AAI – Authentication and Authorization Infrastructure

Results of the Pilot Phase

Document management

Version/status:	1.1 / final	
Date:	3-FEB-2004	
Author(s):	Christoph Graf	SWITCH
	Ueli Kienholz	SWITCH
	Thomas Lenggenhager	SWITCH
	André Redard	at rete ag
	Daniela Isch	at rete ag
File name:	AAI_Pilot_Results_v11.doc	
Replacing:		
Approved by:		

Table of Contents

1. Management Summary

The idea of developing and implementing an Authentication and Authorization Infrastructure (AAI) for the higher education community in Switzerland goes back to an inter-university study group in 2001. An ensuing preparatory study carried out by SWITCH in 2001/2002 had concluded with the recommendation to start a pilot phase, the main goal of which should be to gain practical experience with pilot implementations in order to decide on the definitive selection of an architecture. At the end of the phase, technical, organizational and legal feasibility as well as the benefits of an AAI were to be presented, preferably with pilot projects to serve as show cases.

The pilot phase was started in September 2002. Originally meant to go from July 2002 to June 2003, it was extended until end of 2003 due to the late availability of the selected software. Thanks to the valuable contribution of members of various organizations who committedly teamed up in task forces or worked on their pilot projects, the pilot phase closed successfully.

Results:

- The three candidates, Tequila, Shibboleth and PAPI that were evaluated all had the required functionality and there was no clear leader. Shibboleth was finally selected because international commitment to the architecture was given top priority, while present shortcomings regarding the Attribute Release Policy (ARP) were considered to be of minor importance.
- The parties involved in the operation of Shibboleth components are Home Organizations, Resource Owners and the Service Provider SWITCH. The project team has described the specific tasks that need to be carried out by the parties when participating in the AAI.
- A set of authorization attributes that will be exchanged across organizations has been defined. The pilot projects confirmed that organizations are able to provide these attributes out of existing databases. Sample configuration files are available.
- Since the communication between AAI systems is secured by using SSL, X.509 server certificates are needed. A model for a CA infrastructure which can be extended in the future has been worked out. SWITCH is going to offer a CA service for server certificates.
- The AAI not only requires a legal framework which allows participants to exchange information, but also the mutual trust of organizations. An organizational construct has been developed which serves these purposes by setting up rules for the participants' behavior by means of service agreements and a policy document. Moreover, the project management has specified the roles and tasks of all AAI participants as well as the processes involved.
- An AAI Base Package has been defined with services for all participants of the AAI. In addition, optional AAI services have been developed which can be ordered separately on demand.
- Contrary to what the preparatory study had postulated, the SUK is not in the position to make a decision which regulates data protection and liability issues among organizations. Therefore, a new legal framework has been defined, requiring a bilateral Service Agreement between SWITCH and each participating Home Organization. A survey carried out by the SUK among all the universities showed that the AAI can be operated within the legal boundaries already in force, but that some organizations will have to adapt their "Acceptable Use Policy".
- The integration of the Home Organizations turned out to be easier than expected. By the end of the pilot phase, several Home Organizations had successfully AAI-enabled their existing user directories containing all their users and students.
- While some resource integration projects did not encounter any major difficulties, others turned out to be rather tricky. This led to the development of tools such as the AAI Portal and the AAI Proxy so that there are now three possible ways of integrating a resource within the AAI.

- A cost estimation model has been defined and rough cost estimates for initial and recurring cost are given which may help the organizations to define their own AAI budget. In order to partly finance the implementation of AAI from 2004 to 2006, SWITCH has applied for subsidies at SUK.

Recommendation:

Project team and steering committee consider the AAI a feasible solution for authentication and authorization of access to web resources. They recommend SWITCH to offer the AAI Service Base Package and to extend the service range on demand. Consequently, they recommend organizations to order the AAI Service with SWITCH and to integrate their resources, authentication systems and user directories in the AAI.

They also recommend SUK to support the building of a nationwide AAI by granting the subsidies applied for by SWITCH.

2. Introduction

The implementation of an Authentication and Authorization Infrastructure (AAI) is a means to simplify inter-organizational access to networked services. The core functionality of an AAI is to tightly couple the three basic interactions between a user, his or her Home Organization and a Resource during the authentication and authorization process. These three basic interactions are user authentication, access request and delivery of authorization attributes from the Home Organization to the Resource, as shown in Figure 1:

