Realization of a Vision: Authentication and Authorization Infrastructure for the Swiss Higher Education Community

EDUCAUSE 2003

Marc-Alain Steinemann steine@iam.unibe.ch
Torsten Braun braun@iam.unibe.ch
Christoph Graf graf@switch.ch
Martin Sutter sutter@switch.ch

Institut für Informatik, Universität Bern
Neubrückstr. 10, CH-3012 Bern, Switzerland

SWITCH
P.O. Box, CH-8021 Zürich, Switzerland

Executive Summary

This article describes the vision and its translation into reality of an authentication and authorization infrastructure for the Swiss higher education community. The main goal is to establish a virtual community letting all persons associated with the higher education system in Switzerland access its electronic resources in a secure manner. An important missing piece is an infrastructure dealing with authentication and authorization across organizational boundaries. SWITCH, the Swiss Education and Research Network, is the coordinator and provider of central services for this infrastructure. In pursuing our vision a roadmap was proposed in 2001, and in 2002 a preliminary study describing the technical, organizational, financial and legal issues was published. In several pilot projects the findings of the preliminary studies are tested and – after the decision to use the Shibboleth architecture for our authentication and authorization infrastructure – the electronic resources are being adapted. Possible solutions for connecting all kinds of resources to the authentication and authorization infrastructure are presented. A special portal is being developed to support campus-wide efforts for the connection of existing resources to the authentication and authorization infrastructure.

KEYWORDS: Authentication, Authorization, Switzerland, Shibboleth

1. Commuting in a Federal Higher Education Community

Switzerland is a federalist country with ten county universities, two federal institutes of technology and seven universities of applied sciences, with a total of about 130000 students in some 60 small or large campuses. Proprietary authentication and authorization infrastructures are used on many campuses, even though they belong to the same university. With the upcoming internationalization of the studies and growth of the Internet, it becomes more popular to access resources at foreign universities. This trend was massively increased by the foundation of the *Swiss Virtual Campus [4]* by the Swiss government in 1999. The Swiss Virtual Campus supports some 50 projects of the higher education community. Supported projects are developing Internet-based courses that should be accessible by the whole student community. Although never planned, the Swiss Virtual Campus was one of the initiators of the now ongoing development and deployment of an Authentication and Authorization Infrastructure (AAI) in Switzerland. As a matter of fact, in a federalist system, students cannot easily access resources located at other educational institutions, sometimes not even within the same institution.

2. Authentication and Authorization Today and Demands to an AAI

In the realm of networking many different authentication and authorization architectures exist, such as *TACACS+ [8],* the *IBM Grid Computing [1]* or architectures used in mobile networks. Most of these systems are deployed in layers lower than the Internet's application layer. They are rather hard to implement and manage, especially when taking into account that many different networking technologies and existing authentication procedures must become a part of the new AAI. Another restraint applying to the AAI is the fact that the respective resources are provided by the world-wide web, most of them being courses accessed by web browsers.

Figure 1 depicts the generic interactions between a user and the resource, e.g. information on a web server, e-learning applications or electronic libraries:

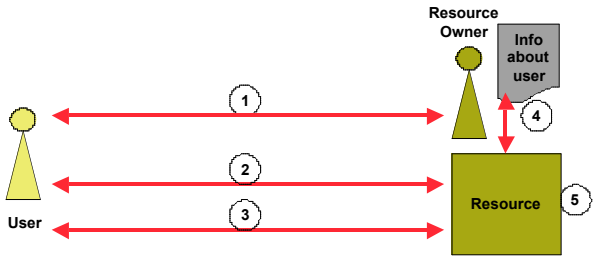

Figure 1: Generic resource access

Users who would like to access resources, as shown in step ①, have to register first with the resource owner. The resource owner then creates a virtual identity for each registered user, stores the necessary information about them and provides identifiers, typically login names and credentials for later authentication to the resource. Step ② shows how registered users access a resource. They submit an access request to the resource by means of their virtual identity. In step ③ the users are asked to authenticate, i.e. to provide the credentials belonging to the presented virtual identity. In step ④ the resource retrieves the previously stored information about users and - step ⑤ - decides whether access to the resource is granted or not.

This approach is fine for closed user groups but it does not scale if one user wants to access many resources belonging to different owners. Figure 2 symbolizes the increasing complexity when multiple registration and credential management procedures need to be carried out.

