

# Discovery Service Options



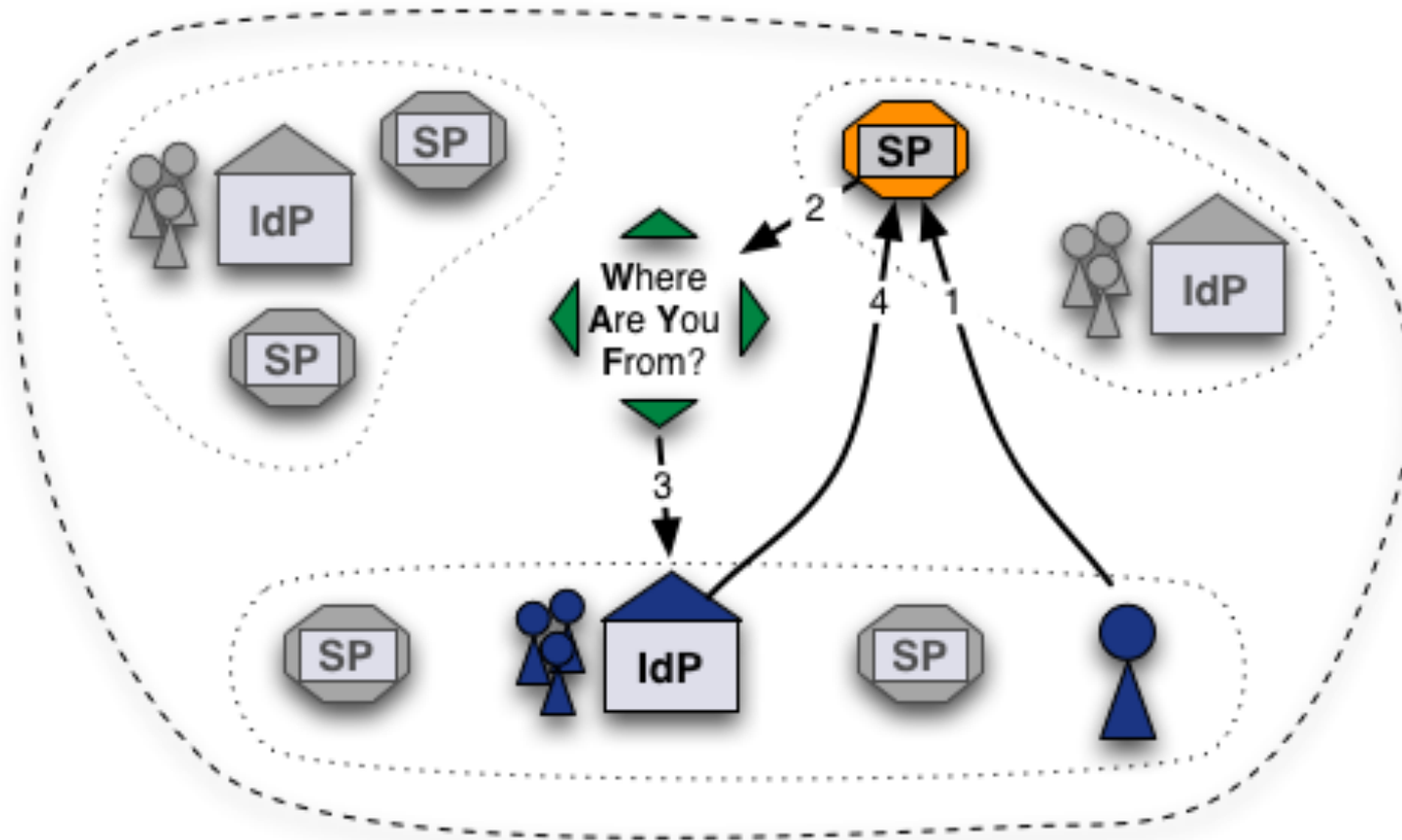
SWITCH

Bea Huber  
[aai@switch.ch](mailto:aai@switch.ch)

Interfederation Crash Course  
Bern, 1. March 2013

# No Central WAYF for Interfederation

- The classic way: One WAYF per Federation



# Alternatives

- Direct Login URLs
- SWITCH Embedded WAYF
- Shibboleth Embedded Discovery Service



# Solution 1: 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

## **Login links:**

[Login via SWITCH \(SWITCHaai\)](#)

[Login via Stockholm University \(Interfederation\)](#)

[Login via University of Gothenburg \(Interfederation\)](#)

# Composing Login URLs

## Service Provider Login Link Composer

This web page lets one compose login links for a Shibboleth-protected resource. The link will redirect users directly to a specific Home Organization for authentication. This way users will skip the WAYF/Discovery Service.