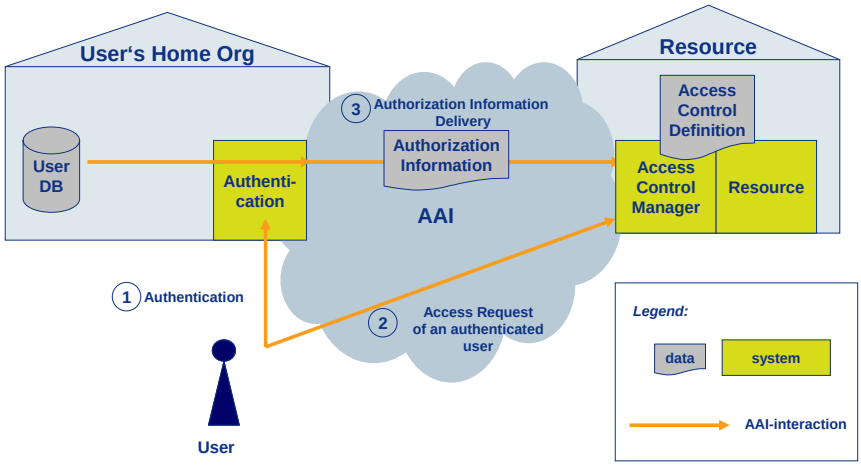

Figure 1: AAI model

The preparatory study [AAIStudy] carried out in the study phase of 2001/2002 attested that the AAI project was promising and could not identify any show stoppers. It concluded with the recommendation to start a pilot phase, the main goal of which would be to gain practical experience with pilot implementations in order to decide on the definitive selection of an architecture. At the end of this phase, technical, organizational, and legal feasibility as well as the benefits of an AAI were to be presented, preferably with a pilot project to serve as show case.

The AAI steering committee followed the recommendation and started the pilot phase in September 2002. The document at hand briefly sums up its course and results.

3. Goals

The goals of the pilot phase were defined as follows:

- gain practical experience with pilot implementations;
- decide on an AAI architecture;
- confirm technical and organizational feasibility;
- implement a show case;
- specify the first AAI Release;
- specify AAI services;
- work out a more in-depth cost estimation for the implementation phase; and
- implement the legal framework with all parties involved.

4. Course of the Pilot Phase

Originally, the pilot phase was planned to go from July 2002 to June 2003; due to the late availability of the selected software, however, the AAI steering committee decided to extend the pilot phase until end of 2003.

Figure 2 shows the project organization during the pilot phase:

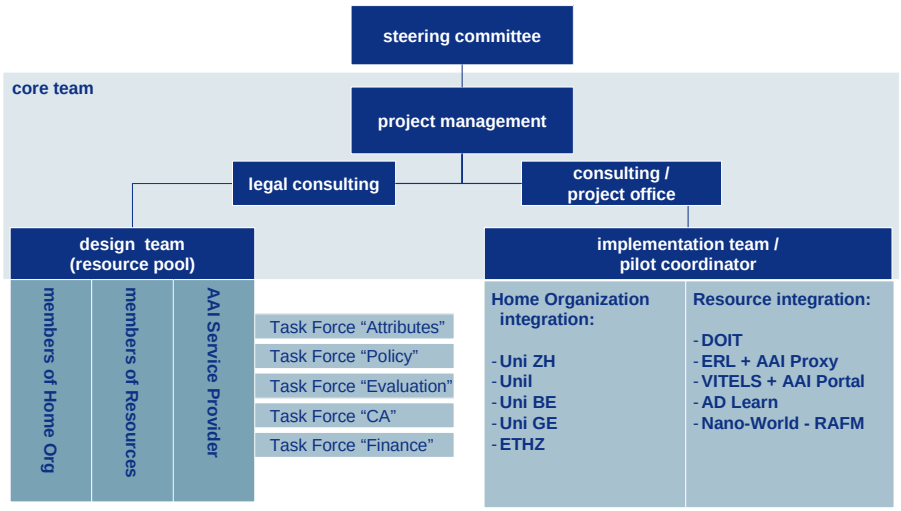

Figure 2: Project organization

The design team consisted of a pool of members of Home Organizations, Resource Owners, the AAI Service Provider and the pilot project teams. Out of this pool, several task forces formed as required to tackle tasks such as architecture evaluation, the definition of authorization attributes, costs estimation and financing, CAs, or the drawing up of an AAI policy. The latter was later revised and integrated into the overall legal framework by the legal consulting team.

The implementation team consisted of a number of pilot project teams led by pilot project leaders as well as a pilot project coordinator whose task it was to coordinate all activities among the pilot projects, to keep in touch with the developers of the architectures, to ensure information sharing, and to coordinate the pilot project evaluation. The pilot project teams for their part were responsible for the implementation of their pilot projects as well as for documenting their findings.

As it turned out, little coordination among the pilot projects was required all in all, for most of them did not encounter major difficulties. Therefore, exchange of information among all participants of the pilot phase occurred by mailing list, in the form of two Info Days, and a pilot project meeting.

5. Results

5.1 Selection of the Architecture

Tequila, an architecture developed by EPFL, had not been considered in the preparatory study, because it had not been finished by then and only been presented to the project team at the beginning of the pilot phase. Nevertheless, it was accepted as a candidate for evaluation since it appeared to be a promising solution. Of the three candidates Shibboleth, PAPI and Tequila that were evaluated by a task force, it was Shibboleth[1] that was finally selected by the steering committee as the architecture of AAI. Shibboleth is

[1] http://shibboleth.internet2.edu

being developed as part of the Internet2 middleware initiative and is designed as a federated identity management infrastructure based on SAML[2].

All three candidates showed the required functionality, but there was no clear leader among them. The main arguments that led to the selection of Shibboleth were:

- Tequila had short-term advantages speaking in its favor, such as availability, support, completeness of features, or low complexity;
- although the only architecture in operation at that time, PAPI did not offer any significant advantages but also bore the risk of a costly migration in the future;
- international commitment to a solution was given top priority; Shibboleth was clearly the top candidate regarding this aspect; and
- shortcomings with respect to Shibboleth's Attribute Release Policy were of minor importance for most pilot resources.

