TF-EMC2 Meeting  
28-29 March Florence, Italy

Introduction  
Diego opened the meeting and welcomed the participants.

SCS updates – Guy  
Guy gave an update on the SCS service.  
There were some recent changes within GlobalSign (GS) as results of which GlobalSign is not part of Cybertust anymore.  
TERENA had a phone call with GS management (in February), who confirmed that nothing would change for TERENA until 2011.  
Guy reported on the status on planned tasks:  
- OCSP implementation is under preparation. There will be 5 servers running for this at SURFnet and CESNET.  
- HTTP POST interface: GS committed to deliver this feature, but there are some delays compared to what was scheduled.

TACAR Updates - Licia  
Licia reported that the final version of the policy is on-line.  
No other major things were reported.

ECAM - Diego Updates  
Diego gave an update on ECAM, the steering committee group for both TF-EMC2 and TF-Mobility. ECAM members are the work item leaders for both task-forces, plus representatives of the other relevant organisations, such as AARNET. Internet2 representative has not been appointed yet.  
The group meets approximately once per month via phone-conferences.  
ECAM addresses issues related to the middleware developments in the various continents.

REFEDS - Mikal Linden  
Mikael gave an updates on REFEDS.  
Thanks to Mikael inputs, lots of information is now available on the refeds wiki, which is publicly available (read-only) at:  
http://www.rediris.es/wiki/tf-emc2/index.php/Federations

Not all NRENs have provided their contributions, so Mikael invited those missing to update the wiki.  
**Action:** Licia to send an email to the refeds list to remind the missing federations to fill in the wiki.

Campus issues (Torbjorn Wiberg)  
Torbjon gave an update on issues that arise at campus level. Torbjorn pointed out that some issues go beyond technology and include user management and other business processes.
Torbjorn also reported that a survey showed that only 7,000 of 50,000 users in Sweden have used a proper AAI. The survey also shows that some campuses prefer to deal with only one preferred vendor.

**OGF – Milan**

Milan reported on the last OGF held in Raleigh (North Carolina). One of the things of interest for EMC2 community was the workshop on federations that took place, focused on how to integrate Shibboleth with Grids. The link with the programme and the presentations was circulated on the list by Licia. ([http://www.ogf.org/gf/event_schedule/?event_id=6](http://www.ogf.org/gf/event_schedule/?event_id=6))

During OGF in North Carolina there was also a BoF on level of Assurance. There are some suggestions to introduce (within the IGTF) level of assurances in order to match those introduced by NIST (in US).

**Monitoring - Miroslav Milinovic (SRCE)**

Miro presented the plan for a monitoring infrastructure at federation level. The monitoring system should be able to allow for e2e users’ report as well as to identify problems in the infrastructure at a particular point in time. Miro proposed a modular approach:

- Step1: The first step should be the collection of available tools. One the things that Miro suggested were to add an extra field on the refeds wiki, to report whether a monitoring system is available.
- Step2: Identify the elements to monitor
- Step 3: Start building the tools; the first tool could be a weather map.

Miro also suggest to use the on the refeds wiki to collect information related to tools like PERFsonar and Internet detective. There was a discussion on the middleware diagnostic in terms on how far and detailed we should go. Diego suggested having something similar to the PerfSonar for middleware.

Step2: The wiki should contain more more detailed info on the IdPs that are part of the federations.

**Action**: Licia and Miro to work to have Step 1 completed by the summer.

**Directory - Victoriano Giralt, University of Malaga**

Victoriano reported on the developments on SCHAC. He mentioned that the University of Malaga and RedIRIS have been awarded the first honour mention (November 2006), for the implementation of user controlled attribute release policies based on schacUserPrivateAttribute.

The latest SCHAC schema (v1.3) was released in January 2007. The adoption of the Schema is progressing. Currently SCHAC is being used by:
- 11 IdP in HAKA use SCHAC
- Rok Papez reported that SCHAC is being used in Slovenia
RedIRIS uses SCHAC internally and recommends the SCHAC usage to the Spanish universities. University of Seville, the University of Basque Country and the University of Malaga use SCHAC in production way.

GEANT IdP will use some schac attributes.

Victoriano suggested using an experimental version of SCHAC, with some experimental attributes for testing purposes. The new attribute that were suggested to be added, (mainly to match some requirements coming from GEANT2 project are):

- schacProjectMembership
- schacProjectSpecificRole

The proposal to have a SCHAC test release was approved. However there was no consensus on the attributes suggested and therefore it was agreed to discuss which attributes to have on the experimental version on the SCHAC list.

**Action:** Victoriano to coordinate the release of the test version and get consensus on the attributes.

Victoriano pointed out that SCHAC document section 4.3 (related to students’ information) is still empty, but there seems to be sufficient interest to work on this. One of the issues to be address is how an university can distinguish between the local students and the foreign students. His suggestion was to use a sort of federative approach, where the local university gets information about foreign students from the students’ home organisations.

