AA Workshop Report
26-27 November, 2002
Stockholm, Sweden

Programme

The first workshop about authentication and authorization infrastructure, foreseen in the Terms of Reference of TF-AACE, was arranged on 26 and 27 November in Sweden, in conjunction with GNOMIS workshop to promote the co-operation between TERENA activity and the Nordic countries activity in the same area.
The two workshops were two separate events each one with its own programme.
Authorisation and Authentication (AA) workshop saw the participation of people from Internet2 as well and was attended by more than forty people. The workshop aimed to disseminate the results of the projects focused on AAA inside the NRENS and Universities in Europe, in particular of those who are involved in the task force and to investigate possible collaborations among these projects and with the middleware activity carried out by Internet2.

Unfortunately it was not possible to have people from GRID, so the scenario described in this reports is not complete.

The workshop was chaired by Ton Verschuren (SURFnet), whose help gave a big contribution to the good result of the event.

The first day of the workshop was opened by Licia Florio from TERENA, who shortly welcomed the participants.

Ken Klingstein: Internet2 Update

The real programme started with an overview on the activities related to authentication and authorisation in US by **Ken Klingenstein**. In general, PKI is in the States moving slower than in Europe, except from the Federal Bridge CA (FBCA).
Ken talked first about **Shibboleth**, whose new release, the version 0.7, appears much easier to install, although there is still some improvement to be done. For the next release, v.08 scheduled for 01-03-03, they will improve the security features (including authentication of SHARs). Shibboleth supports now OpenSAML, the open source reference implementation of the Security Assertion Markup Language (SAML), developed by the global non-profit consortium OASIS to allow authentication and authorization information to be exchanged among Web access management and security products. Starting from December 2002 WebCT, the world's leading provider of integrated e-learning systems for higher education, will become the first e-learning management technology vendor to support "Shibboleth" access and authorization technology across its entire product line. Ken said that in a longer-term view they would like to have conference calls with PAPI to find a possible convergence between PAPI and Shibboleth.

Ken talked then about NSF Middleware Initiative (**NMI**), which will include in its next release (expected in January 2003) KX.509 credential converter, Shibboleth, Globus Toolkit, OpenSAML and Pubcookie. In principal the software included in the NMI suite

can be divided in two categories, the one coming from Internet2, which is loosely integrated and the one coming from GRID, which is on the contrary deeply integrated.
Club Shib the particular group of trusted sites operated by UCAID and intended to be a co-operative environment for higher education is now called InCommon.

Thomas Lenggenhager and Rolf Gartmann: AAI Update

Thomas Lenggenhager and Rolf Gartmann presented the Authentication and Authorization Infrastructure **(AAI)** model that is being used by Switch. The objective of AAI is to simplify inter-organizational access to networked services, which without a model would require a user to register with each resource or service he would like to use and as result of this, to get a pair of credentials from each one. AAI has modelled the problem space in an efficient way, compared to the traditional way. The user registers only once at his own organisation, getting his pair of credentials. All AAI-enabled resources (i.e. managed by the AAI) are available with a single set of credentials, with no need to store a lots of credentials for those resources and with no need on the resource operator side, to register new users, as the resource gets the required information directly from the user's home organization. The users' attributes are based on EduPerson definition.
In Switch Papi, Shibboleth and Tequila have been tested, in order to build up a centre of competence. The result of the comparison among the three software above mentioned pointed out that PAPI 1.1.0 is well suited at enterprise level, but less for federations and it is group based and attribute based, while Shibboleth (Alpha 2.5/Beta1) is not easy to install and not ready for pilot project, as it is not yet deployed besides the alpha pilots.

Alan Robbiette: Current Developments in the UK

The following presentation was made by Alan Robbiete, who talked about the current developments in UK and in particular about the Athens project, which is operated by EduServ (http://www.eduserv.org.uk/) and it is used by JISC community and National Health Service (NHS). Athens, which was created to be a trusted third party, is now a large database of userID and authorisation data, where each participating site (college ,university, etc) administers its own part of the database.
Service providers need to run special software to carry out the dialog with Athens, whose agent plug-ins are provided either as toolkit (C, Java, Perl implementation) or modules/filters (Apache, IIS).

A "single sign-on" mechanism has been introduced recently in the software; limited-life tickets created at initial sign-on allow access to all service providers running the latest software plug-in.
Alan said the EduServ announced their intention to add Shibboleth compliance to Athens, to allow sites in Athens community to access Shibboleth protected resources, which will be possible after the introduction of SAML support, planned for the beginning of 2003 (http://www.athensams.net/development/),

Roland Hedberg: SPOCP: A General Authorisation Server

After lunch Roland Hedberg presented SPOCP (http://www.umu.se/it/projupp/spocp/ or http://www.spocp.org/), a one-year project, ending on 31 May 2003 and run by Umea

University with the participation of Stockholm University, Lund University, Uppsala University, Karolinska, SUNET, UNINETT and NYA & LpW.
SPOCP provides middleware functions for the authorization and uses existing directory and other information servers (SMTP, NTP...) for (user) data.
The rules/queries are defined as S-expressions (which is either a byte string or a finite list of simpler S-expressions) with fixed syntax and undefined semantics. S-expression can be ordered and tested for consistency (mathematically proved).
By default everything is disallowed, rules can only allow actions like (A <= R).
Examples of applications expressed using s-expressions can be:
- member of (thru an ldap lookup)
- reimbursement forms (fill out, check, approve, pay)
- mail relaying (preventing spam)
- delegation

Roland provided a comparison between XAMCL/SAML and SPOCP, which proved that SPOCP is much simpler and more server-based.