For more information on the findings of the Task Force "Evaluation" see the final report [AAIEval].

5.2 AAI System Architecture

The AAI system architecture is based on Shibboleth components operated by the Home Organizations, the Resource Owners and the Service Provider SWITCH.

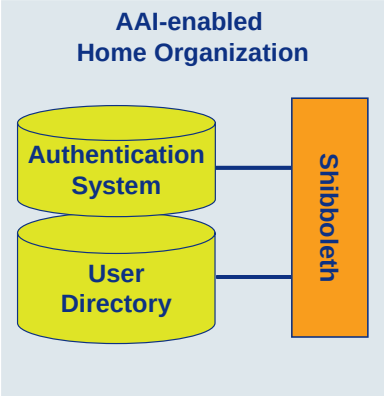

Figure 3: Home Organization integration

A Home Organization has to be able to register and authenticate its users and to provide a minimal set of authorization attributes about them. The authentication system and the user directory, which stores authorization attributes, have to be integrated with the Shibboleth components (cf. Figure 3).

[2] SAML = Security Assertion Markup Language, standardized by OASIS (Organization for the Advancement of Structured Information Standards) – http://www.oasis-open.org/

For Resource Owners, there are various methods of how to integrate their Resource within the AAI:

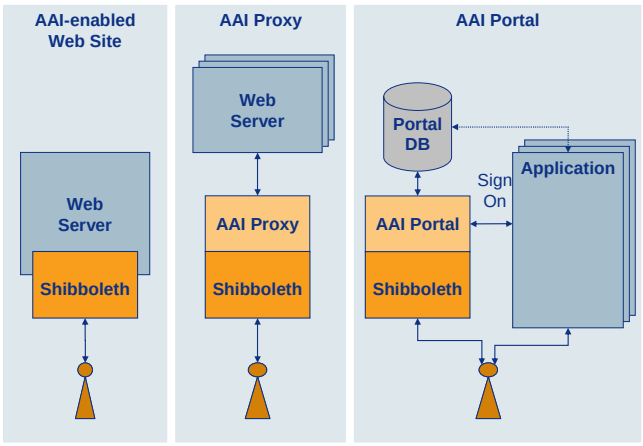

Figure 4 Resource integration methods

Type	Description
AAI-enabled web site	Standard web servers • Apache or Microsoft web server • access rights per group of users • static web pages or dynamic web pages (CGI, PHP, Perl, etc.)
AAI Proxy	Web Proxy, transparent for users, suitable for non-personalized web sites which cannot be integrated with Shibboleth (black boxes)
AAI Portal	Portal with user management and resource management, suitable for personalized web sites which cannot be integrated with Shibboleth

The role of SWITCH as AAI Service Provider is to operate the “Where Are You From” (WAYF) server and a resource registry. The WAYF provides the user with a list of Home Organizations from which he or she selects the correct one and gets redirected to the authentication system at his/her Home Organization. The purpose of the resource registry is mainly to ease the administration of the attribute release policy (ARP) by administrators of Home Organizations and end-users and to increase the transparency and the trustworthiness of resources.

The AAI Proxy and the AAI Portal have been developed by AAI pilot projects and the various AAI components have been installed, integrated and tested by several organizations (cf. chapter 5.8).

An overview of the Shibboleth architecture, the interfaces between the various components and further information about the AAI Proxy and AAI Portal solutions can be found in [AAISpec]. Deployment guides are available from http://www.switch.ch/aai.

5.3 Authorization Attributes

Authorization attributes for AAI users will be exchanged across organizations and need to be standardized. Therefore, a task force defined a set of authorization attributes[3], based on existing LDAP standards (e.g. inetOrgPerson, eduPerson) and data definitions from SIUS/SHIS[4]. The pilot projects proved that or-

[3] E.g. study branch, study level or staff category; see [AAIAttr] for the complete list.

[4] Service d'Information Universitaire Suisse / Schweizerisches Hochschulinformationssystem

ganizations are able to provide these authorization attributes out of existing databases. Sample configuration files for Shibboleth are available at the AAI project homepage.

5.4 Certification Authority (CA)

The communication between AAI systems is secured by using SSL. Therefore, AAI systems need X.509 server certificates. The Task Force “CA” collected information about current PKI related projects, defined a list of requirements and worked out a model for a Certification Authority (CA) infrastructure which suits the current needs of the AAI and other systems using server certificates and can be extended in the future (e.g. CA for end-user certificates).

SWITCH is going to offer a CA service for server certificates (independent of the AAI).

5.5 Organization and Processes

Establishing an AAI to ease interactions between end users and information providers across organizations not only requires a legal framework which allows participants to exchange information, but also the mutual trust of organizations. The SWITCHaai Federation serves these purposes by setting up rules for the participants’ behavior by means of service agreements and a policy document.

The SWITCHaai Federation is defined as a group of organizations (universities, hospitals, libraries, etc.) that agree to cooperate in the area of inter-organizational authentication and authorization and, for this purpose, operate a Shibboleth-based AAI infrastructure. These organizations agree to abide by a common set of policies and practices.

