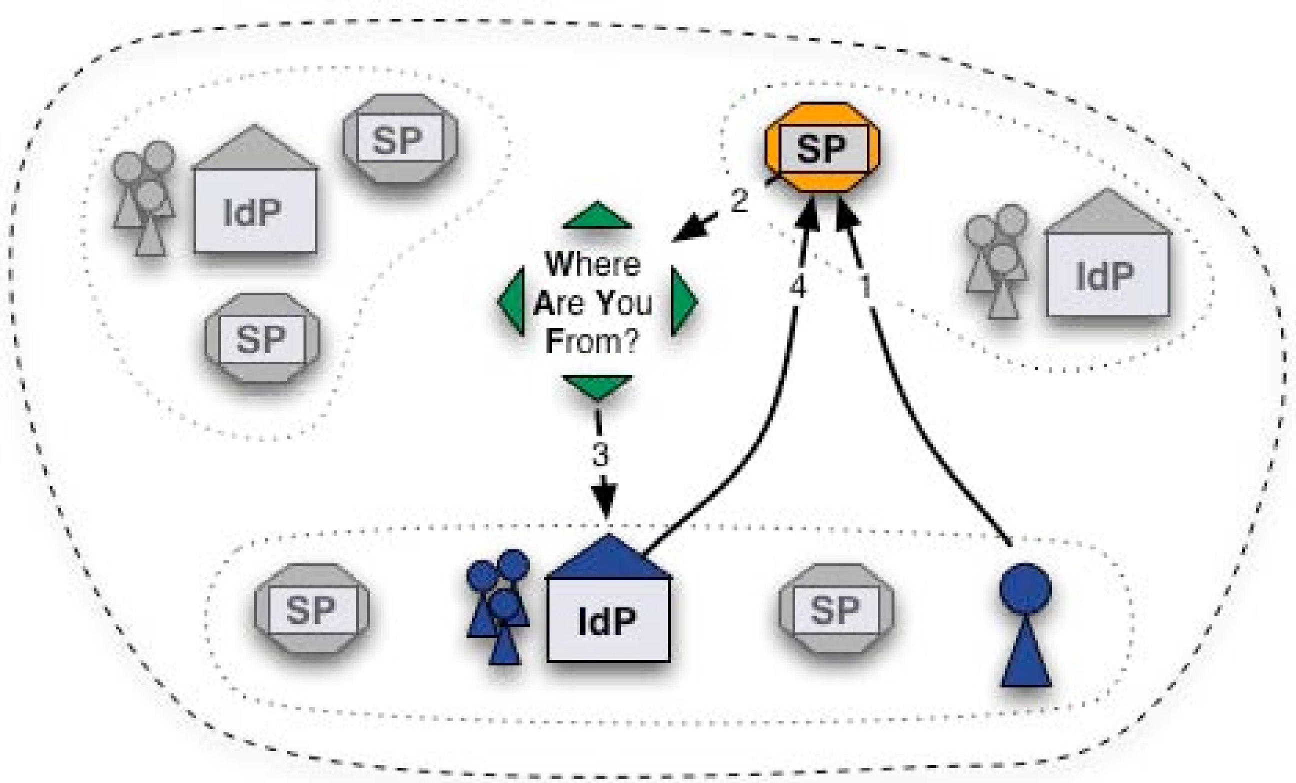
In a federated environment, the user has to declare where he wants to authenticate.



The easiest way is to ask the user “Where Are You From?”

Solution 1: Central WAYF

- The classic way: One WAYF per Federation



Centralized WAYF: Considerations

- “The WAYF is the worst possible way of doing IdP Discovery except for all the others”

