

**TF-EMC2 Meeting  
16-17 February 2005  
Amsterdam**

**Attendees list**

Ann Borda	JISC
Tom Barton	University of Chicago/Internet2
Yuri Demchenko	University of Amsterdam
Licia Florio	TERENA
Tony Genovese	DoE
Peter Gietz	DAASI International GmbH
Victoriano Giralt	Málaga University
Maja Gorecka-Wolniewicz	NCU, PIONIER
David Groep	NIKHEF
Florent Guilleux	CRU
Roland Hedberg	Umeå University
Reimer Karlsen-Masur	DFN-PCA
Mikael Linden	CSC (Funet)
Diego Lopez	RedIRIS
Jesus Luna	Polytechnic University of Catalonia
Miroslav Mllinovic	Srce/CARNet
Manel Medina	Polytechnic University of Catalonia
Jan Meijer	SURFnet
Maurizio Molina	DANTE
Jose A. Montenegro	Malaga University
Teun Nijssen	Tilburg University
David Orrell	Eduserv
Massimiliano Pala	Politecnico di Torino
Juergen Rauschenbach	DFN-Verein
Alan Robiette	JISC
Ton Verschuren	SURFnet
Torbjörn Wiberg	Umeå Universitet
Klaas Wierenga	SURFnet
Holger Ziemek	DFN-Verein
Bas van Oudenaarde	University of Amsterdam

**Welcome and opening**

Diego and Licia welcomed the attendees and reminded that the aim of this meeting was to foster discussion and cooperation to define a roadmap for the future months.

**AA-RR Jose Manuel**

Jose Manuel provided an update about the Authentication Authorisation Request Responder, AA-RR ([www.rediris.es/app/aarr](http://www.rediris.es/app/aarr)).

The AA-RR is composed by different modules with different functions. The Protocol Adaptor converts internal requests to comply with the protocol that it is requested (RADIUS, SAML, LDAP etc). The protocol adaptor available in the current developed version uses SAML.

The Diagnostic module logs all the information to a log file, so it was asked whether this module could be used diagnostic tool. Diego said that at the moment it is a bit premature because they have just started using the AA-RR, so there no standard format for the log files yet. It was agreed to discuss this in the next months.

Working is being undertaken to connect Shibboleth and PAPI through the AA-RR.

## **TACAR**

TACAR is being used as a trust repository by NRENs and especially by various Grid CAs. At the moment TACAR hosts more than 20 certificates. The TACAR policy has been reviewed to include the statement about the use of a self signed certificate for the secure download of certificates (SSL) and the new version is on line. The certificate has been installed.

**Users are requested to verify the fingerprint of the certificate using the information that is provided online.**

The fingerprint of the self signed certificate will be available in the next TERENA Annual Report, which will be distributed to all institutions whose CA is in TACAR.

During the meeting some proposals to use TACAR not only to store trust-anchors where presented.

### **1. Proposal to use TACAR – Polytechnic University of Catalonia (Manuel Medina)**

Manuel Medina presented CertiVer, a digital certificate verification and revocation service to support certification authorities. The automated certificate revocation module is able to work via voice recognition. This allows users to revoke their certificate via phone in case they have lost their password. The recognition process works in 90% of cases and it is secure. The certification status is checked using OCSP.

Some extensions for the OCSP have been defined for some applications, which means that a standard OCSP might not be able to work with these extensions.

Mauel proposed to use TACAR in connection with CertiVer Service, in order to publish in the TACAR repository root certificates managed by CertVer, and/or use TACAR as the initial trust anchor for CertiVer CRLs.

In the GGF there is a group that is working on a document how to run an OCSP internationally. OCSP is a very critical resource for grid applications.

### **2. Proposal from University of Malaga (Jose A. Montenegro)**

Monte presented the Cert'eM which is a protocol to search for certificates, based on a proprietary solution that uses DNS names to locate certificates, simpler than others that are available on the market. Cert'eM provides real-time keys revocation without using CRLs.

