Introduction

The faculty of medicine of the University of Zurich promotes the integration of ICT-supported learning environments into the curriculum. Since 2001, the virtual medical platform VAM (Virtuelle Ausbildungsplattform Medizin) is providing the medical students in Zurich with a growing number of highly interesting e-learning offers (figure 1). The e-learning projects on the VAM-platform presently cover approximately 7% of the total curricular teaching / learning time. An analysis of the (anonymous) server-statistics shows that the VAM-platform is used extensively: every weekday one third of all medical students is online for 12 minutes on average (Data: 2003/2004).

The two main factors for its success are: (1) VAM only publishes e-learning offers anchored in the medical curriculum, and (2) the “keep it simple” strategy towards technology. The latter means that the learning management system used, is selected mainly on “ease of use” for end-users and authors. One crucial factor in this strategy is the login-procedure. With the introduction of the federated identity management system from SWITCH the login procedure was considerably simplified for both end-users and platform administrators.

This paper gives an overview of the federated identity management system and its advantages, followed by its application for access to medical e-learning courses at the University and the University Hospital of Zurich.

The Federated Identity Management System AAI

The federated identity management solution run by SWITCH is called AAI, Authentication and Authorisation Infrastructure. Participants eligible to take part in the SWITCH AAI federation are institutions of the Swiss higher education like universities and universities of applied sciences, university hospitals and research institutes. Apart from federation members, so called federation partners can offer services to federation members. Federation partners are for instance commercial e-journal providers.

A federation member can act as 1) a “Home Organization” by identifying persons, and 2) as a “Resource” that provides services to these persons (figure 2). Federation's partners can act as Resources.

The AAI Home Organization

The “Home Organization” is typically a university that has a database for their staff members and students. It checks the identity of the persons in the database by means of an identification paper and keeps their records up to date. The Home Organization matches physical persons with a digital identity and vouches for the correctness of the data provided for this digital identity. The authentication of a user takes place at the Home Organization usually by means of username and password. Stronger authentication is possible, eg with certificates using smartcards.

The AAI Resource

The “Resource” is a web server, offering services over the internet, for example an e-learning program. A Resource relies on the user authentication provided by the Home Organization. If a user wants to access a service, he submits his credentials at the Home Organization's server. The Resource then receives the information whether the user has been authenticated along with supplementary information (attributes) about the user. The user's attributes are checked to make an authorisation decision: if the attributes satisfy the Resource's access rules, access to the web server is granted.

Shibboleth

The servers of Home Organizations and Resources are connected to the internet like every other web server. However, to communicate together within a federation, there is some...
special software needed: AAI uses the implementation of Shibboleth from Internet2 for its federation. Shibboleth is open source software and uses the Security Assertion Markup Language (SAML) standard for the exchange of authentication and authorisation information. Shibboleth is a widely deployed middleware in federations of higher education and can be seen as a counterpart to the commercial Federated Identity Management efforts like “Liberty Alliance Project” and “Web Services Federation”. This does not mean that Shibboleth is going a way of its own: as the Liberty Alliance also uses the SAML standard, the basis is laid for interoperability.

The role of SWITCH is to run the federation as a service for its members and partners. Among other things, this service comprises the provision of a legal framework for the federation, which establishes the legal basis for the trust between the federation members. Trust is one of the basic elements, which makes it possible for a federation to function: its members are part of a “circle of trust”.

Implementation of AAI for Medical E-Learning Resources

In 2004 the faculty of medicine decided to migrate their e-learning content VAM from a commercial learning management system to the OLAT platform. One of the main reasons was the possibility to organize the access to the VAM contents for students and staff from all Swiss universities with AAI. OLAT (Online Learning and Training) is an open source, Java-based learning management system, used in the public sector of Switzerland. The AAI login procedure has been implemented in OLAT since September 2004. The AAI authentication functions are executed by the previously mentioned Shibboleth interface. For the integration of AAI-attributes, the OLAT group was supported by SWITCH.

