Authentication and Authorization Infrastructure (AAI)
Preparatory Study

Report

20-Jun-02

Document management

Version/status:	1.0 / final
Date:	20-Jun-02
Author(s):	see Appendix C
File name:	AAI_Study_v10.doc
Approved by:	PAS

Table of Content

Table of Figures

1. Management Summary

The longstanding tradition of collaboration amongst our institutions of higher education in Switzerland resulted in some important achievements relevant in the context of this report: standards in the form of a uniform access policy to the institutions of higher education. The processes dealing with access policy are mostly based on paper. This severely impacts the deployment of networked resources requiring some form of authorization, be it a proof of membership, academic degree or role. Therefore, an inter-university study group published a report in September 2001 proposing a roadmap to develop and implement an Authentication and Authorization Infrastructure (AAI) for the higher education community in Switzerland ("AAI-concept").

SWITCH took on the task to implement the phase "preparatory study" as outlined in the AAI-concept and invited specialists from the higher education community in Switzerland to work on the organizational, technical, legal and financial issues of such an infrastructure.

The present report is understood as the final report of the "preparatory study" phase. A close examination of various aspects of authentication and authorization has shown that there are feasible solutions available with real benefits, mainly in the field of enabling students' mobility and improving the protection of valuable information, the support for nomadic users, user convenience and the efficient use of IT resources. There are also considerable risks involved in *not* building an AAI, like growing registration overhead due to increased mobility or isolation due to not being able to access resources from remote locations.

The main findings of the study are:

- Two promising architectures of an AAI were identified: PAPI (Spain) and Shibboleth (Internet2). Both of them have been developed for a large academic community and are promising enough to go into an extensive test and pilot phase, although they do not fulfill all evaluation criteria. The main functionalities of these architectures are authentication and authorization of web access. Other functionalities, like document signing and encryption can be added in a later release of the AAI.
- The AAI can be well integrated into existing processes of participating institutions, like the registration process for students or employees. Institutions may stay responsible for authenticating their users and Resource Owners may keep full control of their resources and access rights.
- The AAI will be able to interface with existing systems such as user databases and authentication systems. Institutions may select the authentication technology by themselves and are not forced to implement any PKI or smart-card-based authentication solution as a preliminary requirement to participate.
- The main legal issues are data protection and abuse. A legal framework has been worked out which solves these issues between the institutions, service providers, and users.
- A detailed cost estimation of an AAI implementation has proved impossible at this stage. First, the final architecture has to be selected and experience be gained with pilot implementations.
  The costs of pilot projects will basically be staff costs. Since the participating organizations, including SWITCH, are willing to pay for their projects by themselves, the financing of this next phase is guaranteed.

Recommendation

The project team recommends to build a virtual AAI organization across the participating institutions and to immediately start a pilot phase in order to get

- practical experience with pilot implementations which is to lead to the final selection of the AAI architecture;
- more detailed results covering the organizational and technical issues;
- a more in-depth cost estimation for the implementation phase.

As many organizations as possible should be brought in in the pilot phase so as to secure their active interest in the project.

Until the end of the pilot phase, the legal framework between all parties involved has to be implemented. Until all the legal instruments are in place, a Letter of Intent (LoI) should be signed in order to have a sufficient legal basis to start with the pilot projects.

2. Introduction

The longstanding tradition of collaboration amongst our institutions of higher education in Switzerland resulted in some important achievements relevant in the context of this report: standards in the form of a uniform access policy to the institutions of higher education, mutual acceptance of academic degrees, and trust relationships enabling sharing of resources like libraries or course offerings in a controlled way. The processes dealing with access policy, proof of academic degrees, granting access to libraries and courses are mostly based on paper. This is well adapted to situations where attending a course or entering a library means you are physically entering the corresponding site.

The emerging networking technology has had a tremendous impact on the way we do our daily business. Location, distance and physical presence become less important as does the perception of organizational boundaries: distant and local resources are both a mouse click away. Presenting a paper is not a concept easily applied to networked resources even though the underlying trust relationships as well as the above-mentioned standards regarding access and acceptance of degrees still apply. This severely impacts the deployment of networked resources requiring some form of authorization, be it a proof of membership, academic degree or role.

This report shows a way to map the existing paper-based processes into a networked environment: Data collected during physical registration processes can be made available in electronic form allowing for subsequent electronic enrolments. That way, academic degrees and other person-related information becomes available to automated control mechanisms protecting access to networked resources.

An inter-university study group published a report in September 2001 proposing a roadmap to develop and implement an Authentication and Authorization Infrastructure (AAI) for the higher education community in Switzerland. This report is named “AAI-concept” and is available from http://www.switch.ch/aai/

SWITCH took on the task to implement the phase “preparatory study” as outlined in the AAI concept and invited specialists from the higher education community in Switzerland to work on this issue. The present report is understood as final report of the “preparatory study” phase and refines the proposals of the AAI concept.

2.1 Problem Description

In order to access a single resource (e.g. information on a web server, e-learning application, library catalog etc.), the following generic interactions between a user and the resource occur:

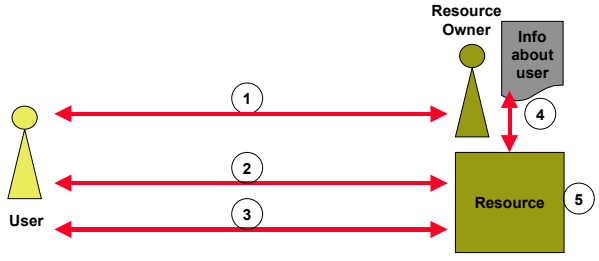


Figure 1: Granting access to a single resource

1. A user (e.g. student, employee, library user, but also application) who wants to access a resource has to register with the Resource Owner. The Resource Owner creates a virtual identity for this user, stores the necessary information about him/her and provides an identifier, like a login name, as well as credentials to the user. Later on, the user may use identifier and credentials to authenticate him-/herself to the resource.
2. The registered user wants to access a resource and submits an access request to the resource, claiming the virtual identity by identifying him-/herself with the identifier.
3. The resource asks the user to authenticate him-/herself (i.e. to provide the credentials belonging to that virtual identity).
4. After checking the credentials, the resource retrieves previously stored information about the user and,
5. based on this information, decides on granting access.

The disadvantage of this approach is that it does not scale if a user wants to have access to large numbers of different resources:

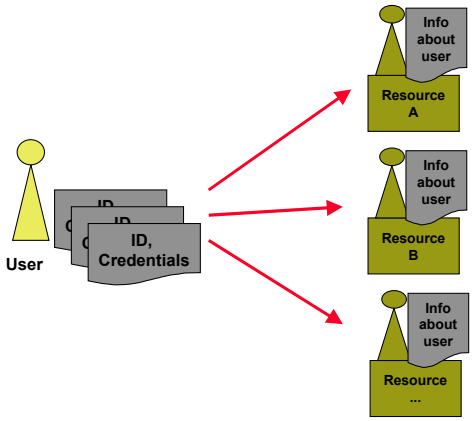


Figure 2: Accessing large numbers of resources

- Registration: The user has to register with each resource. This is the case even if many Resource Owners do not need to know the exact identity of a user (e.g., resources which grant access to all students of a particular university only need to know if a user belongs to this university or not).
  The Resource Owner has to make sure that the information about its users is always correct (e.g. to know if a person is still a student or not).
- Authentication: The resources themselves may use different technologies to authenticate users. Therefore, a user has to be able to handle different authentication technologies (e.g. password-based, certificate-based, smart-card-based, etc.) and for each technology at least one (but often more) identifier.

Recently, larger organizations have started to implement local authentication and authorization infrastructures for their users and resources:

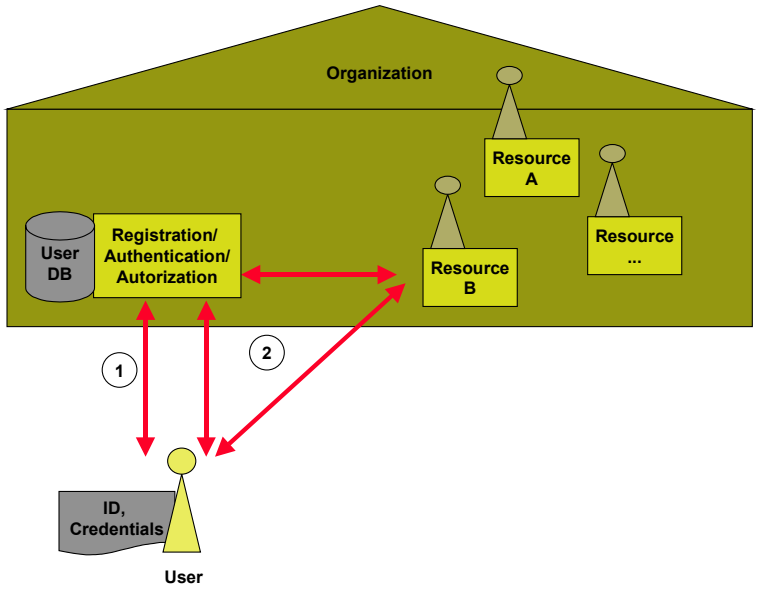


Figure 3: Granting resource access with centralized registration, authentication and authorization

1. Centralized user registration and storing of authorization attributes in a central user database
2. Authentication and authorization interactions between user, resource and central infrastructure of the organization

This approach solves the authentication and authorization issue for resources belonging to the user's home organization, but it is no solution for authentication and authorization across organizations.

- Users of one organization would like to be authorized to use resources of other organizations (without registering with each of these organizations).
- Organizations would like to open their resources to (some) registered users of other organizations in a controlled way, without having to register all these "foreign" users by themselves.

These issues will be dealt with in the following. It goes without saying that already existing infrastructures of organizations have to be taken into account.

2.2 AAI Model

A solution to the problem of inter-organizational authentication and authorization is the implementation of an AAI. The core functionality of an AAI is to tightly couple together the three basic interactions between a user, his of her home organization and a resource during the authentication and authorization process. These three basic interactions are:

1. user authentication, which is always carried out by the User's Home Organization;
2. access request; and
3. delivery of authorization attributes from the Home Organization to the Resource.
   The set of authorization attributes, which is transmitted to an access control manager, has to be configurable and extendible, depending on the needs of the Resource Owner and respecting the restrictions from the data protection law.

In order to describe the functionality of the AAI, the following generic model will be used:

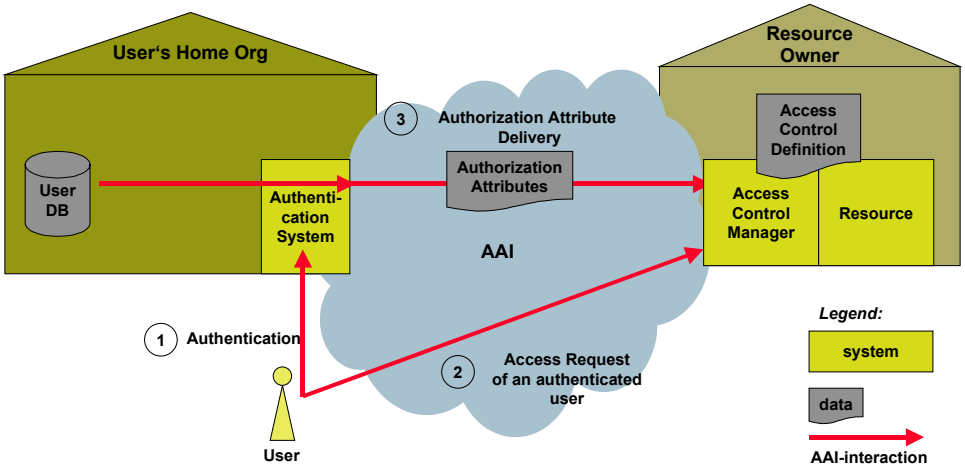


Figure 4: Generic functional model of an AAI

The terms introduced in Figure 4 and in this chapter are defined as follows:

(User's) Home Organization	Representative of a user community, e.g. universities, libraries, university hospitals etc. • registers their users and stores information about them • is able to authenticate their users
User	Registered member of a Home Organization
User-DB	Database storing information about a registered user, maintained by the Home Organization
Authentication system	System which can authenticate a previously registered user
Resource	Application, web site
Resource Owner	Entity owning a resource and offering resource access to users
Access control manager	Gatekeeper functionality of the resource which grants or denies access to the resource based on the access control definition and the authorization attributes retrieved
Access control definition	Configuration parameters used by the access control manager implementing the access control policy
Authorization attributes	User data needed for access control decisions
AAI-related systems	Resources, registration and authentication systems which will interact within the AAI and are a prerequisite to use the functionality of the AAI
AAI core systems	Systems which provide the core functionality of the AAI

After having received the authentication acknowledgement and the authorization attributes from the User's Home Organization, the access control manager, on behalf of the Resource Owner, can decide whether to grant or deny access to the resource.

2.3 Goals and Scope of this Study

This study's goal is to define shape and scope of an AAI addressing the problems described in the preceding chapter 2.1 and to outline the next steps in establishing such an infrastructure. The following areas need to be addressed specifically and consolidated recommendations be presented:

- Legal issues: Elaborate on data protection issues, liabilities and responsibilities of participating institutions as well as of users within an AAI. Drafting policies for an AAI.
- Organizational issues: Show organizational requirements towards AAI, AAI requirements towards participating organizations and which processes within organizations need to be established or changed.
- Technical issues: Provide overview of available technologies, technical feasibility and relevant standards and profiles. Assess technology specific advantages and drawbacks.
- Financial issues: Estimate costs of participating in the next steps towards establishing AAI.

A common student and staff card within the higher education community in Switzerland could be very beneficial to a future AAI. In the scope of this report, however, we do neither require such a card nor start from the assumption that there will be one available before the rollout of a future AAI. We clearly see the definition of such a student and staff card as outside the scope of this report.

2.4 Benefits of an AAI

The reason why this project was launched in the first place was that there were certain expectations of the benefits of an AAI. Without knowing anything yet about potential solutions, we imagine that the main benefits will be the following:

- Enabling students' mobility: AAI is a required building block for all resources which shall be shared between students of different institutions. Therefore, an AAI will enable initiatives which promote cross-organization studies, like Swiss Virtual Campus, and helps implementing the Bologna Agreement.
- Better information protection: Today, securing information access is often skipped, because it is too complicated or expensive. An AAI will offer a standardized procedure of authenticating and authorizing resource access. Therefore, resource owners can concentrate on protecting their assets, because they do not have to implement registration and authentication procedures themselves.
- Support for nomadic users: Today, users expect to be able to access the resources they are allowed to from anywhere, not just from a workplace at their university. An AAI will enable resource owners to define their access control policy based on personal attributes of users and not based on IP addresses.
- Improved user convenience: After registering once, users will be able to access many resources with a single authentication technology.

- Improved IT efficiency: IT organizations can share their security knowledge and profit from common AAI developments and from standardizations. This will make the implementation of AA functionality within their organization more efficient.

This study will show whether there are solutions that can come up to our expectations.

Notice that there are not only benefits that can be derived from an AAI, but there are also considerable risks involved in *not* acting:

- Growing registration overhead: increased mobility puts additional load on user registration, namely to register remote users from outside the resource hosting organization. The inability to handle this additional load can lead to loss of potential customers, or to additional security risks due to simplified, incomplete or lacking access control to protected resources.
- Isolation: ease of access to remote resources as well as easy access from outside to local resources in a controlled way is a crucial precondition to be part of a community that increasingly relies on virtualized, distributed resources. It is also crucial for teams to form across organizational boundaries.
- Image problem: complicated access procedures to networked resources will be perceived as outdated. This can be very damaging to an organization's reputation, particularly for technology-oriented ones.

3. Method of Proceeding

General approach:

As a first step, the project management identified ten cases where a future AAI could be used (see Appendix B) as well as the potential benefits of such an AAI. These cases then served as the common basis for four different teams of specialists which addressed technical, organizational, legal, and financial issues as stipulated in chapter 2.3. The form of the project organization (see Appendix C) proved to be very efficient: maximum benefit could be derived from the know-how of specialists, while at the same time coordination of all efforts was guaranteed by the introduction of a core team. This approach ensured that the findings of one team were considered in the work of the others.

The organizational team defined the AAI model (chapter 2.2), worked on organizational requirements, and developed a process model where the authentication and authorization process was put into a broader context of already existing processes (chapter 4).

The goal of the technical team was to collect the requirements and to evaluate possible AAI architectures (see chapter 6). The legal team worked out a legal framework between all parties involved (i.e. users, institutions and service providers; see chapter 7) and checked whether an AAI architecture was conform with the law.

Since cost was not a differentiator between the evaluated architectures, the financial team focused on general financial considerations as well as on the cost estimation of the pilot phase and the implementation phase (chapter 8.1).

Technical Evaluation:

The rather different nature of the infrastructures that were considered made a classical evaluation (i.e. with simple criteria and yes/no answers) not applicable. Moreover, it was almost impossible to fully evaluate a solution without test implementation. The technical evaluation therefore followed two goals: describing the key elements of the various solutions and selecting the most promising ones for closer scrutiny by eliminating the others thanks to a set of “killing arguments”.

The evaluation criteria have been grouped as follows:

Functional criteria	For evaluating the added value of an infrastructure; see chap.3.1
Technical criteria	For evaluating the technical complexity of an infrastructure; see chap.3.2
Administrative criteria	For evaluating the administrative tasks linked to the use of a solution; see chap.3.3
Other criteria	For identifying interesting functionality for the future; see chap. 3.4

3.1 Functional Criteria

The evaluation was driven by a few postulates that the majority of the project team agreed on:

- The basic access mechanism to numerous resources is the Web. The AAI has to provide a schema for sharing such resources between organizations.
- Users are affiliated to one AAI-member organization (e.g. universities, libraries, etc.), called user’s home organization. These home organizations have to know their users and have to be able to authenticate them. It is the home organization’s responsibility to operate

an adequate authentication system. AAI cannot give any directives which authentication technology or end user equipment (smart cards or any similar media) has to be used as a prerequisite to participate in the AAI.
- Resource owners want to keep control of their resources. Therefore, AAI should not propose a solution where access control has to be taken away from the Resource Owner.