Figure 5 gives an overview of the participating parties:

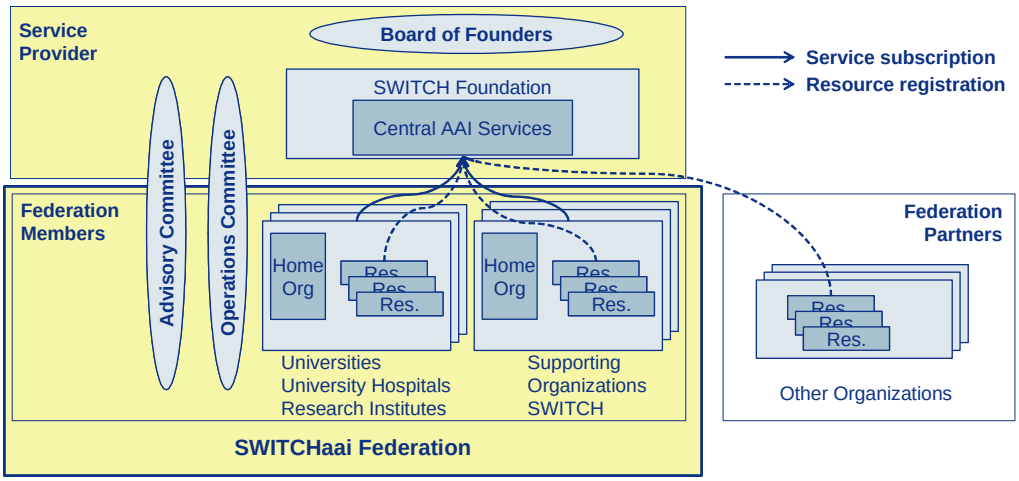

Figure 5: The SWITCHaai Federation and related organizations

In line with the *General Rules of Use for SWITCH Services*[5], there are two categories of organizations which can participate in the Federation: Category A, "Education and Research", and Category B, "Supporting Organizations".

[5] http://www.switch.ch/network/aup.html#GRU

More details on all AAI participants, their roles and tasks as well as the processes

- How to AAI-enable Home Organizations
- How to AAI-enable Resources
- Incident and problem management
- Change management
- Release management

can be found in [AAIOrgProc].

5.6 AAI Services

As Figure 6 shows, SWITCH will provide different AAI services:

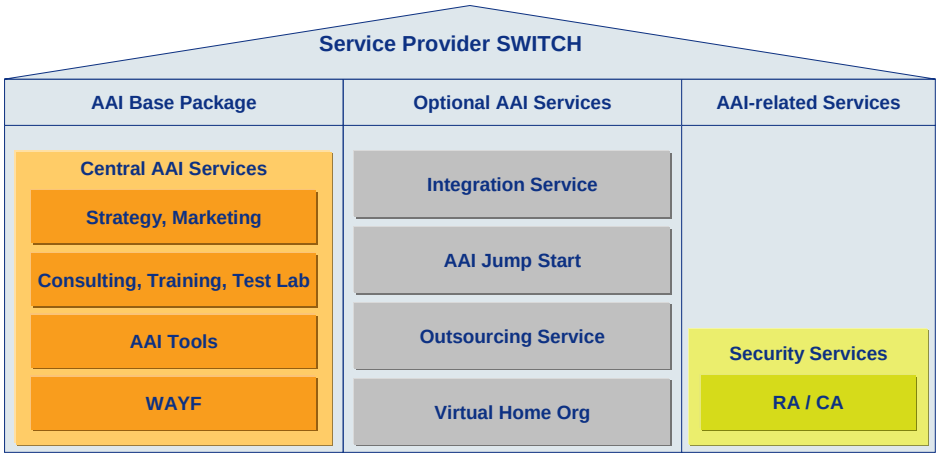

Figure 6: Service overview

By signing the AAI Service Agreement (cf. chap. 5.7), Federation members order the AAI Base Package, which covers central services necessary for running an AAI. It is available to the signing Home Organizations as well as all Resource Owners belonging to these Home Organizations and comprises the following services provided by SWITCH:

- Center of Competence (test infrastructure, information sharing and know-how transfer among Federation members, coordination of Advisory and Operations Committee, and contact with the Shibboleth developers)
- operation of the central WAYF-server, a register of the AAI Federation's authentication services used by resources, and coordination of all the WAYF-servers in the Federation operated by individual organizations
- development and implementation of AAI tools such as AAI Proxy, AAI Portal or a resource registry
- strategy and marketing (strategic, well-coordinated further development of the AAI as well as adequate AAI marketing initiatives, both nationally and internationally)

For more details on the AAI Base Package see [AAIServBP].

There are additional, optional services in planning which are not included in the Base Package and can be ordered separately on demand (see also chap. 7). The Security Service RA/CA is – although mandatory for members of the Federation – not exclusively intended for AAI purposes and therefore labeled "AAI-related".

5.7 Legal Framework / Service Agreement

Access to resources and transfer of user information across organizations raise questions about data protection and liability among participating organizations. The preparatory study suggested the Swiss University Conference (SUK/CUS) making a decision which would regulate these issues. Yet it turned out that, the AAI being an infrastructure project, the SUK is not in the position to make such a decision. Therefore, a new legal framework had to be defined.

