

7th TF-EMC2 Meeting

October 16 – 17, 2006

Malaga, Spain

Welcome

Victoriano Giralt welcomed the participants on behalf of the University of Malaga.

Introduction and ECAM announcement (Diego Lopez)

Diego opened the meeting announcing that the new TF-EMC2 charter was approved by TERENA Technical Committee in September 2006.

Diego also introduced ECAM, the joint steering committee for both TF-Mobility and TF-EMC2. Current ECAM members are the chairs and the work item leaders for both task forces namely:

- for TF-EMC2: L. Florio, D. Lopez, T. Wiberg, V. Giralt, M. Linden, M. Sova
- for TF-Mobility: K. Wierenga, S. Winter, J. Howlett, P. Hanset, D. Simonsen
- involved in both task forces: M. Milinovic.

Other members can be appointed by unanimity of the ECAM members.

ECAM will meet twice per month via multi-conference.

It was also agreed to create a ECAM mailing list, a web page to gather information on ECAM and if needed a wiki.

Action 20061016-01: TERENA to set up an ECAM mailing list and ECAM web page.

AA-RR update (Diego)

Diego gave an update on the AA-RR tool. The latest AA-RR version (version 1.1) supports different protocols, such as SAML (currently 1.1, 2.0 coming soon) as well as the Spanish SSO system PAPI.

The AA-RR design offers an open framework for easily incorporating support for new protocols (for instance A-Select and RADIUS).

The AA-RR tool could provide support to validate new component in an eduroam environment.

The OSIRIS (Open Source Infrastructure for Run-time Integration of Services) project (<http://itea-osiris.org>) supported by several national industrial bodies has requested the use of the AA-RR for validating some service bus components. Initial contacts with the Eclipse (<http://www.eclipse.org/>) development team have been initiated.

Diagnostics (Miroslav Milinovic)

Miro presented his plan on how to carry out the new TF-ECM2 Work Item ‘Diagnostic-related Activities’. The work item aims to create some instrument to detect problems when they occur and to gather information about the status of a task in a certain period of time.

Miro pointed out that cross-campus diagnostics tools are not always welcomed by the campus administrators, but they certainly help to detect (inter-)campus troubles.

Action 20061016-02: Everybody to send Miro information (url and/or documentations) on tools currently used for monitoring/troubleshooting. Miro will set-up a wiki to host the information by the end of November.

Directory Schemas (Victoriano Giralt)

Victoriano presented the plan for the work item on directories, which includes the work on SCHAC and two new proposals: URN Registry and SCHAC based federated Student Registration System.

a. SCHAC Updates

SCHAC is progressing well.

The current version SCHAC SCHEMA LDAP v1.3.0.b is currently being discussed and available at: <http://www.terena.nl/activities/tf-emc2/schacbeta.html> .

SCHAC SCHEMA is used by:

- FUNET
- In Slovenia - The universities use SCHAC to deploy centralised LDAP.
- University of Malaga (UMA) is planning to load SCHAC attributes onto the institutions smartcards. UMA is also phasing out the current iris* attribute for which a schac* equivalent exists.

b. URN Registry proposal

Victoriano proposed the usage of two SCHAC objectClasses (schacURNDescription and schacURNDelegation) to support the URN registry. Leif argued that with the usage of DDDS one of them may become unnecessary, which was agreed.

Victoriano initial proposal to access the registry included a web interface for operators and LDAP for machines. Leif pointed out that it would not be of much use due to people fear of exposing their directories to the wide open Internet.

Victoriano agreed to use a unique web interface SOAP-based.

Victoriano will start work on implementing the proposed solution and will report to the group.

Action 20061016-03: Victoriano to report to the group on the URN Registry.

c. SCHAC based federated Student Registration System

Victoriano proposed to create a SCHAC based Identity Federated Student Registration System.

The system would use a federated service for sending students' credits back to their home organizations. The infrastructure would use a hierarchy of MetaDirectories for routing the information (a la eduoam's RADIUS hierarchy). With this solution information could be retrieved by the participating institutions when needed and personal data could be stored only at the users' home institutions.

