

**TF-EMC2 Meeting  
4-5 February 2008,  
Marseilles, France**

**Introduction**

Diego welcomed the participants and opened the meeting.

**JISC – Jason Campbell (JISC)**

Jason reported on a study conducted by JISC to investigate how to bring convergence on the legal side in access management federations. There is a dedicated website where to find out more about the study:

<http://www.jisclegal.ac.uk/access/index.html>

Jason's talk was very much appreciated by the group, due to the easy way he highlighted some important legal issues that should be taken into account when dealing with data in identity management federations.

**SCS Report – Licia Florio (TERENA)**

Licia gave a short update on the current status of SCS. She said that after the problems in the last months of 2007, the service seems to be working smoother.

Licia informed the EMC2 attendees that a face-to-face meeting between TERENA and GlobalSign would take place on 11<sup>th</sup> February. During this meeting TERENA would discuss most of the issues related to the service, among which the massive renewal of the RA administrator personal certificates and problems with the service.

Licia said that she would report more about the outcome on this meeting on the SCS list.

Licia also said that a first meeting with all the SCS representatives would take place in Amsterdam on 21<sup>st</sup> of February. More about the outcome of this meeting will be made known on the SCS list.

**Grid Report - Milan Sova (CESNET)**

Milan reported that the initial plan to IGTF- accredit GlobalSign CA used to issue SCS certificates will not go through. Milan feels that GlobalSign is not reliable enough and therefore he would not expect any support from GlobalSign should any issue related to GlobalSign policy come up during the IGTF accreditation process.

Milan explained that to get accredited by the IGTF a CA is supposed to go through an internal audit every year; the results of the audit are then

presented at the IGTF meetings and finally if the CA matches the requirements agreed within IGTF, the root CA is then published on the IGTF website.

The implication of not having GlobalSign accredited by the IGTF is that SCS certificates cannot be used for Grid purposes.

Milan then reported that in the Grid community work is currently being undertaken to liaise the institutional IdMS and the VOs IdM, but there is currently no agreed solution.

## **REFEDs Report – Jane Charlton (JISC) and Mikael Linden (CSC)**

Jane and Mikael gave an update on the status of refeds.

Mikael reported on the status of the REFEDs wiki; the wiki hosts information about 14 federations. Most of the federations are Shibboleth 1.3 based, even if there are some exceptions such as in Spain (PAPI), in the Norway (SAML2) and in the Netherlands (A-Select).

SWITCHaai (Switzerland), HAKA (Finland) and Feide (Norway) have the highest number of users, covering more than 70% of the user community in their countries.

Mikael pointed out that most of the SPs are providing eLearning and libraries services.

Jane has added some considerable amount of material to the REFEDs wiki, mainly concerning publishers. She gave an update on the SPs and publishers in UK.

## **SCHAC Report – Victoriano Giralt (University of Malaga)**

Victoriano reported on the progresses of SCHAC. Recently Victoriano has initiated some discussion with EUNIS to understand whether SCHAC could be used to support exchange of students' data (Bologna process).

Victoriano has worked very closed with the Australian auEduPerson working group, which has produced an attribute recommendation document, which includes some SCHAC attributes.

SCHAC is currently used by Finland (mandatory attributes are schacHomeOrganization and schacHomeOrganizationType), Spain (RedIRIS and at least the University of Malaga), and Norway (norEdu version 1.4.1 included 2 attributes).

The University of Torun (Poland) has recently agreed to use SCHAC schema. GEANT Identity Provider (GIdP) will use some of the SCHAC object classes. Experimental SCHAC attributes have also been defined to work with PerfSONAR.

Other SCHAC related work concerns the preparation of a draft RFC for registering the **urn:schac** (currently SCHAC is host under the urn:mace:terena.org:schac).

Mikael pointed out that in SAML2.0 the standard is to use OIDs rather than URNs, therefore he recommended not to change the SCHAC OID. Concerning the OIDs, Milan pointed out that these numbers should remain unique even if the attributes are moved from the SCHAC experimental branch to the SCHAC production. The description of the OID should indicate whether the attribute is experimental or operational.

SCHAC URN registry is in production (used also by eduGAIN).

Victoriano finally said that at the last eChallange conference he presented the schacUserPrivate and he suggested looking at the privacy management extension for Firefox and other privacy enhancing technologies.