**Example link:** [Login via SWITCH \(SWITCHaai\)](#)

However, in case your resource has users from more than a hand full of different organizations, it is recommended to use a WAYF/Discovery Service or the [embedded WAYF](#).

## Required information

### Service Provider Session Initiator Handler URL

**Session Initiator**  /Login  /DS

Since Shibboleth 2.5 the default Session Initiator is **/Login**, for older version you might have to use the **/DS** Session Initiator.

Enter the hostname of your SWITCHaai or AAI Test service and select one of the matching entries from the auto-completion feature.

Examples for valid Service Provider Session Initiator handler URLs are

**https://myhost.uni.ch/Shibboleth.sso/Login** or

**https://otherhost.uni.ch/Shibboleth.sso/DS.**

### Service Provider Target URL

Specify here the URL of the web page that the user shall be redirected after authentication. This is usually a Shibboleth protected page. If you don't have such a page yet, use

**https://your.host.ch/Shibboleth.sso/Session** provided you are using a Service Provider 2.x. This page then will display all available attributes and other session information.

### Identity Provider entityID

#### Universität Bern (SWITCHaai)

<https://aal-ldp.unibe.ch/ldp/shibboleth>

#### Universität Bern - Test-Homeorg (AAI Test)

<https://aal-testldp.unibe.ch/ldp/shibboleth>

Examples for valid entityIDs

with IdP 2.3 or newer)

provider-initiated URLs work

in some cases but are generally not

recommended to use.



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



# Solution 2: Embedded WAYF

ILIAS  
Universität Bern

OLAT login

Please select your university.

You will be redirected for authentication.

SWITCH

Login



Login with:

SWITCHHai

SWITCH

Remember selection for this web browser session.

Login

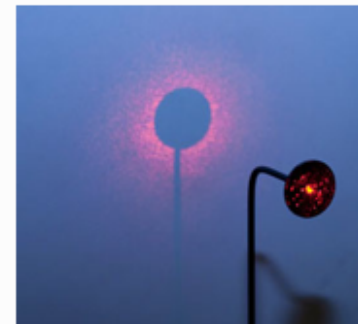
Um sich über SWITCHHai mit Ihrem Campus Account anzumelden, wählen Sie bitte oben Ihre Organisation aus und klicken Sie auf "Anmelden". Falls dies nicht funktioniert, verwenden Sie bitte [diesen alternativen Zugang](#).

Bei Fragen dazu, wenden Sie sich bitte an den [ILIAS Administrator](#).

WSL - Eidg. Forschung

Login

Anleitungen und Merkblätter



# Embedded WAYF

Select the organisation you are affiliated with ...

## Universities

- EPF Lausanne
- ETH Zurich
- Universität Basel
- Universität Bern
- Universität Liechtenstein
- Université de Genève
- Universität Luzern
- Universität St. Gallen
- Universität Zürich

