

Embedded WAYF

Integration of the Discovery Service into a service



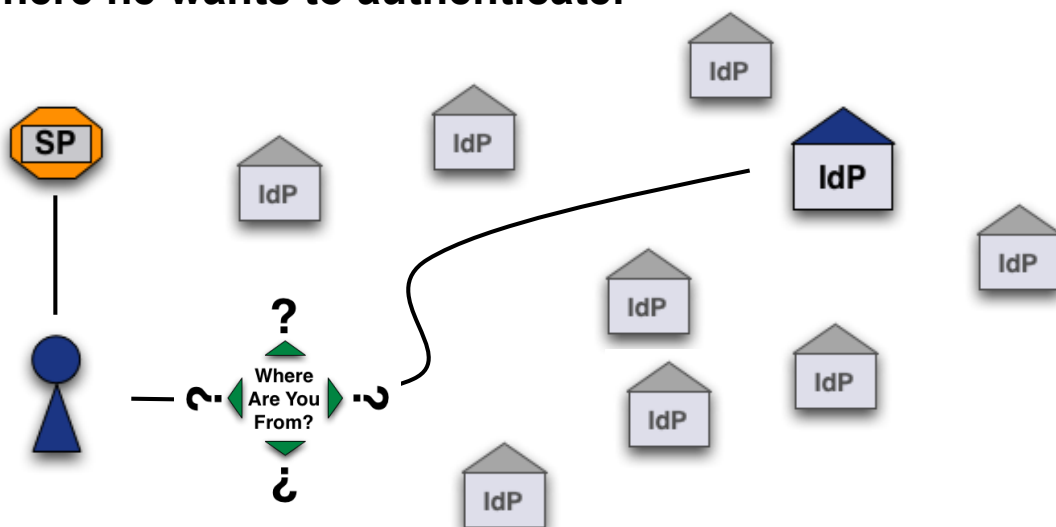
SWITCH

Serving Swiss Universities

SWITCHaai Team
aai@switch.ch

The Problem

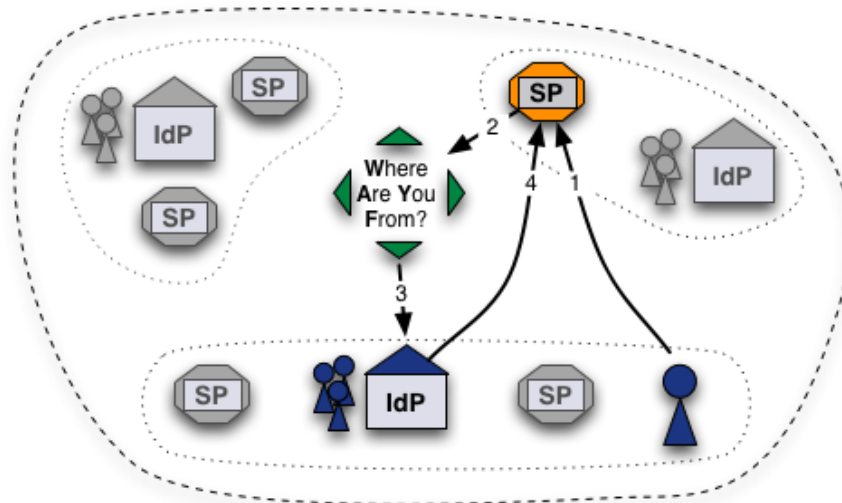
In a federated environment, the user has to declare where he wants to authenticate.



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

Solution 1: Central WAYF

- The classic way: One WAYF per Federation

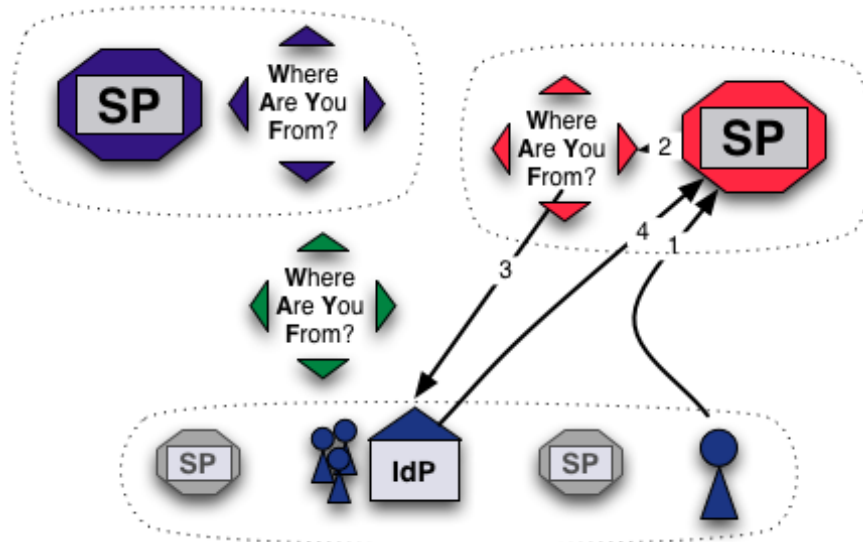


Centralized WAYF: Considerations

- “The WAYF is the worst possible way of doing IdP Discovery except for all the others” (Scott Cantor, SP developer)
- 👍 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

