

- **Home Organization**
- Resources
- Support
- Data protection
- Statistics
- Outlook 2008 - 2011

AAI at the University of Fribourg



Overview

SERVICE INFORMATIQUE

2004 : Start AAI project

1,7 persons dedicated to Home Organization, Service Provider, support and maintenance

October 2005 : Home Organization in production

Windows 2000 (WLB) / IIS 5 / Tomcat 4 / Shibboleth 1.3

2006 : Home Organization Upgrade

Migration → Windows Server 2003 (virtual machine) / IIS 6 / Tomcat 5 / Shibboleth 1.3

11.04.2007 : Shibbolethization of Moodle

11.08.2007 : Shibboleth update

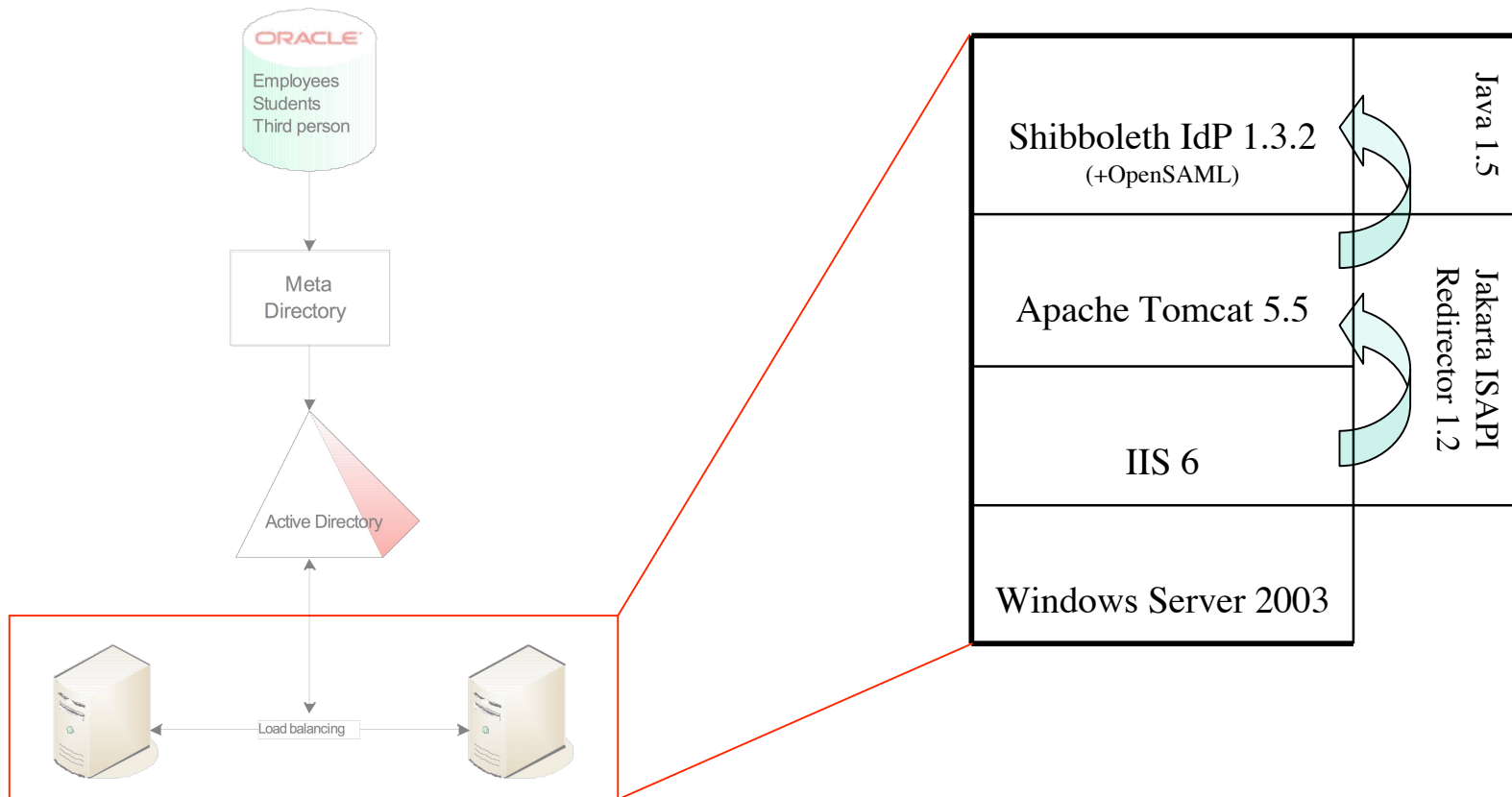
Shibboleth 1.3b → Shibboleth 1.3.2

AAI at the University of Fribourg

Home Organization infrastructure



SERVICE INFORMATIQUE



- Home Organization
- **Resources**
- Support
- Data protection
- Statistics
- Outlook 2008 - 2011

AAI at the University of Fribourg

Service Provider



SERVICE INFORMATIQUE

Two possibilities to protect a resource

1. Create your **own Service Provider**
 - E-Learning module (Vitels)
 - Moodle
 - Mailing list (Sympa)
 - Wiki
 - Student

2. Use the **web server** www.unifr.ch
 - Protect with an `.htaccess` file
 - Create a new host (www.chem.unifr.ch)

AAI at the University of Fribourg

Service Provider



SERVICE INFORMATIQUE

Several hosts in a same Service Provider



```
...
<RequestMapProvider type="edu.internet2.middleware.shibboleth.sp.provider.NativeRequestMapProvider">
  <RequestMap applicationId="default">
    <Host name="www.unifr.ch" authType="shibboleth" requireSession="false"/>
    <Host name="www.chem.unifr.ch" applicationId="www-chem" authType="shibboleth" requireSession="false"/>
  </RequestMap>
</RequestMapProvider>
...
<Applications id="default"
  providerId="https://www.unifr.ch/shibboleth"
  homeURL="https://www.unifr.ch/"
  xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  ...
    <Application id="www-chem"
      providerId="https://www.chem.unifr.ch/shibboleth"
      homeURL="http://www.chem.unifr.ch/">
    ...
  </Application>
</Applications>
...
```

- Home Organization
- Resources
- **Support**
- Data protection
- Statistics
- Outlook 2008 - 2011

AAI at the University of Fribourg

AAI support



SERVICE INFORMATIQUE

User Support

- Helpdesk, for administrative personnel
- Micromus, for students