The main advantage of the implementation of AAI is, that all 8000 registered OLAT users (status: May 2005) are authenticated and authorised by one single system. This means that (1) for authentication the user needs his digital identity from the Home Organization, and (2) for authorisation the e-learning courses running on OLAT only have to define a rule, specifying which user-attributes are needed to get access to the course or course node.

4 The Shibboleth project. http://shibboleth.internet2.edu
6 Liberty Alliance Project. http://www.projectliberty.org
8 Online Learning and Training (OLAT). http://www.olat.org
VAM users on OLAT coming from the University of Zurich Home Organization are handled by the UniAccess system. Since a number of VAM users does not belong to an AAI Home Organization (e.g., guest lecturers), SWITCH decided to establish a Virtual Home Organization (VHO) for VAM. User accounts in the VAM-VHO are administrated by the Resource, in this case the e-learning coordinator of the faculty of medicine.

The SWITCH AAI has been in use since mid 2003. The first web server connected with the AAI was the dermatology e-learning resource for medical education DOIT. This Swiss Virtual Campus project is developed and hosted in Zurich and is used by all medical schools in Switzerland. The login procedure is controlled by AAI, so that students are authenticated at their own Home Organization. In this specific case, the access is restricted to Swiss medical students in the clinical stage of their curriculum.

The University Hospital of Zurich as AAI Home Organization

Many employees of the University Hospital of Zurich need to access the e-learning contents of VAM. To facilitate the OLAT-login, the university hospital decided to become an AAI Home Organization. The university hospital has over 4000 employees and is a complex organization. The IT-infrastructure is Windows-based, various Unix systems are running for critical applications. The Active Directory Service (ADS) from Microsoft is used for user identification and authentication. The structure of the in-house ADS is rather flat; the employee’s data are stored in a separate database.

The AAI logon server is linked to the ADS using Kerberos. The ADS data is transformed to an open form by an export into an LDAP-database. The shallow structure of the ADS data does not allow a distinction between employee, professor, technical staff etc. Rather than merging the LDAP-database with the employee database, the ADS schema got enhanced by specific groups. Access to VAM services will be given depending on the group-membership of the employee.

The University Hospital AAI-logon-server can be accessed from anywhere in the internet. Since the secure socket layer does not protect from key-logging programs, the potential danger exist, that the ADS username of employees is logged. Since the ADS account is the key to the computer resources of the University Hospital, giving users a different login name for AAI circumvents this security problem.

One problem still to be solved is that the AAI-logon-server sees the un-NAT-ed IP of the computer in the intranet (NAT: Network Address Translation). This address is interlaced into the AAI-ticket. The address verification by the OLAT-server fails, because the OLAT-server sees the address of the USZ firewall and it cannot pass over the NAT.

The integration of the AAI-server is planned to be operative from autumn 2005. With the AAI infrastructure more web services can be made available over the internet, like access to the hospital phonebook, currently only available from the intranet. Other specific intranet contents may follow.

Conclusions

The introduction of AAI has been a success for e-learning in Zurich. Since September 2004 the access to the VAM-content on the OLAT server is organized by AAI and therefore the users can access the medical e-learning content with a single login and password that is authenticated at their Home Organization. The advantage for the user is that the amount of digital identities is reduced; the advantage for the Resource is that the user administration is reduced to implementing an access rule for each e-learning course, since the authentication is organized and administrated by the Home Organization.

The implementation of the AAI in a Resource or Home Organization is illustrated by the examples of the learning management system OLAT and the University Hospital respectively. With the help of SWITCH the technical implementation of the AAI is rather uncomplicated. However, the consequences of coupling the login system of the Home Organization to the AAI system and the resulting possibilities of access internet resources from anywhere, forces organizations to reconsider their security strategy, as shown by the example of the University Hospital of Zurich.

9 UniAccess of the University of Zurich. http://www.access.unizh.ch
10 DOIT: http://aai.cyberderm.net