The source code available at moment consists of two server implementations (apache module with SAML/SOAP/HTTP and standalone), server as library and PAM module.
An example of a current implementation of SPOCP is Roland's mail server

Sassa Otenko: Comparison of Existing Authorisation Schemes

Sassa Otenko, from University of Salford made a presentation about an interesting comparison of existing authorisation schemes, such as PERMIS, PAPI, CAS, Shibboleth and others, to evaluate the architectures and do performance and manageability comparisons. The key issues considered for the analysis were about issuing authorisation tokens, distribution of the authorisation tokens, and the authorisation server protection.

Diego Lopez and Rodrigo Castro: PAPI 1.2. An usage-driven release

Diego Lopez, from RedIRIS, presented the features of PAPI1.2, whose code has been written in Perl, using Apache mod_perl and specific Perl bindings to the low-level functions of openSSL. PAPI supports attributes-based authorisation.

Rodirgo Castro presented PAPI 2.0. This presentation was more focused on PAPI-Shibboleth interoperability and on PAPI trust model. Compared to the previous release PAPI 2.0 has features, which allow it to convergence to other solutions (for instance Shibboleth), runs on new platforms (IIS and Apache) and has a new distributed trust model. The core modules are available (openssl, libxml, xmlsec).
PAPI model tries to converge to Shibboleth model, using an Attribute Authority (AA), which is contacted by the PoA.
Rodrigo described PAPI trust model, which has two components one horizontal, between authentication servers (ASs) and target sites, and one vertical, between PoAs of an organisation. There is no centralised third trust party (TTP).

Nathan Dors: WebISO and Pubcookie: Efforts in Web Authentication

Nathan Dors from University of Washington talked about Web authentication and in particular about Web Initial Sign-On
(WebIso systems) systems, designed to allow users to authenticate to Web-based services using a standard.
WebIso components are weblogin service, verification service, web application agent, web application and web browser.
The final part of the presentation was about PubCookie, the software developed by University of Washington. The new release 3.0 is open software and written in C.

Ton Verschuren: Hitchhiking in Authentication Space

Ton Vershuren closed the first day of the workshop with the presentation about A-Select, SURFnet weblogin system. A-select applications are Web applications, which use the API offered by the A-Select Agent, which runs on top of the Web application server to implement their access control. Another component of the A-select system is the A-Select server, which contains a database where information about the users and how to authenticate them are stored. When a user needs to be authenticate he is redirect to the A-Select server, which does not authenticate users himself but rather redirects him/her to an A-Select Authentication Service Provider (ASP).. When the user is authenticated, the A-Select Server will issue the user credentials and redirect him/her back to application. Ton made a demo of the software and talked about its future, which is not clear yet.

Ingrid Melve: Gnomis in the Northern light

In the second day of the workshop there have been two presentations. The first one given by Ingrid Melve from UNINETT and was about the Greater Nordic Middleware Symposium, GNOMIS (the next GNOMIS meeting will be in April 2003), and the Nordic countries (Sweden, Norway, Soumi/Finland, Denmark and Iceland) middleware projects, such as FEIDE (a project to create a common academic ID in Norway), FEIDHE/HSTYA (a project to investigate possibilities for implementing a smart card based electronic identification), SwUPKI (the Swedish university PKI), and SPOCP (Simple Policy Control Project).

Cato Olsen: Evaluation of Shibboleth, PAPI and A-Select

The second was made by Cato Olsen, from UNINETT as well, about a comparison made among, A-Select, Shibboleth and PAPI, to identify the most important features they could need for FEIDE implementation. Shibboleth's architecture was considered quite attractive, but its use of ARP (it could effect the scalability), the proprietary mechanism to locate users, where are you from, WAYF (FEIDE uses its own LIMS server) were considered not necessary for FEIDE purposes.
PAPI's scalability was considered (maybe there could be too much traffic through the PoAs) and its easy integration with Web resources.
A-Select lacks good cross-organizational support, but is easy to integrate with existing authentication solutions and Web resources.

Ken Klingenstein: International Issues and Opportunities

The rest of day was reserved for discussions. Ken led the discussion talking about international issues and opportunities. A summary is reported below:

- -standard for exchange of attributes, is converging to eduPerson on an international scale.
- -interfacing with grids: inter/intra grid (IBM's vision of a utility grid)
- -the introduction of new APIs should be very limited
- -more regular meetings, advanced camp and workshop should be arranged to increase the co-operation at international level. The information to exchange should be on a technical level and on a policy level.

The participants found the workshop very interesting, the presentations well focused and the overall organization was positively evaluated, but the need of an event providing more implementation details to stimulate the integration among different software emerged. At the time this report is being written, the preparation of such a technical workshop is under discussion and it is foreseen during the spring.