AAI - Authentication and Authorisation Infrastructure for the Swiss Higher Education System

Christoph Graf, Thomas Lenggenhager

SWITCH
Postfach
CH-8021 Zurich
Switzerland
cert-staff@switch.ch
http://www.switch.ch/aai/

Keywords: inter-organisational authentication, authorisation, infrastructure

1 ABSTRACT

Authenticating on-line users and authorising their access to on-line resources is a well-understood problem. To solve it for a single organisation various solutions are available today. Not yet properly solved is the resource sharing among organisations. Initiatives like the Swiss Virtual Campus or increased student mobility between higher education sites require a functional inter-organisational authentication and authorisation infrastructure (AAI).

SWITCH proposes to design and build such an AAI as an add-on to the existing common networking infrastructure.

This paper outlines ideas behind this approach, steps taken so far and elaborates on plans for the future. Contrasting approaches to the same underlying problems in similar communities are covered briefly.

2 MOTIVATION

Services, today requiring physical presence or relying on exchange of signed paper, will be under pressure to get complemented or replaced with network based services: be it for cost reasons, increase of reach, change in customer behaviour or others. Such resources require a reliable, scalable and secure method to authenticate on-line users and authorise their access.

New services with similar demands towards authentication and authorisation are on-line courses like the ones being developed by the federal programme Swiss Virtual Campus (SVC). Due to the reach of those courses beyond the hosting organisation, the scope of such an authentication and authorisation service needs to be inter-organisational and open for future international interoperability. The same is true for the library services co-ordinated by the Consortium of Swiss Academic Libraries.

Solving the authentication and authorisation problem for each service individually, as it is quite common today, results in an unnecessary multiplication of efforts. Existing approaches covering whole organisations are much more efficient, but they are presently not covering the needs for inter-organisational services.

With an inter-organisational AAI, the gain in economy of scale is even bigger and offering protected services beyond ones own organisation's management boundaries is facilitated. In the future, the services offered by an AAI might be perceived as part of the commodity network service. This is the approach SWITCH is proposing.

3 EARLIER ACTIVITIES

To promote the establishment of an AAI, SWITCH applied for a Swiss Virtual Campus mandate to that end in November 1999. The proposal was accepted in December 2000. In this context, SWITCH organised a workshop dedicated to AAI in November 2000. By broad consensus among the participants, it was agreed that the establishment of an AAI for the higher education system in Switzerland should be studied. An inter-university working group was formed and to draft the road map for an AAI. Its final report, the AAI-Concept, was published in September 2001 at http://www.switch.ch/aai. It received the blessing of the Conférence des Recteurs des Universités Suisses (CRUS), which encouraged SWITCH to take the lead in implementing what was proposed in the AAI-Concept.

4 SWITCH PROJECT AAI

The AAI-Concept proposes to define shape and scope of an AAI in a first phase, the preparatory study, in close collaboration and consultation with the involved parties. Special attention should be paid to the following four areas: Legal, organisational, technical and financial issues.

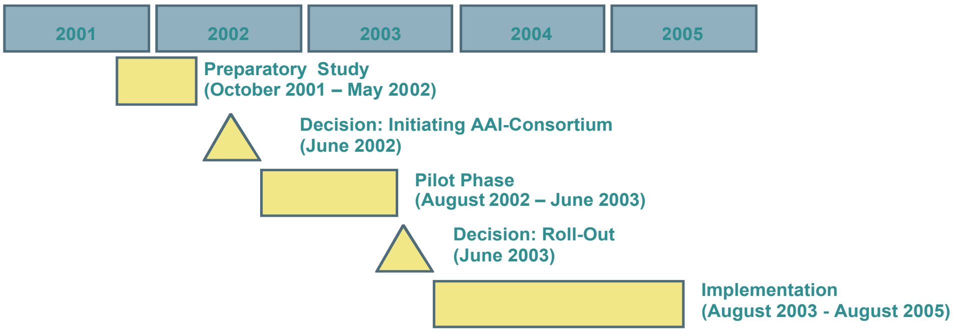
2001
2002
2003
2004
2005
Preparatory Study
(October 2001 – May 2002)
Decision: Initiating AAI-Consortium
(June 2002)
Pilot Phase
(August 2002 – June 2003)
Decision: Roll-Out
(June 2003)
Implementation
(August 2003 - August 2005)

Figure 1: Proposed AAI roadmap

SWITCH initiated the project AAI to implement this first phase, the preparatory study, as outlined in the AAI-Concept.