## Universities of Applied Sciences

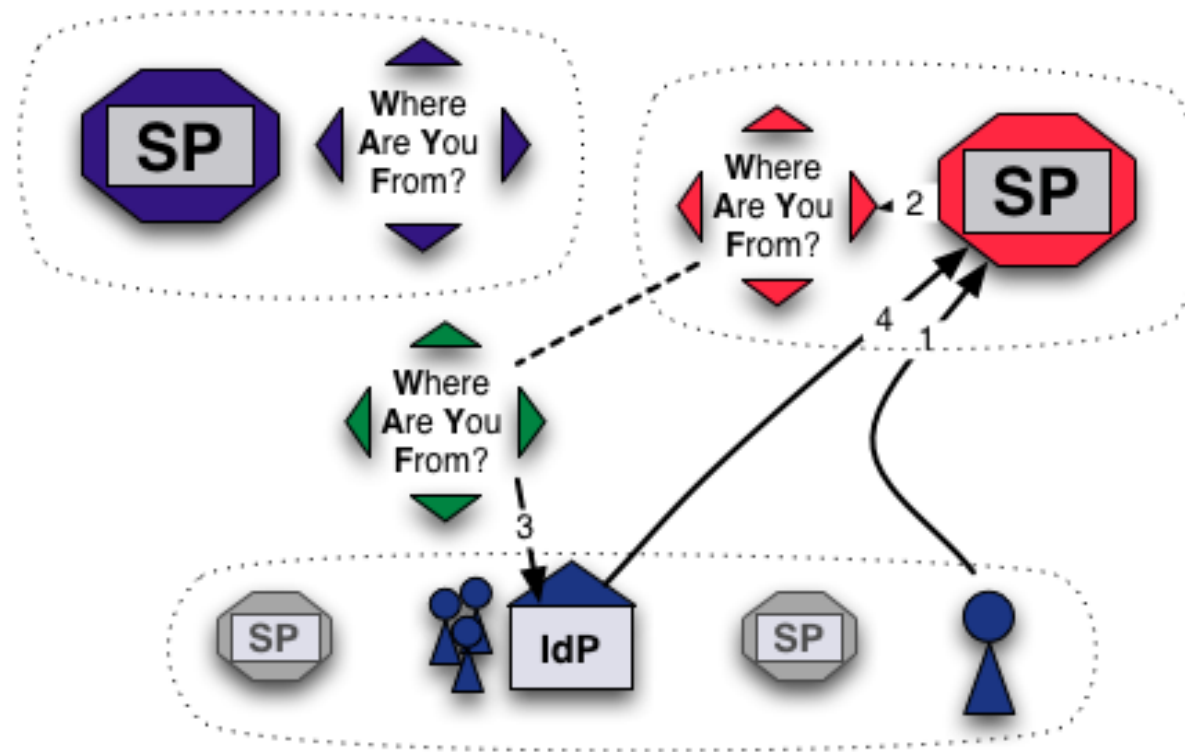
- FFHS – Fernfachhochschule Schweiz
- FHS St. Gallen – Hochschule für Angewandte Wissenschaften
- FHNW – Fachhochschule Nordwestschweiz
- HEPVS – Valais University of Teacher Education
- ✓ HES–SO – Haute école spécialisée de Suisse occidentale
- HSLU – Hochschule Luzern
- HSR – Hochschule für Technik Rapperswil
- HWZ – Hochschule für Wirtschaft Zürich
- NTB – Hochschule für Technik Buchs
- PHBern – Pädagogische Hochschule Bern
- PHGR – Pädagogische Hochschule Graubünden
- PHTG – Pädagogische Hochschule Thurgau
- PHZ – Pädagogische Hochschule Zentralschweiz
- PH Zug – Pädagogische Hochschule Zug
- SUPSI – Scuola Universitaria Professionale della Svizzera Italiana
- ZHAW – Zürcher Hochschule für Angewandte Wissenschaften
- ZHdK – Zürcher Hochschule der Künste

## From other federations

- Stockholm University
- University of Trieste IdP

# Embedded WAYF

- Embed WAYF on Web Application
- customize look and feel
- still transparently use central WAYF





# Information and Configuration

More information about the embedded WAYF:



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

Generate the embedded WAYF code for your SP:



[https://rr.aai.switch.ch/gen\\_embedding\\_code.php](https://rr.aai.switch.ch/gen_embedding_code.php)

# Configuration

## Configuration Example of embedded wayf

```
// Example of how to add Identity Provider from other federations
```

```
var wayf_additional_idps = [  
  
    {name:"University of Trieste IdP",  
      entityID:"https://idemfero.units.it/idp/shibboleth"},  
  
    {name:"Stockholm University",  
      entityID:"https://idp.it.su.se/idp/shibboleth"}  
];
```

# Configuration

## Configuration Example of embedded wayf

```
// EntityIDs of Identity Provider that should not be shown at all
// [Optional, commented out by default]

var wayf_hide_idps = new Array ("https://idemfero.units.it/idp/shibboleth",
"https://idp.it.su.se/idp/shibboleth");

// Categories of Identity Provider that should not be shown
// Possible values
// are:"university","uas","hospital","library","vho","others","all"

var wayf_hide_categories = new Array("library","vho","others","hospital");
```

# Enable JSON Discovery feed



In shibboleth2.xml:

```
<Sessions lifetime="28800"  
    timeout="3600"  
    relayState="ss:mem"  
    checkAddress="false"  
    consistentAddress="true"  
    handlerSSL="true"  
    cookieProps="https">
```