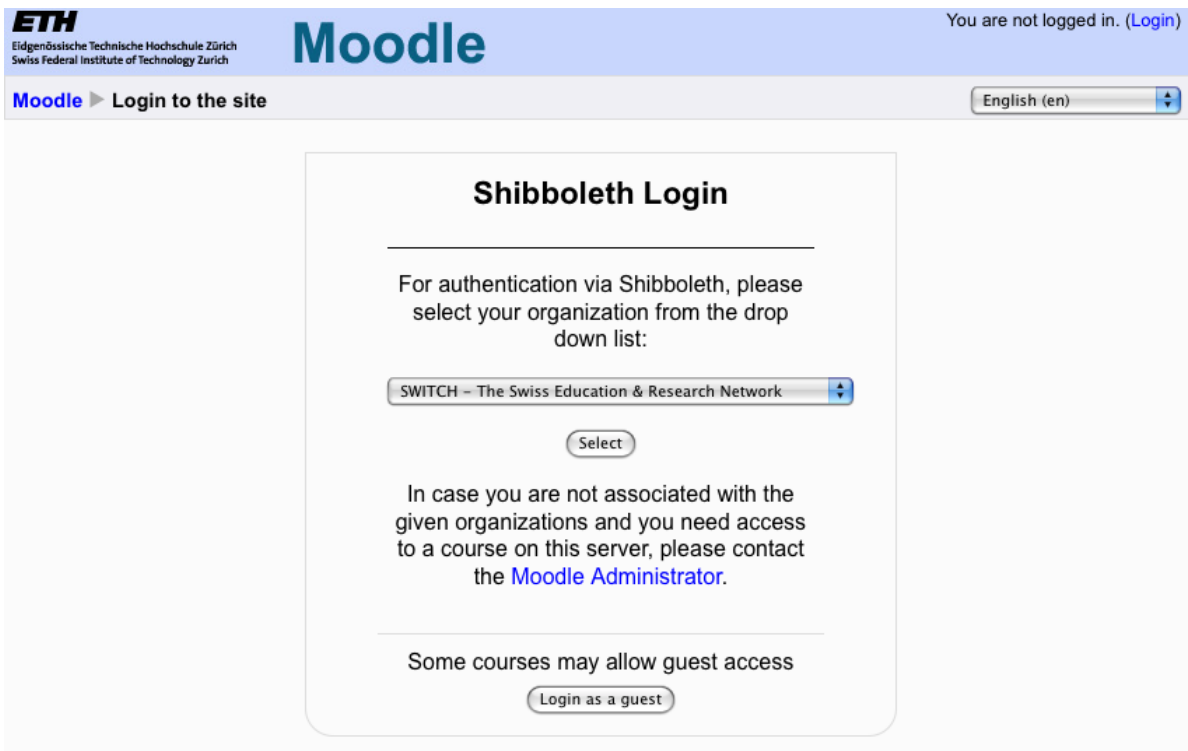
- More and more used: One WAYF per Resource



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



The screenshot shows the Moodle login interface. At the top left is the ETH logo with the text 'Eidgenössische Technische Hochschule Zürich' and 'Swiss Federal Institute of Technology Zurich'. The word 'Moodle' is prominently displayed in the center. On the top right, it says 'You are not logged in. (Login)'. Below the header, there is a navigation bar with 'Moodle' and 'Login to the site'. A language dropdown menu is set to 'English (en)'. The main content area is titled 'Shibboleth Login'. It contains the following text: 'For authentication via Shibboleth, please select your organization from the drop down list:'. Below this is a dropdown menu showing 'SWITCH - The Swiss Education & Research Network'. A 'Select' button is positioned below the dropdown. Further down, it says: '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.' At the bottom of the main content area, it says 'Some courses may allow guest access' with a 'Login as a guest' button.

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-viewer

SWITCH, Attributes Viewer 1.3 (SWITCHaai)

