
SWITCH

The Swiss Education & Research Network

Integration of Resources

The AAI Team, aa@switch.ch

- Installation and Configuration
- Le tour de Resource Registry
- AAI-enabling IIS Web Servers
- AAI-enabling Apache Web Servers
- Already Adapted Web Applications



SWITCH

The Swiss Education & Research Network

Installation and Configuration

Patrik Schnellmann, schnellmann@switch.ch

- HOWTOs and Guides

<http://www.switch.ch/aai/howto/>

- Apache

- Linux (Debian stable)
- Solaris 8, 9, 10
- Mac OS X (10.4)

- IIS

- Windows Server 2003

Installation and Configuration Steps

1. Get X.509 Server Certificate
2. Install and configure Shibboleth Service Provider (SP)
3. Register SP in AAI Resource Registry
Get configuration files from Resource Registry
4. Install and configure federation metadata update script
5. Configure Shibboleth authentication (access rules)



SWITCH

The Swiss Education & Research Network

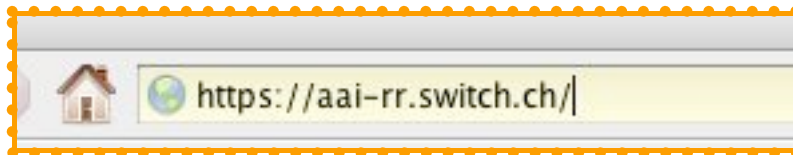
Le tour de Resource Registry

Lukas Hämmerle, haemmerle@switch.ch

Le tour de Resource Registry I

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



3 Complete the forms

a.)

Edit the Basic Information for new Resource

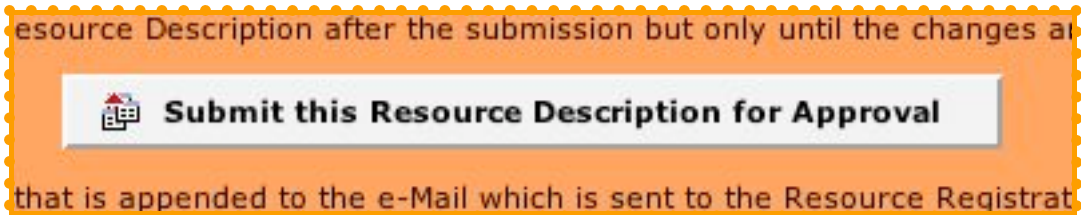
Basic Resource Information	
Home Organization *	switch.ch (SWITCHaai) <input type="text"/>
	<small>You only can register Resources for Home Organizations which you have Resource Registration Authority administrator for or for Home Organization</small>
Main language	English <input type="text"/>
Main Descriptive Name *	Test Resource
	<small>A name that briefly describes this resource, e.g. "e-Learning Moodle"</small>
Main Description *	This is a test resource <input type="text"/>

b.)

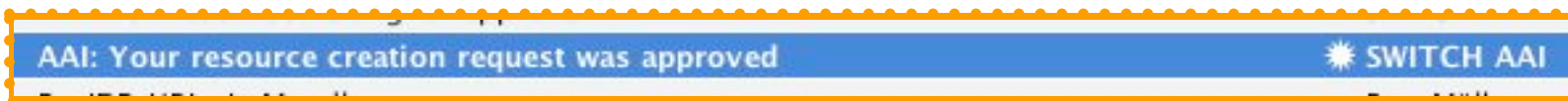
 Basic Resource Information	OK
 Multilingual Descriptions	Incomplete

