AAI at the University of Fribourg

UNIVERSITAS FRIBURGENSIS

SERVICE INFORMATIQUE

- **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

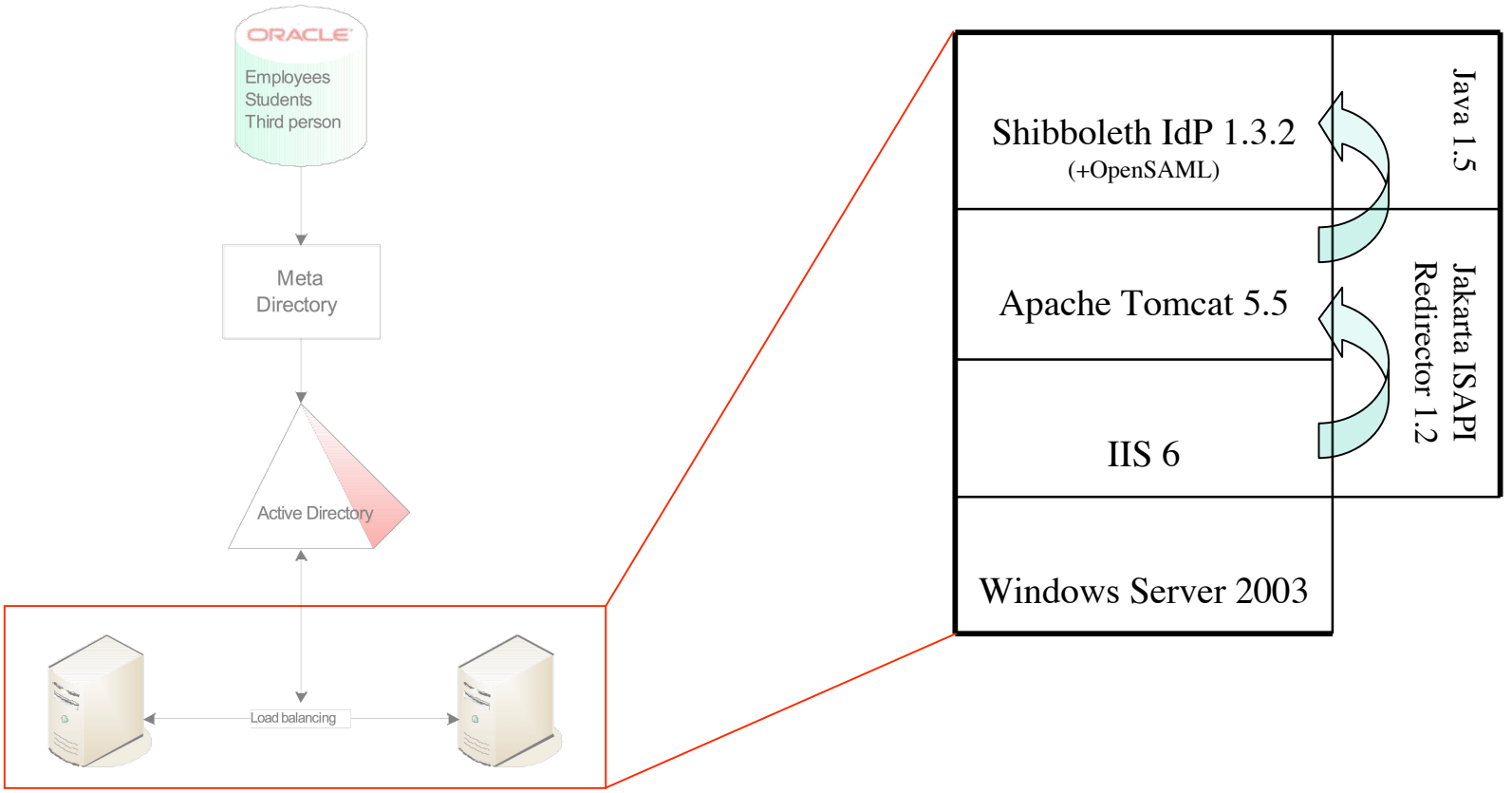
11.08.2007 : Shibboleth update

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 ressource

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

UNIVERSITAS FRIBURGENSIS

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

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

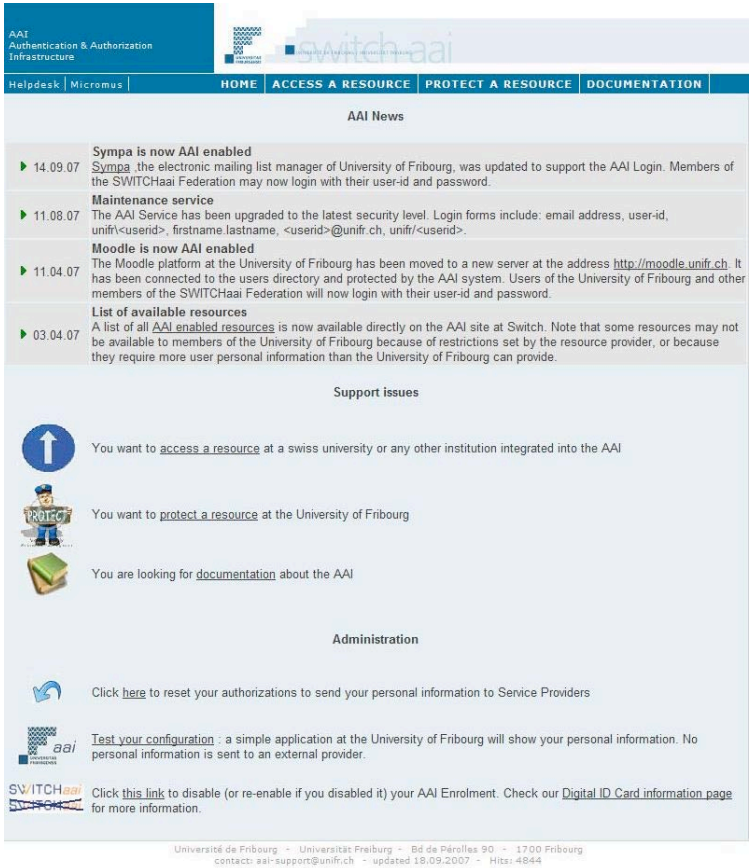
AAI web page

UNIVERSITAS FRIBURGENSIS

SERVICE INFORMATIQUE

www.unifr.ch/aai

- News
- Support
