

## **TF-EMC2 Minutes**

**8-9 September, 2005**

**Barcelona, SPAIN**

### **Introduction**

The 4<sup>th</sup> TF-EMC2 meeting was held at the University Politecnico of Barcelona.

Diego welcomed the participants and bashed the agenda. A short round table of the participants followed.

### **Use of SAML for authN and authZ**

#### **Stefan Winter – RESTENA**

Stefan reported about the use of SAML for authN and authZ proposed in JRA5.

The first part of the talk provided an overview about SAML as protocol.

Then the talk covered the way SAML is used to create authN and authZ queries, and more specifically how is applied to the authZ interactions defined by JRA5.

The new idea is to add some information about the source where the authZ engine can retrieve attributes after the authN has taken place.

In order to have a first prototype ready in the next 6 months, JRA5 agreed to use SAML 1.1. It was asked whether the migration to SAML2.0 (when it will be ready) will be easy or there will be problems. Bob said that the main difference between SAML1.1 and SAML2.0 is related to the extensions; therefore these should be defined in a proper way. There is no date about the new Shibboleth release based on SAML2.0.

### **Network access authentication and authorization based on SAML**

#### **Antonio F. Gómez Skarmeta - University of Murcia**

Antonio presented the infrastructure partially developed by university of Murcia in the framework on the European project DEDALUS to provide resources to users based on the role the play.

The important element is the separation between the authentication and the authorisation at network level.

Users authenticate to the network first, using their certificates. If the authentication succeeds, users can use a push or a pull model to access other resources. SAML is used to exchange attributes.

The plans are to keep using the infrastructure and work is ongoing to standardise some models within the IETF and PANA.

### **Guan Xi: An Alternate Shibboleth, With Distributed SP And SAML Toolkit**

#### **Sean Mehan & Alistair Young - University of the Highlands and Islands**

Guanxi is a project founded by JISC. The project has 3 main objectives:

- implement Shibboleth;
- extend and development AA functions among institutions;

- create and use shibboleth federations, based upon Bodington (<http://bodington.org/index.jsp>).

Guanxi allows for the use of Shibboleth in a virtual learning environment.

## **End-to-End & Campus Issues**

### **Martin Sutter - SWITCH**

Martin presented a collection of end users issues that are currently not really tackled and might find a place within the emc2 group.

Some initiatives focused on end-2-end (like Internet2 end-2-end diagnostic, Surfnet detective) are already ongoing, but more focused on possible problems over the network, rather than reaching end users.

Martin proposed to invest some effort in end-2-end, starting with defining a glossary.

An ad-hoc working group, whether this is a new task force or a just another working item of EMC2 might be a solution to carry out the work.

Martin asked anybody who is interested in this work to contact him.

## **SCS updates**

### **Licia Florio – TERENA**

Licia reported about the status of the proposal.

A call for tender has been issued and it is available at:

<http://www.terena.nl/tech/task-forces/tf-emc2/scs.html>

The deadline to submit proposal is September 30<sup>th</sup>. The group will be kept updated about the results of the tender after the official deadline.

## **SCHAC**

### **Diego Lopez - RedIRIS**

Diego provided an update about SCHAC of which a version 0.3 was submitted to the list before the summer. Diego proposed to define an OID and to start define and XML schema.

**ACTION:** to send an email to the SCHAC list to collect the OIDs

At the end of September the SCHAC 1.0 version will be released.

## **Update about UDS and openMetaDir**

### **Roland Hedberg – Umea University**

Roland talked about UDS, the OpenMetaDirectory based on an information routing system. The routing is dynamic (based on the information content) and SPOCP is used as the route engine. The UDS provides a mean to route information about events (expressed in RDF language) from one place to another. The RDF expressions are verified against rules to establish where the expression should be sent.

The UDS has been successfully running since April 2005.

## **AA-RR update**

### **Diego Lopez - RedIRIS**

The AA-RR has been conceived with the purpose to provide an easy way to verify AA interactions.

Two new protocol adaptors based on PAPI and SAML have been added. The PAPI adaptor is able to emulate PAPI's behaviour including the WAYF function. The PAPI authZ mechanism is still pending.