The Federation SWITCHaai and the AAI itself will be legally based on legal regulations already in force[6] and the standing orders of the SUK of February 22, 2001. In addition, a bilateral Service Agreement [AAIServAgr] between SWITCH and each participating Home Organization needs to be signed, with the binding AAI Policy [AAIPol] governing the relationship between Federation members as an integral component. Also, a survey carried out by the SUK among all the universities showed that the AAI can be operated within the legal boundaries already in force, but that some organizations will have to adapt their "Acceptable Use Policy" (AUP); a sample clause that may be included has been drawn up for this purpose (see [AAIAUP]).

5.8 Pilot Projects

The delay in the availability of Shibboleth postponed the start of the pilot projects. The integration of the Home Organizations turned out to be easier than expected. By the end of the pilot phase, several Home Organizations had successfully AAI-enabled their existing user directories containing all their users and students.

While some resource integration projects did not encounter any major difficulties, others turned out to be rather tricky. This led to the development of tools such as the AAI Portal and the AAI Proxy so that there are now three possible ways of integrating a resource within the AAI.

For details of the pilot projects see Appendix A.

5.9 Cost Estimation

Based on the experience of the whole pilot project, a cost estimation model has been defined and rough cost estimates for initial and recurring cost are given, which may help the organization to define their own AAI budget. In order to partly finance the implementation of AAI from 2004 to 2006, SWITCH has applied for subsidies at SUK. See also [AAICostEst].

6. Recommendations

The project team considers the AAI a feasible solution for authentication and authorization of access to web resources and recommends SWITCH to offer the AAI Service Base Package as described in [AAIServ] and to extend the service range on demand. Consequently, the project team as well as the steering committee recommend organizations to order the AAI Service with SWITCH and to integrate their resources, authentication systems and user directories in the AAI.

They also recommend SUK to support the building of a nationwide AAI by granting the subsidies applied for by SWITCH.

[6] cf. [AAIPol]

7. Next Steps

The first implementation and roll-out phase is planned for January to September 2004. By the beginning of the summer term end of March 2004, SWITCH will have implemented its productive infrastructure.

The next tasks are to

- design and implement the resource registry
- design and implement additional services such as Home Organization Outsourcing Service and AAI Portal / Proxy Outsourcing Service (to ease the participation of resources in the AAI)
- test and deploy new releases of Shibboleth
- specify new attributes (if necessary)
- specify and implement new features of the AAI

As for the Federation members, they will make their existing pilot projects productive in due time, and new projects are expect to be added throughout the entire implementation phase.

8. References

[AAIAttr]	AAI Authorization Attributes, Version 1.1, 15-JAN-2004 http://www.switch.ch/aai/docs/AAI_Attr_Specs.pdf
[AAIAUP]	SWITCH – AAI Service Agreement, Exhibit 5: Sample Clause http://www.switch.ch/aai/docs/AAI_Sample_Clause.pdf
[AAICostEst]	AAI Cost Estimation, 1.0, 28-MAY-2003 http://www.switch.ch/aai/pilot-docs/AAI_CostEstimation_v10.pdf http://www.switch.ch/aai/pilot-docs/AAI_CostEstimation_v10.xls
[AAIEval]	AAI Architecture Evaluation, 1.0, 10-JAN-2003 http://www.switch.ch/aai/pilot-docs/Arch_Eval_v10.pdf
[AAIOrgProc]	AAI Organization and Processes, 1.0, 15-JAN-2004 http://www.switch.ch/aai/docs/AAI_Org_Processes.pdf
[AAIPol]	SWITCH – AAI Service Agreement, Exhibit 3: AAI Policy http://www.switch.ch/aai/docs/AAI_Policy.pdf
[AAIServAgr]	SWITCH – AAI Service Agreement http://www.switch.ch/aai/docs/AAI_Service_Agreement.pdf
[AAIServBP]	SWITCH – AAI Service Agreement, Exhibit 2: AAI Services Base Package http://www.switch.ch/aai/docs/AAI_Services_Basepackage.pdf
[AAISpec]	AAI System and Interface Specification, 1.0, 15-JAN-2004 http://www.switch.ch/aai/docs/AAI_System_Specs.pdf
[AAIStudy]	AAI Preparatory Study, Version 1.0, 15-JUL-2002 http://www.switch.ch/aai/AAI_Study_v10a.pdf

Appendix A: Pilot Projects

1. Home Organization of University of Bern

Contact	Peter Geiser, Informatikdienste, Universität Bern
Description	Home Organization installation of the University of Bern. The user directory runs on a LDAP server with 3 replicas. The directory is fed nightly from two sources: a database that contains all student data and another database that contains staff data. The Shibboleth installation follows very closely the standard described in the installation guides and currently uses basic authentication.
Status	Operational
Usage	While all users of the University are AAI-enabled, it is only used for test purposes so far. Starting from end of February, medical students from Bern will use the DOIT course (see description of the DOIT project) on a regular basis with AAI login.
Benefit of AAI	Apart from the obvious benefit of using AAI for authorization and authentication purposes, it also supported the goal of building a central user directory (based on LDAP), which is of great advantage also for non-AAI applications and purposes.
Problems encountered	There were no significant problems with the installation of Shibboleth. Following the installation guide made it quite easy (also some details were missing). Operation is unproblematic.
Next steps	- Installation of the AAI Portal in order to ease the integration of many internal web resources. - Improve data merging (originating from two sources) upon import into the LDAP server.
Platforms used	Shibboleth 1.1 on Debian Linux

