

5th TF-AACE Meeting

June 6th Rhodes, Greece

Attendees List

<i>Angelos Varvitsiotis</i>	<i>GRNET</i>
<i>Bart Kerver</i>	<i>SURFnet</i>
<i>Christian Claveleira</i>	<i>CRU</i>
<i>Christos Kanellopoulos</i>	<i>GRNET</i>
<i>David Orrell</i>	<i>Eduserv</i>
<i>Diego Lopez</i>	<i>RedIRIS</i>
<i>Dimitris Daskapoulos</i>	<i>GRNET</i>
<i>Dimitris Zacharopoulos</i>	<i>GRNET</i>
<i>Harri Kuusisto CSC</i>	<i>(Funet)</i>
<i>James Sankar</i>	<i>UKERNA</i>
<i>Jan Meijer</i>	<i>SURFnet</i>
<i>Jan Ruzicka</i>	<i>CESNET</i>
<i>Jan-Paul Leguigner</i>	<i>CRU</i>
<i>John Dyer</i>	<i>TERENA</i>
<i>Juergen Rauschenbach</i>	<i>DFN-Verein</i>
<i>Karel Vietsch</i>	<i>TERENA</i>
<i>Ken Klingenstein</i>	<i>Internet2</i>
<i>Klaas Wierenga</i>	<i>SURFnet</i>
<i>Kolbjorn Barneb</i>	<i>UNINETT</i>
<i>Kostas Koumantaros</i>	<i>GRNET</i>
<i>Licia Florio</i>	<i>TERENA</i>
<i>Magnus Stromdal</i>	<i>UNINETT</i>
<i>Massimiliano Pala</i>	<i>Politecnico di Torino</i>
<i>Mikael Linden CSC</i>	<i>(Funet)</i>
<i>Milan Sova</i>	<i>CESNET</i>
<i>Miroslav Milinovic</i>	<i>SRCE</i>
<i>Olivier SALaun</i>	<i>CRU</i>
<i>RL Bob Morgan</i>	<i>University of Washington/Internet2</i>
<i>Sally Chambers</i>	<i>University of London</i>
<i>Serge Aumont</i>	<i>CRU</i>
<i>Stig Venaas</i>	<i>UNINETT</i>
<i>Ton Verschuren</i>	<i>SURFnet</i>
<i>Ueli Kienholz</i>	<i>SWITCH</i>
<i>Valentino Cavalli</i>	<i>TERENA</i>

Agenda

(The presentations are on-line at:

<http://www.terena.nl/tech/task-forces/tf-aace/meetings/Meet06-06-04/Agenda.html>)

1. Welcome and Update on TF-AACE activities
2. Taskforce closure (final report and deliverables)
3. AARR update
4. TACAR update
5. Discussion on the new middleware TF (TF-EMC) charter

Welcome

Diego welcomed the participants and provided an update of the work of the group. The task force started in May 2002 and officially terminated its mandate at the end of May 2004. Some final work is being carried out to finalise some deliverable and to produce the final report.

Diego went through the list of items that need to be finalised and listed the most interesting results achieved by the group.

Task Force Closure: Final Report

It was agreed that a final report to describe the result achieved by the group will be produced by Diego and delivered in September 2004. Diego will circulate the report through the list and he asked everybody to contribute.

Action: DL to prepare the final report by September 2004.

Deliverable B2

(Define components and protocols to guarantee an harmonized operation of A&A systems)

Terminology Document

The need of a common terminology came up many times during the TF-AACE meetings. Torbjörn Wiberg prepared a terminology, based on a high level description of the most important AA terms. Comments to the document have been circulated on the list and new version of the document is expected in July. As Torbjörn could not attend the meeting, it was agreed to discuss more about this on the list.

Deliverable B3

(Set up a reference implementation)

AA-RR (Authentication and Authorisation Requester-Responder)

The main aim of the deliverable B3 was to produce a reference implementation guide for AA systems. Since the original proposal, technologies have evolved; therefore more than a guide to implement AA systems, interoperability assessment mechanisms are required when different pieces of software are plugged together. The Authentication and Authorisation Requester-Responder (AA-RR) tries to provide these assessments.

The idea of defining common components to allow different systems to interoperate among each other arose during a meeting held in TERENA in March 2003, called developers meeting. During this meeting an analysis to find out the characteristics of systems like Shibboleth, PAPI, A-Select, FEIDE, Spocp was carried out. After that, RedIRIS attempted to produce a first draft of a model that could work as AA request responder. The proposal was discussed during the meeting in Malaga in November 2003. In the beginning SAML seemed to be the selected technology, but lately it was agreed to define a model that would work with different standards.