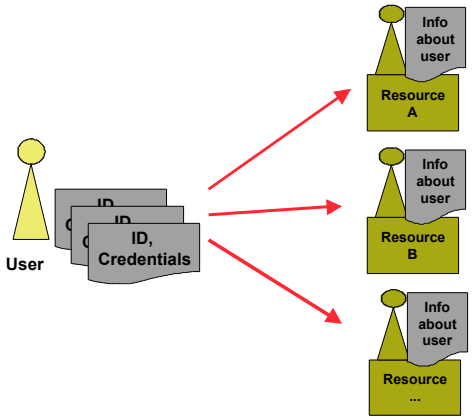

Figure 2: Accessing large numbers of resources belonging to different owners

The user has to register with each resource independently. Even if resource owners do not need to know the exact identity of a user (e.g. resources granting access to all students of a particular university) some kind of registration is required. As resource owners may use different authentication technologies, the users must be able to handle those (e.g. user name / password, certificates, smart-cards, etc.).

Recently, some large organizations have started to implement local authentication and authorization infrastructures for their home users and resources.

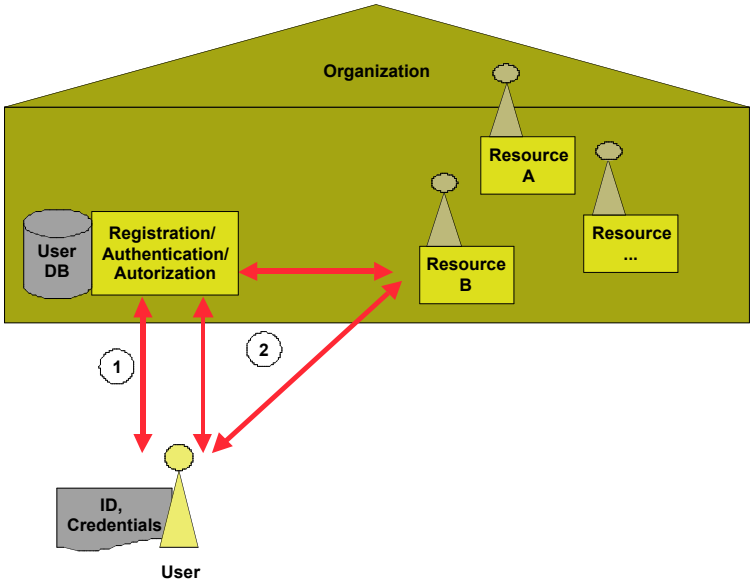

Figure 3: Resource access with centralized registration, authentication and authorization

In Figure 3 the flows of information in organizations using centralized registration, authentication and authorization are shown. In step ① the registration of the users and the storage of the authorization attributes in a central user database take place. Step ② shows the authentication and authorization interactions between the users, the resources and the central infrastructural services of the organization.

Such an approach, albeit effective, does not address authentication and authorization issues for resources belonging to other organizations and vice versa.

A solution to the problem of inter-organizational authentication and authorization is the implementation of an authentication and authorization infrastructure. The core functionality of an AAI aims to tightly couple three basic interactions during the authentication and authorization process between users, their home organization and a resource. These three basic interactions are

- user authentication – always carried out at the user's home organization
- access request
- providing 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 extensible, depending on the needs of the resource owner while respecting the restrictions given by data protection laws.

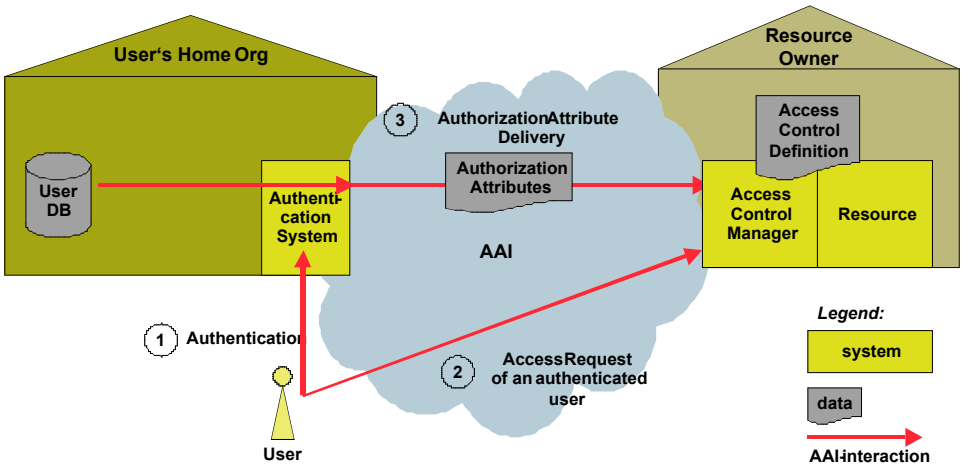

Figure 4: Generic functional model of an AAI

Figure 4 summarizes the functionality of an AAI. In step ① users authenticate with their home organizations. After a successful authentication, as shown in step ②, a set of authorization attributes is sent to the resource in step ③. For privacy protection it is necessary that users have the right to define which attributes they are willing to send to a resource. Based on a positive acknowledgement to the authentication request, the received attributes are compared to the resource's access control definition in order to determine the users' access rights.