👍 Very convenient for Resource administrators

  No deployment, installation or maintenance needed

👍 User statistics can be generated for federation

👍 User has to select his IdP only once per session

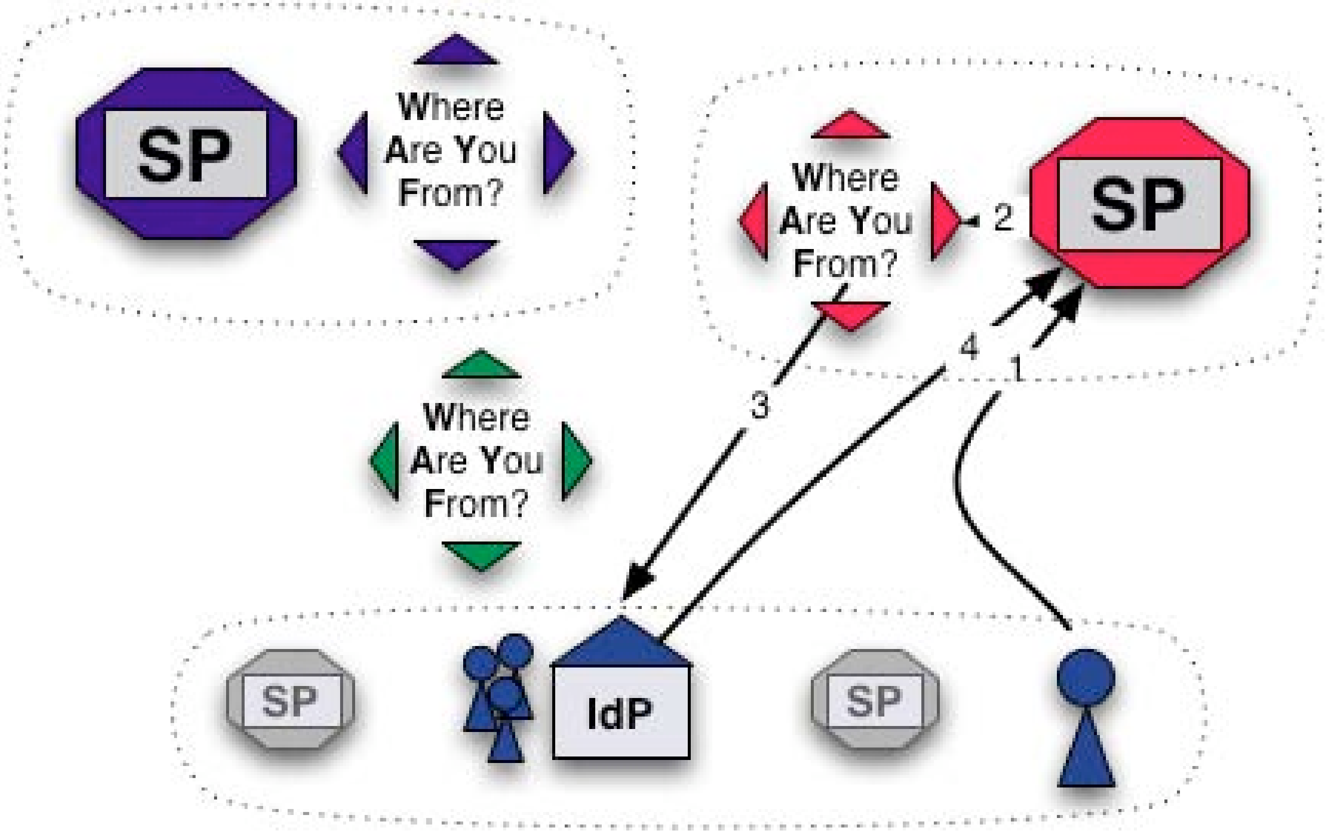
👎 Yet another domain the user comes across

👎 Another custom look & feel

👎 No controls regarding IdPs that are displayed

Solution 2: Distributed WAYF

- More and more used: One WAYF per Resource



Distributed WAYF: Considerations

- Mostly e-learning administrators of larger resources want best usability and look&feel for their user