- “Correspondants Informatiques” (Informatikkorrespondenten) in most departments

Different AAI Support places

- Web page
- Contact persons per Resource
- SiUF, for Resource Owners
- Switch

AAI at the University of Fribourg

AAI web page



SERVICE INFORMATIQUE

www.unifr.ch/aa

- News
- Support
- Administration

AAI Authentication & Authorization Infrastructure

switch aai

Helpdesk | Microms | HOME | ACCESS A RESOURCE | PROTECT A RESOURCE | DOCUMENTATION

AAI News

- ▶ 14.09.07 **Sympa is now AAI enabled**
Sympa, the electronic mailing list manager of University of Fribourg, was updated to support the AAI Login. Members of the SWITCHaai Federation may now login with their user-id and password.
- ▶ 11.08.07 **Maintenance service**
The AAI Service has been upgraded to the latest security level. Login forms include: email address, user-id, unifr<userid>, firstname.lastname, <userid>@unifr.ch, unifr/<userid>.
- ▶ 11.04.07 **Moodle is now AAI enabled**
The Moodle platform at the University of Fribourg has been moved to a new server at the address <http://moodle.unifr.ch>. It has been connected to the users directory and protected by the AAI system. Users of the University of Fribourg and other members of the SWITCHaai Federation will now login with their user-id and password.
- ▶ 03.04.07 **List of available resources**
A list of all [AAI enabled resources](#) is now available directly on the AAI site at Switch. Note that some resources may not be available to members of the University of Fribourg because of restrictions set by the resource provider, or because they require more user personal information than the University of Fribourg can provide.

Support issues

- You want to [access a resource](#) at a swiss university or any other institution integrated into the AAI
- You want to [protect a resource](#) at the University of Fribourg
- You are looking for [documentation](#) about the AAI

Administration

- Click [here](#) to reset your authorizations to send your personal information to Service Providers
- [Test your configuration](#) : a simple application at the University of Fribourg will show your personal information. No personal information is sent to an external provider.
- Click [this link](#) to disable (or re-enable if you disabled it) your AAI Enrolment. Check our [Digital ID Card information page](#) for more information.