**Action:** Victoriano and Licia to work together to add a new arc for URNreg attributes (suggested arch: 1.3.6.1.4.1.25178.2) and install the root registry at terena.org

### **Campus Issues – Torbjörn Wiberg (Umeå University)**

Torbjörn gave an overview on the implications of IdMs for campuses. After the initial effort to set-up a proper IdMs, campuses will have the possibility to reduce the costs for managing users accounts and for deploying new systems.

In order to gain this benefit however, institutions (especially the smaller ones) need support to improve the quality of their IdMs, to have proper roles management tools and to deploy meta-directories.

The presentation triggered lots of discussion as everybody agreed that the deployment of IdM at campus level would be easy with the support of best practice documents.

**Action:** Torbjörn to start gathering documentation that are important to write best practice documents.

### **TACAR – Licia Florio**

Some small TACAR policy updates have been requested by the EuGridPMA/IGTF group. The changes are related to the trusted introducer (TI) role; the mandatory role of the TI will be reduced to collect the PGP keys of the applying CA, which in turn will be in the position to send electronically the TACAR documentation to the TACAR representatives.

TACAR will be used by eduGAIN to gather the various root CAs that will be used for eduGAIN.

**Action:** Licia to circulate the updated version of the TACAR policy.

## **JRA5 Updates – Jürgen Rauschenbach (DFN)**

The JRA5 work on eduroam is more limited to the research work, as most of the operational work is now part of the SA5.

JRA5 work is very much focused on eduGAIN, in particular in extending eduGAIN to other federations. Work has started also to migrate eduGAIN to a service, which will also include the definition of a policy.

## **ECAM report – Diego Lopez (RedIRIS)**

Diego provided a short updated on ECAM.

A new session called suggestedByECAM was added to the ECAM page in January 2008. SuggestedByECAM contains links to documents and/or software that are relevant for the community. The aim is populate this page to include more links coming from discussions or results of EMC2.

Andrew gave a quick overview on the document on securing IdM systems that he wrote together with the support of Jan Meijer, Ingrid Melve and Jürgen Rauschenbach. This document is available on the SuggestedByECAM page.

<http://www.terena.org/activities/tf-emc2/ecam/repository.html>

It was suggested to add a section or a wiki to collect the list of AA-enabled applications. Licia mentioned that a similar recommendation came from the last EuroCAMP. A possibility for such a thing would be to use the refeds wiki, rather than the suggestedByECAM page.

**ACTION:** Miro to look at the info on the refeds wiki and see where the list of AA-enabled application could fit. This page should be open.

## **NRENs Updates**

An update on the AA activities followed.

### **a. Internet2 Updates**

Ken reported on Shib and InCommon developments.

Shibboleth2 has been tested and it should be released soon. An OpenId platform within Shib will also be supported.

InCommon is growing and counts now 75 members. There are many federations and the overlap among some of the federations is quite big.

Ken reported that some discussion is ongoing in US to close the I2 Middleware Group. The reasons for this are due the fact that it is felt that I2 might not have in the future the possibility to keep supporting Middleware in the same way as they are doing now. If these would be the case, activities like Shibboleth and InCommon will have to continue elsewhere.

**b. AAF Update – Patty McMillan (University of Queensland) (via Skype)**

Patty reported on the progresses of the Australian Federation (AAF). AAF is in a test-phase, but nevertheless it counts 35 members. A dedicated working group is defining schemas and attributes for the AAF federation, see:

[www.aaf.edu.au/attributes](http://www.aaf.edu.au/attributes)

AAF plans also includes some major work to put AusCERT root certificate in the browsers.

**c. RedIRIS Update – Diego Lopez**

Diego reported on the work done to formalize the Identity Services. Since recently PAPI supports a gateway for OpenId. Some more effort has been put into ARCA (the RSS aggregator for the academic community); ARCA counts today 11 institutions. Future plans for ARCA cover support for integrating digital identity and repositories.

**d. SWAMI – Torbjörn Wiberg**

Most of the current work on SWAMI is concentrated on established a SAML2.0 federation.

**e. AAleye – Mikael Linden**

Mikael reported work is ongoing to set-up a confederations framework for the confederation work for the Nordic federations.

The plan is to use eduGain BE to interconnect the various federations, using different technologies.

HAKA federation has defined templates to support the audit of participating institutions; the audit is a self-audit. The government federation will require stronger procedures.