- Administration



AAI at the University of Fribourg

AAI support page

UNIVERSITAS FRIBURGENSIS

SERVICE INFORMATIQUE

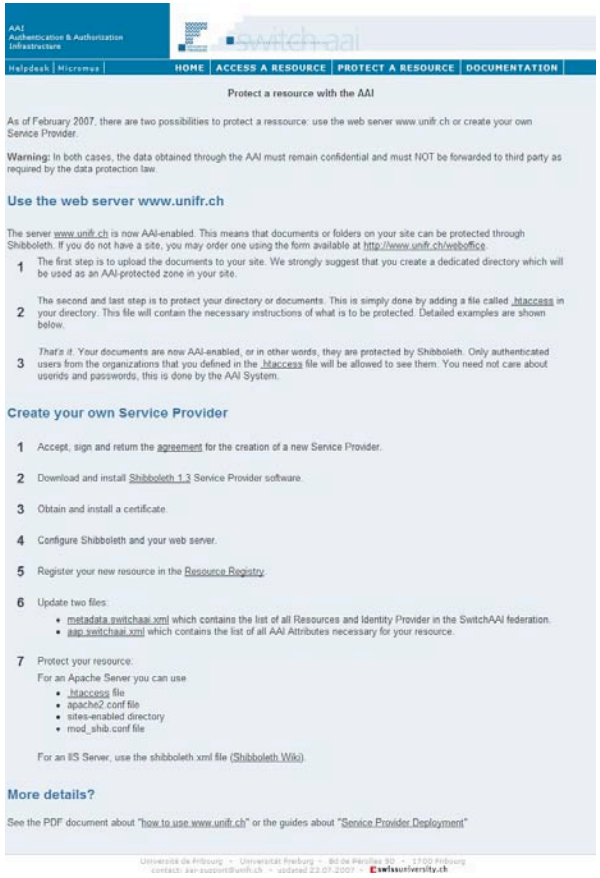
Support

Information on the resources availabilty

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


AAI Authentication & Authorization Infrastructure

switch aai

Helpdesk | Micromus | 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 ressource: 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 userids 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.
   - aap.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"

