



SWITCH

The Swiss Education & Research Network

Installation and Configuration

Patrik Schnellmann, <schnellmann@switch.ch>

- ❑ **HOWTOs and Guides**

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

- ❑ **Shibboleth Target Deployment Guides**

 - <http://www.switch.ch/aai/targetdeployment.html>

- ❑ **Apache**

 - ❑ **Compilation and Installation on Linux (debian stable)**

 - ❑ **Compilation and Installation on Solaris**

 - ❑ **Configuration Guide for Linux and Solaris**

- ❑ **IIS**

 - ❑ **Deployment Guide for Windows**

What you need to get...

- ❑ **Shibboleth Install Package:**

<http://www.switch.ch/aai/docs/shibboleth/internet2/1.2/>

- ❑ **Sample configuration files for SWITCHaai**

<http://www.switch.ch/aai/docs/shibboleth/SWITCH/1.2/>

- ❑ **SWITCHpki certificate for your Web Server**

<http://www.switch.ch/aai/certificates.html>

❑ shibboleth.switchhai.xml

❑ Identifier in <Applications>

providerId=urn:mace:switch.ch:SWITCHhai:pilot:{HOSTNAME}

❑ SWITCHpki Server Certificate Location in <Credentials>

/etc/apache/ssl.key/{HOSTNAME}.key

/etc/apache/ssl.crt/{HOSTNAME}.crt

❑ Error Pages Customization in <Errors>

supportContact={CONTACT_EMAIL}

HTML pages, logo and stylesheet

❑ SWITCHhai Federation Metadata

{FederationProvider} for sites.switchhai.xml

{TrustProvider} for trust.switchhai.xml

{AAPProvider} for AAP.switchhai.xml

- ❑ IIS specific settings in shibboleth.xml
 - ❑ Protected Web Locations in <RequestMapProvider> (Access Rules Configuration)
 - ❑ IIS Site ID Mapping in <Implementation>

□ SWITCHai Federation Metadata

- Accepted Certification Authority certificates within SWITCHai

⇒ trust.xml

- Home Organizations participating within SWITCHai

⇒ sites.xml

- More information:

<http://www.switch.ch/aai/metadata.html>

<http://www.switch.ch/aai/ca-acceptance-policy.html>

❑ Siteresh

- ❑ Shell script (Standard Linux shell / Windows Cygwin)
- ❑ Automatical updates of the Federation Metadata (sites.xml / trust.xml)
- ❑ Security given by verification of the files' signatures

❑ Get the script and documentation:

<http://www.switch.ch/aai/siteresh.html>



SWITCH

The Swiss Education & Research Network

AAI-enabling Apache

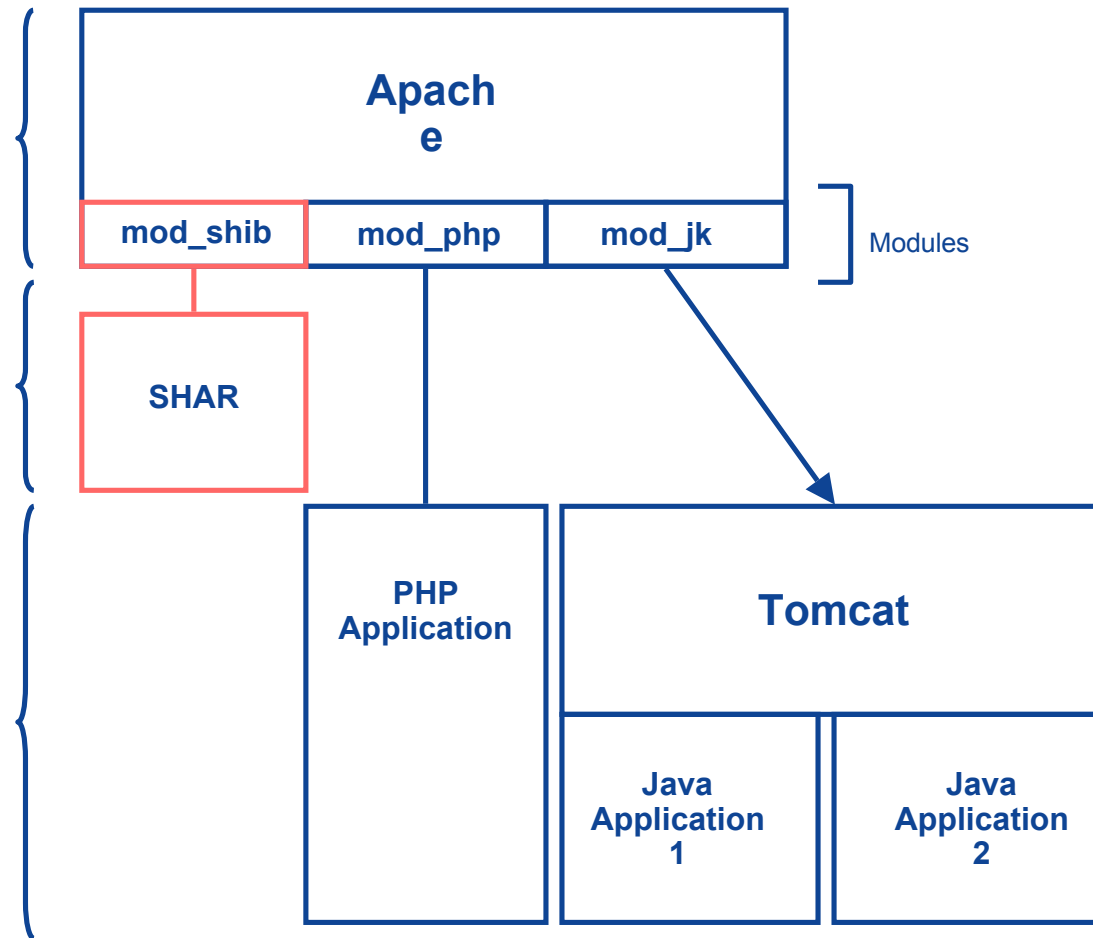
Patrik Schnellmann, <schnellmann@switch.ch>

Apache Software Components

- Apache Webserver
- Shibboleth Target (mod_shib)
- Tomcat Connector (mod_jk)
- PHP (mod_php)

- Shibboleth Target (SHAR)

- PHP Applications
- Java Applications (Tomcat, ...)