There was a discussion about single log-out; due to the complexity of the problem and on the sake of time, Diego suggested to organize a longer slot about this topic in the next meeting.

**Action:** Add a single log-out session during the next EMC2 meeting.

**f. UK Federation – Josh Howlett (JANET(UK))**

Josh reported about the developments in the UK federation. She said that institutions are joining quickly, maybe due to the fact that Athens (the former system) will not be supported anymore.

Josh reported about his involvement in OpenSEA, about which he said that the supplicant is being tested. There are still some problems, especially to make it work on with different type of software installed.

Josh managed to convince the people working in TCG that the posture should be validate by the IdP, which should then send the results of the validation to the SP. The SP based on the IdP response should decide to allow the machine on the network or not. There is now a WG to look at how to do this.

Josh reported that JANET is discussion with BT the possibility to create an 'Open zone' which would enable JANET users to access this open zone.

#### **g. CESNET Updates - Milan Sova**

Milan presented the FedCA, set up by CESNET to support multiple CA via a web interface (or other interfaces among which XKMS). The CA can also work as an SP.

Future plans for FedCA include HSM support, better way to support the WAYF functionality and the implementation of the RA functionalities.

#### **h. SWITCH – Thomas Lenggenhager (SWTICH)**

Thomas gave an update on the deployment of SWITCHaai federation.

#### **Shintau – David Chadwick (Kent University)**

Shintau conceptual model is ready and the mapping phase should start soon. David presented the conceptual model.

David asked for feedback on his presentation and in particular on the implementation proposal.

#### **AAI for network-oriented services – Candido Rodríguez (RedIRIS)**

Candido presented how to use the implemented federation infrastructure for a client with no web capability. The solution, SASL CA, is what RedIRIS is testing. Within SASL CA users receive a short live certificates after authentication; this certificate is used to access services.

The topic was considered were interested but due to the lack of time there could not be enough discussion. It was suggested to address this topic again and more in detail during the next meeting.

#### **LoA – James Farnhill (JISC)**

Very quickly at the end of the meeting James reported on a survey conducted by JISC on LoA. The main finding was that 70% of SPs would like LoAs.

James asked for comments on the report published by JISC, see:

[http://www.jisc.ac.uk/whatwedo/programmes/programme\\_einfrastructure/esloa.aspx](http://www.jisc.ac.uk/whatwedo/programmes/programme_einfrastructure/esloa.aspx)

James said that JISC has also looked for use cases for OpenId.

#### **Next Meeting**

The next TF-EMC2 meeting will take place in Umeå on 9-10 July.

#### **List of Actions**

**Action2008-02-01:** Victoriano and Licia to work together to add a new arc for URNreg attributes (suggested arch: 1.3.6.1.4.1.25178.2) and install the root registry at terena.org

**Action2008-02-02:** Torbjörn to start gathering documentation that is important to write best practice documents.

**Action2008-02-03:** Licia to circulate the updated version of the TACAR policy.

**Action2008-02-04:** Miro to look at the info on the refeds wiki and see where the list of AA-enabled application could fit. This page should be open.

**Action2008-02-5:** Add a single log-out session during the next EMC2 meeting.

## List of Attendees

Serge Aumont	CRU
Jason Campbell	JISC Legal
David Chadwick	University of Kent
Jane Charlton	JISC
Andrew Cormack	JANET(UK)
James Farnhill	JISC
Licia Florio	TERENA
Brian Gilmore	The University of Edinburgh
Victoriano Giralt	University of Malaga
Maja Gorecka-Wolniewicz	PIONIER
Roland Hedberg	Umeå University
Josh Howlett	JANET(UK)
Christos Kanellopoulos	GRNET - AUTH
Ken Klingenstein	Internet2
Thomas Lenggenhager	SWITCH
Mikael Linden	CSC
Diego Lopez	RedIRIS
Miroslav Milinovic	Srce
Dubravko Penezic	Srce
Juergen Rauschenbach	DFN-Verein
Cándido Rodríguez	RedIRIS
Olivier Salaün	CRU
Milan Sova	CESNET
Torbjörn Wiberg	Umeå Universitet
Klaas Wierenga	Cisco
Stefan Winter	RESTENA
Tomasz Wolniewicz	PIONIER
Hans Zandbelt	SURFnet