3.2 Technical Criteria

The technical key issues are:

- Interoperability between AAI core and AAI related systems: Does the architecture include interfaces to authentication, user database, and resources? Are they based on standard protocols?
- Is user privacy taken into account and part of the design?
- How does a user know the services he/she can have access to?
- Are centralized resources required?
- Is a public key infrastructure required?
- Is enhanced end-user hardware required (e.g. smart card reader)?
- Is the architectural design streamlined to the basic needs (no additional complexity)? Is it interoperable with common operating systems and network equipment, like firewalls?
- Security: Are all interactions encrypted? Is there a risk of security breaches?
- Scalability of the infrastructure (regarding # of sites, # of users and # of resources)
- Performance / bottlenecks to be expected ?

3.3 Administrative Criteria

The following points cover the aspects of software availability, support and operation:

- Is the software available, documented and supported?
- What is the current level of deployment of the infrastructure? Is it used in a productive environment?
- What is the software licensing schema (Open source, commercial software, etc.)?
- Can it be operated across organizations?
- Is the autonomy of participating organizations respected? Is there a dependency on external partners to operate the AAI?
- Is it possible to outsource (parts of) the infrastructure to service providers?
- Complexity of the maintenance of the list of available services

3.4 Other Criteria

In the future, the solution should be extendable in a various ways:

- Is digital signing and encryption of documents supported, either in the standard solution or as a future extension?
- Can the solution deliver the necessary information for future accounting and billing systems?

3.5 Killing Criteria / Show Stoppers

In addition to the evaluation criteria defined above, a few killing arguments (show stoppers) have been identified:

- The mandatory use of physical media to get access to the shared resources (e.g. smart card, electronic token, etc.)
- The inability to provide the AAI core functionality as defined in chapter 2.2 (AAI Model)
- No support, i.e. no collaboration with the development team (as none of the solutions is a fully-packaged product) or lack of documentation

4. Organizational Design

The following chapters will show how the AAI-relevant interactions can and have to be integrated into the standard processes of Home Organizations and Resource Owners.

These interactions can be related to four different phases: initialization, authentication and authorization, resource access, and post-processing. Figure 5 shows the processes of each phase, as well as their owners:

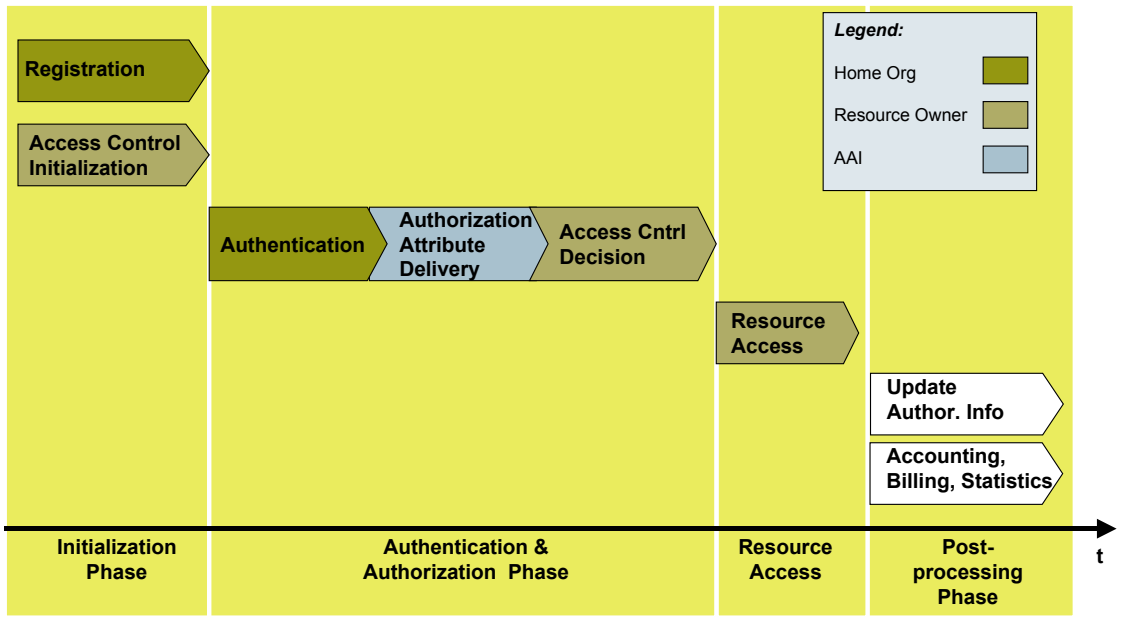


Figure 5: AAI-related processes

The following chapters describe the processes of the initialization and the authentication/ authorization phase in further detail.

Notice that the post-processing phase is beyond the scope of this study. Due to the increasing importance of processes such as accounting or billing, however, the relationship between them and the AAI is discussed in chapter 4.2 in order to show how they fit into the picture.

4.1 Process Descriptions

4.1.1 Process Overview

Figure 6 gives an overview of the process flow and the interactions between the parties involved (Person/User, Home Organization, and Resource Owner). Of course, not only persons want to get access to resources but also systems and applications. All processes defined in these chapters are similarly applicable to systems and applications accessing a resource.

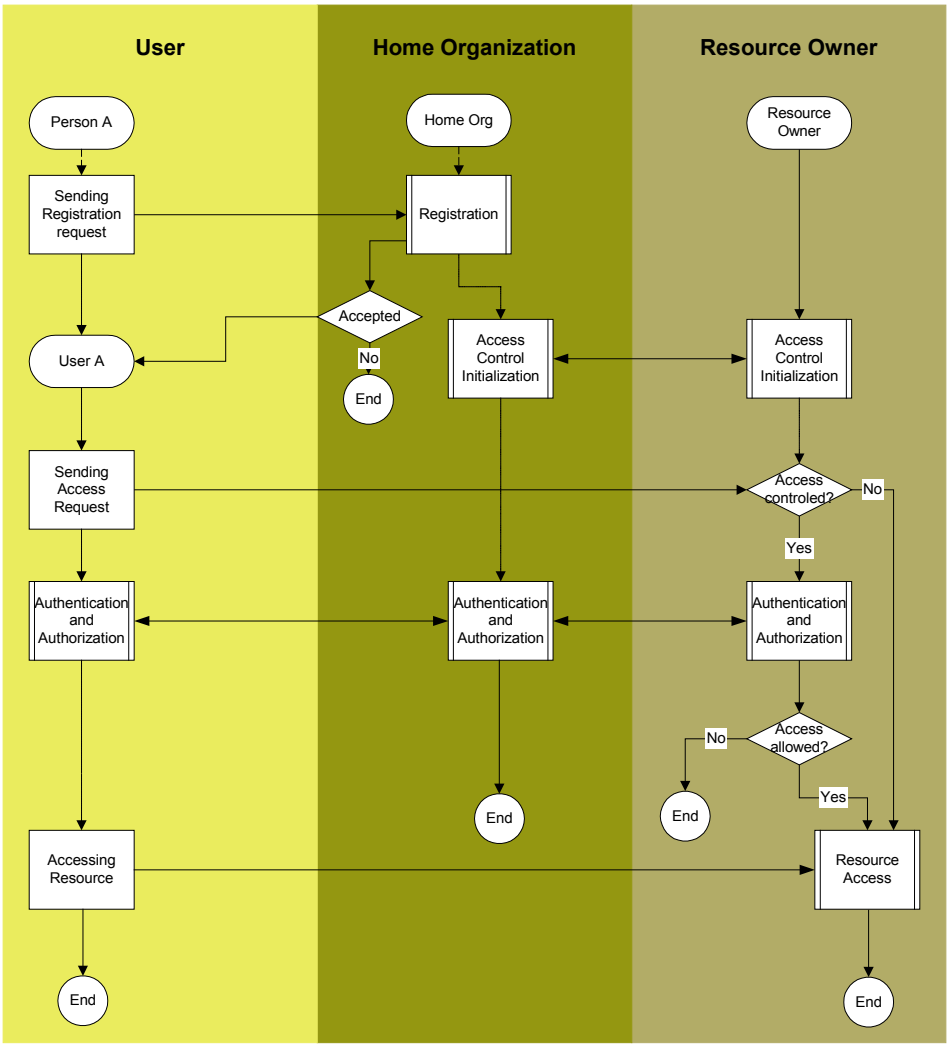


Figure 6: Process overview

The following symbols are used to visualize the AAI processes:

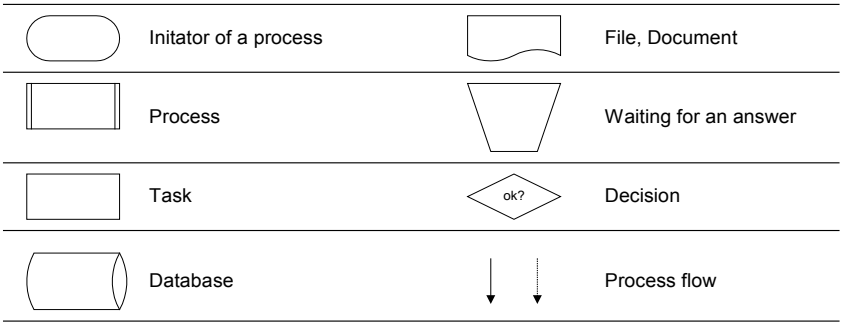


Figure 7: Process design symbols

The processes can be described as follows:

Process	Description
Registration	• Registration of a person as a user of the Home Organization based on the Home Organization's registration policy and the person's credentials • Storing information about the registered person (attributes) in a user database
Access Control Initialization	• Implementation of access rights for each resource
Authentication and Authorization	This is the main process of the AAI. It can be split into three subprocesses: • Authentication of a user by his/her Home Organization • Transfer of authorization attributes about the authenticated user from the Home Organization to the Resource Owner • Access control decision by the Resource Owner (authorization)
Resource Access	Resource access by the authenticated and authorized user

4.1.2 Registration Process

Before a person can use any AAI-enabled resources, he/she has to be registered as a user with an organization of the AAI community ("(User's) Home Organization"). Many organizations already have such registration processes, e.g. as part of their recruitment process (for future employees) or their matriculation process (for future students).

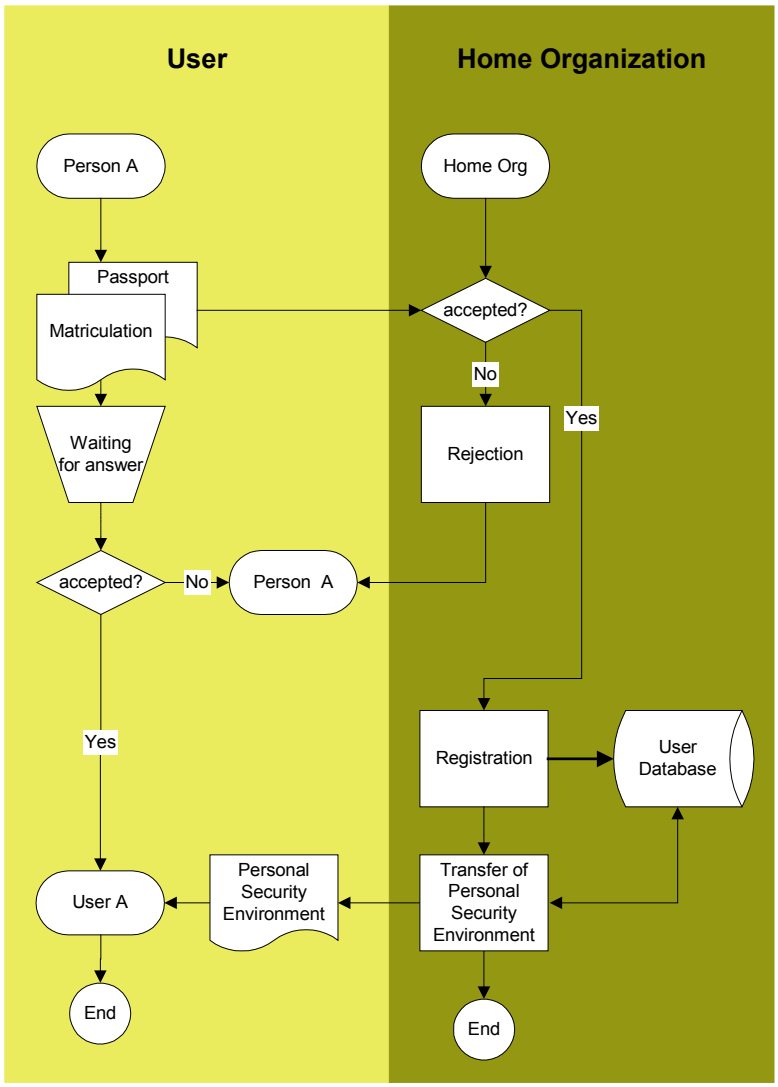


Figure 8: Registration process

The registration process can be split into the three basic steps described below. How these steps are implemented may vary from organization to organization. The intention of this chapter is to show the relation between the AAI and the registration process.

1) Accepting a person as a user

The first step of the registration is to decide whether a person can be accepted as a user or not. This decision is based on the registration policy of the organization and the credentials the person is handing in (e.g. passport, matriculation certificate, etc.).

In order to build a network of trust between all participating organizations, they have to agree on their registration policy (or policies). It might not be possible to have just one registration policy for all organizations, because the security requirements of a library to register its users is probably lower than the requirements of a university to register its students and employees. Therefore, we assume that it will take several (2-3) registration levels.

2) Registration – storing authorization attributes in a user database

Since in an education network every person should be able to use services from everywhere, access control can no longer be based on location, IP addresses, MAC addresses etc. Therefore, authorization in the AAI environment should be based on personal attributes of a user. This set of authorization attributes has to be standardized among all organizations involved. Otherwise, no cross-organizational authorization would be possible (see chapter 5 for further information on authorization attributes).

During the registration process, the Home Organization stores information about their users in a user database (e.g. Students database, Human Resource database, etc.). In order to be able to co-operate with the AAI, the organization also has to gather and store the authorization attributes. Notice that each Home Organization is responsible for the correctness of the stored authorization attributes – not only just after the registration, but also as long as a user belongs to the organization. Therefore, the organization has to develop appropriate processes to keep attributes up-to-date (and to unregister a user as soon as he/she does not belong anymore).

3) Transfer of the Personal Security Environment

The Home Organization has to provide an authentication system for its registered users. As part of the registration process, the Home Organization has to hand out to the user the necessary information for authentication, called Personal Security Environment, like user name/password, smart card, certificate, etc. It is up to the Home Organization to select their authentication technology, but it might be necessary to agree on a minimum security standard among all organization involved.

4.1.3 Access Control Definition Process

After the integration of a resource within the AAI, the Resource Owner has to define its access control policy and to implement the access control definitions based on this policy. The term *access control definitions* refers to any rules, role definitions, user to role assignments, etc. which are needed by a resource (i.e. the access control manager of a resource) to determine the access rights of a user.

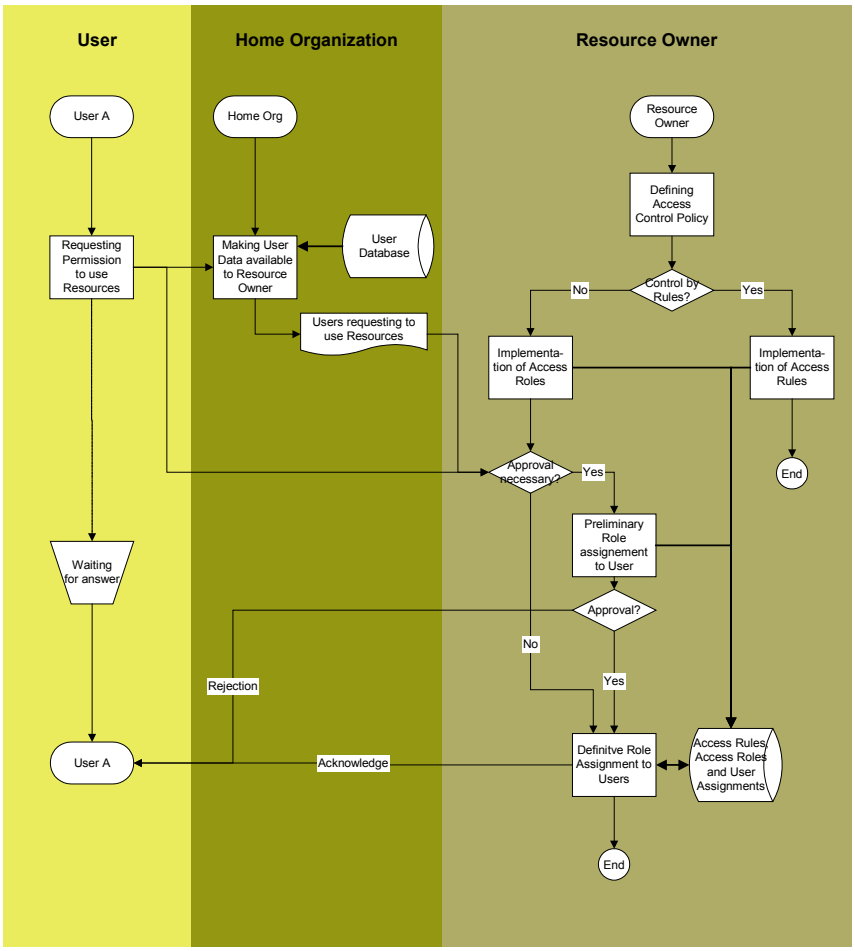


Figure 9: Access control definition process

Briefly, there are two completely different ways to determine the access rights:

A. Often, access control is not given to individual users but to a group of users (e.g. employees of university A, users of library B, students of a specific study branch and/or semester etc.). In this case, access control can be implemented by defining some access control rules based on authorization attributes (e.g. granting access to all students of medicine of university A, B, and C could be formulated as a rule based on the authorization attributes “Name of Home Organization” and “Study Branch”).