Le tour de Resource Registry III

4 Submit resource description for approval



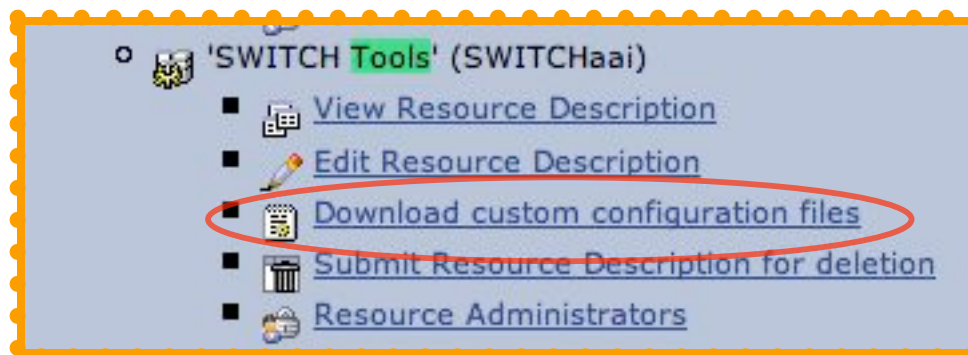
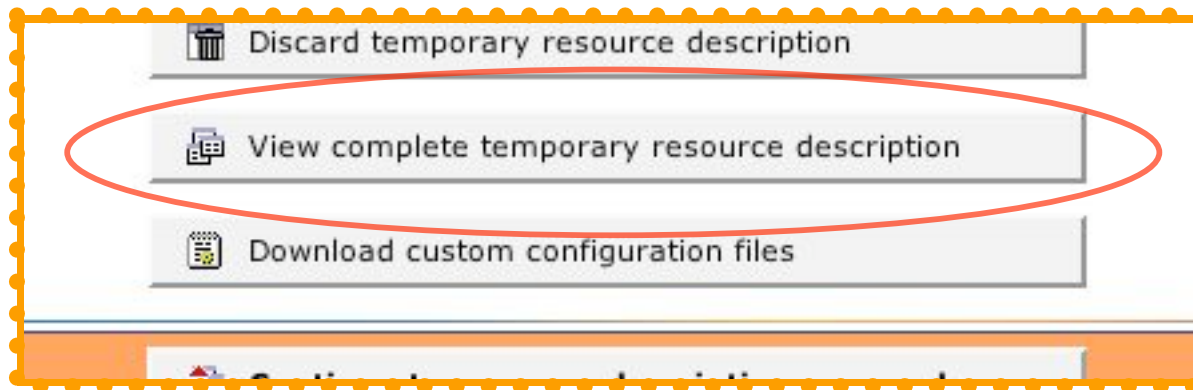
5 Resource Registration Authority administrator (RRA) checks and approves resource description