Université de Fribourg - Universität Freiburg - Bd de Pérolles 90 - 1700 Fribourg
contact: aai-support@unifr.ch - updated 18.09.2007 - Hits: 4844

AAI Info Day, 29.11.2007

AAI at the University of Fribourg

AAI support page



SERVICE INFORMATIQUE

Support

Information on the resources availability

Hints to protect a resource with the AAI:

Using the web server www.unifr.ch

- Create an .htaccess file
- That's it

Creating your **own Service Provider**

- Accept and sign the agreement
- Install Shibboleth + certificate
- Register the Resource in the Resource Registry
- Protect it via .htaccess or shibboleth.xml

A screenshot of the AAI support page from the University of Fribourg. The page title is 'Protect a resource with the AAI'. It contains a warning about confidentiality, instructions on how to use the web server www.unifr.ch, and a section for creating a new Service Provider. The instructions for creating a Service Provider are numbered 1 through 7, covering steps from accepting an agreement to protecting the resource. The page also includes a 'More details?' section with links to PDF documents.

AAI
Authentication & Authorization
Infrastructure

Helpdesk | Micromas | HOME | ACCESS A RESOURCE | PROTECT A RESOURCE | DOCUMENTATION

Protect a resource with the AAI

As of February 2007, there are two possibilities to protect a resource: use the web server www.unifr.ch or create your own Service Provider.

Warning: In both cases, the data obtained through the AAI must remain confidential and must NOT be forwarded to third party as required by the data protection law.

Use the web server www.unifr.ch

The server www.unifr.ch is now AAI-enabled. This means that documents or folders on your site can be protected through Shibboleth. If you do not have a site, you may order one using the form available at <http://www.unifr.ch/weboffice>.

- 1 The first step is to upload the documents to your site. We strongly suggest that you create a dedicated directory which will be used as an AAI-protected zone in your site.
- 2 The second and last step is to protect your directory or documents. This is simply done by adding a file called `.htaccess` in your directory. This file will contain the necessary instructions of what is to be protected. Detailed examples are shown below.
- 3 That's it. Your documents are now AAI-enabled, or in other words, they are protected by Shibboleth. Only authenticated users from the organizations that you defined in the `.htaccess` file will be allowed to see them. You need not care about users' and passwords, this is done by the AAI System.

Create your own Service Provider

- 1 Accept, sign and return the [agreement](#) for the creation of a new Service Provider.
- 2 Download and install [Shibboleth 1.3](#) Service Provider software.
- 3 Obtain and install a certificate.
- 4 Configure Shibboleth and your web server.
- 5 Register your new resource in the [Resource Registry](#).
- 6 Update two files:
 - `metadata SWITCHAAI.xml` which contains the list of all Resources and Identity Provider in the SwitchAAI federation.
 - `app SWITCHAAI.xml` which contains the list of all AAI Attributes necessary for your resource.
- 7 Protect your resource:
 - For an Apache Server you can use
 - `.htaccess` file
 - `apache2.conf` file
 - `sites-enabled` directory
 - `mod_shib.conf` file
 - For an IIS Server, use the `shibboleth.xml` file ([Shibboleth Wiki](#)).

More details?

See the PDF document about "[how to use www.unifr.ch](#)" or the guides about "[Service Provider Deployment](#)"

AAI at the University of Fribourg

AAI documentation page



SERVICE INFORMATIQUE

Documentation

- What is the AAI
- Convenience
- Data protection
- How does it work
- The culture zone

The screenshot shows a web page with a blue header containing the text 'AAI Authentication & Authorization Infrastructure' and a navigation menu with links: 'Helpdesk', 'Micromus', 'HOME', 'ACCESS A RESOURCE', 'PROTECT A RESOURCE', and 'DOCUMENTATION'. The main content area is titled 'The culture zone' and includes the following text:

or: what does Shibboleth mean ?...