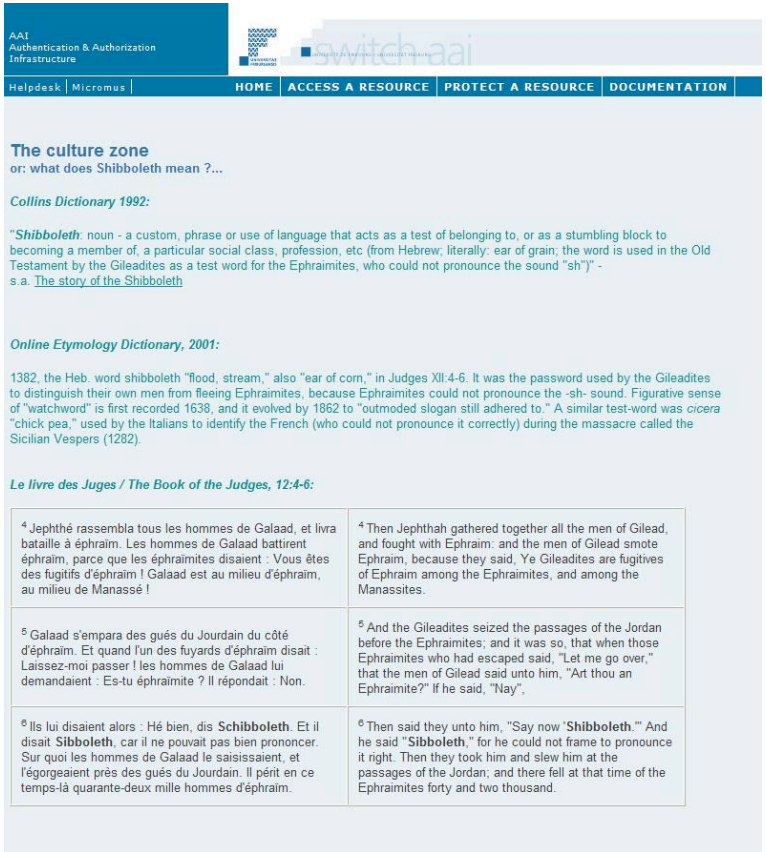
AAI at the University of Fribourg

AAI documentation page

SERVICE INFORMATIQUE

Documentation

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



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

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**

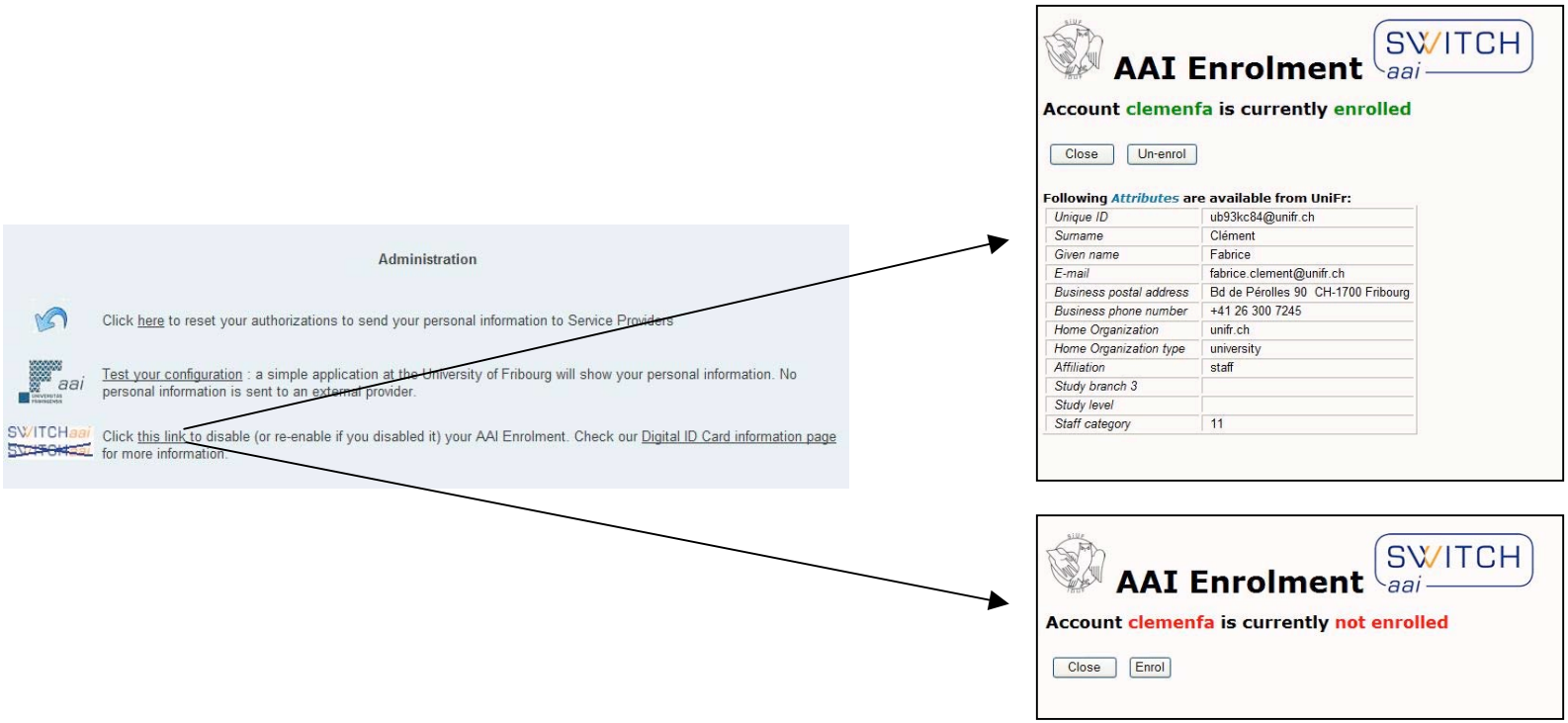
   The IdP and the RRA (Resource Registration Authority) Admin can define which attributes are released to a specific resource