<https://aai-viewer.switch.ch/shibboleth>

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`

Compose Login link

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>
```

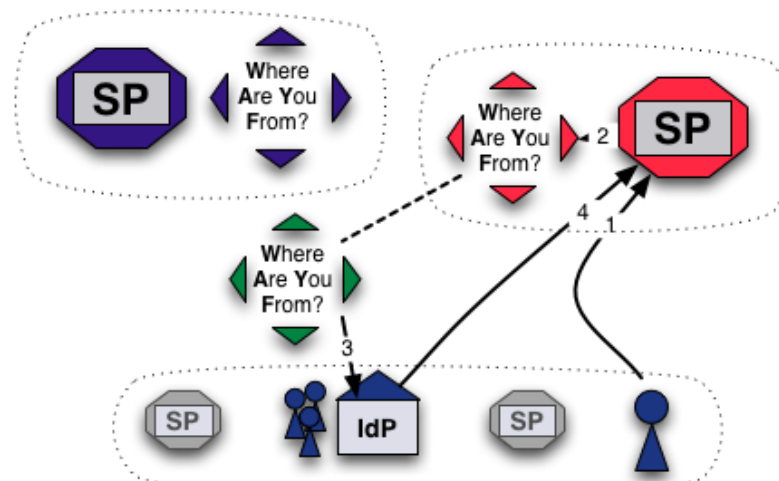
After clicking on the above button, just copy&paste this HTML snippet to your web page.



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

Solution 3: Embedded WAYF

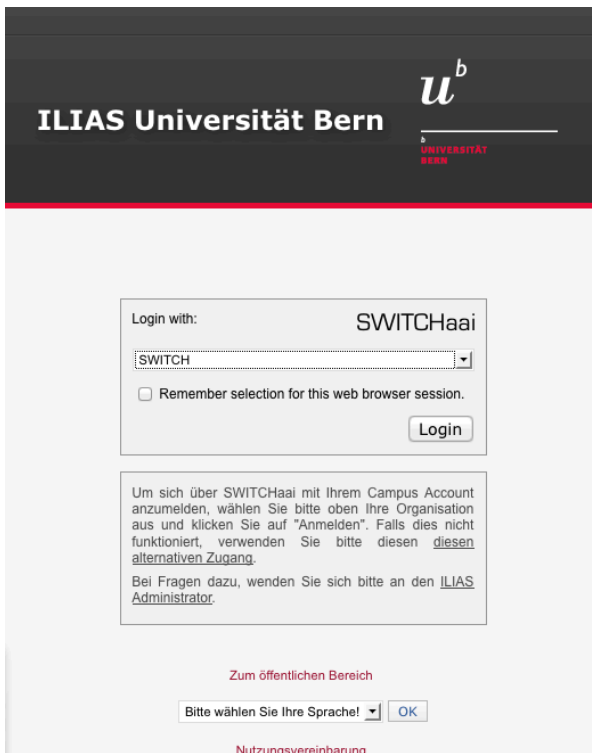
- The new idea: Embed WAYF on Resource, customize look and feel but effectively still transparently use central WAYF



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 instances of the embedded WAYF
 - 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



The screenshot shows the ILIAS Universität Bern login page. At the top, there is a dark header with the text "ILIAS Universität Bern" and the university logo "u^b". Below the header, there is a login form. The form has a "Login with:" label and a dropdown menu currently showing "SWITCH". Below the dropdown, there is a checkbox labeled "Remember selection for this web browser session." and a "Login" button. Below the login form, there is a text box with instructions: "Um sich über SWITCHaai mit Ihrem Campus Account anzumelden, wählen Sie bitte oben Ihre Organisation aus und klicken Sie auf 'Anmelden'. Falls dies nicht funktioniert, verwenden Sie bitte diesen [diesen alternativen Zugang](#)." Below this, it says "Bei Fragen dazu, wenden Sie sich bitte an den [ILIAS Administrator](#)." At the bottom of the page, there is a language selection dropdown labeled "Bitte wählen Sie Ihre Sprache!" with an "OK" button and a "Nutzungsvereinbarung" link.

Instructions:

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

What you get:

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

Example:

 <https://ilias.unibe.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
- 👍 Saves at least one click
- 👍 Very convenient for Resource administrators
 - No deployment, installation or maintenance needed
- 👍 User statistics can be generated for federation
- 👎 (User needs Javascript enabled or use alternative fallback)
- 👎 (Central WAYF must be well secured and high available)



<http://www.switch.ch/aai/support/serviceproviders/sp-embedded-wayf.html>



© 2008 SWITCH

13

Alternative I: Embedded Discovery Service

- Works like Embedded WAYF
- Independent from a central service
- Requires Shibboleth SP \geq 2.4
- Search-as-you-type or select from list
- JS, CSS and HTML only
- Very easy to customize



Choose an Identity Provider

In order to log in to this service, please select the home organization with which you're affiliated. If your organization is not supported, you may select **ProtectNetwork** and create a free account there for our services.

Use a suggested selection:



SWITCH

University of Geneva

ETHZ - ETH Zurich

SWITCH

Or enter your organization's name

Continue

[Allow me to pick from a list](#)

[Help](#)



<https://wiki.shibboleth.net/confluence/display/EDS10/Embedded+Discovery+Service>



© 2008 SWITCH

14

Alternative II: Disco Juice

- Very comprehensive Discovery Service
- Well suited for services with users from many IdPs
- Search-as-you-type only
- Uses Geo IP and metric to guess user's IdP
- Based on PHP and JS

 <http://discojuice.org/>