2. Home Organization of University of Geneva

Contact	Dominique Petitpierre, Division Informatique, Université de Genève
Description	Home Organization for the University of Geneva. Runs on Sun Solaris. All users of the University of Geneva are available from an LDAP directory.
Status	Some internal tests have been done successfully.
Usage	Test only
Benefit of AAI	Once operational, it will immediately increase the number of resources that users can access
Problems encountered	No significant technical hurdles. However, the process of getting the system up and running on Solaris 9 was time consuming because many configuration items had to be modified (some of them in source code) and a few programs/libraries had to be recompiled. It required some learning to understand how the various components and tools used by the Shibboleth system interact, especially due to the number and complexity of technologies involved.
Next steps	Will be turned into a production level system (e.g. by setting up two redundant hosts) and get productive soon.
Platforms used	Shibboleth 1.1 on Sun Solaris 9

3. Home Organization of University of Lausanne

Contact	Alexandre Roy, Centre informatique, Université de Lausanne
Description	Home Organization installation of the University of Lausanne. A central LDAP server containing user names and passwords of all users was already in place when the AAI pilot project started. To host the additional attributes for AAI, a second LDAP server was built. Additionally to the standard Shibboleth installation, the "Pubcookie" Single Sign-On system is installed.
Status	Operational
Usage	While all the users of University of Lausanne are AAI-enabled, only a few have used it so far.
Benefit of AAI	It enables the users to access resources at other universities.
Problems encountered	First, it was quite time consuming to understand Shibboleth and all its components. Once understood, installation was straightforward by following the installation-guides. No major technical hurdles. Meanwhile, there is a support problem for RedHat Linux.
Next steps	Install a new instance of Shibboleth on another OS. Integrate additional attributes.
Platforms used	Shibboleth 1.1 and Pubcookie on RedHat Linux

4. Home Organization of University of Zurich

Contact	Luzian Scherrer, Informatikdienste, Universität Zürich
Description	Home Organization installation of the University of Zurich. An LDAP user directory for authentication and address book purposes already existed prior to the start of the AAI project. A master LDAP server is feeding 2 redundant slave LDAP servers that respond to authentication requests. For AAI, additional attributes were added to the LDAP directory. The Shibboleth installation runs on SuSE Linux and uses the Pubcookie Single Sign-On system.
Status	Operational
Usage	Used by the DOIT users (see description of the DOIT pilot project) on a regular basis. All University of Zurich users are AAI-enabled.
Benefit of AAI	It allows University of Zurich to share applications with other universities.
Problems encountered	It needed some time to understand all technologies used in Shibboleth and how they interact. Not very much support for Shibboleth (error messages and the like) is available on the web but e-mail support from SWITCH was helpful.
Next steps	Import additional attributes for AAI into the LDAP directory.
Platforms used	Shibboleth 1.1 and Pubcookie on SuSE 9 Linux

5. Home Organization of ETH Zurich

Contact	Vladislav Nespor, Informatikdienst, ETH Zürich
Description	Home Organization installation of the ETH Zurich. Runs on Apache 2 and Sun Solaris. A central user directory for authentication purposes was already in place when the AAI pilot project started. Additional attributes were added in order to satisfy the requirements of AAI. The directory runs on three redundant LDAP servers.
Status	operational
Usage	All users of the ETH Zurich are AAI-enabled, but it is only used for test purposes so far.
Benefit of AAI	Will be apparent only when more resources are AAI-enabled.
Problems encountered	Minor technical problems only. The LDAP servers require the connections to be SSL-encrypted. It would have been tedious to implement this with Apache 1.3. Therefore, Apache 2.0 was chosen which already includes a module for LDAP-authentication with SSL.
Platforms used	Shibboleth 1.1 on Sun Solaris 8 with Apache 2.0.47 and Tomcat 4

6. DOIT

Organizations	University of Zurich (leading), Universities of Basel, Bern, Lausanne, and Jena (Germany)
Contact	Roger Kropf and Vahid Djamei, Dermatologische Klinik, Universitätsspital Zürich
Description	A course for the dermatological training of medical students (a Swiss Virtual Campus project).
Status	operational
URLs	http://www.cyberderm.net/, http://aai.cyberderm.net/
Usage	Used by medical students of the University of Zurich on a regular basis since December 2003.
Benefit of AAI	Access to the course is granted based on user attributes provided by AAI. The administrators of the course do not need to care much about user management.
Problems encountered	This project was an early adopter of AAI. First, some of the participating universities had to be convinced about the importance of AAI and therefore to build an AAI home organization during the pilot phase.
Next steps	Starting from end of February 2004 also students from the University of Bern will use the course. They will also be authorized by AAI.
Platforms used	Shibboleth 1.1 on Debian Linux