Before the meeting in Rhodes, Diego produced and circulated a document to the list describing the new AA-RR model. The purpose the AA-RR is to use some kind of

metadata describing the requirements of a certain infrastructure in order to validate (or make at least an assessment) the interoperability of a certain component with other(s). The broad application fields to which AA interactions are aimed implies a variety of potential protocols to be used, considering that currently none of the proposed standards is clearly dominant over the others. The AA-RR will be built using a protocol-agnostic approach.

Diego said that he plans to include definitions for shibboleth, A-Select, FUNET and the SWITCH AA system (which is shibboleth based) by September.

The AA-RR will be developed and tested under TF-EMC.

Action: DL to circulate an updated version of the AA-RR by September.

Deliverable B5

(Collect current authentication practices and policies in European academic networks)

Contribution the eIRG White Paper

The eInfrastructure Reflection Group aims at supporting both at political and advisory level the creation of a policy framework for easy and cost effective use of electronic resources in Europe across different national domains. This group meets twice per year in the countries that host the six months of the European Presidency. At each meeting a white paper that describes how the framework should look like is presented. A group of volunteers is selected to provide inputs to the white paper. Diego Lopez and Licia Florio have been asked to provide a description about TACAR for the version of the white paper presented in Dublin in April 2004. The document is available [here](#).

Diego attended the eIRG meeting in Dublin to present TACAR, which has been endorsed by the eIRG.

Deliverable D

(Investigate existing initiatives on common identity on the Internet)

This deliverable foresees a report about existing initiatives on common identity on the Internet (e.g., Microsoft Passport, Liberty Alliance, others). The results will be included in the task force final report.

Deliverable A

(Define interoperability requirements for a European Academic PKIs)

TACAR update

Diego provided an update of TACAR. The collection of certificates started in November 2004; at the moment these minutes are being written there are 16 root CA certificates on-line and more institutions have asked to join. The TACAR area, started as web page reachable from the TF-AACE site, has evolved (a logo has been provided by RedIRIS) therefore it was agreed to make it independent from TF-AACE. A domain has been bought (www.tacar.org), which is still under development.

The Grid community is very interested in using TACAR as their official repository for Grid CAs. Diego and Licia attended the EUGridPMA (<http://www.eugridpma.org/>) in Florence in April 2004 and have established relationship with this group.

There are some issues still not solved which are:

- Initially it was agreed to collect all the certificates in a single file (PKCS#7), which could be downloaded from the TACAR page. The file can be downloaded properly only using Internet Explorer, but using Mozilla some problem has been reported. In particular after the users authorise the download of the first certificate that appears in the file, by default all the other certificates are downloaded and installed. The problem has been reported to the Mozilla group.

It was proposed to implement a simple interface to an LDAP server (backend) where all root certificates get stored. The interface should let the users choose the certificates they want in the bundle before downloading the pkcs7 file. This approach would solve Mozilla's problems and would make the procedures more efficient. Massimiliano Pala volunteered for this.

Action: MP to report to group about the developments.

- the download of the certificate should be done using SSL. The EUGridPMA group has raised some concerns about the type of certificate used. Jan has suggested having a look at [Diginotar](#), which provides a service used by notaries in the Netherlands. Two other possibilities were proposed by Diego, which are:

- 1) Looking for some other services similar to the one that Jan suggested;
- 2) Generating a key pair and a self-signed certificate, and building trust by publishing in a paper media (a TERENA report or in a scientific publication or similar) the data about the public key (fingerprint, period of validity, etc.). In this case there is no need of P/CPS

Action: LF to look at it Diginotar.

Although not perfect yet, TACAR is ready to be used and to evaluate what advantages it can provide to the community. At the moment there are no data about the numbers of download of the certificates. Licia will try to provide some figures.

Action: LF to monitor the traffic on the TACAR web page.

NREN Service Certificate

TACAR can help in getting the root CA of an institution, but it does not solve the problem of getting the root CA available in the browsers. Certificates are used for different services, for instance applications, RADIUS infrastructure and others. In some case NRENs have agreements with CA, acting as RA, but it is still expensive. The idea, proposed by Jan Mayer, which was discussed during TNC is to have one central service certificate, which would go through the audit to be listed into the browser and each NREN would be a RA of this central CA.

Action: JM to investigate more about this.

Group Updates

Internet2 News (Ken Klingenstein)

Shibboleth 1.2 has been released. It has better support for multiple federations. Behind shibboleth there are new groups, such as mlist for e-mail distribution list, courseID for exchange of teaching materials and others. Ken talked about the campus meeting in Colorado (30 June-2July, 2004), which is focused on development of campus and interrealm authority architectures and related systems. Topics include work in privilege

management systems and Grouper, an architecture and suite of tools to manage groups across applications and user communities.