This idea would be useful also to support the Bologna process.

A discussion developed on where students' data should be kept. Leif said that it is in principle not a problem collecting personal data locally, whereas Victoriano's preference is to store the least necessary information on his own systems and get the needed data from the users' home institutions.

Leif pointed out that it is not clear who the official Bologna people are and that it would be worth understanding this and get in touch with them.

The risk that SCHAC community might run if no official communication will be established with the European Bologna people is that SCHAC could build a system that might not be useful to other communities.

No real consensus was reached on this point, but it was agreed to get in touch with the people involved in the Bologna process.

Action 20061016-04: TERENA to get in touch with somebody involved in the Bologna Process.

Campus issues (Torbjorn)

Torbjorn presented the work item "Campus Issues".

Senior IT leaders spend more and more time on AAI/ID management. Over the last couple of years there has been a general and increased interest for AAI.

Torbjorn pointed out that it would be good to create business cases to explain the increasing need of AAI.

Diego suggested creating a roadmap, which might also include some tools recommendations. In this way it would be possible to monitor the progresses. Torbjorn said he did a cost/benefit analysis that he will send to the list.

Action 20061016-05: Torbjorn to send a draft roadmap the list by the end of November.

JISC seems to have some marketing material available, which will be a very good starting point.

Action 20061016-06: TERENA to set-up some repository to collect marketing material, starting from JISC.

Federation coordination (Mikael Linden)

Mikael presented his workplan on REFEDS, which comprises of three main objectives:

- collection of policy and procedures of those federations involved in REFEDS
- dissemination work
- and whenever possible harmonisation

Diego remembered that a EMC2 wiki (<http://www.rediris.es/wiki/emc2/>) was set-up on the RedIRIS web site a few months ago, but it was never advertised. The wiki has been used so far mainly by Licia to collect some information on the AAI developments.

The wiki could be the best way to collect and disseminate policies and practices. Mikael suggested defining a template/questionnaire on policies and practices (stored on the wiki) and ask all federations to fill this template.

Each federation will be responsible to keep the information on the wiki up-to-date.

It was agreed to have the REFEDS meetings during the EMC2 meetings.

A REFEDS mailing list (refeds@terena.nl) is already available.

Action 20061016-07: Licia, Mikael and Diego to work and make the wiki ready, by end of November.

TACAR Updates (Licia)

Some work has been undertaken to improve TACAR (www.tacar.org) functionalities. The work took longer than planned, also due to the need of comments/coordination with the EuGridPMA group. To date TACAR is being used mainly by the EuGridPMA and some of the new features were in fact requested to ease the download of certificates for this community.

The new TACAR User Interface (UI) was finally presented and approved during the last EuGridPMA meeting (October 5-6). The new features include:

- Multiple downloads of certificates in different format (depending on the users needs)
- Possibility of grouping certificates in categories and visualisation according to the category selected. Currently the categories covered are those defined by the EuGridPMA.

The download of certificates does not longer use a self-signed certificate, but a GlobalSign certificate obtained via SCS service.

A new version of the TACAR policy has been sent to the list (both EMC2 and EuGridPMA) for approval. The change was needed to allow for a new role, the Trusted Introducer (TI). Whenever a new CA requests to join TACAR a face-to-face meeting is needed to collect the signed documentation, the root certificate and the PGP keys if these mean is chosen for further electronic updates.

The TI will act on behalf of TACAR representative during the first face-to-face meeting and will deliver all the material collected to the TERENA Officer, who will upload the root into TACAR.

The TI will be the chairs of the Grid PMAs (EuGridPMA, APGridPMA and TAGGridPMA).

Milan suggested refining the policy to make clear what the TI role is.

Action 20061016-08: Licia to finalise TACAR policy and circulate the document to the lists for final approval by December.

Grid collaboration (Milan Sova)

Milan presented his views on the scope of the work item called Grid collaboration for which he will be responsible.

In Grid there is a separation between authentication, based on X.509 certificates and authorisation, performed by the Virtual Organisation (VO).

The work item will focus mainly on the authentication procedures and will monitor the work of IGTF (International Grid Trust Federation) and OGF (Open Grid Forum).