Collins Dictionary 1992:

"*Shibboleth*: noun - a custom, phrase or use of language that acts as a test of belonging to, or as a stumbling block to becoming a member of, a particular social class, profession, etc (from Hebrew; literally: ear of grain; the word is used in the Old Testament by the Gileadites as a test word for the Ephraimites, who could not pronounce the sound "sh")" - s.a. [The story of the Shibboleth](#)

Online Etymology Dictionary, 2001:

1382, the Heb. word shibboleth "flood, stream," also "ear of corn," in Judges XII:4-6. It was the password used by the Gileadites to distinguish their own men from fleeing Ephraimites, because Ephraimites could not pronounce the -sh- sound. Figurative sense of "watchword" is first recorded 1638, and it evolved by 1862 to "outmoded slogan still adhered to." A similar test-word was *cicera* "chick pea," used by the Italians to identify the French (who could not pronounce it correctly) during the massacre called the Sicilian Vespers (1282).

Le livre des Juges / The Book of the Judges, 12:4-6:

<p>⁴ Jephthé rassembla tous les hommes de Galaad, et livra bataille à éphraïm. Les hommes de Galaad battirent éphraïm, parce que les éphraïmites disaient : Vous êtes des fugitifs d'éphraïm ! Galaad est au milieu d'éphraïm, au milieu de Manassé !</p>	<p>⁴ Then Jephthah gathered together all the men of Gilead, and fought with Ephraim; and the men of Gilead smote Ephraim, because they said, Ye Gileadites are fugitives of Ephraim among the Ephraimites, and among the Manassites.</p>
<p>⁵ Galaad s'empara des gués du Jourdain du côté d'éphraïm. Et quand l'un des fuyards d'éphraïm disait : Laissez-moi passer ! les hommes de Galaad lui demandaient : Es-tu éphraïmite ? Il répondait : Non.</p>	<p>⁵ And the Gileadites seized the passages of the Jordan before the Ephraimites; and it was so, that when those Ephraimites who had escaped said, "Let me go over," that the men of Gilead said unto him, "Art thou an Ephraimite?" If he said, "Nay",</p>
<p>⁶ Ils lui disaient alors : Hé bien, dis Schibboleth. Et il disait Sibboleth, car il ne pouvait pas bien prononcer. Sur quoi les hommes de Galaad le saisissaient, et l'égorgeaient près des gués du Jourdain. Il périt en ce temps-là quarante-deux mille hommes d'éphraïm.</p>	<p>⁶ Then said they unto him, "Say now 'Shibboleth.'" And he said "Sibboleth," for he could not frame to pronounce it right. Then they took him and slew him at the passages of the Jordan; and there fell at that time of the Ephraimites forty and two thousand.</p>

- Home Organization
- Resources
- Support
- **Data protection**
- Statistics
- Outlook 2008 - 2011

AAI at the University of Fribourg

Data protection



SERVICE INFORMATIQUE

Four security levels

1. **Encryption and certificates**

SSL is used for every transaction, in conjunction with a dedicated certificate for each server

2. **AAI (un-)enrolment**

A user can refuse to send his information to any AAI resource

3. **Digital ID card**

A user can refuse to send his information to a particular resource

4. **ARP – Attribute Release Policy**

The IdP and the RRA (Resource Registration Authority) Admin can define which attributes are released to a specific resource

AAI at the University of Fribourg

Data protection : AAI (un-)enrolment



SERVICE INFORMATIQUE

On the AAI web site, a user can disable (or re-enable) his AAI enrolment.

Administration

Click [here](#) to reset your authorizations to send your personal information to Service Providers

Test your configuration : a simple application at the University of Fribourg will show your personal information. No personal information is sent to an external provider.

Click [this link](#) to disable (or re-enable if you disabled it) your AAI Enrolment. Check our [Digital ID Card information page](#) for more information.