7. VITELS and AAI Portal

Organizations	University of Bern (leading), Universities of Neuchâtel, Genève and Fribourg, Ecole d'Ingénieurs de Fribourg
Contact	Marc-Alain Steinemann, IAM, Universität Bern

Description	VITELS is an e-course geared to practical exercises. It covers subjects such as firewalls, network management and server programming (a Swiss Virtual Campus project). The AAI portal is a development by IAM (University of Berne) in order to AAI-enable different types of resources (e.g. VITELS) and to ease user management for resource owners.
Status	The VITELS course itself is used by students of the University of Bern. They currently use a local login and not (yet) AAI. Feasibility of AAI-login to WebCT 4 and 4.1 CE via AAI portal could be demonstrated. The AAI portal now is an open source product maintained by SWITCH.
URLs	http://aaitest1.unibe.ch/ and http://aai-portal.sourceforge.net/
Usage	AAI-login to VITELS and AAI portal only used for test purposes so far
Benefit of AAI	Once AAI-login is operational, user management for VITELS will be much simpler than today.
Problems encountered	The AAI portal needs administrator privileges on WebCT 4 and 4.1 CE in order to create user accounts. The operational unit responsible for the WebCT server did not grant unlimited privileges to the AAI portal – because their WebCT-server is an important system with many thousands of users. This problem should be solvable with WebCT Vista that allows creating users with only limited privileges. Furthermore, the API to WebCT typically changes more or less between subsequent WebCT versions. The interface from the AAI portal to WebCT has to be adapted and tested with each new version. Currently, attempts are made to adapt the interface to WebCT Vista which have not fully succeeded yet. The WebCT product is not open source and is developed by a commercial company – both facts don't make it easy to adapt and test the interface.
Next steps	Once the interface from the AAI portal to WebCT Vista is running, - migrate VITELS to WebCT Vista, - connect it with an AAI portal (where the AAI portal will run and by whom it will be operated is still to be determined), and - migrate VITELS access to AAI (via AAI portal).

8. ERL and AAI Proxy

Organizations	Library Consortium / ETH Library
Contact	Wolfgang Lierz, ETH Bibliothek, Zürich
Description	Feasibility test of AAI infrastructures for access to ERL WebSPIRS databases (OVID technologies, formerly Silverplatter)
Status	Pilot
URLs	http://test.aaiproxy.switch.ch/proxy/erl/webspirs/start.ws?customer=consortium
Usage	Test only, so far

Benefit of AAI	Proper user management and authentication of library-users in special environments like - library institutions attached to the same network as non-library institutions (e.g. UAS within cantonal admin network), - individual users sitting behind a non-university-proxy (e.g. admin.ch), - roaming users with no VPN or proxy access provided by their university, and - roaming users with no VPN or proxy access possibility (e.g. university researchers working temporarily within company networks).
Problems encountered	On the ERL server an Apache webserver is installed for application administration. Originally it was assumed that this webserver also provided the application content. This assumption was wrong – a second (proprietary) webserver was used for this purpose, instead. Because this webserver could not be "shibbolized", the AAI proxy was developed by SWITCH (based on an open source product). For these dedicated AAI proxy access paths, the ERL user access configuration was modified by ETH-Bibliothek. The AAI proxy is now running on a test machine at SWITCH for demonstration of feasability.
Next steps	To be defined.

9. Nano-World – RAFM

Organizations	University of Basel
Contact	Martin Guggisberg, Departement Informatik, Universität Basel
Description	Nano-World (computer supported cooperative learning environment on nanophysics) is a Swiss Virtual Campus project. The RAFM (Remote Atomic Force Microscope) was developed at the University of Basel to be used in education and science. Controlled remote access to the RAFM is part of the Nano-World project. Since the RAFM is a very sensitive instrument and must be used carefully to prevent time consuming and costly repair work, only well-trained people are allowed to use it. Potential users come from some Swiss universities as well as from the Universities of Freiburg (DE) and Strasbourg (FR).
Status	Pilot
URLs	http://www.nano-world.org/ and http://www.rafm.org/aai-portal/web/
Usage	Test usage
Benefit of AAI	Users from Swiss AAI-enabled universities do not need an additional account for their activities on the Nano-World project web site. The use of the AAI Portal allows a rather easy inclusion of students of the foreign partner universities; they get a new login and password, however.

Problems encountered	PHP (as used for within the AAI Portal) was new to the team using previously Java and Python (Zope). However, the learning curve was not steep due to the well-documented PHP code of the AAI Portal. The installation of Shibboleth in combination with the Apache PHP module first caused some headache, but now it is solved. Once a NTP misconfiguration prevented the system to automatically switch back from daylight saving time, thus bringing the Shibboleth transactions to a stand-still. Having proper time synchronization is important. Access authorization for RTSP video streams as delivered by a Darwin Streaming Server cannot easily be accomplished by AAI.
Next steps	Upgrade to the Shibboleth 1.2 release planned.
Platform used	Shibboleth 1.0 & AAI Portal 0.9.2 on RedHat Linux 7.2

