AA Workshop
Malaga 20-21 November 2003

Presentations on line at:

http://www.terena.nl/tech/task-forces/tf-aace/AAworkshop/programmeNew.html

Introduction

The second AA Workshop held at the University of Malaga, was attended by almost 40 people coming from all around Europe with the participation of Americans reporting about Grid scenario in the States.
During the workshop a quite extensive AA scenario in Europe was depicted, thanks to participations of several NRENs and universities. The missing pieces to complete the overall picture are related to countries like Italy, France and Portugal, as there was no representative for them.
A new AA element will be coming shortly, as Croatia will be setting up very soon a proper AA infrastructure.

The first day of the workshop was focused more on requirements, coming from different perspectives, like content providers (Niels Wertmann), librarians (Sally Chambers), grid (Tony Genovese) and videoconference users (Dimitris Daskopoulos and David Collados).
New proposals on access control (Mariemma Yagüe) and cryptographic protocols (Marco Cassassa Mont) were also presented.
One of most interesting results of this group of presentations was that in many cases the real students (or campuses) requirements are not well represented in the TF-AACE community. The NRENs, especially the biggest ones are not aware of what their universities implement and in many cases the universities are not aware of what TF-AACE group is doing.
Having some kind of campus meetings would help, but sometimes the organisation of such events is not easy and they should be organised locally in the various countries. In Sweden something is moving toward this direction.

Federation

Many federations have been set up in Europe, such as the one set up by the Scandinavian countries, which is based on FEIDE system.
FEIDE will be compatible with Globus in the future and at the moment the support for PKI is still in a test phase.

In Switzerland the universities build a federation also. The AA infrastructure is based on Shibboleth. The participating organisations are listed on the WAYF. SWITCH also issues server certificates (pilot so far, rollout planned for early 2004) for the servers of the federation.

PAPI is being used to build federations as well, although RedIRIS is not building a national federation service for the moment. There are four different PAPI-based federations in operation in the Spanish academic network. The new version of PAPI (1.3.0) includes WAYF support and a new model of attribute exchange that can be initiated by targets. The PAPI development team is close to release PADATH (PAPI Adaptor to Athens), so PAPI origins and Athens targets can interoperate. This project takes advantage of the offer made by Eduserv through the TF-AACE list.

UK is using Athens as their AA infrastructure, which can be considered as a particular example of federation for content providers. UK will probably move towards Shibboleth in the future.

The role and the future of federations were discussed. To the question "Federation: is this the future?" the answer was that although there are examples of federations, there is not yet a European federation. The federation model can map the Virtual Organisation problem that is important for Grid people.
The first European attempt to set up a federation is represented by the European top level RADIUS infrastructure set up by mobility group. The requirements of the group (www.terena.nl/tech/taskforces/tf-mobility) were described by Carsten Bormann, who besides the possible approaches to get authenticated to a network while roaming between institutions, presented the European top RADIUS server infrastructure, which aims at creating a Web of trustiness. At the moment the countries which have joined the RADIUS infrastructure are: Netherlands, Croatia, Finland, UK, Germany, Spain (is going to join) and Portugal.
This last point generate a lot of discussion to understand how credential could be stored in this infrastructure and how to make the infrastructure secure.

All the systems need to be harmonised, therefore the need of some more interoperability tests was pointed out.
A comparison with the Internet2 federation model was done. Internet2 (I2) seems to have a different approach in the sense that their federation model involves the universities and it was created to allow different campuses to interact with each other. This model is more campus oriented than the one that could be defined in Europe.

PKI

The present and the future of PKI were discussed. Currently many NRENs have set-up a PKI, but the general use of personal certificates is not deployed. It was asked if Grid and/or the increasing use of 802.1X could enforce this application of PKIs.

The common feeling was that because PKI is hard to maintain for system administrators, is difficult to use for end users and it is expensive, it will be used till a certain level, but will not reach end users (students for instance).
Grid community (this is a quite restricted and specialised community) widely uses PKI, but when Grid started they were forced to use PKI, because of Globus, the toolkit that allows fro grid applications development (http://www.globus.org/). At the time the NRENs were not able to provide certificates, therefore they were forced to set-up certification authorities.
This brought in the main difference between Grid community and the NRENs community: the latter is a wider community and is not end user PKI oriented. The problem of mobile users is quite important for people using certificates, as the mobility of the user implies the "mobility" of the certificates related to those users. The problem is not trivial and it could be solved with the use of smarcards, but there are still some resistances as smartcards require a quite complex and expensive hardware.

An initiative that tries to facilitate the use of certificates inside the academic/grid community in Europe is the repository of root CA certificates that is being setting up under TF-AACE umbrella. The repository is based on personal trustiness and aims at building a wide net of trustiness, where TERENA will play the role of third part.
The policy document, which was also discussed and will be amended to reflect the comments of the group, is on-line at www.terena.nl/tech/task-forces/tf-aace .

Future

There were two presentations about some of the Joint Research Activities (JRA) in Geant2, the follow up of the current Geant project. Nicolas Simar presented JRA1, which will look into monitoring and management issues and therefore some kind of AA infrastructure to authenticate and authorise users is needed.
Nicolas asked for ideas to tackle the issue and invited the group to provide contributions for this activity.

The second presentation made by Claudio Allocchio was about JRA5, which aims at defining a general AA framework to allow for roaming. This activity will build on the result of TF-Mobility and TF-AACE.

A discussion followed these presentations, about the future of TF-AACE. The conclusion was that at the end of its mandate (1st of May 2004), TF-AACE and TF-Mobility (which will be terminated in June 2004) should converge in a bigger group to advice Geant2 research activities. Smaller working groups could be defined inside the big group to investigate more in detail on some specific issues.

The recommendations coming out from the workshop can be summarised as follows:
- making tf-aace and tf-mobility aware of each other activities

- having other AA workshops in the future, trying to have space to describe the AAI technical implementation details
- trying to harmonised the different systems
- trying to reach the campus users