The proposal for connecting TACAR and Cert'eM lays in the fact that Cert'eM (as a DNS-based infrastructure) requires a root point to base all its web of trust. The idea is to locate the root (corresponding to DNS domain '.') certificate provision system associated to TACAR.

### **3. I2 proposal on a federated approach to PKIs (Tom Barton)**

There are a lot of federal agencies that would like to offer services to general users, which translates into designing an authentication service supporting access to applications at US Federal agencies by US citizens and others.

The solution is to have federated identities. The authentication schemas adopted are SAML 1.0 and Bridged PKI.

NIST defined a new standard with 4 levels of authentication assurance and only the first two (lower assurance) are available for SAML. E-authentication Identity Providers (like

universities for example) must be compliant with CAF (credential assessment framework).

TACAR contrasts in a way the bridge approach, as it proposes a global and centralised repository. Bridge software supports is rather complex. Also scalability issues are involved dealing with a bridge model. There is nothing similar to TACAR in the States, maybe could be worthwhile investigating whether and how TACAR could be used in the States.

#### **4. Proposal from Politecnico of Turin (Massimiliano Pala)**

Massimiliano proposal is meant to integrate TACAR into applications. The most common trust model is based on trust lists (used mainly by applications), hierarchies, bridge CAs and cross certification. At the moment TACAR is used only as trust list of CAs.

The idea is that a CA can decide to cross certify the root CAs (or some of them) that are hosted by TACAR. This is a one way process so no agreement is needed.

The advantages of this proposal are that no trust links would be used and that there would be only one point of trust. Microsoft supports cross-certifications, whilst it is not available in Mozilla-based browsers.

Diego proposed to develop the proposal further more to have some people in Spain working on it too.

If anybody is interested in joining they can send an email to Massimiliano Pala (massimiliano.pala@polito.it).

**ACTION:** Massimiliano to send more details about the proposal.

#### **Pop-up-free, flat-rate NREN server-certificate service update (Jan Meijer)**

Jan provided an update about the status of the project to acquire a service that offers NRENs pop-up free X.509 server certificates at a flat rate fee for NRENs or national organisations representing the academic community. Since the last meeting in November 04 some work has been undertaken to prepare the documentation necessary to set-up the framework which is constituted by 9 organisations paying a fee to start the procurement for the service, plus TERENA which will offer man-power to carry out the project. Licia has circulated the documentation among the people interested.

### **CAMPUS area**

#### **EuroCAMP report (Licia Florio)**

Licia reported that the preparation for the first EuroCAMP was ongoing and that the registration was very successful and most of people seem to come from university which what is was hope. The number of attendees exceeded what was expected.

#### **EUNIS (Diego Lopez)**

Diego gave a quick overview about EUNIS, the European University association. Torbjorn reported of a possible agreement between TERENA and EUNIS to foster collaboration. Unfortunately nobody from EUNIS could attend this meeting but Ligia Ribeiro asked Diego to introduce EUNIS.

Licia has submitted a paper for the next EUNIS Conference in Manchester (still waiting for answer).

**ACTION:** Licia to investigate about the agreement between TERENA and EUNIS.

### **Directory area**

### **Metadirectory tool (Roland Hedberg)**

Roland presented the metadirectory tool developed by Umea university.

Umea looked at the products available on the market, but they discovered that they had to do a lot of work to adapt them. Therefore they decided to produce something which fulfilled their needs.

The information that comes to system is split in two paths and this is very handy for them. The organisation part and the adaptor is most of the work anyway.

The metadirectory tool is in python and it is open source. The role of SPOCP is in the routing module of the tool.

### **Privacy enabled directory (Victoriano Giralt)**

The purpose directories are created for makes them very vulnerable to the privacy. The solution to protect users' data is to use a particular attribute, which can be set by the users via a Web interface. Access control rules are rather complicated, but no performances problems have been detected. The system is based on openLDAP access rules, although during the discussion it was confirmed that it can also be supported by other LDAP servers.

### **Proposals on attribute co-ordination (Diego Lopez)**

Diego wrapped up the first day and discussed two proposals for attribute co-ordination and federated access.