10.AD Learn

Organizations	University of Zurich (leading), Universities of Basel and Lausanne and the company Boomerang from France
Contact	Pascal Py, Division of Psychiatry Research, University of Zürich
Description	An e-course including video streaming sessions. Covers Alzheimer's dementia and associated disorders (a Swiss Virtual Campus project).
Status	Pilot. Demonstrates AAI login to a resource running on Microsoft technology.
URLs	http://aaidemo.alzheimerlearn.net/
Usage	Apart from AAI login, also local login is possible. Most users use the local login so far.
Benefit of AAI	It significantly reduces individual users' subscription work, since AAI stands for trusted user data.
Problems encountered	Little support for Shibboleth on IIS available (at least in Switzerland). A technical problem (sudden stop of IIS) could be solved with a patch.
Next steps	Upgrade to Shibboleth 1.2 as soon as released.
Platform used	Shibboleth 1.1 on Microsoft IIS

11.UNIL-EPFL-CSS (CSS = Common Services for Students)

Organizations	Université de Lausanne, EPFL
Contact	Alexandre Roy, Centre Informatique, Université de Lausanne
Description	The resource 'Common Services for Students', where students of Unil and EPFL can find information about housing and jobs, was chosen as test resource for integration into AAI.
Status	Pilot
URLs	http://www2.unil.ch/sasc/

Usage	Not yet
Benefit of AAI	Having that resource integrated into AAI would no longer require two different entry points for students of Unil and EPFL, as it is the case today. Now, the resource is protected by both authentication systems in place.
Problems encountered	The resource runs on an iPlanet server under Solaris and uses an Informix database. Since Shibboleth is not available for iPlanet, the application was ported to an Apache webserver running under RedHat Linux. However, the attribute transfer from Shibboleth to the Informix database via the Web DataBlade module was never successful. These tests took place in early 2003 with the Shibboleth pre-release 0.8 (current version is 1.1). Since then, the people involved have not been able to spend more time retrying it with an up-to-date Shibboleth version, which would most probably be more successful.
Next steps	Upgrade to the Shibboleth 1.2 release planned for spring 2004.
Platform used	Shibboleth 0.8 on RedHat Linux 7.2

Appendix B: Acknowledgement

The following people contributed to the results of the pilot phase:

Nicole Beranek Zanon	SWITCH
Dr. David Billard	Université de Genève
Prof. Dr. Torsten Braun	Universität Bern
Dr. Rolf Brugger	Université de Fribourg
Armin Brunner	ETH Zürich
Thomas Brunner	SWITCH
Ion Cionca	EPFL
Yan Corneille	Universität Zürich
Roland Dietlicher	ETH Zürich
Vahid Djamei	Universitätsspital Zürich
Dr. Serge Droz	PSI
Dr. Andreas Dudler	Präsident SWITCH; Informatikdienste ETH Zürich
Jean-Jacques Dumont	EPFL
Derek Feichtinger	CERN
Rolf Gartmann	SWITCH
Peter Geiser	Universität Bern
Christoph Graf	SWITCH
Karl Guggisberg	Universität Bern
Martin Guggisberg	Universität Basel
Gerhard Hassenstein	Berner Fachhochschule
Christian Heim	Universität Bern
Dieter Hennig	ETH Zürich
Dr. René Hüsler	Fachhochschule Zentralschweiz
Patrick Husi	Arpage AG
Daniela Isch	at rete ag
Dr. Pascal Jacot-Guillarmod	Université de Lausanne
Dr. Maximilian Jäger	Universität Zürich
Thomas Jordan	Universität St. Gallen
Prof. Dr. Bengt Kayser	Université de Genève
Ueli Kienholz	SWITCH
Dr. Roger Kropf	Universitätsspital Zürich
Dr. Annette Langedijk	Universitätsspital Zürich
Claude Lecommandeur	EPFL
Thomas Lenggenhager	SWITCH
Wolfgang Lierz	ETH-Bibliothek
Marc Luder	Universität Zürich
Roberto Mazzoni	Universität Zürich
David McLaughlin	ETH Zürich
David Meier	Universität Zürich
Ian Neilson	CERN
Dr. Vladislav Nespor	ETH Zürich
Dr. Wolfram Neubauer	ETH-Bibliothek
Susanne Obermayer	CRUS
Frederik Orellana	CERN
Martin Ouwehand	EPFL
Dominique Petitpierre	Université de Genève
Arlette Piguet	Konsortium der Schweizerischen Hochschulbibliotheken
Fabio Poroli	SWITCH
Dr. Pascal Py	Universität Zürich
André Redard	at rete ag
Dr. Cornelia Rizek-Pfister	CRUS
Dr. Alexandre Roy	Université de Lausanne
Alberto Salerno	at rete ag
Dr. Markus Schaad	at rete ag
Luzian Scherrer	Universität Zürich
Dr. Stephane Spahni	Hôpitaux Universitaires de Genève; Nice Computing
Thomas Spreng	Universität Bern
Marc-Alain Steinemann	Universität Bern
Martin Strässler	at rete ag
Alex Sutter	Universität Bern
Elsa Sutter	Universität Basel
Dr. Martin Sutter	SWITCH
Dr. Constantin Tönz	SWITCH
Dr. Hans Rudolf Trüeb	Prager Dreifuss
Gerhard Tschantre	Universität Bern
Valéry Tschopp	SWITCH
Bruno Vuillemin	Université de Fribourg
Prof. Maia Wentland Forte	Université de Lausanne