B. For some resources, access permission is given only to individual users (e.g. an e-learning system which can be used only by a limited number of students who have received a certain degree). The Resource Owner may accept requests for permissions directly from users or only from Home Organizations. In the second case, the users first have to inform their Home Organization that they want to use the resource; then, the Home Organization has to transfer the information about these users to the Resource Owner.

   Before the Resource Owner assigns access rights (i.e. predefined roles) to the users, it will check whether the users fulfill its access control policy. This check may be done automatically based on the attributes received from the Home Organization or manually based on other criteria. In any case, it will be completely controlled by the Resource Owner.

4.1.4 Authentication and Authorization Process

Authentication and authorization is the main process of the AAI. Assuming that only authenticated users are allowed to access a resource, the basic authentication and authorization steps are as shown in Figure 10:

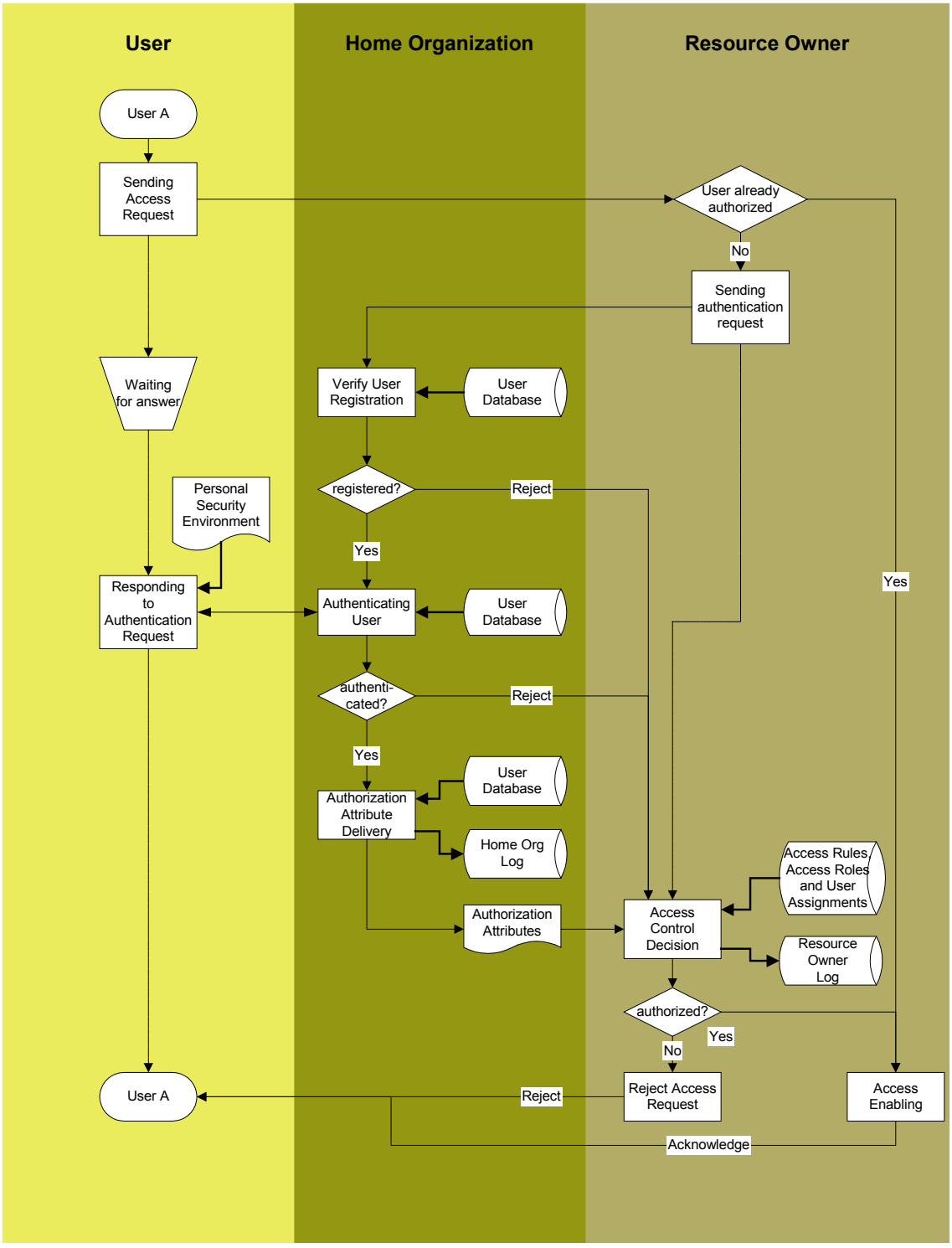


Figure 10: Authentication and authorization process

The process is initiated by a user requesting access to a specific resource.

1) Authentication

The first step is to authenticate the user. Since this authentication can only be carried out by the user's Home Organization, the resource will send an authentication request to it.

If the user is registered with this Home Organization, its authentication system will interact with the user. Using the Personal Security Environment he/she has received during the registration process, the user can prove his/her identity.

2) Delivery of authorization attributes

After a successful authentication, a set of authorization attributes is sent to the resource. This set of attributes should be as small as possible. Only the attributes needed for the (predefined) access control decision must be transferred.

It would be best if the resource could specify this minimum set of attributes it needs for the access control decision. To protect the privacy of users, they, too, should be able to define which attributes they are willing to send to a resource.

3) Access control decision

Based on the received positive authentication answer, the authorization attributes and the access control definition, the resource can determine the user's access rights. If he/she is authorized to access the resource, the functions he/she is allowed to use are enabled; if not, a rejection message has to be sent to him/her.

Other considerations

- In order to improve the user-friendliness and the efficiency, the underlying system of the authentication and authorization process should offer some functionality to recognize users which have been authorized by a resource before, and to skip the three steps described above. Without going into details how this functionality should be implemented, there would be a need for an expiry date of the authentication answer and the access control decision. The expiry date of the authentication would have to be controlled by the Home Organization (which is responsible for the correctness of the authentication); the expiry date of the access control decision would have to be controlled by the Resource Owner, which keeps full control of the resource access.
- In cases in which the Resource Owner is identical with the User's Home Organization, the authentication request could be forwarded directly to the authentication system without using the AAI if this way of proceeding is easier to implement.
- Depending on the requirements of other systems like accounting and billing applications, there will be a need to log some authentication and authorization information by the Home Organization and the Resource Owner (e.g. who has been authenticated/authorized for which resource)
- Caching and/or logging of authentication answers and authorization attributes by the resource have to be in line with legal requirements, especially with the data protection law (see chapter 7).

4.2 Post-processing Phase

Post-processing applications like accounting, billing, usage reporting etc. are not part of an AAI, but they will interact with it.

A billing system for a resource, e.g., will need to know who has used the resource and how it has been used (e.g. how many transactions, which information, how long, etc., depending on the tariff model for that resource).

The AAI is able to answer the question of who has accessed the resource, because it is able to link the information the Resource Owner has about users (e.g. anonymous user IDs) back to real persons only known by their Home Organizations. However, the AAI has no information on the question of how the resource was used. This answer can only be given by the resource itself, which can measure the interactions between a user and the resource.

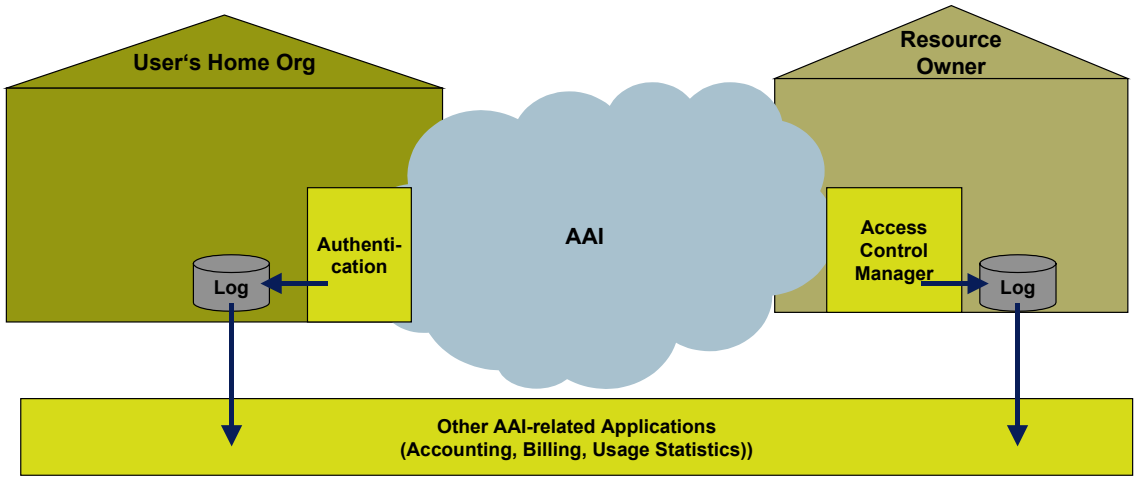


Figure 11: Interface between AAI and post-processing applications

Depending on the requirements of these post-processing applications, AAI (or AAI-related systems like authentication system or access control manager) will have to be able to log authentication and authorization information in a standardized format (to be defined). This will make it much easier to implement post-processing applications across organizations.

5. Authorization Attributes

Authorization Attributes have been previously defined as user data needed for access control decisions (see chapter 2.2). We propose to start with a basic set of such attributes which may have to be extended during the deployment of the AAI, depending on the requirements of the Resource Owners.

The attributes have to be standardized among all organizations participating in the AAI. Nevertheless, it should be possible for an organization or groups of organizations to define local attributes. The technical framework should support such standard and local attribute sets.

It is necessary to install a clear change management to track the implementation of newly required standardized attributes. The AAI Service Provider will be responsible for this change process management in cooperation with the organizations (see chapter 10.1).

The needed attributes are listed below with some brief explanations. It is clear that any technical solution will need a more precise definition of the syntax for each attribute.

Not all attributes are always needed; the resource that is accessed should only ask for the attributes that are needed and the Home Organization should transfer only the attributes that were asked for.

Individual attributes
These attributes are related to an individual: how to identify and how to reach him/her (in real life and via the network). The standardized attributes are the following:

- unique ID
- last name
- first name
- birth date
- sex
- e-mail
- private postal address
- business postal address
- private phone number
- business phone number

With the exception of the unique ID, the definitions of these attributes are straightforward. The unique ID is needed in order to impersonate access to a resource; the identity of the real person should not be directly deductible from the ID. Only the Home Organization of the user should be able to do this linking.

Role or group membership attributes
There already exists a standardization among Swiss Universities and Federal Institutes of Technology (ETH/EPF) for attributes about students and staff. Also the Universities of Applied Sciences (UAS) have standardized this kind of information. These standardizations have been coordinated by the “Service d'Information Universitaire Suisse” (SIUS). The following documents are available on their web site in French[1] and German[2] and contain the details:

[1] http://www.statistik.admin.ch/stat_ch/ber15/fber15.htm

- Système d'information universitaire Suisse, Manuel technique pour les hautes école universitaires
- Système d'information universitaire Suisse, Manuel technique pour le relevé des étudiants et des examens des HES
- Système d'information universitaire Suisse, Manuel technique pour le relevé du personnel des HES

The AAI authorization attribute definitions should be based on the SIUS standard if such definitions already exist:

homeOrganization	This attribute is single-valued and contains the name of the User's Home Organization. The possible values should be in the list of the organizations participating in the AAI.
organizationType	Defines the type of organization. There are five types of organizations, the first two of which are well defined by the SIUS. • Universities and ETH • UAS • SWITCH • Libraries • Hospitals
userType	The type of user defines his or her relation to the Home Organization. The value has to be chosen among the following four values: • student (the documents of the SIUS defines what is a student) • staff • extern, the person is extern to the organization but has access to the resources of the organization • process (computer program or application)
studyBranch1 *studyBranch2* *studyBranch3*	The SIUS has already defined a three-level classification of all "branches d'études" for the Univ.-ETH type of organization. studyBranch1 is the first level and has 8 possible values: "Sciences Humaines + Sociales", "Sciences Economiques", "Droit", "Sciences Exactes + Naturelles", "Médecine + Pharmacie", "Sciences Technique", "Interdisciplinaire + Autre", "Domaine Central". Following the SIUS the second level (studyBranch2) has 22 possible values and the third (studybranch3) 91. For the UAS, the SIUS documents contain also a three-level classification of the "filières d'étude". Our three studyBranch attributes are used to specify this for a student in the case of UAS.
staffCategory	This attribute has only a meaning if userType=staff. The categories defined by SIUS are for Univ.-ETH: • Corps professoral • Corps intermédiaire supérieur • Corps intermédiaire inférieur

[2] http://www.statistik.admin.ch/stat_ch/ber15/dber15.htm

	• Personnel administratif et technique and for UAS: • 10 Enseignement au niveau diplôme • 30 Formation continue: Enseignement au niveau postdiplôme • 40 Recherche et développment • 50 Prestations de services (transfert de technologie inclus) • 60 Administration • 70 Services centraux
organizationUnitPath	This attribute has a meaning only if userType=staff. It defines the position of the user in the structure of his or her Home Organization. There is not a restricted set of values for this attribute. Example of a value: “Institut de physique théorique, Section de physique, Faculté des sciences, Université de Lausanne” According to the SIUS document (p. 21, in French) , each University and ETH has an internal coding of the organization.
memberOf	This attribute contains all the names of the groups to which the user belongs. The groups are managed by the Home Organization and may be used in the context of the AAI.

6. Technical Evaluation

As per the AAI-concept mentioned earlier, one of the results of the subsequent pilot phase is to provide full technical specs of the proposed future AAI. Given the complexity of an AAI and the timeframe being considered, it was ruled out to design a new architecture from scratch. The future AAI is to be based on an existing approach. A survey into potential architecture candidates for an AAI yielded 5 promising results, each described and evaluated in chapters 6.1 to 6.5.

Several of those architectures do cater for secure online transfer of data only, and provide no native support for document signing and encryption. However, we did not rule out those architectures right away, because adding document encryption and signature support to such architectures is possible (as shown in chapter 6.6).

Finally, we give an outlook on international AAI activities and provide a short list of recommended architecture candidates.

6.1 Shibboleth

Shibboleth[3] is a joint project of Internet2/MACE (Middleware Architecture Committee for Education)[4] and IBM. It aims to develop an architecture for standard-based vendor-independent web access control infrastructure that can operate across institutional boundaries.

The focus of Shibboleth is on supporting inter-institutional authentication and authorization for access to web-based applications. The intent is to build upon existing heterogeneous security systems in use on campuses today, rather than mandating particular schemes like Kerberos or PKI based on X.509. Project Shibboleth will produce an architectural analysis of the issues involved in providing such inter-institutional services, given current campus realities; it will also produce a pilot implementation to demonstrate the concepts.

The requirements on which Shibboleth was designed are documented in http://middleware.internet2.edu/shibboleth/docs/draft-internet2-shibboleth-requirements-01.html

Current status of Shibboleth:

Alpha code for use with Apache web server was delivered to a few Internet2 members in March, a beta version is expected in May and a release is planned for summer 2002.

6.1.1 Architecture / System Design

The primary design principles for Shibboleth are:

- No single central piece of infrastructure required, scalable.
- Data protection and privacy are of importance for Shibboleth.
- The user is guided by 'HTTP redirect' from the resource to the authentication server and back to the resource for the authorization

A detailed description of the Shibboleth architecture can be found in *Shibboleth-Architecture Draft v04*[5].

Shibboleth uses a federated administration, a Resource Owner leaves the administration of user identities and attributes to the user's Home Organization, which is also responsible for pro

---

[3] http://middleware.internet2.edu/shibboleth/

[4] http://middleware.internet2.edu/MACE/

[5] Shibboleth-Architecture Draft v045, Marlena Erdos and Scott Cantor, 26 Nov 2001, http://middleware.internet2.edu/shibboleth/docs/draft-internet2-shibboleth-arch-v05.pdf

viding attributes about a user (possibly but not necessarily including a username) that the Resource Owner can use in making an access control decision when the user attempts to use a resource. Users are registered only at their Home Organizations, and not at each resource.

Shibboleth is a system for securely transferring attributes about a user from the User's Home Organization to the site of the Resource Owner, provided the resources are accessible via standard web browsers. In addition, Shibboleth enables the users to decide which information about them gets released to which site. The users therefore have to balance access and privacy.

The major components of Shibboleth are:

WAYF	Where Are You From Server Redirects the user back to the HS at his/her Home Organization. At least one WAYF server is needed, but it may be replicated as desired.
HS	Handle Server Authenticates a local user according to the methods of the Home Organization and provides an opaque handle identifying the user.
AA	Attribute Authority Retrieves the attributes which a user allows to be given to a resource (according to the user's Attribute Release Policy) and passes them to the SHAR on behalf of the resource.
SHIRE	Shibboleth Indexical Reference Establisher Makes sure that the resource gets a 'pointer' (handle) back to the user without requiring more knowledge about a user. In case it is missing it refers the user via the WAYF server back to his/her HS to get one.
SHAR	Shibboleth Attribute Requester Contacts the AA to fetch the available attributes describing the user and passes them on to RM.
RM	Resource Manager Decides on access to the resource based on the information received and where necessary the information about earlier sessions of the same user.