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>
```

- Resource Registry can generate custom SP configuration
- Configuration is ready for use “out of the box”



Configuration Download

configuration file for your Service Provider.

Configuration parameters

Installation setup	Linux, package installation	Set some default values for this form
Path to Shibboleth library *	Linux, manual installation	shibboleth-2.3.0
Path to certificate *	Windows	
	Mac OS X	
	Solaris	shibboleth-2.3.0
Path to private key *	Provide an absolute path to the certificate file that shall be used by Shibboleth.	
	/etc/ssl/private/tools.switch.ch.key	
	Provide an absolute path to the private key file that shall be used by Shibboleth.	
Download options	<input type="radio"/> Download configuration files as ZIP archive	
	<input checked="" type="radio"/> Download configuration files as TAR archive	
	<input type="radio"/> Only download shibboleth.xml	

The complete set of configurations files includes `shibboleth.xml`, `AAP.xml`, `shibd.logger`, `shibboleth.logger`, `native.logger`, the current `metadata.xml`, the `siterefresh` script and all Shibboleth HTML error pages.

After downloading the file:

1. Save and unpack the file in your Shibboleth configuration directory (e.g. `/etc/shibboleth/` or `C:\opt\shibboleth-sp\etc\shibboleth\`)
2. In order to automatically refresh the federation metadata, create a symlink from the `siterefresh.sh` script in the Shibboleth configuration directory to the `cron.daily` directory. Make sure the name of the symlink only contains alphanumeric characters, i.e. `ln -s /etc/shibboleth/siterefresh.sh /etc/cron.daily/siterefresh`
3. Restart your web server and the Shibboleth daemon
4. Define the web pages that shall be [protected by AAI](#)

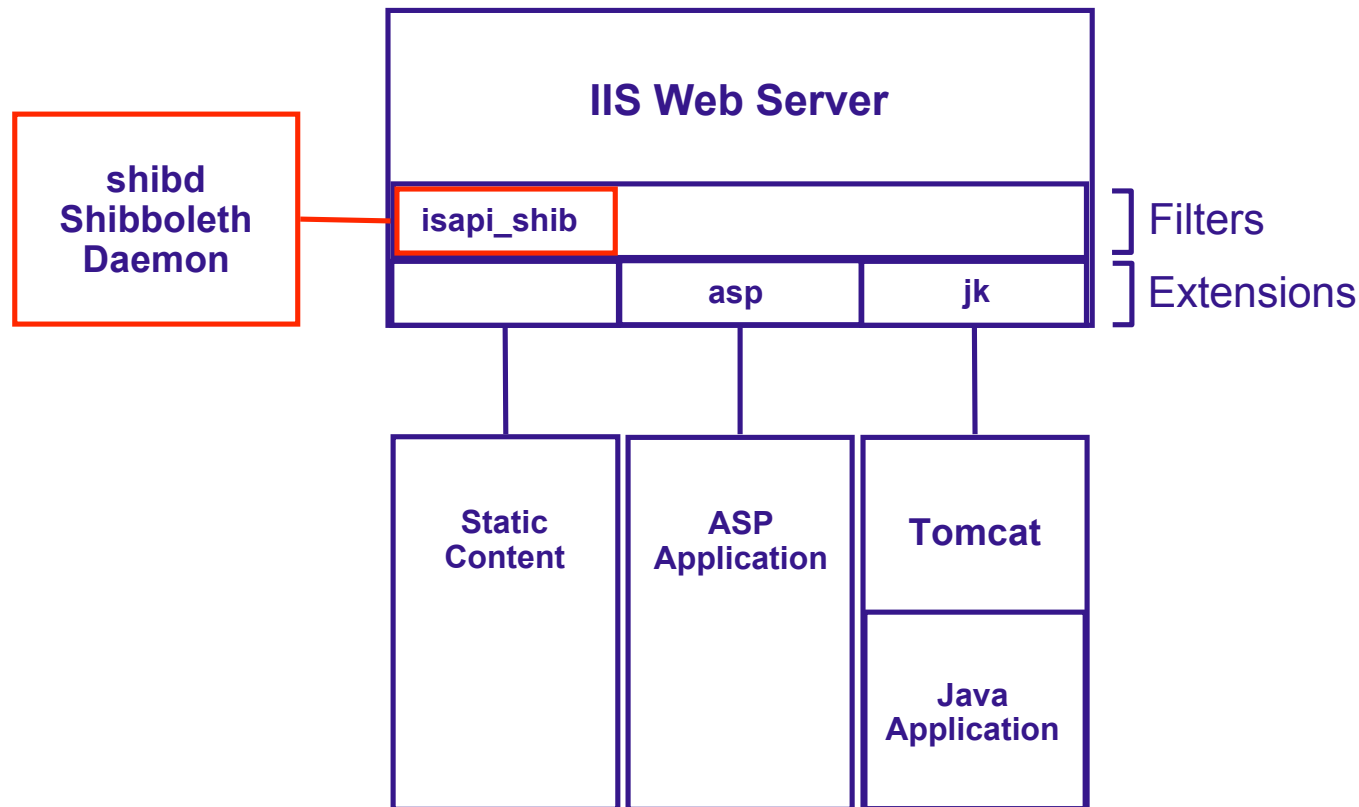
* denotes required field

SWITCH

The Swiss Education & Research Network

AAI-enabling IIS Web Servers

Patrik Schnellmann, schnellmann@switch.ch



⇒ On Windows, the components of the Shibboleth Service Provider are a service (shibd) and an ISAPI filter.

RequestMap in shibboleth.xml