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.



AAI at the University of Fribourg

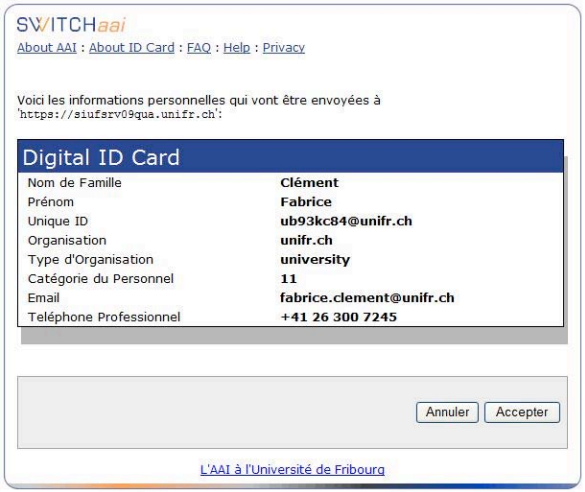
Data protection: locking a particular resource

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

AAI at the University of Fribourg

Data protection: resource locking through ARP

UNIVERSITAS FRIBURGENSIS

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

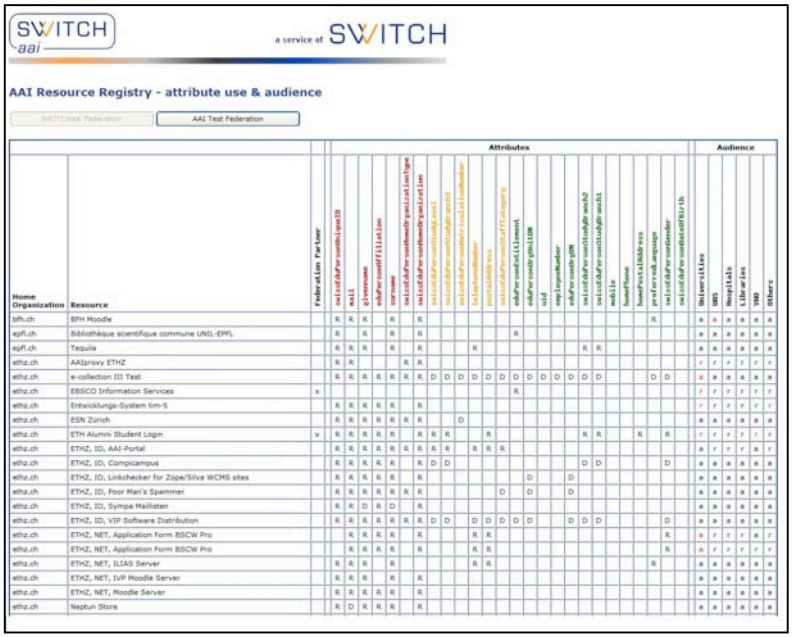
Examples with the resource *aai-viewer.switch.ch*