Bob said that [http://www.pesc.org/](http://www.pesc.org/) has worked at similar issues years ago producing a transcript format. It could be worth looking at this.

* eduPersonAffiliation (ePA)

Victoriano reported about the semantic differences in Europe in the usage of this attribute.

In order to solve the semantic problem, the following proposals were discussed with the MACE group:

- Recommending European institutions not to use ePA, but use instead eduPersonEntitlement
- Scope the affiliation, having a eduPersonScoopedAffiliation
- Using numbers

* URN

Victoriano said that there were some progresses on the interface to handle URNs, even if slower than expected. It was agreed to use REST (instead than SOAP) as language to implement the interface. The project is available at RedIRIS GForge: [https://forja.rediris.es/projects/urnreg/](https://forja.rediris.es/projects/urnreg/)

**DAME Project – Sasha Neinert**

Sasha reported on the status of the DAMe project. The implementation of RADIUS + DIAMETER (NAS-SAML) is being tested. The usage of NAS-SAML gives the possibility of using attributes to perform authorisation (authR). The authentication is done via the standard eduroam infrastructure.
The authorisation attributes are not handled via the RADIUS servers, but by the user’s home organisation. RADIUS is used only as a way to carry attributes. The authorisation is done via NAS-SAML, based on SAML attributes and assertions.

The next step of the project is to provide universal single sign-on, meaning allowing for:
- Authentication for network access, via eduroam / NAS-SAML
- Fetching eduGAIN signed tokens
- Bootstrap eduGAIN authentication from the NAS-SAML one
- No need to re-authenticate

Milan expressed his concerns about the deployment of the project after the research phase.

**SIP AAI - Jan Ruzicka, CESNET**

Jan gave an overview on how SIP protocol works. One of the main issues in using SIP is how to authenticate the users’ requests to access the SIP service. The only available and implemented solution at the moment is to use TLS + http digest.

Another problem to address is how to identify the authoritative servers that are allowed to proxy the data.

It was pointed out that are several aspects to look at when talking about authentication:
- how to authN the users,
- how to secure the channel,
- how to secure the voice etc.

Diego suggested the task forces operating on voice and video issues to produce a set of use cases, in order for the TF-EMC2 to discuss the best way to deal with the AAI. The use-cases should be ready before TNC and discussed during the AAI meeting on Sunday 20 May.

**Action:** Licia to coordinate the presentations topics for the AA meeting on Sunday 20 May.

**International Updates**

**Internet 2 updates – Bob Morgan**

Bob reported on Shib2.0. Its SAML2.0 support is ready for tests. OpenSAML is also ready for tests, but I2 is looking for volunteers. Shibboleth2.0 will provide support for CardSpace as well as openLiberty integration. InCommon federation is progressing and there is on-going work to interfederate with US Gov E-Authorisation.

**Australian MW activities – Patty McMillan**

Patty provided an update on the middleware activities in Australia. Some work is ongoing to establish the Australian Access Federation (AAF), which should be in place by the end of 2007. The AAF will be shibboleth based and we also use PKI. The certificates will be granted via the universities to users and not via the federation.
NRENs Updates

SUNET – Torbjorn Wiberg
Torbjorn reported on SWAMID, the SAML/Shibboleth based Swedish federation. SWAMID also includes eduroam. Digital server certificates are provided via SCS service. Some work led by Roland Hedberg, Leif Johansson is ongoing in the Metadirectory field.

RedIRIS - Diego Lopez
RedIRIS has reached an agreement to integrate PAPI with SUN IdM products. A PAPI implementation for the SUN JAAS is available at the PAPI web site. The result will be that Sun AM will incorporate PAPI proxy capabilities and that PAPI will incorporate SAML2 support.

On the federation side Diego reported that there are currently two main federations in Spain (excluding eduroam): CBIC and SAUWoK. The plan is integrate the two of them. Some test are planned between the CBIC federation and commercial providers (JSTOR and Elsevier).

RedIRIS is also testing some diagnostic aggregators to provide white lists. Tools under evaluation are:
- Comercial: Simplicitia: http://www.simplicita.com/

Diego reported on ARCA (http://arca.uc3m.es/), the RSS tool to aggregate and share multimedia contents. ARCA system is divided into channels. A channel represents a source of multimedia content and each institution is associated with one or more channels. Each channel contains a series of events, retransmissions and/or multimedia contents, called “channel items”. With this structure each institution is responsible for handling their content.

TERENA group PEACHES is evaluating ARCA to handle multimedia material.