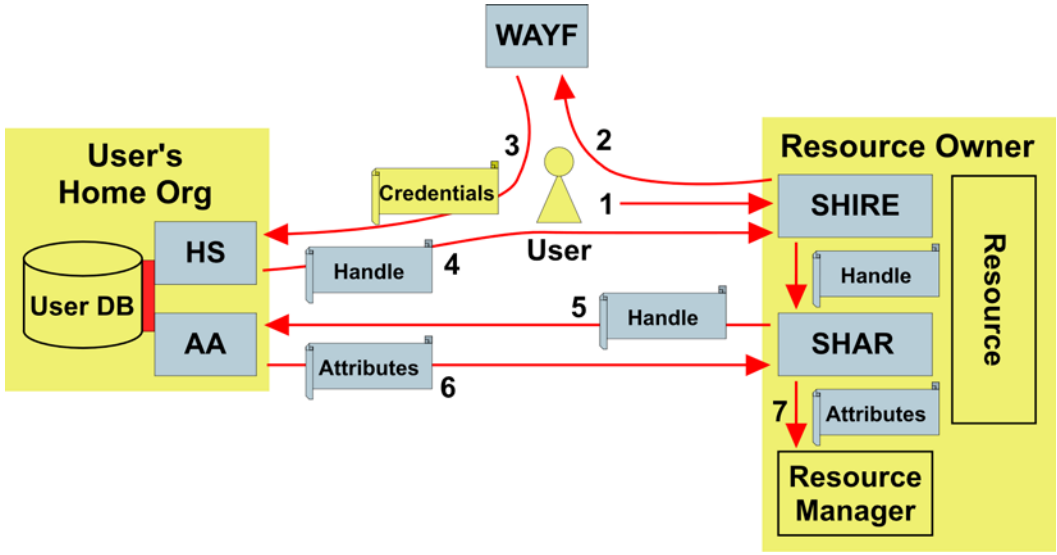


Figure 12: Shibboleth interactions

Example of Shibboleth usage:

A user U, affiliated to the Home Organization O, wants to access a web-based resource R located at some remote site.

- U connects with his or her web browser to the web site R (1). The server R does not detect the required authorization information and redirects U (2) to the 'Where Are You From' web server W. The URL of R gets passed along.
- On W, U selects his/her Home Organization O from a list of organizations participating in Shibboleth. W redirects U (3) to the web server HS (Handle Service) located at the Home Organization O. The URL of R gets passed along again.
- U authenticates him-/herself according the local rules and methods towards HS. Once authenticated, HS generates an opaque handle H for the user U. H is the authentication info U needs to present to R. U gets redirected to R (4).
  R sends handle H together with the URL of R (5) to the Attribute Authority (AA) located at the Home Organization O.
  AA checks which Attribute Release Policy (ARP) of user U applies to resource R. AA returns the attributes it is allowed to send to R (6).
  Within R the attributes retrieved get passed to the Resource Manager RM (7) that decides on providing access.
- U gains access to the resource

6.1.2 Optional Additions to the Shibboleth System Design

We can think of two optional additions to the official Shibboleth System Design that would be beneficial in an operational environment.

The design requires at least one WAYF server and does not specify how more than one interwork. By coordinating the contents of the WAYF servers, each organization that wants to run a local WAYF server could fetch the contents from a single place and could add locally further organizations with which they might have bilateral agreements regarding AAI.

The second addition is a resource registry, describing AAI-enabled resources and listing their required authorization attributes. Registration of resources would be optional. The benefit of such a registry is twofold:

- Portal administrators who want to add lists of resources would have a collection of AAI enabled resources to choose from readily available.
- AA administrators preparing attribute release policy templates for their users would know which attributes a resource requires for proper authorization and could therefore correctly tailor the templates.

As a future extension of Shibboleth, one could imagine a broader use of user certificates; not just for local authentication, but also for authentication against a remote resource. The latter would obsolete the use of a handle server HS. This idea is already mentioned in *Shibboleth-Architecture Draft v04* (see footnote 5), but it needs some more thought to specify the details. Normally, HS provides, together with the handle, the information about which AA to use. That information is not readily available in case of user certificates.

6.1.3 Evaluation

Pros:

- User privacy was from the beginning part of the architectural design. The user controls which information gets released to which resource.
- Federative administration: User's Home Organization is responsible for the authentication, the user is responsible for selecting data to be released, and the Resource Owner is responsible for the authorization.
- Software will be available as open source.
- Supported by Internet2 – good chance for broad adoption.
- Scalable architecture. No singe central infrastructure.

Cons:

- The architecture is designed for web-based resources only. To make it easier for the user, it depends on the HTTP redirection feature.
- Software not yet fully finished, expected for summer 2002.
- No deployment experience yet.

Evaluation:

Shibboleth promises to provide the functionality required; therefore, we should consider gaining operational experience as soon as the software becomes available. Effort will have to be put into the integration of the components AA, HS and RM into the local infrastructure at the participating organizations.

6.2 PAPI

PAPI is a system for providing access control to restricted web-based information resources across the Internet. It intends to keep authentication as an issue local to the User's Home Organization, while leaving the information providers full control over the resources they offer.

The authentication mechanisms are designed to be as flexible as possible, allowing each organization to use its own authentication schema, maintaining user privacy, and offering infor

mation providers the attributes required for access control decisions. Moreover, access control mechanisms are transparent to the user and compatible with the most commonly employed Web browsers, i.e., Netscape/MSIE/Lynx, and any operating system.

PAPI has been designed and is being developed by a small team from the Spanish national research network RedIRIS. Descriptions and the product itself can be found at this location: http://www.rediris.es/app/papi/index.en.html

6.2.1 System Architecture

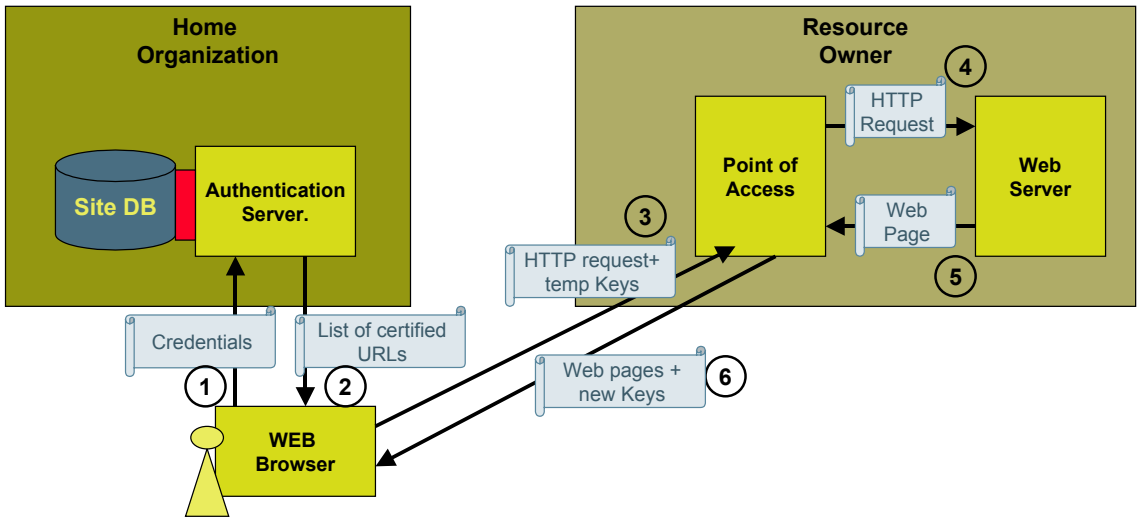


Figure 13: Point of access to providers of information (PAPI) system

System components (see Figure 13)

- Authentication server (AS): The user has to provide credentials to the AS which are in turn verified against the organization's authentication schema (e.g. LDAP, POP, x.509-certs, etc.) [1]. Once successfully authenticated, the AS will consult a local site database and create a web page listing all web resources available to the user. Cryptographically signed authorization information is also coded into those URLs [2].
- User's web browser: While building up the page received from the AS, the user's browser will contact all points of access of those web resources and thus provide them with authorization information.[3]
- Point of access (PoA): This component performs actual access control to a set of protected web resources. It verifies the authorization information it receives from the user's browser and updates cookies in the user's browser to keep track of authorized users [6]. The PoA acts as a dedicated web gateway as shown above and accesses the resource on behalf of the user's browser [4][5]. Alternatively, the PoA can be integrated with the resource as an access control module of the resource's web server.
- Protected web resource: It trusts its PoA(s) to perform access control on its behalf.

Example of PAPI usage

A user, affiliated with Home Organization, wants to access a web-based resource located at some remote site.

1) The user authenticates him-/herself to the AS of the User's Home Organization with whatever method the Home Organization uses for that purpose. The user gets a list of available resources.
2) While the page is being built up, the browser contacts all PoAs of all resources with attribute information embedded in the URL. Each point of access evaluates the received attributes and checks them against a local access policy. Graphical elements in the users browser window will inform about the outcome of that authorization check for each entry in the list of available resources. The PoA will at the same time send cookies to the user's browser allowing the user to access the resource without renewed authentication.
3) The user can now access all listed resources without any further authentication and will only be redirected back to the authentication server after expiry of the cookies.

6.2.2 Optional Additions to PAPI System Design

A very recently released version of PAPI introduces the concept of a GPoA (Groupwide PoA). A GPoA acts as gateway to a set of PoAs with identical access policy. The user gets access to all resources, if the browser initially exchanged keys with the GPoA in charge of those resources. This is an important feature to increase scalability of the PAPI model. Resource hosting organizations are advised to define a short list of different access policies and group all their resources behind a low number of GPoAs, one for each access policy.

The PAPI authors intend to integrate into a future version of PAPI an option that the AS issues lists of resources without instant attribute exchange with all PoAs. The attribute exchange will only take place for the resource the user wants to access. This will further improve scalability and eliminate a potential data protection issue.

One issue still remains: the AS has to know about all resources available to the user. We therefore propose to set up a central database listing all PAPI-enabled resources and their access policies. This will help AS operators to compile a list of resources available to their users.

6.2.3 Evaluation

Pros:

- No requirements to end user software and hardware, besides a web browser with cookie support.
- Supports common authentication methods and can be extended
- Compatible with almost any web-based service. Existing web-based services need not be changed and can be put behind a Point of Access. Only authenticated and authorised users will then be able to access this resource.
- PAPI is operational in Spain to control access to libraries and other university resources. It is being evaluated as access control mechanism to the Open University in the Netherlands and elsewhere.
- Software freely available
- Very responsive development team

Cons:

- The authentication server of the User's Home Organization has to present an exhaustive list of services available to the user. It therefore has to know them all. All available resources need to be registered at the Home Organization.
- All available points of access are accessed after authentication and have to perform authorization checks. It is rather likely that the list of available resources will be rather large, while the user is only interested in a small subset. This is both a potential scalability problem as well as a privacy problem.
- Very small development team.

Evaluation:

PAPI promises to provide the functionality required, but serious concerns over its scalability remain. The scalability issues were promised to be dealt with in future versions and we therefore should consider gaining operational experience as soon as new versions of the software become available.

6.3 GASPAR

GASPAR is used to authenticate users at the École Polytechnique Fédérale de Lausanne (EPFL). People registering for the first time (staff or students) receive a unique ID (SCIPER) and a smart card (CAMIPRO) which holds information on their identity protected by a PIN. This card is primarily used as an "e-key" to gain access to buildings and unit doors but does not store any private key.

6.3.1 Architecture / System Design

GASPAR consists of registration and resource access:

Registration:
(1) Before a user accesses a GASPAR-protected resource, he/she must register with GASPAR. Registration is achieved through terminals using the CAMIPRO card and the PIN code as a means of identification.

Resource Access:
(2) A user tries to access a web-resource. (3) The resource checks whether the user has a valid session before granting access to protected data. If the session does not exist or has expired, the resource uses GASPAR's open API to authenticate the user.

(4) The resource redirects the request to GASPAR's login window and provides necessary parameters. GASPAR identifies the user by SCIPER and password, a digital certificate, or automatically by cookie, if present.

(5) If the user is authenticated, GASPAR sends the identification information (name, e-mail, units, etc.) and a session identifier back to the resource server. It also stores a cookie if the user has previously registered the client machine as his/her default machine. The cookie holds identification information and an encrypted string with a session ID, timestamp, and the IP address of the client.

(6) Upon reception of identification information, the resource server creates a new session for the user (based on the session ID from GASPAR and with the user's identification and a timestamp).

(7) GASPAR then redirects the user's browser to the resource server with session ID and SCIPER as parameters. The resource server checks the session and grants access to protected services.

It is then up to the resource to ensure the security of the communication and a proper access control (identity, session ID, expiration of the session).

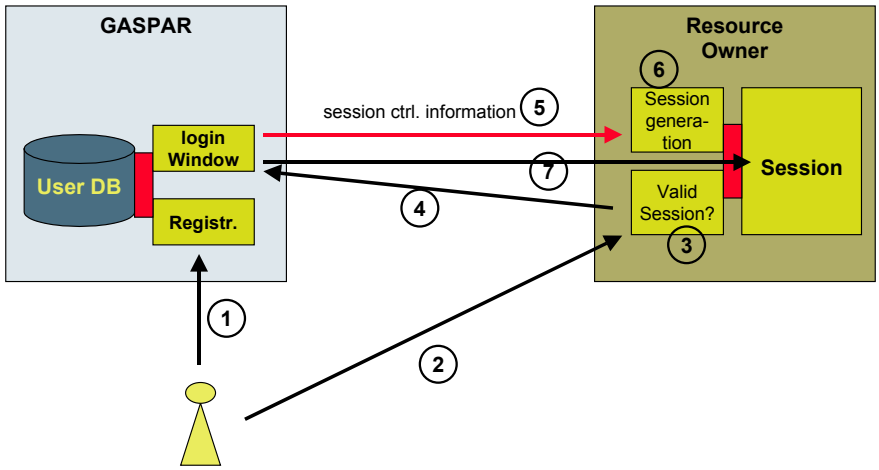


Figure 14: Architecture of GASPAR

6.3.2 Evaluation

Pros:

- Simple, working solution.
- Full control over the development (home made solution).

Cons:

- Solution limited to a single organization: a pathway for generalizing the architecture to many networked organizations is neither available nor planned.
- Extending GASPAR for fitting the requirements of the global AAI may require to fully re-implement the solution, operation which cannot be estimated now.
- Expertise on the tools restricted to a small team, without the necessary resources for extending the solution.

Evaluation:

GASPAR is an interesting, simple solution designed for a single organization. Users trying to access different remote resources must be registered with each single GASPAR authority controlling the remote resource. Thus, the requirement of scalability is not fulfilled.

6.4 FEIDHE

The FEIDHE project is a project of the Finish higher education. It aims at specifying what it will take to implement a public key infrastructure (PKI) based identification system with smart cards in Finnish higher education. Main drivers of the project are data security, flexible use of electronic resources over the network and the national PKI initiative FINEID (Finnish Electronic Identification).

The project is looking for a way to manage identification and authentication when accessing electronic resources and services over networks.

For more details, refer to: http://hstya.funet.fi/

Current status of FEIDHE:

In order to evaluate potential solutions, 9 pilot projects have been initiated and realized during the last trimester of 2001. The final report was expected to be produced by FEIDHE in March 2002. It is not yet available and no English version has been announced.

6.4.1 Architecture / System Design

The main goal of FEIDHE is to clarify the use of PKIs in terms of:

- technical implementation;
- costs: of components (commercial / open source) and of integration in each organization;
- usability;
- large scale deployment.

Nine pilots have been realized, all using smart cards. The smart cards are in general used for storing a certificate. One of the pilots also implemented digital signatures. In eight pilots, commercials certification authorities are used (there is not mandatory use of one specific certification authority).

The major components of FEIDHE are:

Application	Typically a Web Browser. But any application can make use of the infrastructure.
PKI Client	Provides generic access methods to applications for retrieving information from the smart card
SC base components & SC reader driver	Smart-Cards related components
SC reader	Terminal for reading smart cards
Application server	Typically a Web browser, but can be any server
PKI server	Module that validates user's certificates, handles Certification Revocation Lists (CRL), etc.

The following figure illustrates the relationships between these core components:

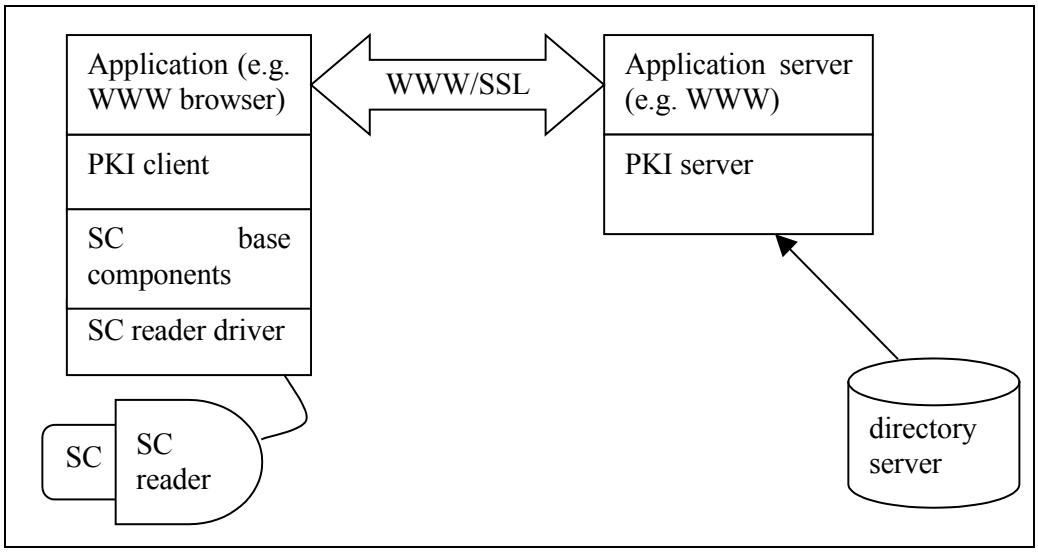


Figure 15: Architecture of FEIDHE

6.4.2 Evaluation

The main goal of the FEIDHE project is to evaluate the use of PKIs along with smart cards for authenticating users. With this objective in mind, the pro and cons can be summarized as follows:

Pros:

- Interesting experience in deploying and using PKIs and smart cards.