Milan reported that the EuGridPMA has decided to accredit Globalsign CA; it seems like the procedure can take place without involving Globalsign.

The advantage of this would allow usage of SCS certificates for Grid portals.

News on SCS (Licia)

Licia reported that the extension of the current contract, which expires in January 2007, is under negotiation with GlobalSign. The new contract it is expected to run for a 3-year period.

The new contract will provision only server certificates, which must be used by the NRENs and related constituency for non-commercial applications.

It was asked whether universities could use SCS certificates to sell on-line courses.

Action 20061016-09: Licia to investigate the usage of SCS certs furthermore.

New features that should be included in the new contract are:

- Implementation of an HTTP Post interface which would connect to GlobalSign (GS) backend. This solution would allow NRENs to customise the interface the way they like and would also allow to define out-of-band SubjectAltName
- SubRAs – to date two subRAs have been implemented for SWITCH as proof of concept. The new contract will allow NRENs to request subRAs (the functionality will be charged extra).
- OCSP implementation – The OCSP service will be ran in reality by CESNET and SURFnet. However GS will need to implement a dedicated certificate profile to allow NRENs to use the service. GS said to be happy to provide support for the OCSP.

Alex reported that in Australia the research and education community has joined forces to establish a CA, which will be audited to be listed in the major browsers/mailers. This approach, although expensive, will allow for flexibility in the definition of the CA policy, certificates profiles and will also allow for user certificates.

Consolidating SCHAC – Schema and document (Javi Masa)

Javi provided an update about SCHAC SCHEMA and the changes made since last meeting in Catania.

There was a discussion about schacUUID (unique identifier) and how to proceed.

A discussion followed and it was agreed to drop this attribute, which originally was defined to create opaque DN.

Action 20061016-10: Javi to modify the SCHAC document as agreed and circulate the new version to the list.

Consolidating SCHAC – Common vocabulary (Mikael)

Mikael presented a proposal to address the SCHAC vocabulary.

Agreeing on the semantic of attributes is relevant for authorisation purposes, especially if SCHAC will be used in the future for cross-national activities.

The meaning of some of the attributes in SCHAC is quite obvious, but for some others (HomeOrganizationType, UniqueCode and UniqueID) a vocabulary is needed.

For these attributes a proposal was presented (see Mikael's slides,

<http://www.terena.nl/activities/tf-emc2/meetings/7/slides/tf-emc-malaga-schac.ppt>)

Action 20061016-11: Javi to produce a new version of the document that describes SCHAC and to include Mikael's slides into this new version.

Action 20061016-12: Javi and Mikael to finalise the vocabulary discussion over the list.

NRENs Updates

RedIRIS update (Diego)

Diego updates covered:

1. COPA, the coding schema developed by RedIRIS. Some COPA-aware tools are available
2. pkIRIS, the CA ran by RedIRIS for Grid applications (also accredited by EuGridPMA). pkIRIS-CA uses a web interface, openSSL based, to manage PKI. The certificates are stored in LDAP.
3. PAPI, the Spanish SSO system. The current version of PAPI is fully compatible with Shibboleth and first real usage tests will start in November 06.
4. PAPI federation is happening. Diego said that we'll need to take into account commercial software and of course SAML2.0.
5. OpenPMI, the Open Privilege Management Infrastructure, which uses attribute certificates to provide authorisation. The current version is available at:
<http://openpmi.sourceforge.net/>

Geant2/JRA5 update (Juergen)

The European eduroam confederation policy was finalised in the summer 2006 and is being implemented.

However, the European eduroam policy is not enough and NRENs will have to take care of defining national policy to reflect their national legislation.

Part of the work of JRA5 currently, beside the research work, focuses on the migration of some of the activities (which have the potentialities) to service; eduroam will be the first activity to migration to service.

It was reported that also Slovakia joined (a few days before the meeting).

Internet2 (Ken)

I2 new network (called Newnet) has been rolled out. Every campus will get from 2 to 10Gb bandwidth with the ability of creating dynamic lambdas. I2 is peering with other networks (including Google).