The generic functional model of the AAI both affects existing organizations and resource providers. On the one hand, there will be clearly defined tasks for home organizations and resource providers, and on the other hand there are a number of important inter-organizational tasks that have to be carried out. It is crucial for a successfully operating authentication and authorization infrastructure that the responsibilities for such tasks are coordinated and assigned to one organization, called AAI service provider. *SWITCH [5]*, the Swiss Education and Research Network, is the likely candidate for adopting such inter-organizational tasks.

3. Roadmap

In 2001, an inter-university study group lead by *SWITCH AAI [6]* developed a roadmap to an authentication and authorization infrastructure for Switzerland. As a first step a *preparatory study [7]* elaborating on technical, organizational, financial and legal issues was to be compiled. Next, in a one-year pilot phase the decision was to be taken whether or not a two-year implementation phase of a nationwide AAI should be tackled.

The results of the preparatory study were presented by the end of 2002. The benefits and feasibility of the AAI were confirmed and it was proposed to start the pilot phase using two different AAI architecture candidates *PAPI [2]* and *Shibboleth [3]*.

In the meantime the findings of the preliminary study have been affirmatively tested in several pilot projects. In early 2003 the decision was taken to use Shibboleth for the implementation of the authentication and authorization infrastructure.

4. Shibboleth

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

Shibboleth focuses 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 such as Kerberos or PKI based on X.509.

Shibboleth uses a federated administration. Resource owners leave the administration of user identities and attributes to their respective home organization that is also responsible for providing user information attributes to resource owners. Shibboleth is a system for securely transferring user attributes from their home organization to resource owners' sites for web browser accessible resources. Shibboleth also enables users to control the scope of information released to resources.

5. Connecting Campuses

Connecting campuses and their resources to an authentication and authorization infrastructure (such as Shibboleth) is a non-trivial affair. Once the AAI reaches the status of a quasi-standard, it can be assumed that many AAI-enabled resources will appear on the market, whereby products with large user communities will be most probably adapted. Despite an increasing number of AAI-enabled web resources many other resources remain excluded from the AAI.

Web-enabled resources of small user communities and proprietary student management systems require special adaptation for connecting to the AAI. The Swiss Virtual Campus has a significant interest in connecting resources emerging from its projects and therefore finances the development of an AAI portal for non-AAI-enabled resources. In November 2002 the AAI portal project start designing the architecture and implementing a first prototype. At the time this article

is written, the prototype is capable of connecting the Shibboleth authentication and authorization architecture to a few exemplary resources.

The AAI portal allows the connection of non-AAI-enabled resources in a rather simple fashion. Attributes received from Shibboleth are written into the course databases that a user would like to subscribe to. The AAI portal includes many more functions apart from AAI-enabling non-AAI-enabled resources. For example, the *Biomed community* fostering eleven e-learning projects in the field of biology and medicine is a prime candidate for using the AAI portal. The portal incorporates a news ticker, discussion boards and other features on demand. The portal ought to provide sophisticated user management. Users can subscribe to courses listed in the AAI portal and the tutors can decide whom to grant access. Access is based on the attribute release policy of the users' home organizations and the attribute acceptance policy of the resource owner. The AAI portal already supports user notification by short message service or e-mail regarding status changes of the resources, tutor announcements or other information.

6. Outlook

The AAI for the higher education community is becoming concrete in Switzerland. Prototype projects are running, the infrastructure is being implemented and conceptual questions solved. The hen-egg problem remains a major obstacle in the path to a fully established AAI. Resource providers would like to connect home organizations to the AAI before they invest money in connecting their resources. Home organizations would like to get resources connected before connecting their own databases to the AAI. The AAI portal helps to overcome such problems in that it offers a simple way for connecting resources to the AAI. In the near future, with many AAI-enabled resources on the market, the AAI portal remains an important tool for user, resource and community management.

In a more distant future the Swiss AAI ought to be connected to other authentication and authorization infrastructures as they become available, reflecting the increasing importance of international student exchange and resource access.

7. References

[1] IBM Grid Computing http://www-1.ibm.com/grid/

[2] PAPI http://www.rediris.es/app/papi/index.en.html

[3] Shibboleth Shibboleth-Architecture Draft v05, Marlena Erdos and Scott Cantor, May 2002 http://middleware.internet2.edu/shibboleth/docs/draft-internet2-shibboleth-arch-v05.pdf

[4] Swiss Virtual Campus http://www.swissvirtualcampus.ch/

[5] SWITCH The Swiss Education and Research Network, http://www.switch.ch

[6] SWITCH AAI http://www.switch.ch/aai

[7] Preparatory Studies http://www.switch.ch/aai/documents.html

[8] TACACS+ http://www.cisco.com/en/US/tech/tk583/tk642/tech_protocol_family_home.html