```
<!-- ... -->
  <RequestMap applicationId="default">
    <Host name="my.sp.ch">
      <Path name="secure"
        requireSession="true"
        exportAssertion="false">
      </Path>
    </Host>
  </RequestMap>
<!-- ... -->
```

⇒ Requests for files in [http\(s\)://my.sp.ch/secure/](http(s)://my.sp.ch/secure/) require Shibboleth authentication.

XMLAccessControl in RequestMap (as of Shibboleth SP version 1.3b)

```
<!-- ... -->
  <Host name="my.sp.ch">
    <Path name="secure" authType="shibboleth" requireSession="true">
      <AccessControl>
        <AND>
          <OR>
            <Rule require="affiliation">staff</Rule>
            <Rule require="affiliation">student</Rule>
          </OR>
          <NOT>
            <Rule require="homeOrganizationType">vho</Rule>
          </NOT>
        </AND>
      </AccessControl>
    </Path>
  </Host>
<!-- ... -->
```

- ⇒ Users with any homeOrganizationType which is not vho and with affiliation staff or student and can access content in http(s)://my.sp.ch/secure/.



SWITCH

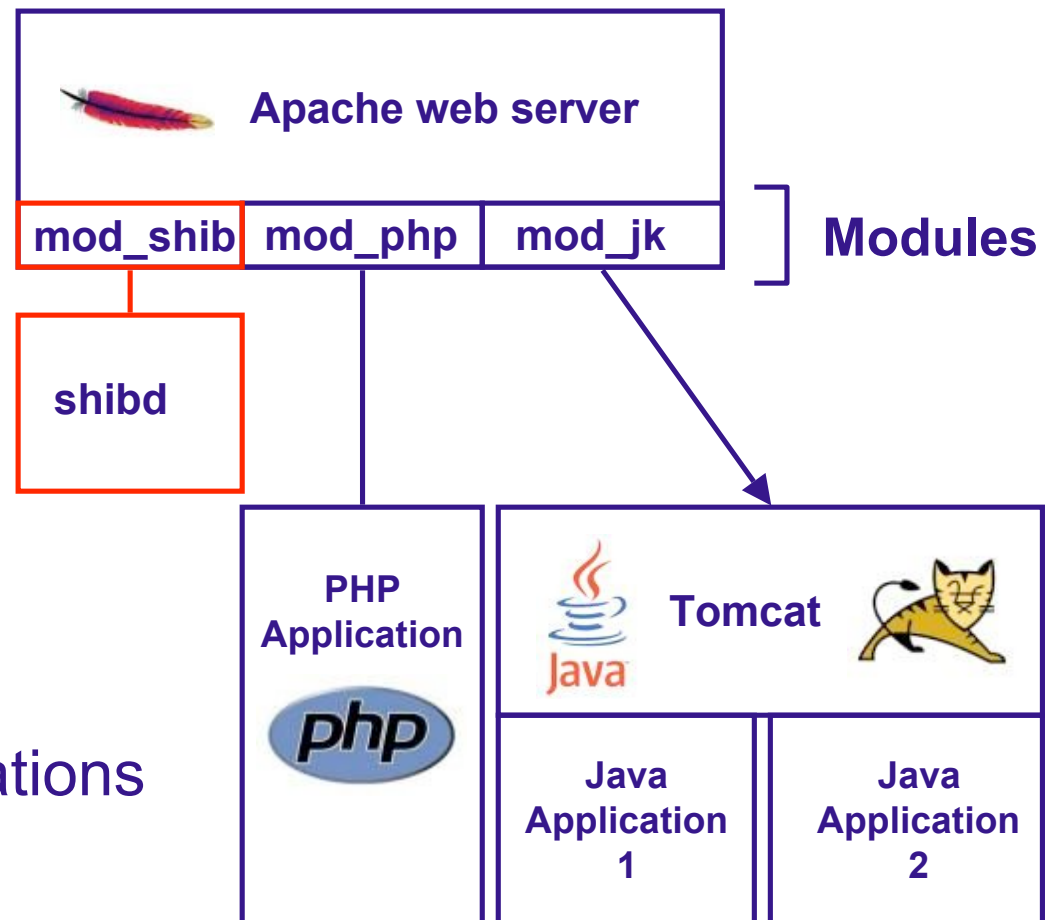
The Swiss Education & Research Network

Shibboleth-enabling Apache

Valéry Tschopp, tschopp@switch.ch

Shibboleth SP/mod_shib for Apache

- Runs on: Linux, Solaris, Windows, Mac OS X, FreeBSD, ...
- Protects web applications
- Gets attributes from shibd
 - Apache directives
 - Shibboleth XML Access rules
- Can authorize users with
 - Apache directives
 - Shibboleth XML Access rules
- Provides attributes to applications



Authorization with Apache require rules

Example rules in `httpd.conf` or `.htaccess`

Any AAI user