A pilot is ongoing to align IdM campuses and Teragrid IdM. The idea is that campus identities can be used to access Teragrid.

In the coming future I2 will concentrate on GridShib family implementation. Shibboleth 2.0 will be out soon.

SWITCH (Thomas)

Thomas reported about SWITCHAAI. SWITCH federation (Shibboleth based) is in place and counts now 21 members (IdP) and more than 100 resources. Thomas also showed ArpViewer, a tool to get users consent for «Attribute Release» and for «Terms of Use» if applicable.

UNINETT (Julie)

Julie reported on FEIDE, the Norwegian federation. Currently there are 23 services (local applications and shared application) up and running. SCHAC is being used.

Since recently UNINETT has moved to SUN software. The choice was driven mainly by the fact that SUN software supports open standards such as SAML 2.0. No tests have been performed to verify the interoperability with other SAML2.0 software yet.

It was asked how long it took to migrate to the new software. Julie said the full migration will take more or less one year time.

FEIDE/UNINETT is Liberty Alliance member

DFN (Juergen)

DFN-AAI is under development. The central operational tasks will cover metadata administration, test system, WAYF-server, CA, training and NOC.

Certificates will be used to support Shibboleth and the other AAI operations.

CRU (Florent)

There are several bodies in France that provide middleware support. CRU works for higher education, whereas UREC supports research.

Florent only reported about CRU.

Efforts are ongoing to establish a shibboleth-based federation in France, which will provide some general framework and not a real WAYF service. The engagements on SPs are quite low-profile and are related mainly to the software, namely security of installation software and compliance with privacy laws.

European SPs can easily join, but it might be quite difficult to include not-EU SPs due to privacy laws.

On the PKI side, CRU runs a CA (since 2003), through which provides users certificates. CRU has joined SCS since the beginning and they hope to see the service running in the future. The main difficulty to deploy SCS in France was to update the WHOIS records.

To ease the control of the RAs, CRU has developed a tool to perform the checks electronically. This tool (<http://www.cru.fr/igc/scs/validation/>) is available for the community.

If interested, contact Florent.

FUNET (Mikael)

HAKA federation (only for higher education) runs Shibboleth and has been operational since August 2005.

There are quite high requirements to join the IdPs and therefore no home for the homeless (which would not have high quality user data) is available.

To date there are lots of library services.

Mikael gave a demo, which showed how to login to a Finnish service with an account from UNINETT. It was asked whether this could be a first example of confederation. Not everybody agreed that this was a real confederation; some people suggested it being a case of peering of different federations.

SURFnet (Bart)

Bart reported that the SURFnet federation project has started. SURFnet federation will be A-Select based.

The first step was to understand the status of IdM in higher education in the Netherlands. A report was made and it is available only in Dutch.

There will be more federations in the Netherlands and the idea is confederate. SURFnet federation will act as IdP for the higher education.

SURFnet plan to use the current agreement they have with their constituency and extend that to add the federation agreement.

Institutions connected to eduroam in the Netherlands can already use the same credential to access the resources currently available via SURFnet.

SURFnet detective has reached a production service level since May 06.

UNI-C (David)

The DK-AAI project, which aims to set up a Danish federation, has started one year ago (2005) and eduroam will be one of the service offered by the DK-AAI federation. The DK-AAI will be Shibboleth-based. The test federation started in June 2006.

The policy development process will take about a year, starting end of November 2006.

David showed the promotional material realised by UNI-C for eduroam. InDesign files can also be downloaded from the eduroam.org website.

JISC – James

The UK federation is ready and will be launched in January 07.

The federation is Shibboleth based. UKERNA is responsible for the federation, however all the work is being done by SDSS.

Athens system will become a super IdP and a super SP, essentially a virtual IdP.

AARNET – Alex

There are a few areas in Australia where middleware is used, such as:

- MAMS (Meta Access Management System), which has established a test Shibboleth federation, with three levels of assurance. Shibboleth federation will get operational as soon as the policy framework will be finalised within the broader Australian federation framework (AHERTF).
- CAUDIT PKI: CAUDIT is the Australian association of IT directors. They have worked over the past months to design a PKI which is meant to suit both HE and Grids. The idea is to apply for the audit to get it accepted by browsers.
- MAPS (Middleware Action Plan & Strategy Project)
- eduroam: it used to be run by GrangeNET, but since the summer 2006 GrangeNET does no longer exist,;AARNET is responsible for eduroam as well.