SWITCH – Thomas
Thomas gave an overview on the SWITCH federation, started in 2004. Currently SWITCH are testing Shibboleth 2.0 and working to support also accounting. The MSDN AA subscription from Microsoft can now be accessed through the federation.

JISC – Nicole Harris
Nicole reported about the developments on the federation in UK. The Shibboleth-based federation in UK was lunched in the fall 2006 and it is progressing very well. Level of Assurance, Virtual Organisation and Identity Management are considered by JISC strategic for the development.
UNI-C
Three years of funding have been allocated to establish a federation. The test federation is in place, but no real IdPs yet. The initial idea was to have a shib based federation, but UNI-C might decide to implement the FEIDE model.

CRU-RENATER
Shib federation. There are already 23 IdP. They have shibbolised captive portals for Wi-Fi roaming.
CRU-PKI, which works to issue both server and end-users certs will terminate at the end of 2007.
CRU-RENATER joined SCS service since the beginning. They developed a pre-validation web interface, which performs all the expected checks. The interface also provides OpenSSL command to generate PKCS#10 requests. CRU has now issued 765 certificates for 80 organisations in its constituency.
Works is ongoing to produce the next version of the directory schema: SUPANN.

FEIDE – Andreas
FEIDE moved from their in house developed federation software to SUN open source solution. Andreas reported UNINETT experience with dealing with a commercial provider.

Updates from the publisher community – Jane Charlton
Jane presented the UK Access Management Federation. Work is ongoing to merge this federation with the UKfederation, the shibboleth-federation for higher education. One of the major concerns raised the by the publisher is related to the legal aspects of the UK federation agreements, in particular those aspect that are different from their current agreement.

JISC has been negotiating content license deals with publishers for the whole of UK education. These deals are/will be business drivers for the UK Federation.

Persistent Ids - Thomas
Thomas raised the issue whether there is a role or an interest from the NRENs in the area of persistent identifiers or DOI. The DOI system assigns persistent names to any entity that is expected to use the Internet. One of the scenarios where persistent IDs could be useful is to handle distribution of material produced by the universities via access grid.

Diego said that they have experienced the problem.
There are several tools for managing users’ references, such reference manager.

Possible activities and decisions on this topic are left for further discussion.

SWITCH Group management tool (GMT) – Lukas
Lukas presented the GMT tool developed by SWITCH to manage groups and privileges. The tool allows group access to resources.
Bob pointed out that there is a similar tool, Grouper developed by Internet2. Grouper is designed to meet the needs of larger organisations and to delegate the management. There was lots of interest in the tool. The current back-end is file-system based to reduce the components to install, but a database back-end could easily be used.

**Trust management in Shibboleth and InCommon (Bob Morgan)**

Bob reported on trust management issues in Shibboleth and InCommon. Shibboleth trust model works in a way that each Shibboleth resource site trusts each shibboleth origin (home), so each assertion signed by the origin site is trusted by the target site. The trust between the home site and the resource sites is established by mean of digitally signed SAML messages where the target and origin server use X.509 key pairs/certificate. Bob explained the pros and cons in using keys and in using a common CAs to issue certificates.

In the future there could be a mix scenario, in which federations still use CAs, but where the peers can offer keys. This implies that the federations should be able to handle both models.

**VOMS – Vincenzo Ciaschini**

Vincenzo presented the latest developments in VOMS. The access to VOMS is based on the DN of the user, which is extracted from the user certificate.

**SWITCHslcs & VASH - Thomas**

Thomas presented the work being undertaken by SWITCH to integrate Shibboleth and Glite, the middleware software developed within EGEE.

The work consists of two phases:

1. Phase 1 is focused on short-lived credentials service (SLCS). In this way the AAI infrastructure will be able to issue X.509 certificates.
2. Phase 2, called VASH, VOMS Attributes from Shibboleth, is focused on making Shib attributes available to grid resources for authR decision. The attributes will be handled by VOMS

He explained that the reason to use VOMS is that VOMS is able to bundle attributes certs into proxy certs that are accepted by the Grid applications.

VASH is a browser-based Shibboleth SP.

There is one VASH per federation and each VASH is connected to VOMS.

**Next Meeting**

The next EMC2 meeting will take place on 4-5 September in Prague.
Summary of the Actions

Action01-03-2007: Licia to send an email to the refeds list to remind the missing federations to fill in the wiki.
Status: Mail sent to the refeds list. There are only two federations for which the information are still missing.

Action02-03-2007: Licia and Miro to collect the monitoring tools already available for the current federations. One the things that Miro suggested were to add an extra field on the refeds wiki to report whether a monitoring system is available.
Status: The field was added to wiki during the meeting.

Action03-03-2007: Victoriano to coordinate the release of the SCHAC test version and to get consensus on the attributes.

Action04-03-2007: Licia to coordinate the presentations topics for the AA meeting on Sunday 20 May.
Status done.