👍 Complete control for Resource administrators

Limit IdPs to relevant ones, adapt look&feel, integrate into resource

👍 No redirects to another host

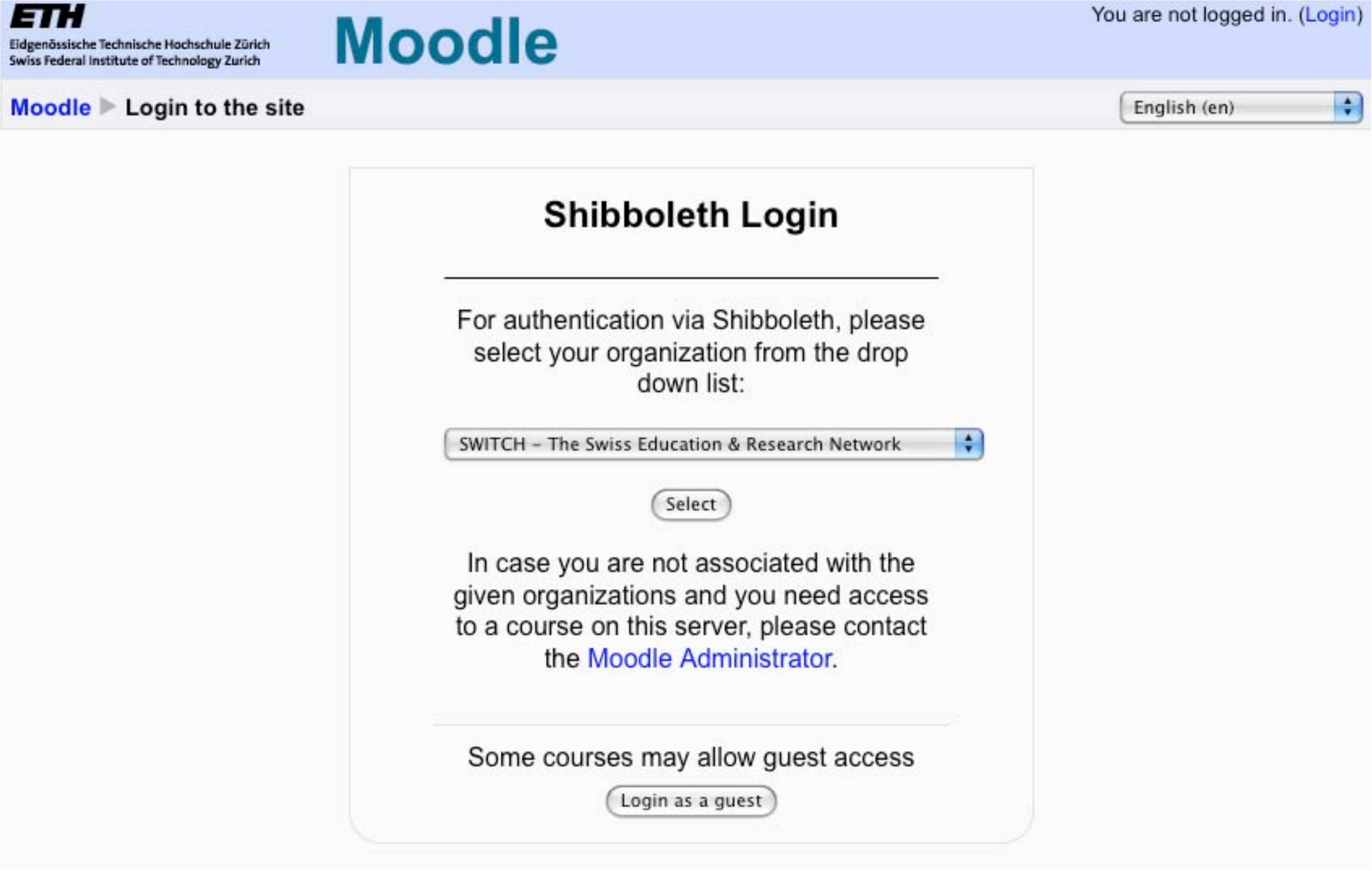
👍 One click less when optimally integrated

👎 Integration/Implementation/Maintenance work for admins

👎 No federation user statistics

👎 User may have to choose IdP for each resource again

Distributed WAYF Example



ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich
Moodle
You are not logged in. (Login)
Moodle ▶ Login to the site
English (en)

Shibboleth Login

For authentication via Shibboleth, please select your organization from the drop down list:

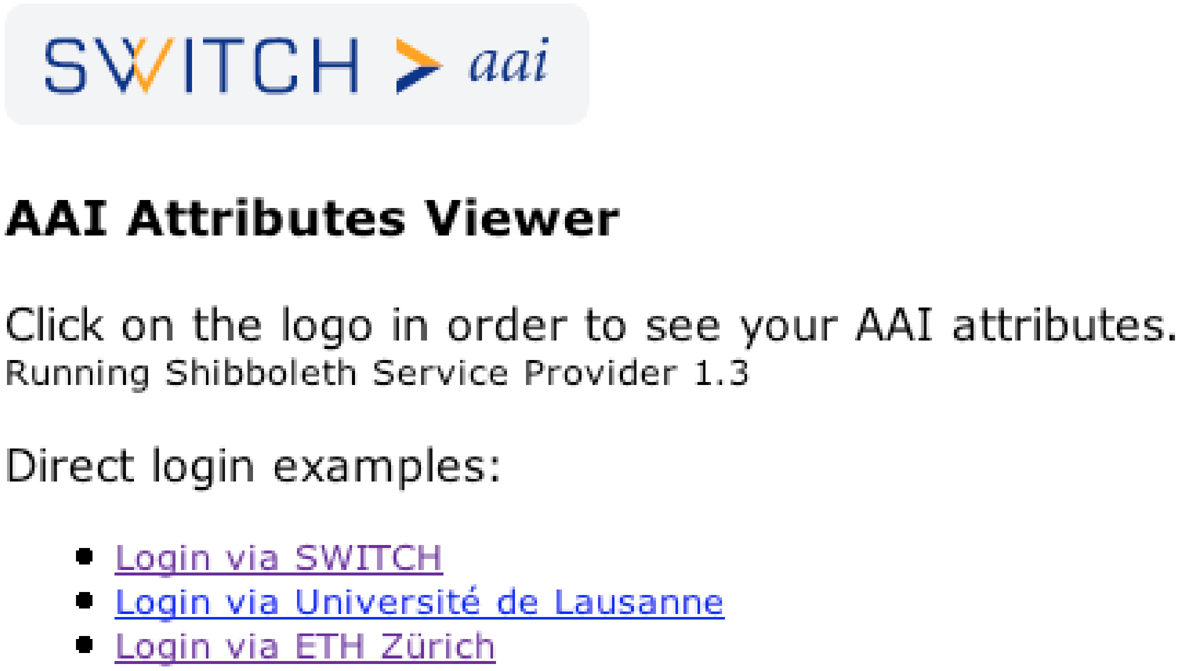
SWITCH - The Swiss Education & Research Network

In case you are not associated with the given organizations and you need access to a course on this server, please contact the Moodle Administrator.

Some courses may allow guest access

2.b Direct Login URLs

- A separate login link for specific IdPs
- 1 click direct redirect to IdP without going via WAYF
- Useful when only users of few IdPs use resource