Cons:

- Major drawback: smart cards are a mandatory requirement.
- The primary goal is user authentication only. Authorization management may be handled in some sites but is not a key element of the project.
- Current status is unclear as no evaluation report is available.

Evaluation:

FEIDHE aims to introduce smart cards and digital certificates in the Finnish higher education environment. It is built around a global PKI infrastructure, which is why we will not pursue it any further. Nevertheless, we recommend to consider it in the context of a Swiss-wide student card.

6.5 Grid Security Infrastructure (GSI)

GSI[6] was primarily designed for the use in computational grids and is based on public key cryptography using X.509 encoded user and server certificates employing SSL/TLS transport. It is implemented in the open source Globus Toolkit™, currently at version 2.0[7].

---

[6] http://www.globus.org/security/

[7] http://www.globus.org/toolkit/

6.5.1 Architecture / System Design

Public key cryptography requires the availability of each party's private key during a communication. Since private keys should be kept secure, one should not leave a private key unprotected (i.e. unencrypted). For automated distributed computing, this is a showstopper – you are not able to decrypt a private key without the secret known by the owner only. Therefore, GSI makes heavy use of delegated proxies acting on behalf of users and resources. Such proxies use not the original long-lived certificates, but their own short-lived ones. Because they are short-lived, their private keys do not need to be protected as vigorously as long-lived ones and automated processing becomes possible.

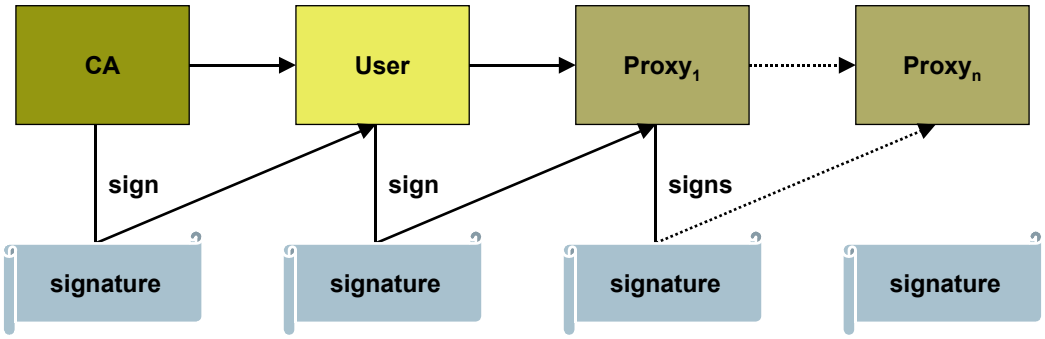


Figure 16: GSI proxy certificate chain

Proxy certificates are not signed by a CA, but by the private key of the issuing user or resource certificate. In addition they can even generate new proxies on their own, e.g. for spawned subprocesses. That way, these proxies can be authenticated and they can securely communicate without involving the real user. Through the chain of certificates, each proxy can be followed back to the original certificate signed by a CA.

When a user wants to access a resource, the resource authenticates the user based on the provided certificate and applies a global-to-local mapping in order to be able to execute the user request in the local environment.

The whole delegated proxy system is rather complex since these proxy certificates include information on the time-to-live and their rights (e.g. are they allowed to spawn off new proxies; to which part of a disk do they have write access).

An article in *IEEE Computer* mentions the use of MyProxy entities for the communication of users with web portals, because the standard web browsers are not able to cope with delegate proxies.[8] One implementation for MyProxy exists, currently at version 1.0[9].

Example of GSI usage for web access:

A user U with certificate UC, affiliated to origin site O, wants to access a web-based resource R located at some remote site via the web portal server WP.

- U generates a proxy UP based on his/her certificate UC and protects it with the password P.
  The proxy UP gets delegated to the trusted host TH that runs a myproxy-server for the portal server WP (or for more than one such server at the remote site).

---

[8] A National-Scale Authentication Infrastructure. R. Butler, D. Engert, I. Foster, C. Kesselman, S. Tuecke, J. Volmer, V. Welch. IEEE Computer, 33(12):60-66, 2000.
http://www.globus.org/documentation/incoming/butler.pdf

[9] http://dast.nlanr.net/Projects/MyProxy/

- U connects via HTTPS to WP and provides the password P.
  WP connects to TH and by providing password P it is able to generate a new delegated proxy UP2 of UP for the use on the web portal server WP.
- U selects the resource R in the web portal WP.
  WP authenticates towards R with the delegated proxy UP2 without having to further involve user U.

6.5.2 Evaluation

Pros:

- Wide deployment in GRID community, mainly for distributed high-performance computing.
- Based on standards (X.509).
- Software is open source.

Cons:

- The architecture is primarily designed for distributed high-performance computing. It is not easily applicable to web-based resources.
- Missing framework for data protection compliant access to authorization attributes.
- GSI requires a standardized authentication infrastructure (X.509 certificates).
- Requires a trusted CA infrastructure.
- Global-to-local mappings need co-ordination, not very scalable.

Evaluation:

The many cons of GSI do not justify further investigation of this technology for AAI purposes. However, it will have its important role in the area of distributed high-performance computing

6.6 Signing and Encryption

Encryption may be used in three different scopes around AAI:

1) Data transfer between components of the AAI.
   When looking at the two recommended architectures, PAPI applies strong encryption for data encoded into URL components. Shibboleth uses SSL encrypted HTTP links. By deploying certificates at both ends of an SSL connection, AAI internal transfers would not just be encrypted but also properly authenticated.
2) Data transfer between an end user and AAI-enabled resources.
   This is not covered directly by an AAI. SSL encryption should be used at least whenever personal information gets transferred.
3) Encryption and digital signing of documents or files in general.
   This is not covered directly by an AAI as discussed in this report. However, chapter 6.6.1 outlines how an AAI can be extended by an overlay infrastructure to cover also that aspect of encryption and signing.

To summarize, authenticating online users and authorizing resource access on the one hand and electronic document encryption and signing on the other hand are rather distinct sets of functions. Authentication and authorization are relevant only during a very short timeframe i.e.

during an online transaction. Document signing and encryption are about protecting data and metadata for future use.

6.6.1 Overlay Infrastructure for Document Encryption and Signing

Bootstrapping a public key based infrastructure for document encryption and signing can very well leverage on an already existing AAI. The two following examples demonstrate how an AAI could be used in establishing an overlay infrastructure and especially how manual administrative interventions can be avoided:

1) By using authentication to identify a user reliably, a public key provided by a user could be bound to an existing identity in the user database. The user could request a certificate for a supplied public-key by communicating with an AAI-protected resource offering certification services.

2) Suppose an organization already distributes smart cards with a pre-loaded unique ID, then AAI could be used to authenticate users presenting their smart card and to authorize them to connect to the service that stores a pair of pre-generated certified secret and public keys onto the card. That way, the link between the public key certificate, the smart card and the user would be established automatically.

A very nice example of such an overlay infrastructure is in use at EPFL:
GASPAR (the EPFL's intra-organizational AAI) is used to protect the initial key handling of their public key infrastructure offering document signing and encryption services.

The requirements to provide encryption and document signing functionality do therefore not rule out AAI architectures without native support for it. Accordingly, we concentrate on the primary functions authentication and authorization and propose to deal with document encryption and signing in a later stage.

6.7 International Activities

We are not aware of an operational infrastructure of similar scale and scope as the proposed AAI covering a nation's academic community. But we are aware of several initiatives with such goals, of which some are mentioned earlier in this chapter. To co-ordinate these activities within Europe, TERENA (Trans-European Research and Education Networking Association) set up the taskforce TF-AACE (Taskforce Authentication, Authorization Coordination for Europe). SWITCH is actively participating in that taskforce, which is chaired by one of the authors of PAPI.

The Swiss AAI project has already attracted attention of other European countries. If the Swiss academic institutions now start building an AAI, they can contribute their experience to the international community and shape the future landscape of an international AAI.

6.8 Technical Recommendation

From a purely technical perspective, none of the studied architectures can be recommended for implementation right away.

The Shibboleth architecture looks very promising but since it is not yet implemented, there is a complete lack of operational experience. PAPI, on the other hand, has been around for a while now. It lacks important functionality and concerns over its scalability remain. Enhancements to overcome those shortcomings were just released or are being implemented shortly. Additional

testing is required to gain operational experience in order to assess their suitability. We recommend testing the two architectures Shibboleth and PAPI.

Document signing and encryption are natively supported neither by PAPI nor Shibboleth. We recommend to build the first release of the AAI without support for document signing and encryption, and to cover those functions as services of an overlay infrastructure in a later release of the AAI.

7. Legal Framework

To implement any of the architectures mentioned previously, a legal framework is needed between the AAI Service Provider and the Organizations (chapter 7.1), between the Organizations themselves (chapter 7.2), and between the Users and their Home Organizations (chapter 7.3) as defined in Appendix A. By legal framework, we understand either existing legislation or a specific contract.

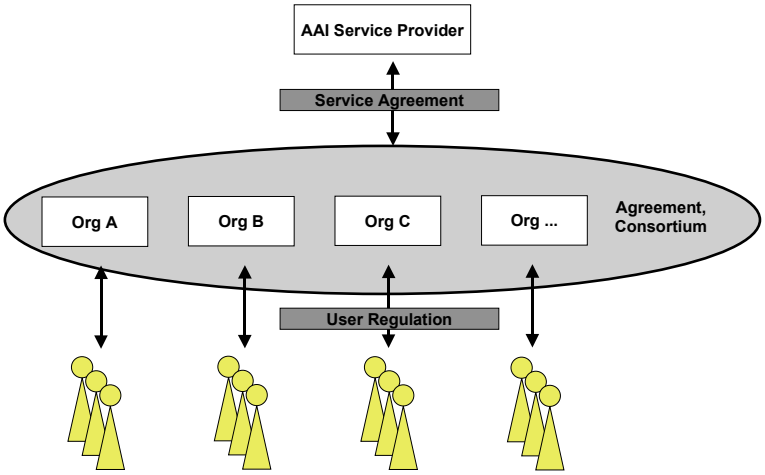


Figure 17: Legal framework

The legal framework must specifically regulate privacy and liability issues relating to the abuse of AAI Resources and AAI Infrastructure. In addition, the selected architectures (chapter 7.4) and the liability issues (chapter 7.5) require detailed review.

Because of the complexity of the AAI, privacy and liability issues may influence the form of the legal framework and vice versa. As a consequence, an isolated study would not be appropriate; a detailed analysis taking into account all the issues mentioned above is needed.

The pilot phase will start in June 2002. It is impossible to set up the legal framework outlined below until early June; therefore a work-around solution is suggested (chapter 7.6).

In addition, license and copyright issues are a specific problem. As each Organization has various license agreements and a different view on copyright issues, the Organizations need to review this matter themselves. *License and copyright issues are consequently the responsibility of the Resource Owners. This is why license and copyright issues are not the subject of this report.* The legal opinion of Mr. Julius Effenberger regarding copyright issues within the Swiss Virtual Campus may be of assistance to the Organizations in their analysis.[10]

7.1 Framework Between AAI Service Provider and Organizations

7.1.1 Issues to be considered

The main issues are those of how the Organizations contract with the AAI Service Provider and what specific formal requirements have to be fulfilled. For this purpose we have assumed that the AAI Service Provider only provides know-how and support in the form of a competence center.

[10] This report may be available at Schweizerische Universitätskonferenz (SUK), from Mrs. Cornelia Rizek-Pfister.

The acquisition of infrastructure and data transmission in the proper sense are the responsibility of the Organizations (it may be that they will call in a third party or use existing transmission lines).

The legal relationship between the AAI Service Provider and the Organizations can take several forms:

- Contracts under private law
- Contracts under public law
- Using the legal vehicle of a foundation.

7.1.2 Contracts under Private Law

A contract governed by private law between a public law entity (e.g. an Organization) and a private party would be possible, provided that the Organization were not acting in fulfillment of its immediate public duties but as a market player (e.g. in the purchase of office supplies).

However, due to the legal provisions and objectives of the constitutions of several Universities, the Organizations fulfill an immediate public duty in providing AAI (see below), with the result that this form of contract is not possible.

7.1.3 Contracts under Public Law

Contracts under public law deal with the fulfillment of an immediate public duty; the Organizations are acting in a manner defined by public law. The legal nature of the participating parties is of no importance (i.e. whether the parties are constituted under private or public law). The only relevant factors are the functions to be performed under a contract and the interests linked to it. In the case of contracts governed by public law, the law of contract is applicable in a subsidiary manner. A public contract creates vested rights (so called "Wohlerworbene Rechte") , which are difficult to modify and terminate.

If the AAI Service Provider were a legal entity under private law that was not related to the Organizations, the contract would be governed by public law, due to the public law tasks and interests that have to be fulfilled.

7.1.4 Foundations

Providing AAI Services to the Organizations can also be achieved by means of an existing foundation, or a new foundation specifically founded for this purpose.

SWITCH, in terms of its Articles, has to deliver “telematic infrastructure and services to the Organizations”. Originally SWITCH was set up as a foundation by the Swiss Confederation and the eight university cantons. The new universities in the cantons of Lucerne and Ticino as well as the UAS are members of the foundation board in accordance with the by-laws of the foundation (Reglement der Stiftung). The objects of SWITCH include in our opinion AAI Services.

The necessary legal framework can be established within a new by-laws of the foundation. With regard to the question of the content of such a regulation, an assessment will have to be made of whether SWITCH would also be subject to the terms of the Federal Data Protection Act.

As the service provided by SWITCH or a third party will be that of a "center of competence", SWITCH will not provide the means of transport and will not process data from or to be used by a Resource Organization, except for its own use. As a consequence, no personal data in the sense of AAI or other kind of data is processed by SWITCH, so data protection issues may not arise. The question of liability for abuse of the AAI-infrastructure will be different in the event that SWITCH or a third party gives the wrong advice. Provision must be made for this. In addi

tion, costs have to be divided between the Organizations according to a distribution key which has to be defined.

The pilot phase will last until June 2003. By this date an appropriate provision must be inserted into the Articles and By-laws of the foundation. A draft thereof will have to be prepared for the next board meeting in October / November 2002 to be on schedule for June 2003.

7.1.5 Recommendations

The JUR Team recommends that the Project Board decide by August 2002 whether a third party or SWITCH should provide the AAI Services for the phase following the pilot phase. In the event that a decision is made in favor of SWITCH, an appropriate provision to be set up in a new by-laws of the foundation must be approved by the board at its meeting in October/November 2002. In the event that a third party is selected, we recommend that a contract under public law be concluded.

7.2 Framework Between the Organizations

7.2.1 In General

The legal framework between the Organizations has to be an instrument which complies with the legal requirements regarding data protection as well as liability for abuse of AAI resources and infrastructure.

In order to verify whether the Organizations are in line with such legal requirements, it must be defined in a first step whether they are acting in fulfillment of a (chapter 7.3.2) Federal or a Cantonal legal duty. The answer to this question will decide the applicable law, i.e. either Federal or Cantonal law.

In a second step (chapter 7.3.3) the nature of the attributes that will be “processed” by the Organizations has to be analyzed carefully: are the attributes regarded as personal data, sensitive personal data or personality profiles?

The answer to this question will confirm the legal basis required and the question how such requirement can be met by a (chapter 7.3.4) legal framework in general and for the universities and the UAS in particular.

The answers to the above questions lead to the general recommendations (chapter 7.3.5) regarding the legal framework between the Organizations.

7.2.2 Applicable Law

AAI’s aim is to coordinate infrastructure use and to allow the users access to the resources of other Organizations.

According to Article 63 of the Federal Constitution, the Federation “shall operate Federal Institutes of Technology. It may create, operate, or support other universities and institutions of higher learning. It may make its support conditional upon the taking of coordination measures”) and according to Article 64 of the Federal Constitution “The Confederation shall encourage scientific research. It may make its support conditional, in particular, upon the taking of coordination measures. It may create, take over, or operate research institutions.

On the basis of these provisions, the Federation has regulated the coordination of education in various enactments, with some of this legislation coming from the Federal government alone, other legislation being enacted at Federal and Cantonal level and further legislation coming from the Cantons themselves. Relevant are especially:

a) Universitätsförderungsgesetz (UFG, SR 414.20) (Universities Promotion Act)

b) Universitätsverordnung (UFV, SR 414.201) (Universities Ordinance)

c) Interkantonales Konkordat über die universitäre Koordination vom 9. Dezember 1999 (Intercantonal Concordat on Coordination between Universities of 9 December 1999)

d) Vereinbarung zwischen dem Bund und den Universitätskantonen über die Zusammenarbeit im universitären Hochschulbereich (SUK Regulation/Agreement between the Swiss Confederation and the University Cantons on Cooperation in the University Sector)

According to Article 10 of the SUK Regulation, the Swiss Universities Conference in particular aims to support cooperation between Swiss Universities and Swiss UAS, and in particular cooperation in the field of universities supporting the common use of infrastructure and the federalist division of labor (SUK Regulation Article 10 al 3 lit. b).

Furthermore, the Intercantonal Concordat on Coordination between Universities also regulates the creation of networks and centers of competence in the fields of both universities *and* UAS, which is especially mentioned when defining the term “Hochschule” as covering universities as well as UAS (Art. 1 al. 2 lit. a together with art. 2 al. 1).

