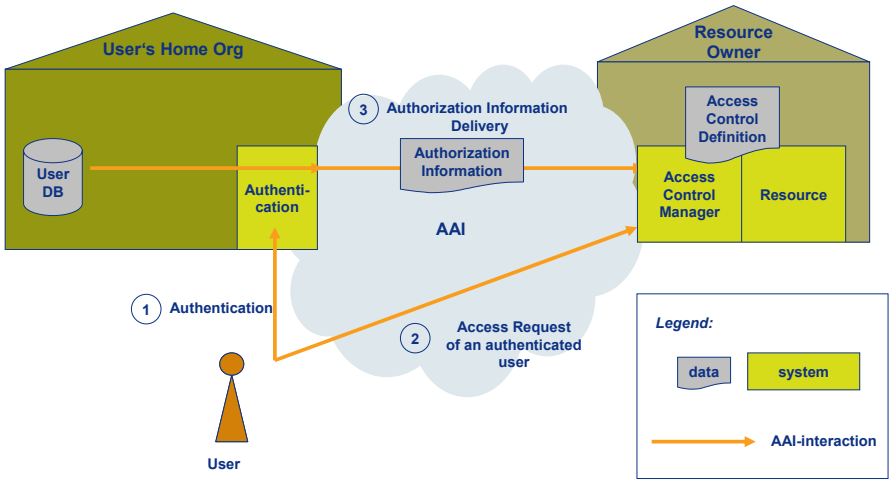
Authentication and Authorization Infrastructure (AAI) Status Report of June 30, 2003

AAI stands for **Authentication and Authorization Infrastructure**. The objective of AAI is to simplify inter-organizational access to networked services. After a study phase in 2001/2002, SWITCH and participating universities started the pilot phase in September 2002.



AAI leverages on existing trust relationship between organizations of Swiss Higher Education

With AAI, the well-established trust relationship between two organizations (Home Organization and Resource Owner) will be extended to a trust relationship between a user of the Home Organization (i.e. a student, staff, faculty member …) and the Resource Owner. The user authenticates him/herself towards his/her Home Organization, and the Resource Owner grants access to its resources based on information about the user (authorization attributes).

Access to resources and transfer of user information across organizations raise questions about data protection and liability. Therefore, the Swiss University Conference (SUK/CUS) has made a survey among all the Universities. The survey shows that AAI can be operated within the legal boundaries already in force but that some organizations will have to adapt their regulations. As a part of the legal framework, it is necessary that participating organizations agree to a common set of guidelines – the AAI policy – which describes the rules of good conduct. The AAI policy has been defined by a task force of the AAI project and will be finalized together with the legal framework until end of 2003.

AAI uses Shibboleth

In January, 2003, a task force has selected Shibboleth among three candidates as the architecture of AAI. Shibboleth is being developed as part of the Internet2 middleware initiative. It is designed as a federated identity management infrastructure based on SAML[1] 1.1, Early Shibboleth releases have been installed at SWITCH and at a few universities. Since June 20, 2003, release 1.0 is available and has been deployed by SWITCH for demonstration and test purposes.

Authorization Attributes

Authorization attributes for AAI users, which will be exchanged across organizations, need to be standardized. A task force has defined a set of authorization attributes, based on existing LDAP standards (e.g. inetOrgPerson, eduPerson) and data definitions from SIUS/SHIS[2], such as study branch, study level and staff category. Early adoptions of the AAI LDAP schema swissEduPerson at the ETHZ and the Universities of Lausanne and Bern demonstrate that organizations are able to provide these authorization attributes out of existing databases. Sample configuration files for Shibboleth are available from the AAI project homepage.

[1] Security Assertion Markup Language, standardized by OASIS (Organization for the Advancement of Structured Information Standards)
[2] Service d'Information Universitaire Suisse / Schweizerisches Hochschulinformationssystem

Server Certificates for secure communication

The communication between AAI systems is secured by using SSL. Therefore, AAI systems need X.509 server certificates. A task force has collected information about current PKI related projects, defined a list of requirements and worked out a model for a Certificate Authority (CA) infrastructure which suits the current needs of AAI and other systems using server certificates and can be extended in the future (e.g. CA for end-user certificates). Certificate Policy and Certificate Practice Statements for a Root CA and a subordinate Server CA has been prepared and the infrastructure will be implemented by SWITCH by end of October.

Pilot projects – the Home Organization side

ETHZ and the Universities of Bern, Geneva, Lausanne and Zurich have started pilot projects in order to integrate AAI with their authentication system and user directory. Until now, the focus has been on the implementation of a LDAP based user directory. Since the final release of Shibboleth is now available, they will start integrating their existing systems with Shibboleth. From a technical and organizational point of view, the integration of AAI within a Home Organization seems to be feasible.

Pilot projects – the Resource side

Currently, the owners of the following resources are participating in the pilot project:

- VITELS (University of Bern / SVC), nanoWorld (University of Basel / SVC)
- Bio Medicine (11 SVC projects)
- Common Services for Students (UNIL, EPFL)
- Shared database for Students in Medicine (UNIL/CHUF, UNIGE/HUG, EPFL)
- ETH Library
- Virtuelle Ausbildungsplattform Medizin VAM (UNIZH/USZ)

The integration of these resources within AAI is delayed, mainly because of the late availability of Shibboleth 1.0. The AAI pilot projects have to investigate further how existing resources can be integrated with Shibboleth: either directly or by implementing a proxy solution in front of the resource. The portal developed by VITELS might be such a portal solution. Some vendors (e.g. WebCT) and Content Providers (e.g. JSTOR) have already announced that they will integrate Shibboleth. For new resources, it is recommended planning the integration of AAI from the beginning.

Pilot projects – the Service Provider side

SWITCH as AAI Service Provider has implemented an AAI demo and test infrastructure based on Shibboleth 1.0 and is going to implement the central components of AAI in their production environment, namely the WAYF server (“where are you from”) and the CA infrastructure described above. The “AAI Center of competence” has established a good relationship with the Shibboleth developers and is prepared to support organizations by integrating Shibboleth in their environment or by offering outsourcing services to Home Organizations.

Cost estimation and financing of AAI

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

AAI Roadmap

Due to the late availability of Shibboleth, the AAI steering committee has decided to extend the pilot phase until end of 2003. The focus within the next quarter will be on the integration of Shibboleth within pilot projects, the implementation of the CA infrastructure and on setting up the legal framework. The first implementation and roll-out phase is planned for January to September 2004.

Further Information

The project documentation can be found at http://www.switch.ch/aai. Please contact the project team for further information: aai@switch.ch