On Evolution of an Authentication and Authorisation Infrastructure in Academic and Research Community:
AAI@EduHr – From RADIUS Hierarchy to an AAI Federation

Miroslav Milinović, Mijo Derek, Dubravko Penezić, Denis Stančer, Dubravko Vončina
University Computing Centre, University of Zagreb, Zagreb, Croatia
aai@srce.hr

Abstract. In this paper we explain the evolution of the authentication and authorisation infrastructure (AAI) of the Croatian research and higher education community (AAI@EduHr). AAI@EduHr evolved from the RADIUS hierarchy build to fulfil the needs of the dial-up service into fully established AAI. This paper provides an overview of the AAI@EduHr architecture together with information about it’s deployment. We conclude with the information on current usage and future plans.

Keywords. authentication, authorisation, identity management, AAI, RADIUS, LDAP

1. Introduction

In order to seamlessly provide a uniform, easy to use and secure access to network and networked resources it has become an imperative to build an authentication and authorisation infrastructure (AAI).

In general AAI is seen as the solution for the inter-institutional authentication and authorisation (AA) problem. General AAI model has 3 key elements:

- user,
- home organisation,
- service provider (resource owner).

There are 3 basic actions in each AAI:

- user authentication performed by his home organisation - the one that issued his digital identity;
- delivery of user’s attributes from home organisation to resource owner; set of attributes has to be configurable to meet the needs of both parties and at the same time preserve user’s privacy;
- service provider’s decision about the access (authorisation).

General AAI model is shown on Fig. 1.

However, the task of building an AAI requires a number of technical and organisational activities to be performed.

As a response to the increasing community demands, University Computing Centre, University of Zagreb (Srce) and Croatian Academic and Research Network – CARNet (CARNet), endorsed and funded by the Ministry of Science, Education and Sports of the Republic of Croatia, started in May 2004 a two-year project, lead by Srce.

The main goal of the project was to build the authentication and authorisation infrastructure of the Croatian research and higher education community (AAI@EduHr). Project has been successful, resulting in productional AAI system. AAI@EduHr has been fully operational since March 1, 2006.

Proceedings of the ITI 2008 30th Int. Conf. on Information Technology Interfaces, June 23-26, 2008, Cavtat, Croatia
2. Pre-conditions

At the time when the AAI@EduHr project has been started Srce was experienced in running distributed directory services especially LDAP. Also, network access, more precisely dial-up access, has been perceived as an important application that will enforce LDAP deployment. For the needs of the dial-up access service a national radius server hierarchy has been build and tied with the local LDAP directories – as a simple identity management systems in each and every institution connected to the CARNet network. Fig. 2 describes the established hierarchy by the end of 2003.

The next goal was to enhance the existing RADIUS/LDAP hierarchy to meet the needs and expectations for an AAI. Other AAI architectures which were in design or production phase at that time [8] like Shibboleth, PAPI or A-select were evaluated.

Due to the specific conditions, needs for rapid deployment and later automated maintenance in highly distributed environment we decided to build a specific AAI@EduHr architecture on top of existing RADIUS/LDAP hierarchy [6]. The basic AAI@EduHr architecture is presented in Fig. 3.

3. AAI@EduHr architecture

Establishment of the proper identity management system in AAI@EduHr was considered to be the first and the most important goal. Specific hrEdu directory schemas (hrEduPerson and hrEduOrg) were defined and deployed in LDAP directories across the community. We also established the hrEdu schema registry [4] in order to provide necessary reference to the current versions of hrEdu directory schemas.
developed client that meets the home institution’s needs as long as it uses AOSI-WS to contact LDAP directory.

Thus, AAI@EduHr architecture demands from a home organisation to establish and maintain a well defined set of services:

- LDAP directory with proper hrEdu schemas,
- RADIUS server,
- AOSI-WS.

This set of services acts as home organisation’s identity management (IdM) system. It is described with Fig. 4.

**Figure 4. Home organisation’s IdM service**

Basic AAI@EduHr architecture foresees 2 main central services:

- RADIUS proxy server,
- FWS server.

While the RADIUS proxy concept is known from earlier RADIUS/LDAP hierarchy the FWS concept presented in Fig. 5 is a new one, based on AOSI model.

So-called “routing information” is kept in the metadata repository (MDS) and maintained as a central service.

4. Deployment

A special challenge in the deployment phase was to ensure smooth transition for all of the running services as well as the LDAP schema harmonisation.

AAI@EduHr has been officially put to work on March 1, 2006. In order to allow easy to establish and maintain IdM system for home organisations a repository of Linux/Debian software packages has been established and maintained as a part of central support services.

AAI@EduHr today puts together over 200 identity providers with the total of approximately 580000 electronic identities and over 30 services including both the network and the application access.

AAI@EduHr has been connected to the European roaming service eduroam [3] since the very beginning. It has also been connected to the pan-european AAI superstructure eduGAIN [2].

The use of AAI@EduHr is steadily growing as the number of AAI@EduHr-enabled services is growing. Currently approximately 4.000.000 requests per month are being processed. Fig. 6 and Fig. 7 provide graphs with numbers of request processed by FWS and RADIUS proxy servers. Currently, in order to provide load balancing and fail-over functionality, there are 3 FWS servers and 5 RADIUS proxy servers in simultaneous work.

**Figure 5. FWS concept**

**Figure 6. FWS traffic**
Figure 7. RADIUS traffic

All information about the AAI@EduHr, its members and services as well as the monitoring system are publicly available at the AAI@EduHr web site (http://www.aaiedu.hr/).

5. Future work

Although AAI@EduHr works smoothly and provides reliable service a number of improvements are considered. The technical part includes adding SAML, Shibboleth interoperability and more advanced privacy protection through the attribute release policies. As AAI@EduHr is planned to be connected to the new-coming international AAI superstructures like eduGAIN work on harmonisation of hrEdu directory schemas with European efforts like SCHAC [7] is foreseen.

Detailed AAI@EduHr architecture with elements under development marked with gray letters is presented with Fig. 8.

Figure 8. AAI@EduHr architecture

Finally further efforts in non-technical aspect of AAI@EduHr are needed. It is important to strengthen the organisational aspect of the whole AAI@EduHr federation in order to enhance the trust between key players: home organisations, service providers and users.

6. Conclusion

In this paper we presented AAI@EduHr - the authentication and authorisation infrastructure of the Croatian research and higher education community.

AAI@EduHr is at the same time
- an AAI technology and architecture
- an AAI federation, an implementation of a specific AAI system.

Unique element of AAI@EduHr architecture is the AOSI system and the way how the AA process is handled.

Further work on AAI@EduHr includes strengthening both its’ technology and organisation.

7. References

[1] Denis Stancer, Mijo Djerek, Miroslav Milinovic AOSI: The Identity management system for AAI@EduHr. CARNet Users’ Conference - CUC 2005; 2005 November 21-23, Dubrovnik, Croatia
[8] Ton Verschuren AA systems – do you like to puzzle?. 1st EuroCAMP; 2005 March 2-4, Turin, Italy