As a consequence, the AAI fulfils a Federal duty and Federal law has to be applied.

7.2.3 Nature of the Attributes: Personal Data

To determine the nature of the attribute, it must be clear whether Federal or Cantonal law is applicable or not. The Federal Data Protection Act regulates the processing of data on physical and legal persons undertaken by private bodies and Federal bodies (Article 2 DPA). Federal bodies are defined as all federal authorities and services as well as **persons entrusted with federal public duties** (Article 3 lit. h DPA). As outlined above, the duties which AAI and the Organizations fulfill are public duties.

They therefore act as Federal bodies in terms of the DPA and the following principal rules apply:

a) the Home Organizations are, to the extent they qualify as public bodies, subject to the data protection provisions of the Swiss Federation with regard to the AAI. For other data processing, the rules of the Canton where they are domiciled apply in addition to the DPA

b) the foregoing also applies to the Resource Organizations.

c) In the event that he provides more than just a competence center, the AAI Service Provider will be subject to Art. 12 et seq. of the DPA if it is a private company. If SWITCH is commissioned to provide further infrastructure services in relation to the AAI over and above those outlined above under chapter (i), then the provisions of the DPA relating to public bodies are likely to apply.

The fundamental rules of the DPA and most Cantonal data protection legislation are:

a) Only "personal data" is protected; personal data includes all information about a specific or identifiable person such as his or her name, address, birth date, etc.

b) "Sensitive personal data" such as religious beliefs, health information or any criminal record, together with personality profiles benefit from heightened protection. Such data includes all personal information which is only known to a small number of selected persons and which is of particular emotional importance to the affected person. The Federal Data Protection Commission has clarified that personality profiles by definition require a critical mass of data covering a certain time period which allow a recipient to reach a value judgment about a specific person. Information including the name and address of a person, birth date and exams taken (pass/fail, repetitions etc.) are not deemed to constitute a personal profile. On

the other hand, the resource history of a user, including inter alia his or her favorite library titles, delays in returning resources, preferred classes and exams taken, may well amount to a personal profile.

c) Personal data may only be processed if
   (i) authorized by law;
   (ii) the processing is reasonable, i.e. useful, necessary and proportionate;
   (iii) data is not used outside the scope of use anticipated at the time of collection; and
   (iv) the integrity and security of the data is guaranteed.

d) Sensitive personal data and personality profiles may be processed only if such processing is specifically authorized by a formal law or exceptionally if,
   (i) it is absolutely indispensable for a clearly described task contained in a formal law
   (ii) the Federal Council approves the processing because the rights of the persons concerned are not jeopardized; or

e) A person may, in an individual case, agree that data may be processed without legal authorization, if such consent is given voluntarily and expressly. Where personal data has been made publicly available, such consent to its processing may be presumed.

f) If personal data is anonymized, it may be used for planning and statistics without a person's consent if such person is not identifiable from the data so processed.

g) Databases containing personal data require to be registered with the Federal Data Protection Commissioner.

h) Personal data may not be exported to countries which lack adequate data protection systems. The Federal Data Protection Commissioner has published a list of countries that meet the adequacy threshold.

As a consequence of sections c and d above, it is necessary to have a solid legal basis or the consent of the user for every single transmission of personal data. As users normally give their consent for the use of their personal data by the Home Organization (within the acceptable use policy), the consent must be extended to the Resource Organization and to each request for access to a Resource Organization. If this condition cannot be met a legal basis (statute or ordinance) is needed.

Within Shibboleth, each single request for access to a Resource Organization provokes the consent of the user to the transmission of his or her personal data, whereas PAPI does not provide such a tool. It would therefore be safest to have a statutory basis therefore.

Depending on the qualification of the processed data the legal basis has to be a primary source of law (statute) or a secondary source (ordinance). The ORG-Team outlined the Attributes as follows (see chapter 5):

a) Individual Attributes such as: unique ID, last name, first name, birth date, sex, e-mail, private postal address, business postal address, private phone number, business phone number.

b) Organization Attributes such as: homeOrganization, organizationType, userType, organizationUnitPath

c) Role and Group membership Attributes such as: studyBranch, staffCategory, memberOf

According to the principles outlined above, this set of data qualifies as personal data. No sensitive data is mentioned and a personal profile is not given. Adding some more Attributes, i.e. points or scores in the context of the European Credit Transfer System (ECTS) may change this result. We recommend that the list of Attributes is re-examined before its is enhanced.

7.2.4 Legal Framework

As outlined above, the processing of personal data needs to have a legal basis. A specific legal basis in the form of statutory law is currently missing. However, we have explored certain secondary sources.

According to Article 10 sec. 2 of the SUK Regulation, the universities work together with the UAS; according to Article 2 of the Intercantonal Concordat the definition of Universities includes both universities and UAS. The SUK can make decisions to promote the common use of infrastructure. For such decisions, each university and UAS has a vote.

This democratic procedure gives these decisions a certain legitimacy which is inherent to legal sources. Decisions based on the SUK may be sufficient for data protection purposes for as long as the Attributes are deemed to be personal data (and not sensitive data or profiles). We therefore recommend that SUK takes a new decision addressing at least some guidelines for the processing or handling of personal data: although not compulsory from the juridical point of view, this will certainly enhance the legitimacy of any new data transmission project.

The UAS which are not part of the SUK Regulation may wish to join the Intercantonal Concordat for the purpose of AAI (in the event that any UAS is not already affiliated to it). This specific decision lies with in the competence of each canton.

7.2.5 Recommendations

The AAI is subject to Federal law. The selected Attributes qualify as personal data, with the result that the consent of the User is needed, or alternatively an adequate legal basis in the material sense, which regulates data protection issues as well as the liability among the Organizations. Such a legal basis may be established by a decision of the SUK. UAS from Cantons that are not signatories to the Intercantonal Concordat may wish to sign up to it for the purposes of the AAI.

7.3 Framework Between Organizations and their Users

7.3.1 General

The peculiarities resulting from the AAI's creation have to be integrated into acceptable use policies (AUP) of the participating universities and UAS (or into parts thereof, e.g. the policies of libraries). AUPs are *based on public law* and are of a *quasi-legislative nature*. They are based upon rules resulting from the legislative procedure (German: "Gesetz im formellen Sinn") (e.g. University Acts of the Cantons, Acts establishing the Swiss Institutes of Technology (German: "ETH") or a concordat). As a result of the launch of AAI, each AUP has to be supplemented with a clause of identical content, dependent on the prevailing law.

7.3.2 Sample Clause

A sample clause, which may be inserted in the home institutions use regulations and which **should be signed by the user**, may read as follows:

"The user notes that personal data about the user is compiled from generally available sources and from communications received from the user and other universities as well as from off-site

sources. The policy relating to the use and procession of such data is posted on the University website at XXX. Such data will be used inter alia to authenticate and authorize the access to and use of various resources within the University and on other sites (*Approved Uses*). The user hereby consents to the collection, processing, use and release of such data to the extent reasonably necessary for the Approved Uses. Such consent includes (but is not limited to) the release of personal data to other institutions by employing cookies and electronically exchanging, caching and storing personal authorization attributes."

This clause will have to be reviewed after the final architecture has been selected.

7.3.3 Recommendations

The relationship between User and Organization has to be set up in the AUP, in particular for data protection reasons. While the above sample clause may in many instances prove to be appropriate , it must be reviewed when the final Architecture is chosen.

7.4 Review of Selected Architectures

7.4.1 Preliminary Remarks

The following analysis draws from a short summary of the two Architectures, Shibboleth and PAPI. Our understanding of these architectures is thus of a preliminary nature only.

7.4.2 Shibboleth

The "federated" administration approach used in Shibboleth gives rise to the following remarks:

- Since authentication occurs at the home institution, no personal data needs to be exchanged with the resource institution for authentication purposes. Data protection issues will only arise at the home institution and may already be dealt with at this level.
- Authorization to use resources will depend on attributes exchanged between the Attribute Authority and the Attribute Requester (SHAR). To the extent that personal attributes are exchanged (i.e. name, birth date, year of study) which make the person identifiable, the above rules regarding legal authorization and restrictions on the processing of data apply. However, we note that the attributes are selected by the home organization and are released in accordance with its Attribute Release Policy. In the event that (i) a user may restrict the attributes to be forwarded to the resource organization (and is aware of such means), and (ii) no sensitive attributes or personality profiles are forwarded, he or she may be deemed to have consented to the release.
- If personal attributes are stored or "cached" at the SHAR or the Resource Manager of the resource institution, further issues relating to security, integrity, administration, updating and relaying of such data arise. Since the statutory data protection rules apply a subsidiarity standard, it should be checked whether such storing or caching is actually required for Shibboleth to work properly. In addition, the user should be informed of such data processing by third parties.

7.4.3 PAPI

PAPI applies an access control based on public key encryption. Our preliminary comments thereon are:

- In the PAPI architecture, **authentication** data appears to be centralized in one location, the Authentication Server. We assume that this server as well as the Site Database Module is located within the home institution, and governed by the rules thereof. If so, AAI does not raise any particular concerns in this respect.

- Certain user data is "transported" in the HTTP requests to the Point of Access by means of encoded information in the URL. We understand that such information may, although encrypted, allow the identification of a user, dependent on the accessed resource. Therefore, the user must be informed about the purpose, the use and the content of such URLs (cf. bulletin 2/2000 of the Federal Data Protection Commissioner).
- The PAPI architecture appears to generate any number of authentication keys (in the form of cookies) that are required for a user to access all the authorized information at the resource institution. Furthermore, all this information appears to be released to the PoA without the requirement to request specific authorization from the user. This procedure raises concerns as regards the proportionality of such use of personal data. *It is presumably technically feasible to modify the next release of PAPI so that such information is forwarded only to resources that are actually accessed by the user. Without this PAPI cannot be recommended from a data protection point of view.*
- Any user will leave traces in the PoA modules and the web servers of the information provider. Collection and use of such data are, to the extent the user is identifiable, subject to the generic data protection rules outlined above. We would recommend that such data is (i) deleted from the PoA at the end of each session and (ii) not passed on to the resources.

7.4.4 Further Remarks

The export of personal data to foreign resource institutions under either of the above architectures is subject to further restrictions.

Irrespective of the chosen architecture, the home institution should use a disclaimer informing users inter alia of the following:

- from which sources and for what purposes, i.e. intended uses, personal data is collected;
- where and for how long the data is stored and how it is protected;
- which body is responsible for controlling the processing of such data;
- whether and for what purposes personal data is disclosed to third parties;
- whether internal guidelines govern the collection and processing of personal data; and
- what rights a user may assert to receive information about his or her personal data and what options are available to prevent the disclosure of personal data to third parties.
- Additional information (e.g. regarding the equivalence of foreign data protection rules) is required if the data is to be exported outside Switzerland.

7.4.5 Recommendation

From a legal point of view Shibboleth seems to be much more appropriate, in particular because users can decide in each case what kind of personal data they wish to send, and because they can manage their data profile themselves. If PAPI's handicap of sending data to all Resources instead of only to the one that actually requires the data can be eliminated technically in the next release, and an individual consent can be set up, PAPI is an alternative to Shibboleth, with the proviso that users cannot manage their own sets of data. We therefore favor Shibboleth.

7.5 Liability for Abuse of Resources and AAI Infrastructure

7.5.1 In General

As the Organizations are public bodies, their liability is governed by public law, either by Federal or Cantonal statutes, depending on the nature of the public body. A SUK decision can therefore only be within that scope. The following principles may apply nevertheless:

7.5.2 Abuse of Resources

In principle, the injured party and in particular the Resource Organization has to identify the person responsible for the abuse of the Resource. If the Resource Organization could not identify the person responsible (because the Resource Organization did not ask for enough Attributes to identify the person), a cascade of liability applies. In such case, the Home Organization has to identify the responsible person. If the Home Organization is not able or unwilling to reveal the identity of the person responsible for the abuse, the Home Organization is liable. Liability restrictions and the degree of care required (relogging, password, user identification for Authentication etc.) have to be defined in the contract or within the legal framework between the Organizations.

7.5.3 Abuse of AAI Infrastructure

The principal rules of abuse of resources as outlined above apply here as well. If the person responsible for the abuse could not be identified, the Organization providing the AAI-Component (authentication, administration of attributes, change and transmission of attributes, access control, etc.) is liable for the abuse according to the provisions of the contract or the legal framework between the Organizations.

7.5.4 Recommendation

The JUR-Team recommends that the above outlined principles are established as binding between the Organizations by a SUK decision.

7.6 Work-around Solution for the Pilot Phase

7.6.1 Starting Point

As shown above, a proper legal framework has yet to be established. This cannot be done until the beginning of the pilot phase, with the result that a work-around solution is needed.

7.6.2 "Agreement"

The mere intent or duty to negotiate can be made the subject of an agreement or undertaking. The title of such "agreement" (Letter of Intent, Memorandum of Understanding, Term Sheet) is irrelevant. What matters is the content of the respective undertaking. In particular, the available instruments may be divided into binding and non-binding undertakings.

In general, Letters of Intent oblige the parties to lead good faith negotiations towards a common goal. However, if appropriate wording is used, such instruments are non-binding as regards the results of the negotiations. If no common ground on the major deal points can be found, each party is free to proceed as it likes. This being said, the appropriate form of an "agreement" between the Organizations for the pilot phase would appear to be a non-binding Letter of Intent.

7.6.3 Recommendations

We therefore recommend drafting a Letter of Intent of a non-binding character before the beginning of the pilot phase.

8. Financial Considerations

Authentication and authorization is an issue that all organizations have to deal with nowadays. Most of them are – more or less intensively – looking for solutions that fulfill their own needs, while some have already started making investments. These efforts had best be coordinated from a very early stage on in order to prevent costly harmonization and adjustments later on. Therefore, a Swiss-wide strategy that takes into account the needs of the individual organizations would have the advantage of generating a solution with compatible components right from the beginning.

Standardization offers even more advantages, for as soon as all organizations use the same system architecture, parts of the AAI can be operated by a service provider. In terms of finances, outsourcing may make sense, because costs tend to be lower if the operation is handled by a single service provider (economies of scale). We therefore recommend at least those organizations which do not yet have their own solution to outsource the running of the AAI.

From a financial viewpoint, the success of the entire AAI project depends primarily on the question of whether or not the demand for mobility, i.e. cross-organizational access to resources, will grow considerably. If so, increased coordination between organizations will be necessary; the implementation of an AAI will then be advantageous as it reduces administrative expenses. Besides, one should bear in mind that in many cases, AAI-related costs will represent but a small portion of the overall costs that increasing mobility will entail.

Even if mobility will not grow as expected, the investments made in the pilot phase will never be in vain, because the organizations can profit from the insights gained there (e.g., with location-independent access to their own resources).

One more aspect needs to be considered: even if the mere AAI-enabling act turns out to be affordable, some organizations might find that the opening of their resources to large numbers of users is too expensive (additional licenses, bandwidth, hardware, etc.). As a consequence, the total number of AAI-enabled resources might stay limited. Yet this risk can be reduced to some extent by careful financial planning that includes cross-organizational billing.

8.1 Cost Estimation

It proved impossible to make accurate cost estimations at this stage since too many questions (e.g., detailed functionality, number of resources and thus number of users, etc.) remained unanswered.[11] Therefore, what is presented here is only a rough overview of the costs, divided into pilot phase and implementation phase[12]. The pilot phase will provide the necessary data for working out a more detailed estimation for the implementation phase.

8.1.1 Pilot Phase

The costs that will arise in the pilot phase are mainly staff costs. The estimation shown below is based on the budgets of the pilot projects.

---

[11] Notice that these uncertainties were one of the reasons why we refrained from considering the development of a new solution; the financial risks can be diminished by adapting already existing international solutions.

[12] See chapter 10 for more details on pilot and implementation phase.

Aspect	time expenditure per project (person days)	number of projects covering this aspect	total estimated time expenditure (person days)
Integration of registration and authentication	20 - 150	4	400
Resource integration	15 - 30	8	200
Central AAI services	220	1	220
Strategy, marketing, project management	440	1	440
Total			1260

8.1.2 Implementation Phase

Costs for Home Organizations

As for the implementation phase, we assume that authentication and authorization are already implemented in the systems of Home Organizations. Their integration into the AAI will consist of the following tasks:

- Adaptation of existing registration due to additional authorization attributes
- Integration of the existing user database with the AAI:
  We assume that an AAI-specific user database has to be implemented between the existing user database and the AAI. It will contain an extract of all the relevant authorization attributes in the appropriate AAI format.
- Integration of the authentication system
- Adaptation of all AAI-related processes, e.g. the registration process

The costs for carrying out these tasks depend on the actual infrastructure of each Home Organization and the functionality of the selected architecture. Therefore, it can only be estimated by each organization after the final architecture has been selected in the pilot phase and more information has been collected.

Costs for Resource Owners

Costs of resource integration depend on the system architecture of the resource as well as on the access control policy that is to be implemented. An estimated time expenditure of 5 to 20 days per web-based resource seems reasonable.

Costs for the Service Provider:

An annual fee will compensate the AAI Service Provider for building and operating central parts of the AAI (see also chapter 10.1).

8.2 Financing

It is not within the scope of this study to make elaborate suggestions to Resource Owners of how to finance the AAI project. Especially since the AAI has to be seen in the context of in

creased mobility and cooperation between organizations, only Resource Owners are able to work out their own financing models.

8.2.1 Pilot Phase

The pilot phase is meant to provide data which will help to plan the implementation in further detail, and, as such, is an indispensable step in the entire AAI project. We therefore suggest a cost-splitting for the pilot phase analogous to the one for this study; i.e., SWITCH will pay for coordination, marketing etc., whereas the organizations pay for their own pilot projects.