AAI Attributes Viewer

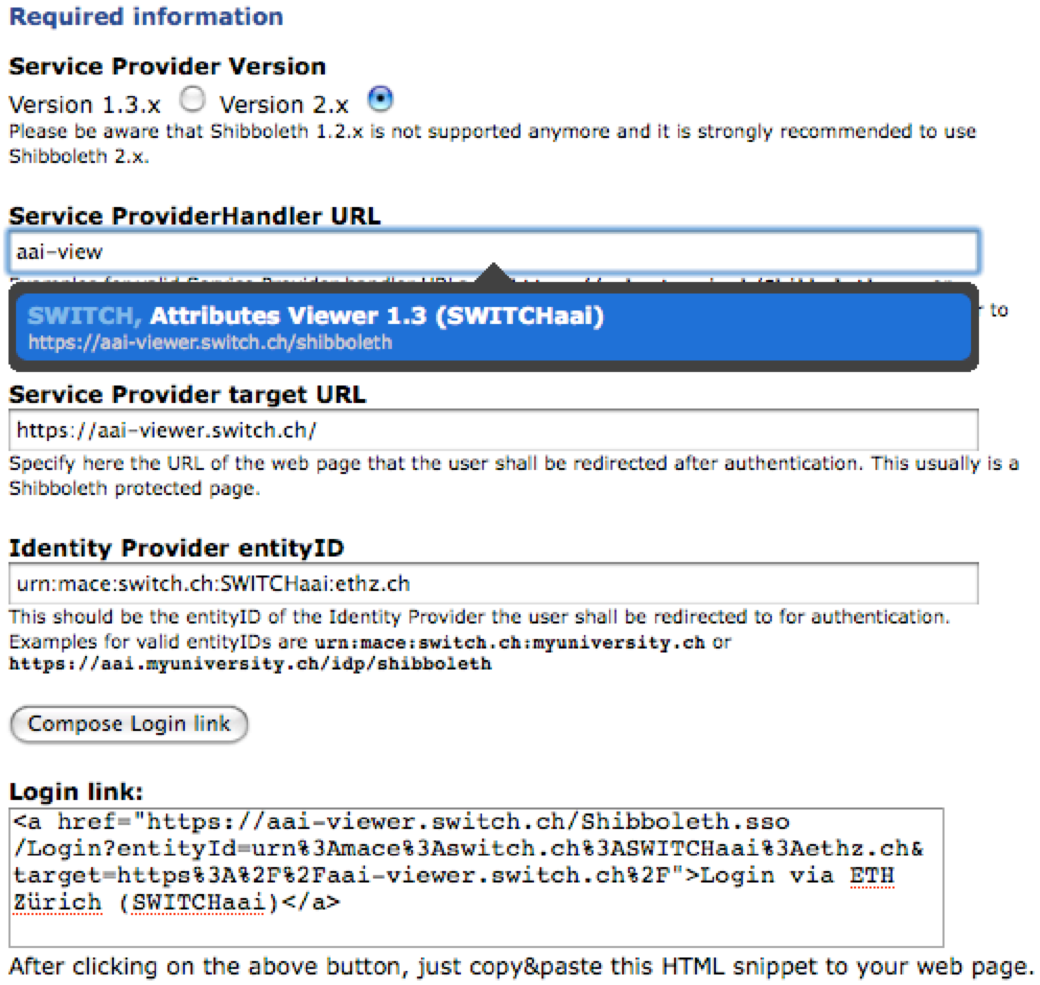
Click on the logo in order to see your AAI attributes.
Running Shibboleth Service Provider 1.3

Direct login examples:

- Login via SWITCH
- Login via Université de Lausanne
- Login via ETH Zürich

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

Composing Login URLs



Required information

Service Provider Version

Version 1.3.x ○ Version 2.x ●

Please be aware that Shibboleth 1.2.x is not supported anymore and it is strongly recommended to use Shibboleth 2.x.

Service ProviderHandler URL

aai-view

SWITCH, Attributes Viewer 1.3 (SWITCHaai)
https://aai-viewer.switch.ch/shibboleth

to

Service Provider target URL

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

Specify here the URL of the web page that the user shall be redirected after authentication. This usually is a Shibboleth protected page.

Identity Provider entityID

urn:mace:switch.ch:SWITCHaai:ethz.ch

This should be the entityID of the Identity Provider the user shall be redirected to for authentication. Examples for valid entityIDs are **urn:mace:switch.ch:myuniversity.ch** or **https://aai.myuniversity.ch/idp/shibboleth**

Login link:

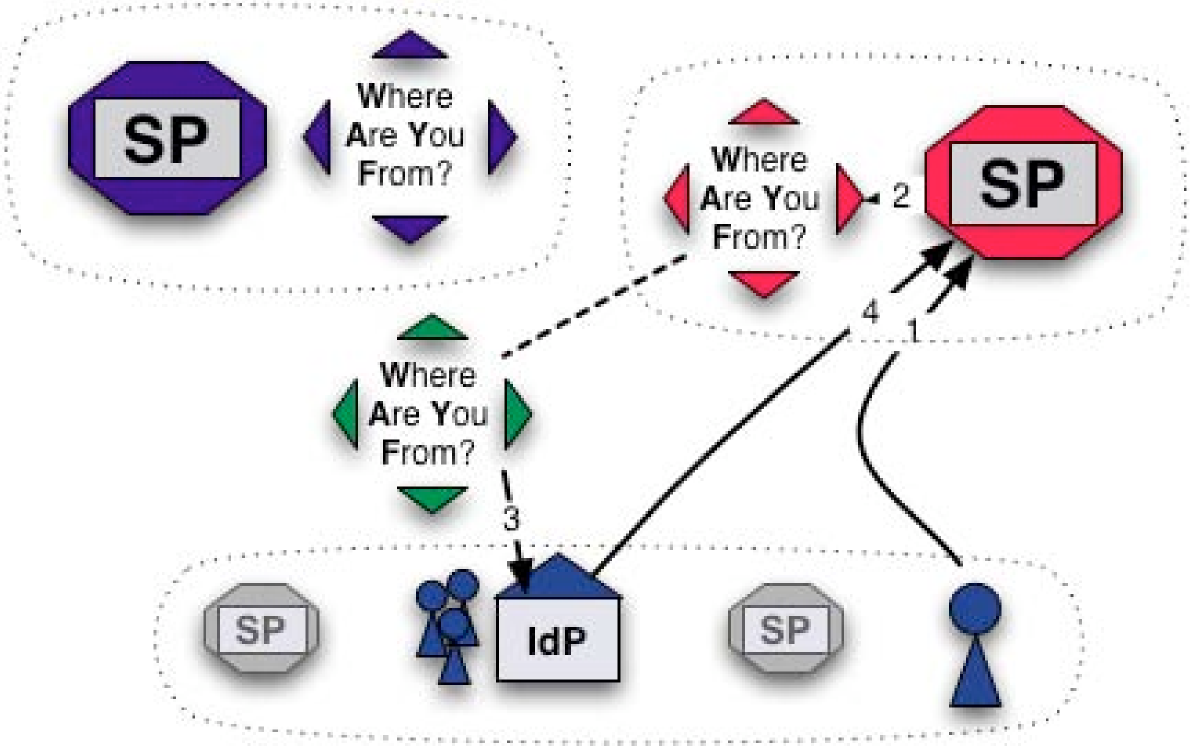
```
<a href="https://aai-viewer.switch.ch/Shibboleth.sso
/Login?entityId=urn%3Amace%3Aswitch.ch%3ASWITCHaai%3Aethz.ch&
target=https%3A%2F%2Faai-viewer.switch.ch%2F">Login via ETH
Zürich (SWITCHaai)</a>
```

After clicking on the above button, just copy&paste this HTML snippet to your web page.

http://www.switch.ch/aai/support/serviceproviders/sp-compose-login-url.html

Solution 3: Embedded WAYF

- The new idea: Embed WAYF on Resource, customize look and feel but effectively still transparently use central WAYF