AAI Enrolment

Account **clemenfa** is currently **enrolled**

Following **Attributes** are available from UniFr:

Unique ID	ub93kc84@unifr.ch
Surname	Clément
Given name	Fabrice
E-mail	fabrice.clement@unifr.ch
Business postal address	Bd de Pérolles 90 CH-1700 Fribourg
Business phone number	+41 26 300 7245
Home Organization	unifr.ch
Home Organization type	university
Affiliation	staff
Study branch 3	
Study level	
Staff category	11

AAI Enrolment

Account **clemenfa** is currently **not enrolled**

AAI at the University of Fribourg

Data protection: locking a particular resource



SERVICE INFORMATIQUE

Before the very first connection, the user must accept the Terms Of Use

Before the first connection to a resource, the user can:

- Check his information (no modification allowed)
- Accept or decline to send his information

If a change occurs in the information sent to a resource, the Digital ID card will be displayed again.

The granularity level is limited to the resource. It is not possible to choose which attribute is sent to a resource.

No personal information is saved in Log files and the user name is md5 encrypted

Digital ID Card	
Nom de Famille	Clément
Prénom	Fabrice
Unique ID	ub93kc84@unifr.ch
Organisation	unifr.ch
Type d'Organisation	university
Catégorie du Personnel	11
Email	fabrice.clement@unifr.ch
Téléphone Professionnel	+41 26 300 7245

AAI at the University of Fribourg

Data protection: resource locking through ARP



SERVICE INFORMATIQUE

See the table **Attribute use & audience** to display the attributes required by resources

Create specific rules in the configuration file of the script used for the ARP update

Examples with the resource `aai-viewer.switch.ch`

Send UniqueID and refuse DateOfBirth

ProviderID `https://aai-viewer.switch.ch/shibboleth`
 urn:mace:switch.ch:attribute-def:swissEduPersonUniqueID permit
 urn:mace:switch.ch:attribute-def:swissEduPersonDateOfBirth deny

Send no attribute

ProviderID `https://aai-viewer.switch.ch/shibboleth` deny

Home Organization	Resource	Federated User	UniqueID	DateOfBirth	Other Attributes	Audience
switch.ch	SPN Moodle	R	R	R	R	R
switch.ch	Bibliothèque scientifique commune UNL-EPFL	R	R	R	R	R
switch.ch	Tesquila	R	R	R	R	R
switch.ch	AAIproxy ETHZ	R	R	R	R	R
switch.ch	e-collection III Test	R	R	R	R	R
switch.ch	EBSCO Information Services	X				
switch.ch	Erekschung-System lim-S	R	R	R	R	R
switch.ch	EDN Zurich	R	R	R	R	R
switch.ch	ETH Alumni Student Login	X				
switch.ch	ETHZ, ID, AAI-Portal	R	R	R	R	R
switch.ch	ETHZ, ID, Compocampus	R	R	R	R	R
switch.ch	ETHZ, ID, Linkchecker for Zope/Sive WOMS sites	R	R	R	R	R
switch.ch	ETHZ, ID, Floor Men's Spammer	R	R	R	R	R
switch.ch	ETHZ, ID, Sympa Mailman	R	R	R	R	R
switch.ch	ETHZ, ID, VIP Software Distribution	R	R	R	R	R
switch.ch	ETHZ, NET, Application Form BSCW Pro	R	R	R	R	R
switch.ch	ETHZ, NET, Application Form BSCW Pro	R	R	R	R	R
switch.ch	ETHZ, NET, SLAC Server	R	R	R	R	R
switch.ch	ETHZ, NET, DVP Moodle Server	R	R	R	R	R
switch.ch	ETHZ, NET, Moodle Server	R	R	R	R	R
switch.ch	Neptun Store	R	R	R	R	R

- Home Organization
- Resources
- Support
- Data protection
- **Statistics**
- Outlook 2008 - 2011