```
<Location /aai>  
  AuthType shibboleth  
  ShibRequireSession On  
  require valid-user  
</Location>
```

One specific user

```
<Files ~ "login.jsp|authorize.jsp">  
  AuthType shibboleth  
  ShibRequireSession On  
  require uniqueID 314592@aatest.switch.ch  
</Files>
```

All users except from VHO

```
<Directory /opt/www/aai>  
  AuthType shibboleth  
  ShibRequireSession On  
  require homeOrganizationType ~ ^[^\v][^\h][^\o]  
</Directory>
```

See <http://www.switch.ch/aai/support/serviceproviders/sp-access-rules.html>

Authorizing VHO users (Apache & IIS)

- How does a Service Provider know it's a VHO user?
- User specific attributes
 - UniqueID, Firstname, Lastname, Email
- Attributes common to all VHO users
 - HomeOrganization: `who-switchaai.ch`
 - HomeOrganizationType: `who`
 - Affiliation: `affiliate`
- Attributes specific for each individual VHO
 - Entitlement: `http://www.olat.unizh.ch/ifi/tuwien`

⇒ See <http://www.switch.ch/aai/join/vho.html>



SWITCH

The Swiss Education & Research Network

Already Adapted Web Applications

Valéry Tschopp, tschopp@switch.ch

- **WebCT CE 4, CE 6 and Vista**
Shibbolized through AAIportal
- **OLAT**
Native shibbolized, since version 3.0
- **Moodle**
Shibboleth authentication mostly implemented by SWITCH, since version 1.5
- **Various proprietary SVC-projects**
DOIT, VITELS, Alzheimerlearn
- **ILIAS**
Shibboleth authentication implemented by SWITCH, since version 3.3
- **Blackboard**
Working demo at Internet2, Project at Uni Luzern to adapt to SWITCHaai
- **Dokeos**
Project at Uni Geneva
- **BSCW**
Already used in production, official release with BSCW 4.4 expected
- **Claroline**
Co-developed by NTB and University of Neuchâtel

Shibboleth® Enabled Applications and Services

Main Shibboleth Site: shibboleth.internet2.edu

For corrections and additions to this table please contact <shib-info AT internet2 DOT edu>. On this page you will find:

Information Providers:	Learning Management Systems:	Other Systems:
<ul style="list-style-type: none">• ArtSTOR• CSA• Digitalbrain PLC• EBSCO Publishing• Elsevier ScienceDirect• ExLibris - SFX• ILIAS• JSTOR• NSDL• OCLC• Ovid Technologies Inc.• Project MUSE• Proquest Information and Learning• Serials Solutions• Thomson Gale• Useful Utilities - EZproxy	<ul style="list-style-type: none">• Blackboard• Moodle• OLAT• WebAssiqn• WebCT	<ul style="list-style-type: none">• Bodington.org• Condor• Confluence Wiki• Darwin Streaming Server• DSpace• eAcademy• Fedora• GridSphere• GridShib• Higher Markets• Horde• Hupnet• LionShare• Media Wiki• MyProxy• Napster• PHEAA• Sharepoint® from Microsoft• SYMPA• Symplcity• TurnItIn• TWiki• uPOrtal• Zope + Plone

Internet2 SEAS List: <https://wiki.internet2.edu/confluence/display/seas/Home>