**First proposal:** One of the objectives of the group is the attributes coordination. Diego proposed to build an initial kernel from already existing local attributes, agreeing on syntax and semantics. The kernel would evolve via a collaborative approach to become the standard for objects and classes. Some light policies would be discussed within the group. The proposal should not be only LDAP-focused.

**ACTION:** Diego, Roland, Miro, Peter, Maja, Reimer, Victoriano , Juergen, Mikael, Thomas and Christian Claveleira (who was not present at the meeting, but volunteered at a later stage) to be part of team called Schema Harmonization Committee (**SCHAC**) to work on this item

**ACTION:** Diego/Licia to invite somebody from EUNIS to participate.

**ACTION:** Licia to set up a web site and start the work. (1 month).

**The second proposal** was a about common directories to build a directory of middleware resources which uses each organisation data source and install a Searchy (<http://jsearchy.sourceforge.net/> developed by RedIRIS and another Spanish university) agent on the local systems.

TERENA TF-VVC should also be invited to participate.

Searchy glues different search engines, so the results of a query show results that are not always available over the internet.

A short report could be prepared as feedback.

People interested should contact Diego Lopez.

### **Collaboration with US Grid (Tony Genovese)**

Aim of presentation was to find out how NRENs can support Grid and what role TERENA can play.

Authorisation and authentication are in Grid separated procedures. The authentication is done by the PMAs, whereas the authentication is carried out by the local institutions.

There three major PMAs: EuGridPMA (in Europe), AmericaPMA (USA) and AsiaPacificPMA (Asia and Australia). The umbrella that coordinates those three PMA is IGF (International Grid Federation, <http://www.gridpma.org/>). TERENA, in respect to TACAR is now a 3<sup>rd</sup> party, trusted by Grid CA to exchange critical datas. Tony asked whether TERENA would be interested in playing any role in IGF, for instance proving a 'home' for IGF, primarily to provide a trusted publishing model. EuGridPMA policy is a dynamic document and the publishing procedures of GGF are maybe to slow. It was agreed that this question requires some consideration in terms of effort that TERENA can invest. TERENA's resources are limited.

Tony asked the group to contribute to the Authentication document, which is going to publish within GGF as an informational document. The aim of the document is to define procedure to establish trust, to create a federation and to identify federation.

A part of authN documents is about requirements for a federation. This part was considered by the group a very useful starting point.

**ACTION:** LF to circulate the authN doc on the list.

**ACTION:** all to comment the document.

### **I2/NMI update: Signet, Grouper, and GridShib**

Tom presented the way Signet, a privilege management system. There is an abstract privilege view, which is translated to be integrated into the system.

Tom talked also about GridShib with allows the use of Shibboleth-transport attributes for authorisation in Grid environment.

Identity based access can be hard to manage on a large scale. The use of attributes provides a solution to this problem. Signet and Grouper can delegate the attribute management to allow the authenticate users inside systems.

### **AAI update on the TF-EMC2 web site**

Licia asked how to maintain up-to-date the information gathered via the questionnaire circulated at the end of 2004 (<http://www.terena.nl/tech/task-forces/tf-emc2/aa.html>). It was agreed to try and use a PAPI-based Wiki server, which will be hosted by RedIRIS. Licia will prompt people for update every six months.

**ACTION:** Diego to install the Wiki.

### **Summary of the actions**

**ACTION:** Massimiliano to circulate over the list more details about the proposal to use TACAR.

**ACTION:** Licia to investigate about the agreement between TERENA and EUNIS.

**ACTION:** Diego, Roland, Miro, Peter, Maja, Reimer, Victoriano, Juergen, Mikael, Thomas and Christian Claveleira (who was not present at the meeting, but volunteered at a later stage) to be part of team called Schema Harmonization Committee (**SCHAC**) to work on this item

**ACTION:** Diego/Licia to invite somebody from EUNIS to participate.

**ACTION:** Licia to set up a web site to start the work about the schema harmonisation (end of March).

**ACTION:** LF to circulate the authN doc on the list (done)

**ACTION:** all to comment the authN document circulated over the list.

**ACTION:** Diego to install the Wiki.