IETF middleware highlights (Leif)

Leif reported on NEA (Network Endpoint Assessment), which is the set of checking and patches to be performed before allowing a pc on a network. This procedure is taking off in US. NEA has serious implications for eduroam, due to the federated EAP and will conflict with third party EAP-clients like secure W2 (currently heavily used by all Microsoft users that want to implement EAP-TTLS).

It is not clear whether the problem will be solved within the IETF.

Leif pointed out that if NEA is solved within the IETF then it will be possible for the NRENs community to work and take EAP federations into account.

There is a dedicated IETF WG, EMU that pushes EAP-TLS to standard-track.

SAML is also very much discussed within IETF and in particular the WG to monitor on this are:

- krb-wg (kerberosWG). The wg is worth looking at, as they are using Kerberos to provide what Shibboleth provides.
- dix-wg
- SIP SAML

Leif also reported on a BoF on Web AuthN Enhancements (WAE) that took place at the IETF recently.

Identity Commons (Bob)

Bob presented OpenId (<http://openid.net/>) an open, decentralized, framework for user-centric digital identity.

OpenID builds on the concept of using URIs as user-IDs, whereas the users' passwords (or other credentials) are safely stored on the user OpenID Provider. To login to an OpenID-enabled website (even if a user has never been to before), a user needs to type his/her OpenID URI. The website will then redirect the user to his/her OpenID Provider to login using whatever credentials it requires. Once authenticated, the user OpenID provider will send the user back to the website with the necessary credentials to log in.

Bob also reported on other Identity-related projects:

- Microsoft is working on 'live-id' which will replace the current Microsoft passport and will federate via WS-Fed.
- Yahoo and Google are also working to establish themselves as IdPs, but it is still not clear how and with whom they will federate.
- AOL are Liberty/SAML participants

Bob also suggested monitoring the work of <http://identityschemas.org/> .

IDM in-a-box (Roland)

Roland presented the implementation of IdM supported by SWAMI (Swedish MiddleWare alliance) and already used by some universities.

The system is not finalised yet, but whoever interested can get in touch with Roland. The system is scalable; multiple the nodes can be added as needed.

The only concern was about the speed of the registry, which is quite low but so far it has not been a real problem.

It was asked the use of a meta-directory like the one presented by Roland in a context of VO. This system would allow passing only some information about a user to another institution and keep the rest of the information stored at the user's home institution.

Next meeting dates

The next TF-EMC2 will take place on 28 and 29 March, 2007 in Florence (hosted by INFN).

Summary of the Actions

Action code	Description	Status
Action 20061016-01	TERENA to set up an ECAM mailing list and ECAM web page.	Done
Action 20061016-02	Everybody to send Miro information (url and/or documentations) on tools currently used for monitoring/troubleshooting. Miro will set-up a wiki to host the information by the end of November.	
Action 20061016-03	Victoriano to report to the group on the URN Registry project.	
Action 20061016-04	TERENA to get in touch with somebody involved in the Bologna Process.	Ongoing
Action 20061016-05	Torbjorn to send a draft roadmap the list by the end of November.	
Action 20061016-06	TERENA to set-up some repository to collect marketing material, starting from JISC.	
Action 20061016-07	Licia, Mikael and Diego to work and make the wiki ready, by end of November.	
Action 20061016-08	Licia to finalise TACAR policy and circulate the document to the lists for final approval by December.	
Action 20061016-09	Licia to investigate the usage of SCS certs furthermore.	
Action 20061016-10	Javi to modify the SCHAC document as agreed and circulate the new version to the list.	Ongoing
Action 20061016-11	Javi to produce a new version of the document that describes SCHAC and to include Mikael's slides into this new version.	Ongoing
Action20061016-12	Javi and Mikael to finalise the vocabulary discussion over the list.	