### **VO session: Diego Lopez – Ken Klingenstein – Dave Kelsey**

This session was focused on VOs and the way they are implemented by grids as well as by NRENs.

Diego introduced the topic talking about irisgrid ([www.irisgrid.es](http://www.irisgrid.es) at the moment the site is available in Spanish).

### **Ken Klingenstein – Internet2**

There are several type of VOs that span over different fields like grids, museums, libraries and they vary not only for scope, but only for lifetime and size.

In all cases a VO manages resources and tend to cluster and to use some domain specific tools. Internet2 is working to produce GridShib which will integrate Shibboleth with Grid middleware.

JISC has started a project called ShibGrid.

### **VOs from Grids perspective**

#### **Dave Kelsey – CCLRC**

Dave presented the grid VO perspective. Grids use very heavily VOs, for instance in EGEE there are almost 40 different virtual organisations.

VOs can have long lifetime as well as a short lifetime. For long-lived VOs, the global authZ must be managed by the VO. There is need for short VOs and at the moment EGEE is not able to provide this.

Roles in a VOs do not map the roles that people cover in a real organisation.

The security model is based on a single electronic identity (today X.509 certificate).

Users register once per VO and they are not required to register at each site, which is to say that the site has to trust the VO. To make the system scalable each VO register to the Grid infrastructure.

The single sign on is in Grid based on X.509 certificates.

In Grid authN and AuthZ are separate. The authN is based on X.509 certificates and is done at institute level, whereas the authZ is done at VOs level.

The authZ technology used in EGEE (based on glite) is based on VOMS that assigns groups and roles and follows a "PUSH" model, per instance base.

Users can select the attributes via a client that communicates with the server.

In terms of Acceptable Use Policy (AUP) the aim was to get something simple and usable in many projects (like EGEE and OSG and other national grids). The AUP binds users to VO AUP.

Dave also covered the legal issues related distributed computers. The user registration database stored by the VO must be readable by all the institutions to track users, but VOs are not legal entities, which brings up some problems (not solved yet).

The last part of the talk covered the relation between NRENs and Grids. Grids are running services (CAs for instance) more due to a necessity than to a real wish, which leaves room to NRENs to take up this role.

## **VO in Dynamic Resource Provisioning**

### **Yuri Demchenko – UvA**

UvA made a GAAP analysis to see how to use AAA architecture. Yuri highlighted the problems with VOs.

## **Status of validation and authentication service for TACAR and Grid platforms**

### **Oscar Manso - CertiVeR**

CertiVeR is providing a new service to manage OCSP for GRID and TACAR. The idea is to use CertiVeR to validate the certificates in TACAR. Any CA that wishes to provide CertiVeR as an Authorized Responder should sign the CertiVeR signing certificate request which can be obtained from: [support@certiver.com](mailto:support@certiver.com) For further information contact Oscar Manso ([o.manso@certiver.com](mailto:o.manso@certiver.com)).

More information is available at:  
<http://www.certiver.com>

The pilot service provided is available at:  
<http://globus-grid.certiver.com>  
<http://tacar.certiver.com>

They plan is to release the client as open source.

## **One policy statement**

### **Milan Sova – CESNET**

Milan outlined the problem that led to the proposal for the so called “one policy statement”. Relying parties should be able to verify that a certificate has been issued to a person or to a software agent or some sort of agent (ie mailing list certificate). It is important to notice that the proposal aims to define attribute about a certificate itself and not about attributes of the subject in the certificates. Milan proposed to issue certificates containing references to all the single policy statements they fulfill.

Milan will discuss his idea with the EUGridPMA group first (possibly during the next meeting in Poznan at the end of September). He will report to the EMC2 group about the progresses of this activity.

### **Delegation of Authority**

#### **David Chadwick – University of Kent**

David provided a short demo about a project that allows delegation authority among organisations.

The system implemented is not a centralized system, but it based on policies that define who can delegate to whom. End users are not required to have a certificate, but they can use shibboleth. The system is available at:

<https://issrg-testbed.cs.kent.ac.uk:8443/dis.html>

### **Cross certification proposal**

#### **Massimiliano Pala – Politecnico of Turin**

Massimiliano proposed a way to trust certificates based on a half cross certification process, which is very similar of a real bridge process.