8.2.2 Implementation Phase

The benefit of an AAI environment grows with every resource which is made available for members of other organizations. The financing model as suggested below might be an inducement to organizations to open their resources:

- Home Organizations bear the cost of adapting their own processes and systems (registration and authentication), because the AAI can also be used only for internal purposes.
- The expenditures on the AAI core system are shared among all parties involved (e.g. on a per organization or per user basis), which means that the Service Provider has to finance it in advance.
- Resource Owners bear the costs of making resources available.[13]

[13] This, of course, does not exclude any agreements between individual Organizations about charging for the use of resources.

9. Conclusion

A close scrutiny of various aspects of authentication and authorization has shown that feasible solutions exist. We are convinced that the implementation of an AAI will bring about the benefits as outlined at the beginning of the project (see chapter 2.4). In many cases, an AAI will improve the security, enable new functionality and lower the total security cost.

Technical aspects:

There are two promising architectures of an AAI available: PAPI and Shibboleth. Both of them have been developed for a large academic community. While Shibboleth is still in the course of development, PAPI has been running in a productive environment for a while. Neither of the architectures fulfills all evaluation criteria but both are promising enough to go into an extensive test and pilot phase.

Organizational aspects:

It has been shown in chapter 4 that an AAI can be well integrated into existing processes of academic institutions. The selected architectures (i.e. Shibboleth and PAPI) are designed in a way that they are in line with the most important organizational requirements:

- User's Home Organizations stay responsible for authenticating their users
- Resource Owners keep full control of their resources an the access rights
- Existing user databases and authentication systems do not have to be replaced but can interface with the AAI

Authorization attributes, which have to be sent from Home Organizations to Resource Owners, are generally already collected by the Home Organizations, because they need them for statistical reasons anyway.

Legal aspects:

The main legal issue of an AAI is to be conform with the data protection law. We have been able to work out a framework which solves the legal issues between organizations, service providers, and users and can be set up in a reasonable amount of time. Until all the legal instruments are in place, a Letter of Intent (LoI) will be a sufficient legal basis to start with the pilot phase.

Since personal data will be exchanged between organizations, we will have to continue to review the Shibboleth and PAPI implementations to make sure that they fulfill the requirements of the data protection law.

Financial aspects:

The costs that will arise in the pilot phase basically consist in staff costs. Because the participating organizations, including SWITCH, are willing to pay for their pilot projects by themselves, the financing of the pilot phase is guaranteed.

A more detailed cost estimation will have to be worked out for the implementation phase; therefore, the necessary data will have to be collected during the pilot phase.

Final recommendation

The project team recommends to build an AAI organization and to start a pilot phase which is to lead to the final selection of the AAI architecture. Also, the recommended solutions of the organizational, technical, legal, and financial issues has to be worked out in more details.

10. Next Steps

10.1 AAI Organization

As the generic functional model of the AAI (chapter 2.2) illustrates, the AAI both affects existing organizations and provides new functionalities. This means that on the one hand, there will be clearly defined tasks (as described in chapter 4) that a Home Organization or a Resource Owner has to perform itself; on the other hand, there is a number of important inter-organizational tasks that have to be carried out. It is crucial that responsibilities for these tasks are coordinated and/or assigned to some organization, called AAI Service Provider. SWITCH might be one possible candidate for such inter-organizational tasks, but not inevitably the only one.

We suggest to group these activities, which occur both in the pilot phase and the implementation phase, into the following categories:

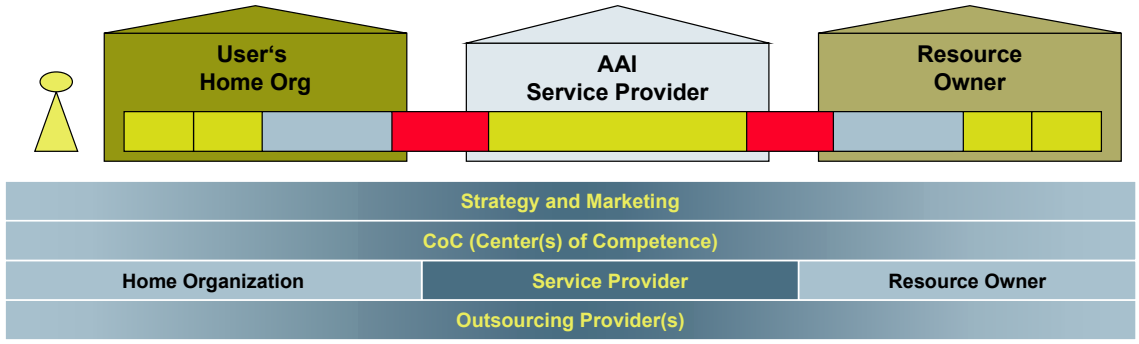


Figure 18: AAI Organization

- **Strategy & Marketing**:
  Responsible for AAI business alignment, marketing, financing, contracting, and policies. Especially the heterogeneous environment requires that someone assumes the role of "ambassador," promoting further the AAI idea.
- **Center(s) of Competence**:
  They act as information and coordination hub by
  - serving as interface to developers of the AAI kernel, international organizations, etc.;
  - coordinating and performing inter-organizational tasks such as change and release management or defining attribute specifications; and
  - building up and sharing its knowledge by means of implementing sample solutions, running a test lab, and creating a knowledge base.
- **AAI Service Provider:**
  Provides central AAI services.
- **Outsourcing Provider(s):**
  Providing outsourcing services such as user directory or authentication may lower the entrance barrier for some Home Organizations, because it becomes easier for them to join in and may also reduce internal costs.
  Services that may be provided for Resource Owners are e.g. AAI-enabled portals.

10.2 Roadmap

The further proceeding includes the following steps:

- Letter of Intent (LoI): June 2002
- **Pilot phase**: June 2002 - June 2003
- Implementation decision: June 2003
- **Implementation**: July 2003 - June 2005
  roll-out release 1.0 mid 2004
  roll-out release 2.0 mid 2005

10.2.1 Pilot Phase

Main goal of the pilot phase is to finally be able to answer questions that can only be found by means of practical testing, and thereby get the basis for the definitive selection of one architecture. It is also the pilot projects that will produce all detail specifications. At the end of this phase, technical, organizational, and legal feasibility as well as the benefits of an AAI can then be convincingly presented, and some projects may also serve as show cases.

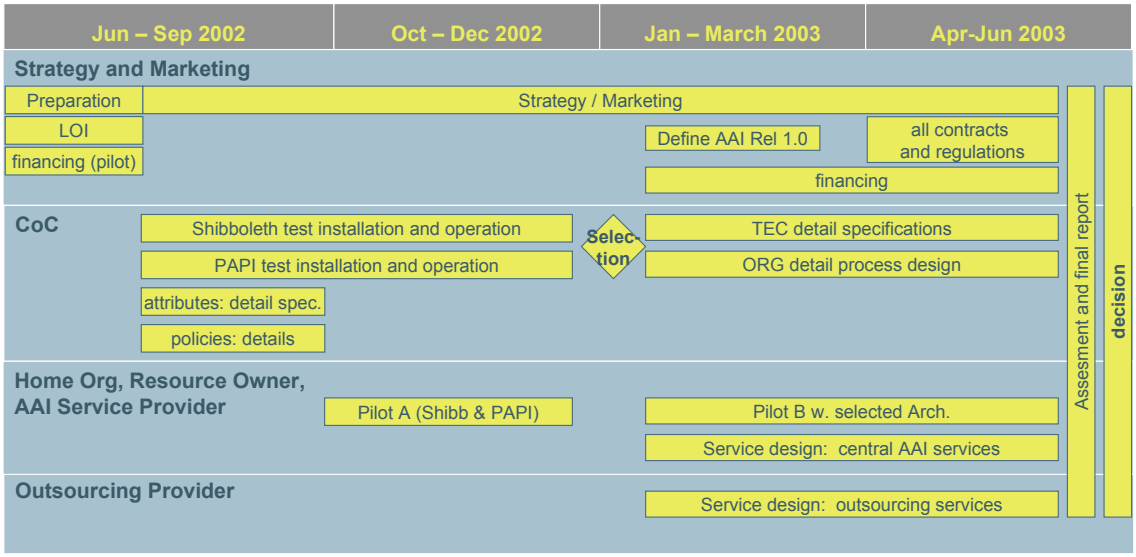


Figure 19: Roadmap of pilot phase

As Figure 19 shows, Strategy & Marketing has to be active right from the beginning: Apart from carrying out marketing activities, they are also responsible for the LoI, issues regarding the financing of the pilot projects, as well as the definition of AAI release 1.0. At the end of this phase, the legal basis as well as the financing of the AAI should be clarified.

The Center(s) of Competence will run Shibboleth and PAPI test installations. The insights gained from these installations as well as from the pilot projects will lead to the selection of one architecture beginning 2003. The detailed attribute specification has to be written at the beginning of the pilot phase because it is prerequisite for some pilot projects. Technical detail specifications and organizational processes will only be defined after the selection so that the work needs to be done but for one architecture.

Home Organization and Resource Owner will run pilot projects with either of the two architectures until beginning 2003; then, pilots should preferably be run with the selected architecture in

order to focus on its particularities. The pilot phase closes with an assessment and a final report.

Beginning 2003, the AAI Service Provider as well as the Outsourcing Provider each start designing their AAI services for the selected architecture.

For a list of pilot projects, see Appendix E.

10.2.2 Implementation Phase

Figure 20 shows the implementation phase in detail:

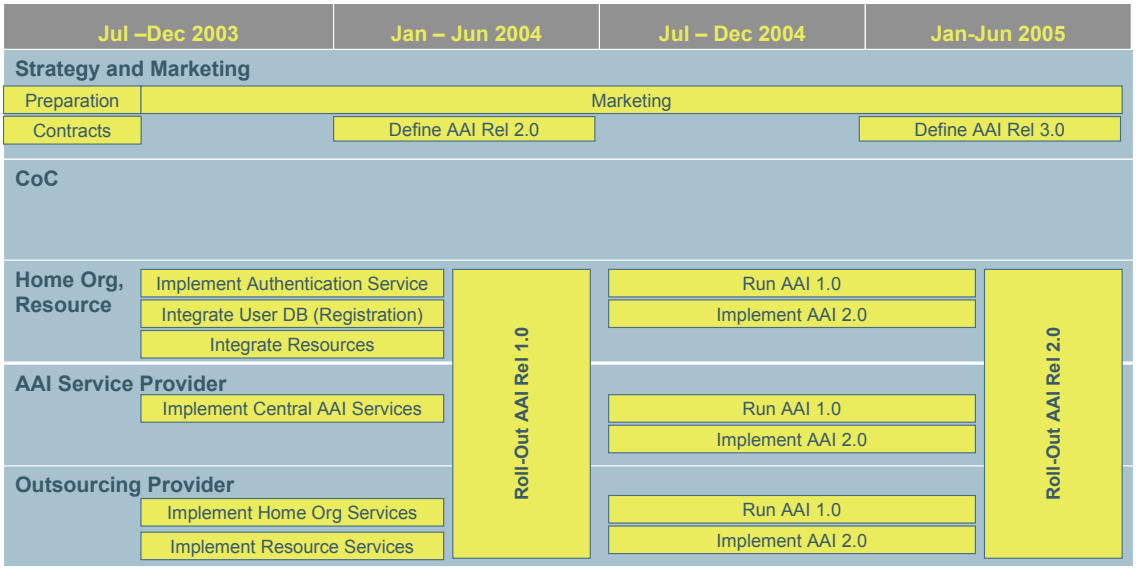


Figure 20: Roadmap of implementation phase

The functionality of the AAI releases needs to be defined by the strategy committee based on the insights gained during the preceding phase and the priorities set by the organizations involved. We recommend to implement one major new release per year.

The main functionality of release 1.0 should be:

- Implementation of central AAI services and authorization attribute delivery from the User's Home Organization to the Resource Owner
- AAI@Home Org: interface to user database and authentication systems
- AAI@Resource: interface to web-based resources.

Additional functionalities of release 2.0 could be:

- Interfaces to major non-web-based resources
- Encryption and signing of documents
- Interfaces to billing and accounting.

Appendix A Definitions and Abbreviations

AAI	Authentication and Authorization Infrastructure
AAI core systems	Systems which provide the core functionality of the AAI
AAI Outsourcing Provider	Organization providing AAI services on behalf of Home organizations or Resource Owners, e.g. authentication services
AAI Service Provider	Organization providing central AAI services to Resource Owners and Home Organizations
AAI-related systems	Resources, registration and authentication systems which will interact within the AAI and are a prerequisite to use the functionality of the AAI
Access control decision	Determining the access rights of a user; carried out by the access control manager
Access control definition	Configuration parameters used by the access control manager implementing the access control policy
Access control initialization	Process of configuring the access control manager
Access control manager	Gatekeeper functionality of the resource which grants or denies access to the resource based on the access control definition and the authorization attributes retrieved
Authentication	Process of proving the identity of a previously registered user
Authentication system	System which can authenticate a previously registered user
Authorization	Process of granting or denying access rights for a resource to an authenticated user
Authorization Attributes	User data needed for access control decisions
CUSO	Conférence universitaire de Suisse occidentale
ECTS	European Credit Transfer Systems
EPF / ETH	École Polytechnique Fédéral / Eidgenössische Technische Hochschule
FEIDHE	PKI Project of the Finish higher education
GASPAR	Authentication system for the users at the École Polytechnique Fédérale de Lausanne (EPFL)
GSI	Grid Security Infrastructure
Organization	Participating institution, e.g. universities, libraries, university hospitals etc.
PAPI	AAI Implementation from Spain (Point of Access to Providers of Information)
Personal security environment (PSE)	e.g. smart cards, passwords, certificates
PKI	Public Key Infrastructure

Registration	Process of becoming an official member of a user community. During the registration, a person has to prove his/her identity
Resource	Application, web site, network, system, etc.
Resource Owner	Entity owning a resource and offering resource access to users
Shibboleth	Joint project of Internet2/MACE (Middleware Architecture Committee for Education) and IBM
SIUS	Service d'Information Universitaire Suisse
SUK	Schweizerische Universitätskonferenz
UAS	Universities of Applied Sciences / Hautes écoles spécialisées (HES) / Fachhochschulen (FH)
User	Registered member of a Home Organization
User's Home Organization	Representative of a user community, e.g. universities, libraries, university hospitals etc.
User-DB	Database storing information about a registered user, maintained by the Home Organization

Appendix B Fallbeispiele

Mobilität

Beteiligte	• Hochschulangehörige • Hochschule (eigene)
Interaktion	Hochschulangehörige wollen unabhängig von ihrem Standort auf die von ihrer Hochschule zur Verfügung gestellte persönliche Arbeitsumgebung (E-Mail, Dokumentenablage, persönliche Homepage) und die für ihre Gruppe bereitgestellten Informationen (Vorlesungen, Mitarbeiterinformation, Dozenteninformation etc.) zugreifen.
Rolle der AAI	- Authentifizierung und Autorisierung für den Zugang zum Hochschulnetz (Remote Access, VPN) - Lieferung der Gruppenzugehörigkeit als Basis für die Autorisierung zum Zugriff auf für diese Gruppe bestimmte Informationen
Ohne AAI	• Der Benutzer braucht die Berechtigung für den Netzwerkzugang an der anderen Hochschule. Falls dafür eine Authentifizierung benötigt wird, wäre sie ohne AAI auf bilateraler Basis zu realisieren. Für wenige teilnehmende Organisationen ist das realisierbar, skaliert aber schlecht. • Sobald ein Benutzer am Internet ist reicht eine rein lokale Authentifizierungsmethode der Heimorganisation aus, eine AAI bringt hier keine spezifischen Vorteile.

Studierendenadministration

Beteiligte	• Studierende • Hochschule (eigene)
Interaktion	Immatrikulierte Studierende wollen unabhängig von ihrem Standort auf die von der Hochschule betriebene Applikation für die Studierendenadministration zugreifen und - persönliche Daten mutieren (Adresse, etc.) - sich für Vorlesungen einschreiben - sich für Prüfungen an- und abmelden - etc.
Rolle der AAI	- Authentifizierung und Autorisierung für den Zugang zum Hochschulnetz (Remote Access, VPN) - Authentifizierung der Studierenden gegenüber Applikation

Ohne AAI	Gleiche Situation wie in „Mobilität“

Einschreibung an anderen Hochschulen

Beteiligte	• Studierende, immatrikuliert an Hochschule A • Hochschule A • Hochschule B
Interaktion	Studierende, immatrikuliert an Hochschule A, wollen im Rahmen ihres Lehrplanes eine (obligatorische/freiwillige) Vorlesung an Hochschule B belegen oder ein bis mehrere Gastsemester an Hochschule B belegen. Sie müssen dazu: - sich für die Vorlesung / das Gastsemester einschreiben - dabei belegen, dass die Zulassungsbedingungen erfüllt werden - die den Studierenden zustehenden Informationen und Systeme der Hochschule B nutzen können - nach Abschluss der Vorlesung / des Gastsemesters dies gegenüber Hochschule A nachweisen können
Rolle der AAI	- Authentifizierung und Autorisierung für den Zugang zum Hochschulnetz B (Remote Access, VPN) - Authentifizierung der Studierenden bei der Einschreibung - Authentifizierung der Studierenden zur Nutzung der Informationen und Systeme der Hochschule B - Allenfalls Authentifizierung der Mitarbeitenden (oder Mitarbeitergruppen) der Hochschulen A und B als Voraussetzung, um administrative Informationen auszutauschen (z.B. Bestätigung, dass Studierende bei Hochschule A immatrikuliert sind und Voraussetzungen für Einschreibung an der Hochschule B erfüllen)
Ohne AAI	• Authentifizierung von Benutzern müsste über Organisationengrenzen hinweg bilateral gelöst werden, was nicht skaliert. • Kontrollierter und vor allem restriktiver Zugriff der Ressourcen-Betreiber auf Autorisierungsinformation zu Benutzern aus einer anderen Hochschule ist aufwändig zu realisieren. Wie kann z.B. ein Verzeichnisdienst ‚wissen’ wann welche Ressource einen legitimen Bedarf hat eine Information zu erhalten?