A-Select (Bart Kerver)

Currently A-Select core provides a set of authentication methods (web based), such as user/name and password, banking cards, SMS, Passfaces, RSA, but it does not provide yet a "finding federation" support. A-Select supports protocols like RADIUS and LDAP. Diego asked whether SURFnet is considering the use of Kerberos. The answer was that as Kerberos is an interesting way to provide the authentication without using cookies; it would be interesting to work on this. SURFnet hopes to connect A-Select to the Shibboleth platform, to use its authorisation features.

SWISS (Ueli Kienholz)

The AAI project in Switzerland uses Shibboleth. Five major universities throughout Switzerland (covering about half of all users in Swiss higher education) are already SWITCHaai-enabled. Some e-learning resources are used on a day-to-day basis with Shibboleth.

Shibboleth uses two trust fabrics: federation meta-data and server certificates. The focus regarding trust in Shibboleth is moving more towards federation metadata.

The trust in SWITCHaai is also built up on a legal framework. So far, this was a "Letter of Intent". Starting soon, it will be a "Service Agreement" referring to documents such as the AAI Policy. This agreement has to be signed by the participating organizations. The documents are published on the SWITCH website.

Terms of Reference of the new middleware task force (TF-EMC2)

Diego presented the new task force, saying that it should provide an umbrella for all the middleware activities and middleware projects or initiatives like TACAR.

It was agreed to call the new task force European Middleware Coordination Council (TF-EMC2).

The charter presented was quite open, as it was felt that a discussion among the members was necessary to agree the working items. The proposal was to agree a list of items to work on for the first year and to appoint one or more people responsible for each item, whose role will be to breakdown the work and the deliverables. It was agreed to have not more than two deliverables per topic.

The list agreed is appended below:

- Directory schema (DiegoLopez, PeterGietz)
- Campus middleware deployment (SallyChambers, MiroslavMilinovic)
- Trust co-ordination (AlanRobbiette, DavidChadwick)
- Liaison with Grid community and virtual organisation (LiciaFlorio, MilanSova, DavidChadwick, ChristosKanellopoulos, NikosVogiatzis)
- Authorisation (DavidChadwick, Roland Hedberg)
- Middleware diagnostic: promote a model to define a log file (KenKlingstein)
- TACAR (DiegoLopez, LiciaFlorio)
- AA-RR (DiegoLopez)

- Support for Geant2 (JuergenRauschenbach, DiegoLopez)
- Liason with sw developers and vendors (AngelosVarvitsiotis)

When the list of deliverable is finalised the charter will be submitted to the TTC for the approval.

The first TF-EMC was agreed to be arranged in November (4-5) in Amsterdam.

Action: the people appointed to provide a breakdown of the work within 15 July. The name highlighted in yellow are not confirmed yet.

AOB

A campus meeting in Europe was proposed by Ken Klingstein. Provisional dates: March 2005.

Action: LF to check with TERENA to organise the CAMP.

Summary of the TF-AACE Actions and other related activities

Action1	DL to prepare the final report by September 2004.
Action2	DL to circulate an updated version of the AA-RR by September.
Action3	MP to report to the group about the developments to use an LDAP interface for TACAR
Action4	LF to look at it Diginotar.
Action5	LF to monitor the traffic on the TACAR web page.
Action6	JM to investigate the possibilities of issuing NREN/academic server certificates in one PKI whose trust anchor is preinstalled in the browsers
Action7	LF to check with TERENA to organise a CAMP in Europe.

DL= Diego Lopez.

LF = Licia Florio

JM = Jan Meijer

MP = Massimiliano Pala

Summary of Action to prepare the terms of reference of TF-EMC2

The table below summaries the topics of interest that will be included in TF-EMC2 terms of reference. People appointed are supposed to provide their contribution to Diego within 15 July.

Directory schema	DiegoLopez, PeterGietz
Campus middleware deployment	SallyChambers, MiroslavMilinovic
Trust co-ordination	AlanRobbiette, DavidChadwick
Liaison with Grid community and virtual organisation	LiciaFlorio, MilanSova, DavidChadwick, ChristosKanellopoulos, NikosVogiatzis
Authorisation	DavidChadwick, Roland Hedberg
Middleware diagnostic: promote a model to define a log file	KenKlingstein
TACAR	DiegoLopez, LiciaFlorio
AA-RR	DiegoLopez
Support for Geant2	JuergenRauschenbach, DiegoLopez
Liason with sw developers and vendors	AngelosVarvitsiotis