There are still some open issues related to way the standards are implemented by the major browsers. Currently the solution works for Microsoft, but not for other products.

Further more there is the distribution of auxiliary certificates (which would be needed to implement the proposed idea).

Being grid heavily based on OpenSSL, would this solution work for Grid?

### **International Grid Trust Federation (IGTF)**

#### **David Group - NiKEF**

David gave an overview about the authentication process in Grid.

The talk started describing the need that led to creation of EUGridPMA. Over the years the group grew a lot, including members from all over the world. Due to the heavy growth of the group, it was agreed to regionalize in order to have a European, an American and an Asia-Pacific PMA. CAs are requested to apply for the accreditation process to their regional PMA.

IGTF is the federation of the three PMAs and all trust each other.

TACAR is used by the EUGridPMA, therefore is important to maintain the certificates updated. This might result sometimes in a not easy task.

**ACTION:** Licia and Diego to explore a way to verify the ‘freshness’ of the certificates hosted by TACAR.

### **Eduroam AAI Updates**

#### **Klaas Wierenga – SURFnet**

Klaas reported about the status of eduroam and the open issues that are need to be address in the development of eduroam-ng.

## SUN IdM Workshop

The meeting was followed by a SUN workshop on Identity Management. The workshop was attended by around 25 people and presented by Philippe Trautmann ([Philippe.Trautmann@sun.com](mailto:Philippe.Trautmann@sun.com)) and Stuart Sim ([stuart.sim@sun.com](mailto:stuart.sim@sun.com)).

## Next Meeting

The next meeting will be kindly hosted by Srce in Zagreb. Both TF-Mobility and TF-EMC2 will take place in Zagreb. The days reserved for the two meetings are: 31 January, 1-2 February 2005.

## Summary of the actions

Action	Description	Deadline
ACTION1	Milan to report about the progress of one policy statement (1ps)	January 2006
ACTION2	Licia and Diego to explore a way to verify the 'freshness' of the certificates hosted by TACAR.	January 2006
ACTION3	Licia to send an email to the SCHAC list to collect the OIDs	ASAP
ACTION4	Release the latest version of SCHAC (v1.0) at the end of September	ongoing

### ***List of attendees***

Sergio Afonso	University of Porto
Kristof Bajnok	MTA-Sztaki
Vincent Carpier	CRU
David Chadwick	Univ of Kent
Yuri Demchenko	UvA
John DYER	TERENA
Ede Fehér	NIIF/HUNGARNET
Licia Florio	TERENA
Tony Genovese	LBNL/ESnet
David Groep	NIKHEF
Roland Hedberg	Umeå University
Avgust Jauk	ARNES
David Kelsey	CCLRC/RAL
Ken Klingenstein	Internet2
Thomas Lenggenhager	SWITCH
Mikael Linden	CSC
Diego Lopez	RedIRIS
Jesus Luna	UPC
José Manuel Macías Luna	RedIRIS
Oscar Manso	UPC
Manuel Medina	CertiVeR
Sean Mehan	UHI
Ingrid Melve	UNINETT
Manne Miettinen	CSC
Miroslav Milinovic	Srcce
Maurizio Molina	DANTE
Cristina Montserrat	Sun Microsystems
RL 'Bob' Morgan	Internet2
Terry Morrow	JISC
Massimiliano Pala	Politecnico di Torino
Rok Papez	ARNES
Rui Ramos	University of Porto
Juergen Rauschenbach	DFN-Verein
Olivier Salaün	CRU
David Simonsen	UNI-C
Milan Sova	CESNET
Martin Sutter	SWITCH
Mika Suvanto	CSC
Gyula Szabó	MTA-SZTAKI
Philippe TRAUTMANN	Sun Microsystems
Dimitris Vardalis	AUTH
Ton Verschuren	SURFnet
Klaas Wierenga	SURFnet
Maja Wolniewicz	PIONIER
Tomasz Wolniewicz	PIONIER
Alistair Young	UHI
Holger Ziemek	DFN-Verein

### ***Apologised***

Victoriano Giralt	University of Malaga
Vinnie Gupta	Sun Microsystems