Embedded WAYF
A slightly new approach to the discovery problem

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

Shibboleth Login

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

SWITCH – The Swiss Education & Research Network

Select

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

Login as a guest
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

Example: [https://aai-viewer.switch.ch/](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 Provider Handler URL

aaiview

SWITCH, Attributes Viewer 1.3 (SWITCHaai)

https://aaiviewer.switch.ch/shibboleth

Service Provider target URL

https://aaiviewer.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:mae: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:mae:switch.ch:myuniversity.ch or https://aaiviewer.switch.ch/idp/shibboleth

Compose Login link

Login link:


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

Embedded WAYF

- The idea: Embed WAYF on Resource, customize look & feel, but still use central WAYF transparently
How the embedding works

- Works like Google Ads :-)

- Embed 2 JavaScripts
  - Configurator Script
    - Influences look & 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 pre-selection or direct redirection
Example of an embedded WAYF

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](http://kelimutu.switch.ch/Embedded-DS.txt)
Embedded WAYF in SWITCHaai

- WAYF for AAI Test already supports embedding

- Embedding for SWITCHaai production federation available since end of November 2008


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