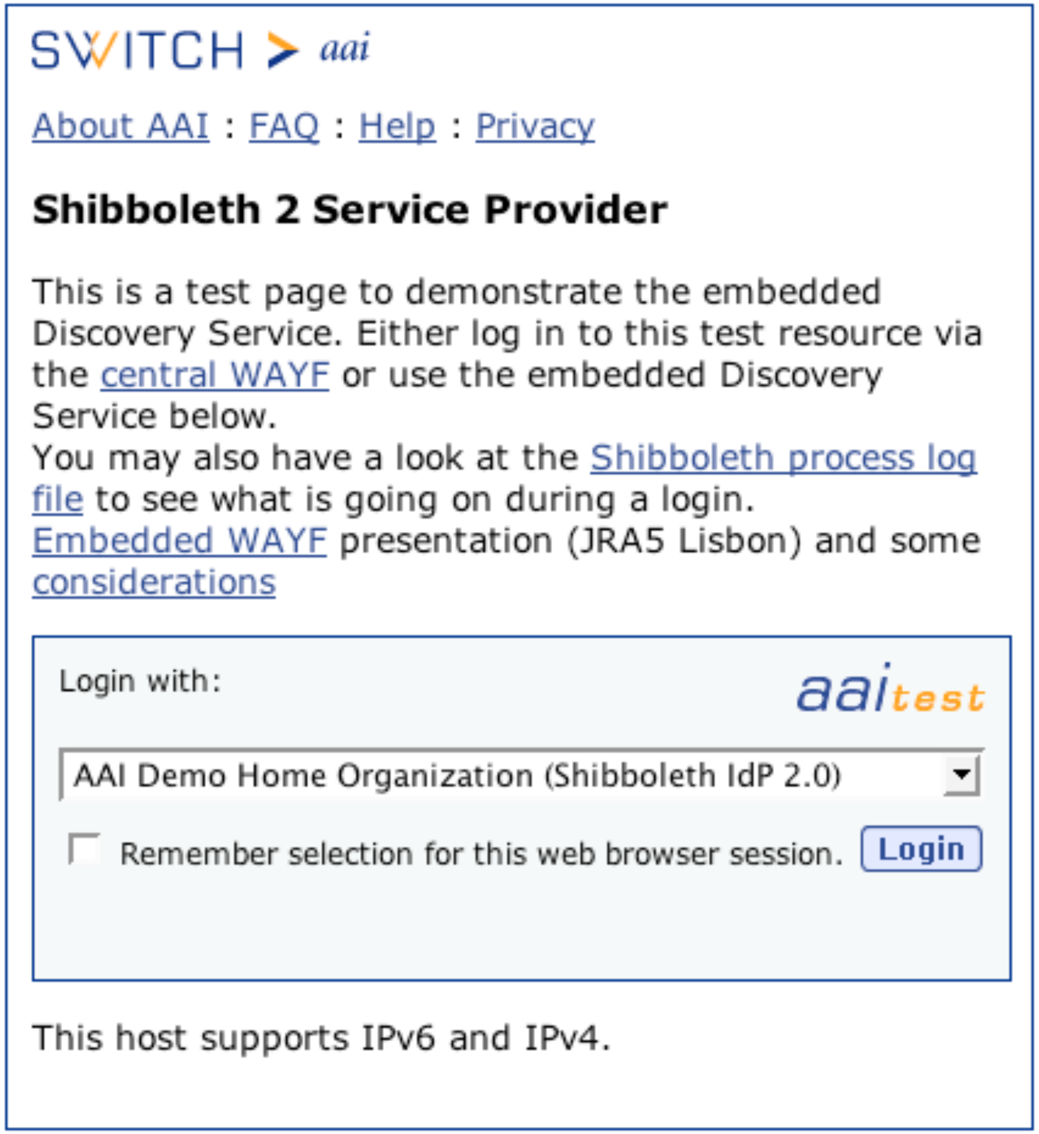


How the embedding works

- Works like Google Ads :-)
- Embedd 2 JavaScripts:
- Configurator Script
  - Influences look and feel (colors, size, etc.)
  - Excludes IdPs from list
  - Add IdPs from other federations

- Logic Script
  - The same URL for all embedded WAYFs
  - Generated by and loaded from central WAYF
  - Cookies from central WAYF can be read this way!
    - This allows IdP preselection or direct redirection

Embedded WAYF Example



SWITCH aai

About AAI : FAQ : Help : Privacy

Shibboleth 2 Service Provider

This is a test page to demonstrate the embedded Discovery Service. Either log in to this test resource via the central WAYF or use the embedded Discovery Service below.
You may also have a look at the Shibboleth process log file to see what is going on during a login.
Embedded WAYF presentation (JRA5 Lisbon) and some considerations

Login with:

AAI Demo Home Organization (Shibboleth IdP 2.0)

□ Remember selection for this web browser session.

This host supports IPv6 and IPv4.

Instructions:

1. Copy & paste sample HTML code to your web page
2. Adapt at least 5 settings
3. Done

What you get:

Always up-to-date, fully customizable, self-maintained, 1 click-saving Discovery Service

Example:

https://kelimutu.switch.ch/

Embedded WAYF: Considerations

- Use advantages of central and distributed approach

👍 Complete control for Resource administrators

Limit IdPs to relevant ones, adapt look&feel, integrate into resource

👍 No redirects to another host

👍 One click less when optimally integrated

👍 Very convenient for Resource administrators

No deployment, installation or maintenance needed

👍 User statistics can be generated for federation

👍 User has to select his IdP only once per session

👎 (User needs Javascript enabled or use alternative fallback)

👎 (Central WAYF must be well secured and high available)

More: http://kelimutu.switch.ch/Embedded-DS.txt

Embbedded WAYF in SWITCHaai

- WAYF for AAI Test already supports embedding
  See source code of https://kelimutu.switch.ch

- Embedding will be available for SWITCHaai before Christmas (after some more testing)

- Comments and suggestions to aai@switch.ch are very welcome