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

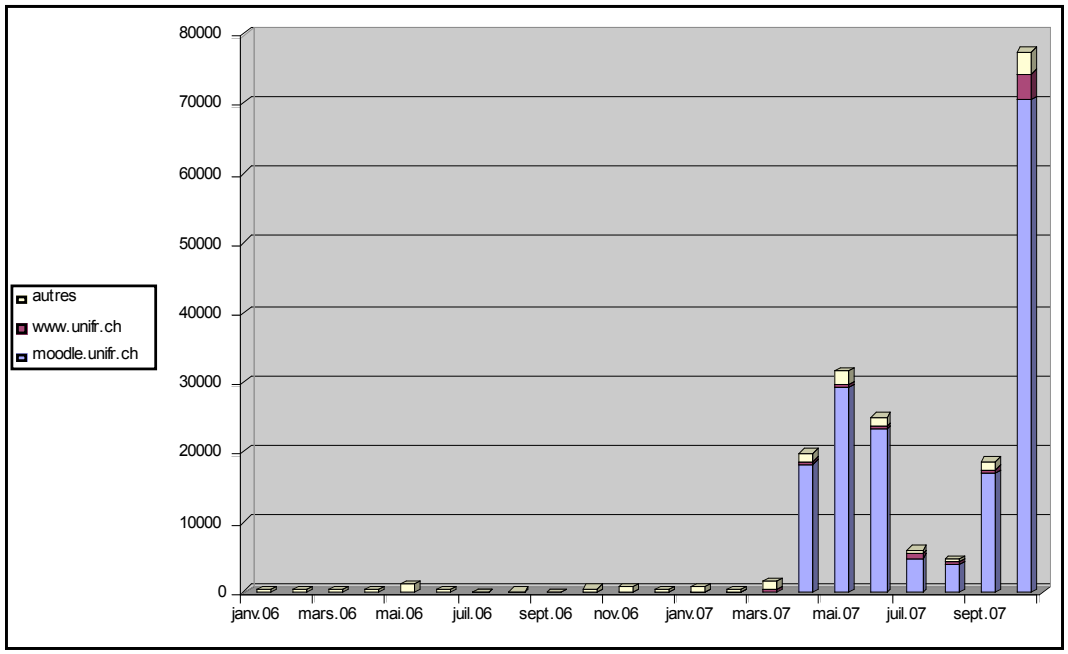
AAI at the University of Fribourg

Connections since January 2006

UNIVERSITAS FRIBURGENSIS

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



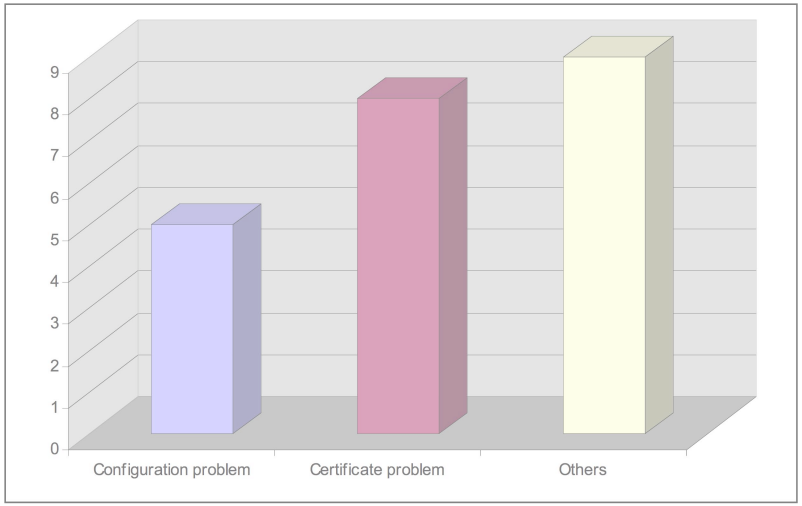
AAI at the University of Fribourg

22 failures in 2 years, no service breakdown

UNIVERSITAS FRIBURGENSIS

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 deamon 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

Q & A