4.1 Project Organisation

SWITCH invited experts from the academic community to contribute to the project's four subgroups each focussing on one of the aforementioned topics. Close co-operation between those groups is required in order to achieve one consolidated view of all groups in the final report.

The composition of the project board reflects the strong involvement of our community as it includes key managers of universities, libraries and the SVC. The president of SWITCH heads the board, which shows the relevance this project has for SWITCH.

4.2 Principles and Guidelines

The AAI project is not about reshaping the existing trust relationships between participating organisations, but it is about mapping those relationships into the electronic world.

Access control to resources is performed close to the resource under direct control of the resource owner.

Existing authentication and authorisation solutions must be considered for integration into the common AAI by means of well-defined interfaces. While a common community-wide authentication token (e.g. student card) would certainly be valuable in a future AAI, it is not considered a requirement and we are explicitly not assuming that there will be one in the future.

The decentralised structure of the higher education community in Switzerland has to be taken into consideration and a solution with little centrally controlled elements is favoured. Where centrally controlled elements are required, SWITCH is considering extending its service portfolio to cover those elements.

4.3 Deliverable

The final report is expected to be available by end of May 2002. It will cover the following topics:

1. Proposed architectural design – possibly more than one – suitable for implementing an AAI, detailing recommended technical architecture, organisational framework, cost estimates and legal framework

2. The benefits of an AAI

3. Recommended next steps, identifying areas requiring further piloting and possible pilot applications, detailed roadmap covering the next phases

5 NEXT STEPS

The final report of the AAI-project will contain a more detailed road map and propose an adequate organisational form, e.g. whether to form an AAI consortium. The pilot phase from mid-2002 to mid-2003 will allow to trial new system components, gain operational experience and provide detail functional specs for the subsequent decision about entering the implementation phase.

6 RELATED INITIATIVES

Of the very few international initiatives similarly scoped as AAI, Shibboleth and FEIDHE are the ones most advanced in state. Therefore, they are well suited as references.

6.1 Shibboleth

Shibboleth is the name of the access control project for web-based applications from the middleware working group of Internet2. A federated user administration is the key idea for the design of this infrastructure and user privacy is of concern. Only origin sites need to register users, providers of web-based resources rely on them for the authentication. Each user shall be able to specify which attributes an origin site is allowed to provide to which resource the user wants to access. These attributes will be used by the resource to decide upon access permission for that user. Anonymous use of resources must be possible in case resources want to allow it.

The open-source software written for Shibboleth gets tested between February and May 2002; its release is planned for June 2002.

6.2 GNOMIS and FEIDHE

The Nordic GNOMIS (Greater Nordic Middleware Symposium) initiative is supported by the national research and education networks (NREN) of the Nordic countries. Its goal is the information exchange and the investigation of possible co-operation in the area of user authentication between organizations. The NRENs of Finland and Norway started their projects already.

The Finnish project FEIDHE (Electronic Identification in Finnish Higher Education) investigates the feasibility of a smart card based national electronic identification system using public keys. It is scheduled for completion at the end of March 2002.

6.3 TERENA initiatives

TERENA, the Trans-European Research and Education Networking Association located in Amsterdam, provides a platform for the European research community to co-ordinate mostly national activities in the area of a high-quality computer networking. NRENs meet with other interested parties to share ideas and experience from pilot projects and work towards interoperable or integrated solutions by trying to minimize ‘re-invention of the wheel’.

Relevant for the AAI project are TERENA activities regarding middleware within the task force for LDAP service deployment (TF-LSD) as well as the co-ordination of European PKI activities (PKI-COORD). Currently, the focus in the AAI area is primarily on the national level, since there is the most pressing need to open web-based applications from one organisation to the users of partner organisations. Cross-boundary interworking is presently of lower priority. Nonetheless, later on the need for international AAI-support will arise and we need to be as open as possible to be able to integrate in the future with similar infrastructures in other countries.