...

```
<!-- JSON feed of discovery information. -->  
    <Handler type="DiscoveryFeed" Location="/DiscoFeed"/>  
</Sessions>
```

# JSON Discovery feed example



```
[ { "entityID": "https://idp.ids-mannheim.de/idp/shibboleth",
  "DisplayNames": [
    { "value": "Institut für Deutsche Sprache (IDS)", "lang": "de" },
    { "value": "Institut für Deutsche Sprache (IDS)", "lang": "en" }
  ]
},
{ "entityID": "https://idp.it.gu.se/idp/shibboleth",
  "DisplayNames": [
    { "value": "Göteborgs universitet", "lang": "sv" },
    { "value": "University of Gothenburg", "lang": "en" }
  ],
  "Logos": [
    { "value": "https://www.gu.se/digitalAssets/1374/1374690_lo_gu_left.png", "height": "50", "width": "344",
      "lang": "sv" },
    { "value": "https://www.gu.se/digitalAssets/1374/1374690_lo_gu_left.png", "height": "50", "width": "376",
      "lang": "en" }
  ]
}
]
```

# Configuration

## Configuration Example of embedded wayf

```
// Whether to load Identity Providers from the Discovery Feed provided by
// the Service Provider.
// IdPs that are not listed in the Discovery Feed and that the SP therefore is
// not able to accept assertions from, are hidden by the Embedded WAYF
// IdPs that are in the Discovery Feed but are unknown to the SWITCHwayf
// are added to the wayf_additional_idps.
// The list wayf_additional_idps will be sorted alphabetically
// The SP must have configured the discovery feed handler that generates a
// JSON object. Otherwise it won't generate the JSON data containing the IdPs.
// [Optional, commented out by default]

var wayf_use_disco_feed = true;
```

## Solution 3: Embedded Discovery Service

- Also uses the Discovery Feed provided by the SP
- Embed the DS directly into the service
- Search-as-you-type or select from list
- JS, CSS and HTML only
- developed and maintained by the Shibboleth team
- download from



<http://shibboleth.net/downloads/embedded-discovery-service/latest/>

- Documentation can be found at:



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

# Embedded Discovery Service

## AAI Attribute Viewer

SWITCH

The AAI Attribute Viewer displays all attributes that are available about an AAI user. All user information is stored 10 days in a log file before it is automatically deleted.

Please select your Home Organization and log in to see the [AAI attributes](#) that are available for you.

Use a suggested selection:



VHO - Virtual Home  
Organization



WSL - Swiss Federal  
Institute for...



SWITCH

Or enter your organization's name

Continue

Help

- FHNW - University of Applied Sciences Northwestern Switz
- HES-SO : University of Applied Sciences Western Switzerl
- HSR - Hochschule für Technik Rapperswil
- PHZ - University of Teacher Education Central Switzerlan
- SNSF - Swiss National Science Foundation
- SUPSI - University of Applied Sciences Southern Switzerl
- SWITCH
- VHO - Virtual Home Organization
- WSL - Swiss Federal Institute for Forest, Snow and Lands



# MetadataFilter Example



In shibboleth2.xml:

```
<MetadataProvider type="XML" .....>
```

```
  <MetadataFilter type="Whitelist">
```

```
    <Include>https://idp.nordu.net/idp/shibboleth</Include>
```



```
    <Include>https://idp.ids-mannheim.de/idp/shibboleth</Include>
```

```
    <Include>https://idp.it.su.se/idp/shibboleth</Include>
```


```
  </MetadataFilter>
```

```
</MetadataProvider>
```

# Embedded WAYF vs Embedded DS

Properties	Login Link	Embedded WAYF 	EDS  Shibboleth.
Independent from central server	✓		✓
Display only “valid” IdPs for SP		(✓)	✓
Search as you type feature			✓
Show Home Org Logo	(✓)		✓
Very easy deployment	✓	✓	✓
Can be used with old SPs	✓	(✓)	
Categories supported	(✓)	✓	
Caches last IdP selection across different services		✓	

# When to use what ?

Numbers of IdPs	Login Link(s)	Embedded WAYF <b>SWITCH</b>	EDS  Shibboleth.
<b>1 - 5</b>	✓	✓	✓
<b>1 - 50</b>		✓	✓
<b>1 - 500</b>			✓

# To mention: 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/>