Static Authorization in Apache

Rules in `httpd.conf` or `.htaccess` for Shibboleth Target 1.2.1

Any AAI user

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

One user

```
<Location /restricted>  
AuthType shibboleth  
ShibRequireSession On  
require uniqueID 314592@aatest.switch.ch  
</Location>
```

All users except from VHO

```
<Location /secure>  
AuthType shibboleth  
ShibRequireSession On  
require homeOrganizationType ~ ^[^\vV][^\hH][^\oO]  
</Location>
```

Reference: <http://www.switch.ch/aai/docs/shibboleth/internet2/1.2/deploy-guide-target1.2.1.html#4.d>.



SWITCH

The Swiss Education & Research Network

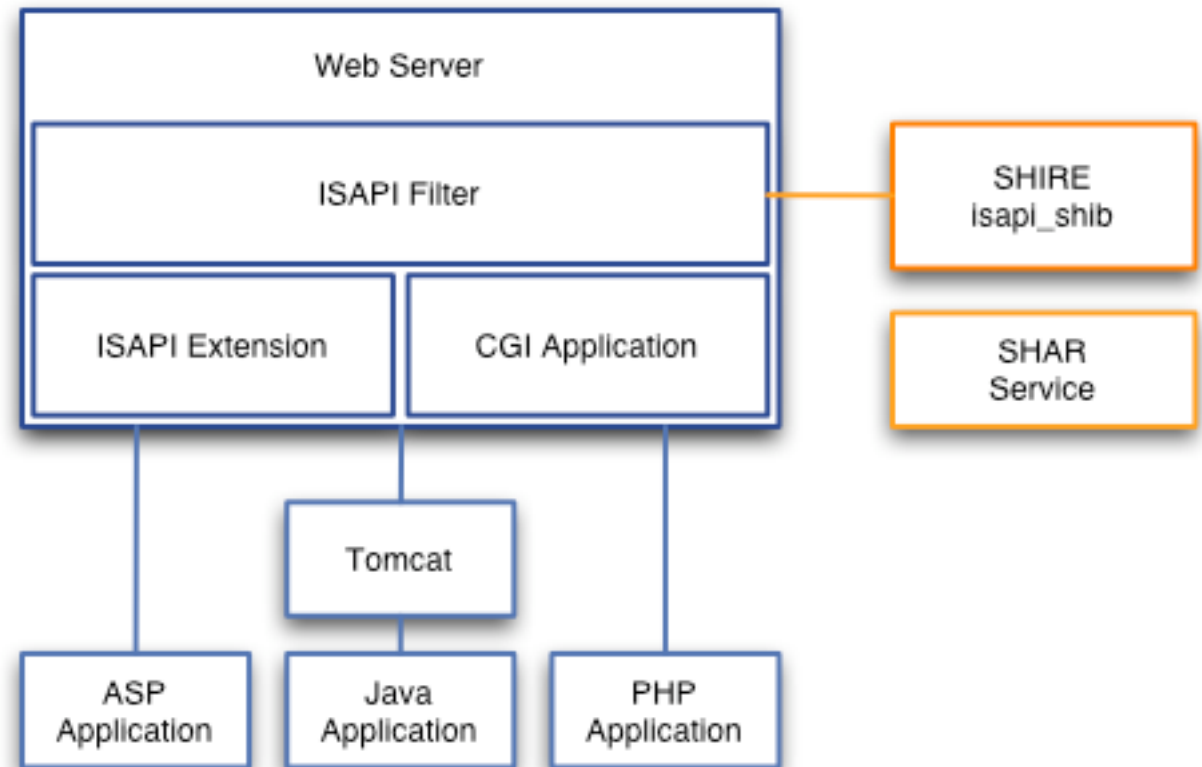
AAI-enabling IIS

Patrik Schnellmann, <schnellmann@switch.ch>

- IIS Web Server
- Shibboleth Target (isapi_shib)

- Shibboleth Target (SHAR)

- Tomcat via JK/JK2
- Dynamic Web Pages (ASP, Java, PHP, ...)



Configuring Access Rules in IIS

Rules in `shibboleth.xml` for Shibboleth Target 1.2.1

...

```
<RequestMap applicationId="default">  
  <Host name="some.host.ch">  
    <Path name="secure"  
      requireSession="true"  
      exportAssertion="false">  
    </Path>  
  </Host>  
</RequestMap>
```

...

⇒ `isapi_shib` forces authentication on requests for files in
`http://some.host.ch/secure/`

- ❑ In the current 1.2.1 version, access configuration is rather limited if compared with the Apache module
 - ❑ Fine grained access control has to be handled by the application

- ❑ The future version (1.3)
 - ❑ Is expected to provide more flexible access control rules
 - ❑ Will to be released mid 2005

Q & A

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

aai@switch.ch