European Credit Transfer Systems (ECTS)

Beteiligte	• Studierende, immatrikuliert an Hochschule A • Hochschule A • Hochschule B
Interaktion	Transfer von Credits nach den Regeln des European Credit Transfer Systems (ECTS): • Studierende der Hochschule A müssen gegenüber Hochschule B belegen, dass sie über die für die Belegung einer Vorlesung vorausgesetzte Anzahl Credits verfügen. • Studierende lassen sich am Ende eines belegten Kurses die Credits elektronisch von Hochschule B gutschreiben und an Hochschule A transferieren.
Rolle der AAI	- Framework, um bilateral sicheren und vertrauenswürdigen Datenaustausch realisieren zu können
Ohne AAI	Gleiche Situation wie in „Mobilität“

Swiss Virtual Campus

Beteiligte	• Studierende, immatrikuliert an Hochschule A • Hochschule A • Swiss Virtual Campus
Interaktion	Studierende der Hochschule A wollen eine durch den Swiss Virtual Campus angebotene Vorlesung belegen. Dabei finden die Interaktionen statt, wie sie in den Fallbeispielen „Einschreibung an anderen Hochschulen“ und „European Credit Transfer Systems (ECTS)“ beschrieben sind
Rolle der AAI	analog der genannten Fallbeispiele
Ohne AAI	analog der genannten Fallbeispiele

Bibliothekszugriff

Beteiligte	• Hochschulangehörige • Bibliothek einer beliebigen Hochschule
Interaktion	Studierende möchten standortunabhängig auf die (web-basierten) Angebote einer Hochschulbibliothek zugreifen: - Katalogabfrage - Bestellung / Ausleihe - Zugriff auf Online-Datenbanken, Periodikas etc.
Rolle der AAI	- Authentifizierung der Hochschulangehörigen - Information über die Gruppenzugehörigkeit (Hochschule, Typ der Hochschulzugehörigkeit, etc.)
Ohne AAI	• Authentifizierung von Benutzern und deren Zuordnung zu Benutzerkategorien müsste über Organisationengrenzen hinweg bilateral gelöst werden, was nicht skaliert.

Dozentenadministration

Beteiligte	• Dozenten • Hochschule, an welcher sie angestellt sind
Interaktion	Dozenten wollen auf die von der Hochschule betriebene Applikation für die Administration zugreifen und - persönliche Daten mutieren (Adresse, etc.) - Prüfungsnoten vergeben - Testate erteilen, Credits vergeben - Berechtigungen erteilen (z.B. an Assistenten), um in ihrem Auftrag Funktionen der Dozentenadministration zu verwenden - etc.
Rolle der AAI	- Authentifizierung und Autorisierung für den Zugang zum Hochschulnetz (Remote Access, VPN) - Authentifizierung der Dozenten gegenüber Applikation
Ohne AAI	Gleiche Situation wie in „Mobilität“

Vorlesungsdokumentation

Beteiligte	• Dozenten • Hochschule

Interaktion	Dozenten wollen die für ihre Vorlesung relevanten Informationen (Vorlesungsunterlagen, Übungsunterlagen und -resultate, e-Learning-Inhalte, etc.)
	- ablegen
	- pflegen
	- Zugriffsberechtigungen erteilen
	  - an die Gruppe der Studierenden
	  - an ihre Assistenten
	- etc.

Rolle der AAI	- Authentifizierung und Autorisierung für den Zugang zum Hochschulnetz (Remote Access, VPN) - Authentifizierung der Dozenten gegenüber der Applikation
Ohne AAI	Gleiche Situation wie in • „Mobilität“

Benutzung von (IT-)Ressourcen

Beteiligte	• Hochschulangehörige • Hochschule
Interaktion	Hochschulangehörige möchten Ressourcen (z.B. allgemein zugängliche PCs, Drucker, Internet-Access) der eigenen oder einer fremden Hochschule benutzen.
Rolle der AAI	- Authentifizierung und Autorisierung für den Zugang zum Hochschulnetz (Remote Access, VPN) - Authentifizierung der Hochschulangehörigen - Lieferung der Gruppenzugehörigkeit (Hochschule, Typ der Hochschulzugehörigkeit, etc.)
Ohne AAI	Gleiche Situation wie in „Einschreibung an anderen Hochschulen“

Virtuelles Forschungsteam

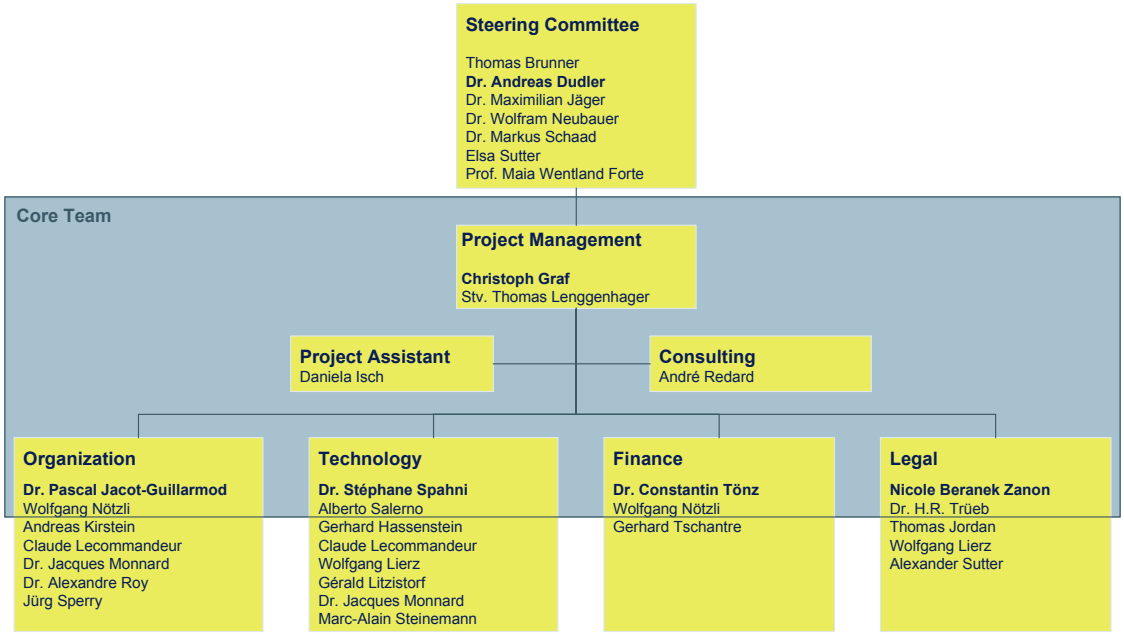
Beteiligte	• Forschungsteam mit Angehörigen verschiedener Hochschulen • Hochschule, welche diesem Team eine Informationsplattform zur Verfügung stellt
Interaktion	Zugriff auf eine gemeinsam genutzte Arbeitsumgebung (Web-Space, Dokumente, etc.)
Rolle der AAI	- Authentifizierung und Autorisierung für den Zugang zum Hochschulnetz (Remote Access, VPN) - Authentifizierung der Mitglieder des Forschungsteams zwecks Autorisierung auf die Arbeitsumgebung des Teams
Ohne AAI	Gleiche Situation wie in „Mobilität“ und „Einschreibung an anderen Hochschulen“

Universitätsspital / Telemedizin

Beteiligte	• Arzt • Patient • Spezialist • Spital des Arztes
Interaktion	Ein Arzt will den an einem anderen Spital tätigen Spezialisten hinzuziehen und ihm Patienteninformationen zur Verfügung stellen. Der Patient muss dazu den Arzt zur Weitergabe seiner Patienteninformationen ermächtigen.
Rolle der AAI	- Authentifizierung und Autorisierung für den Zugang zum Spitalnetz (Remote Access, VPN) - Authentifizierung von Arzt und Spezialist zwecks Autorisierung für den Zugriff auf Patientendaten - evtl. Authentifizierung und Autorisierung des Patienten
Ohne AAI	Gleiche Situation wie in „Mobilität“ und „Einschreibung an anderen Hochschulen“

Appendix C Project Organization

The following people contributed to the results of the study:



Name	Organization(s)
Nicole Beranek Zanon	SWITCH
Thomas Brunner	SWITCH
Dr. Andreas Dudler	Stiftungsrat SWITCH; Informatikdienste ETH Zürich
Christoph Graf	SWITCH
Gerhard Hassenstein	Berner Fachhochschule
Daniela Isch	at rete ag
Dr. Pascal Jacot-Guillarmod	SVC; Université de Lausanne
Dr. Maximilian Jäger	CRUS; Universität Zürich
Thomas Jordan	Hochschule St. Gallen
Andreas Kirstein	ETH-Bibliothek
Claude Lecommandeur	École Polytechnique Fédérale de Lausanne
Thomas Lenggenhager	SWITCH
Wolfgang Lierz	ETH-Bibliothek
Gérald Litzistorf	École d'ingenieurs de Genève
Dr. Jacques Monnard	SVC; Université de Fribourg
Dr. Wolfram Neubauer	ETH-Bibliothek
Wolfgang Nötzli	at rete ag
André Redard	at rete ag
Dr. Alexandre Roy	SVC; Université de Lausanne
Alberto Salerno	at rete ag
Dr. Markus Schaad	at rete ag
Dr. Stephane Spahni	Hopitaux Universitaires de Genève; Nice Computing
Jürg Sperry	Hochschule St. Gallen

Name	Organization(s)
Marc-Alain Steinemann	SVC; Universität Bern
Alexander Sutter	Universität Bern
Elsa Sutter	CRUS; Universität Basel
Dr. Constantin Tönz	SWITCH
Dr. Hans Rudolf Trüeb	Prager Dreifuss
Gerhard Tschantre	Universität Bern
Prof. Maia Wentland Forte	SVC; Université de Lausanne

Appendix D Types of Contracts and Cooperation

Types of contracts / types of cooperation	Essentials	Benefits	Drawbacks
Memorandum of understanding (German: „Rahmenvereinbarung“) between the organizations **Example: Memorandum of understanding concerning the cooperation between the University of Basel and the UAS of both Cantons of Basel (German)** **http://www.zuv.unibas.ch/spezial/fhbb**	• contractual: establishes the rights and obligations of the parties to the memorandum • prevailing law of the Cantons is mandatorily applicable	• short procedure • referendum: not possible • very flexible in the case of modifications • issued solely by the participating parties • no inclusion of the executive and legislative powers	• subordinated to prevailing law of the Cantons • no legislative nature, but individual, solution-oriented cooperation • the freedom of designing the content of the memorandum may be limited by constitutional and civil rights
Concordat (German: „Konkordat“) between the domiciliary cantons of the organizations	• legislative: consists in provisions with a “general-abstract” character • laws resulting from the legislative procedure (German: „Gesetz im formellen Sinn“) • prevailing law of the Cantons is not mandatory applicable and is superseded by the concordat • requirement of official permission (from the Federal Government)	• supersedes the law of the Cantons • higher relevance than a memorandum of understanding because of the legislative character • incorporation of the responsible public body, therefore higher legitimation of the material to covered by the concordat	• lengthy procedure and added difficulty in altering (rule resulting from the legislative procedure) on account of flexibility • possibility of a referendum in several Cantons • clumsy instrument because of the mandatory inclusion of Cantonal executive and legislative bodies in the case of modification of Cantonal competences • no immediate participation of private bodies • influence of political processes may slow down the project • subjects governed by concordats are limited by the relevant public bodies’ sphere of jurisdiction
Decree of the Conference of Swiss Universities	• legislative: consists in rules with a “general-abstract“ character • laws *not* resulting from the legislative procedure (German: „Gesetz im materiellen Sinn“) • prevailing law of the Cantons is not	• supersedes law of the Cantons • higher relevance than a memorandum of understanding, because of the legislative character • simplified type of decree, compared to rules resulting from the legislative procedure	• smaller democratic legitimation (Conference of Swiss Universities = small body) • content must respect constitutional and civil rights • content may be limited because of restricted legislative powers in the Conference of Swiss

	mandatory applicable, material may be continued in the decree	• referendum: not possible • issued solely by the participating parties	Universities' decree
Cooperation by agreement (i.e. without contract)	• cooperation without obligation • declaration of intention	• informal type of cooperation • possibility of quick decisions and quick modification or supplementary addition	• poor enforcement of decisions taken • limited possibility of designing the content in cases of conflict with existing legal rules and/or constitutional and civil rights • poor legal validity
Foundation under public law	• public assets separated from the financial assets, with precise purpose;	• possibility of long-term planning, more or less independent of amendment of specific laws, by separating a duty under public law from the legislative procedure and incorporating the duty in the charter of a foundation	• regulated matters must be covered by the public body's range of powers the charter of a foundation is very rigid, inflexible and not easily modifiable
Foundation under private law	• utilization of financial means according to Art. 80 et seq. of the Swiss Civil Code with the pursuit of public or general interests; not strictly bound to existing public law	• free design of the foundation's charter and free selection of its beneficiaries • no need for a legislative decree for carrying the foundation into effect, even in the case of participation of the public sector	• high threshold for the modification, supplementary addition and transformation of the foundation • strong influence of the public body by means of strict supervision • in case of financial difficulties of the foundation: urgent refinancing to prevent allocation of the foundation's assets to another foundation with similar purpose by the regulatory authority
Corporate body under public law (public-law corporation)	• entities striving for economic success, based upon civil law with duty and aims under public law	• liability restricted to the corporate body's assets; possibility of enforcement of liability against the financial assets of the public body involved in the case of gross breach of duty • the performance target may increase efficiency and ease the operational targets • no unnecessary administrative duties • usually based upon the responsible public body's financial legislation	• (Cantonal) legislation may provide distribution of profits to the public sector without return to the project itself • merely economic view is impossible because of participation of the public body (behavior of the corporate body is limited by constitutional and civil rights) • existing legislative authority must be respected, thereby resulting in limited possibility of creative planning

Appendix E Pilot Projects

Name of project	Organization involved	Architect.		Description	Project focus					Start	End
		Shibboleth	PAPI		Home Org Integr.	Res. Integration	Central AAI Serv.	PAPI/Shib. Core	other		
Basic AAI environment for pilot projects	SWITCH; Pilot projects requiring a test environment	x	x	Offering support to other AAI pilot projects: - By issuing test identities to individuals covering both PAPI and Shibboleth: Limited to users participating in other AAI pilots, excluding users from organizations offering sufficient home org support themselves. Includes setting up and operating home org interfaces to both PAPI and Shibboleth - By providing AAI-enabled resources protected by PAPI and Shibboleth mechanisms for test purposes (e.g.restricted access to network usage statistics). - Operating central elements of both PAPI and Shibboleth infrastructure. Includes setting up and operating a Shibboleth WAYF-Server and a PAPI PoA.	x	x	x	x		start of pilot phase	end of pilot phase
UNIL-EPFL CSS (Common Services for Students)	UNIL, EPFL	x		Exchange of authentication data regarding students registered at UNIL and EPFL	x	x	x			start of pilot phase	end of pilot phase
AAI for students in a CUSO post-graduate program	CUSO, UNIL, UNIGE, UNIF, UNINE, EPFL	x		Management of cursus for students in a CUSO postgraduate program	x	x		x	x	Oct 02	Feb 03
AAI for students in medicine	- HUG / UNIGE (Medical Informatics Division) - UNIL / CHUF - EPFL	x		Access to shared database for students in medicine	x	x		x		Sep 02	Dec 02
ERLaai/WOSaai	ETH library, library consortium, some of their clients	x	x	Feasibility test of AAI infrastructures for information resource provider ETHZ / Consortium of Swiss Academic Libraries for ETHZ-hosted: - Silverplatter ERL (OVID Technologies) databases - Web Of Science (ISI)	x	x				tbd	tbd

Name of project	Organization involved	Architect.		Description	Project focus					Start	End
		Shibboleth	PAPI		Home Org Integr.	Res. Integration	Central AAI Serv.	PAPI/Shib. Core	other		
iPass@SWITCH	- SWITCH - potentially User's Home Org (for cost settling arrangements)	x	x	iPass is a commercial service allowing to access the Internet via a large number of ISPs worldwide. iPass is believed to be AAI-incompatible (authenticating with fixed me-thod via resource instead of with a direct connection to home org). This project is about a workaround to allow people with AAI identity to access iPass. Proposes setting up an AAI-enabled registration service at SWITCH for iPass, handling out dedicated iPass credentials. Cost settling methods need to be found.		x				Jan 03	June 03
SWITCHmobile using AAI	SWITCH	x	x	Mobile university users equipped with a laptop, visiting a remote campus, should have the possibility to connect to the Internet at the remote campus without having to register first at that site, but by reusing their original registration with their home campus.		x				Aug 02	June 03
VITELS	University of Bern, Gruppe Rechnernetze und verteilte Systeme	x	x	VITELS is a sub project of the Swiss Virtual Campus that deals with online hands-on experiments with real hardware. It is now fed with student data from the university WebCT server. The VITELS architecture is designed for the integration of many different modules in the area of remote learning and with the adaption to the SWITCH AAI it will be easier to open the courses for all users covered by the future AAI.		x				asap	
White Pages for Swiss Academia	- SWITCH - some universities with LDAP servers	x	x	Building white pages directory for Swiss academia: SWITCH will set up a web gateway to LDAP servers of institutions with access limited to users authenticated via AAI.		x				Aug 02	June 03