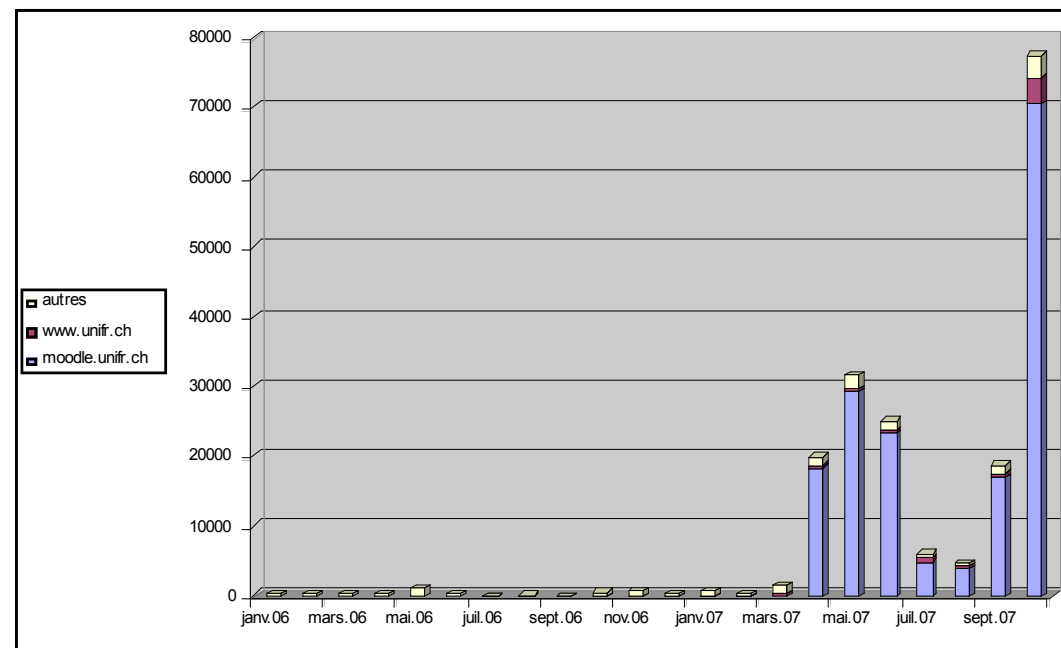
AAI at the University of Fribourg

Connections since January 2006



SERVICE INFORMATIQUE

Service Provider	Oct.07	Since Jan. 06
moodle.unifr.ch	70 678	168 115
www.unifr.ch	3 699	6 767
diufpc200.unifr.ch		413
lists.unifr.ch	121	181
diufpc215.unifr.ch	2	113
sr-svx-40.unifr.ch	10	23
student.unifr.ch	10	13
www.chem.unifr.ch		3



AAI at the University of Fribourg

22 failures in 2 years, no service breakdown



SERVICE INFORMATIQUE

Date	Error	Reason
10.10.2005	Shire failure	Configuration problem
24.10.2005	AAI login	Enrollment problem
13.02.2006	HTTP error 403	Certificate problem
21.02.2006	WebCT Vista no access	Configuration problem
06.03.2006	No connection to any external resources	Certificate problem
16.05.2006	HTTP error 403.16	Certificate problem
29.05.2006	LDAP simple bind failed	Certificate problem
05.09.2006	No answer from Attribute viewer	Configuration problem of the SP
05.09.2006	HTTP error 403.13	Certificate problem
06.11.2006	AD connection problem	Network problem
19.12.2006	Session creation failure	Clock skew
21.01.2007	Endless loop on redirection	Configuration problem of the SP
10.02.2007	Cannot download VPN	Shibboleth daemon problem
26.02.2007	SSL error	Configuration problem of the SP
14.03.2007	Remote User Filter name.firstName	Update remoteUserFilter
03.04.2007	Download VPN not ok with Firefox	URL problem
31.05.2007	No attributes	Certificate problem
25.06.2007	Olat sends IP address	Certificate problem
06.07.2007	2 ids for one person	Administration account problem
12.09.2007	No attribute sent to phbern	Wrong configuration
13.09.2007	Shib SP event every 29h	ISAPI filter
23.10.2007	Authorization failed	Certificate problem



- Home Organization
- Resources
- Support
- Data protection
- Statistics
- **Outlook 2008 - 2011**

AAI at the University of Fribourg

Outlook 2008 - 2011



SERVICE INFORMATIQUE

→ 31.03.2008

Wrap up initial AAI project

December 2007 : projects planning

AAA : Accounting in AAI

Virtual Home Organization

Grid Middleware

E-learning

SharePoint with Shibboleth

Repository (user-friendly management of access rights for AAI protected documents)

Collaboration with EIA-FR

January 2008 : Choice of projects for period 2008 – 2011

1.4.2008 →

Start new project

AAI at the University of Fribourg

Questions ?



SERVICE INFORMATIQUE

Q & A