

TF-EMC2 Agenda Meeting

31 January – 1 February 2006

Zagreb, Croatia

Introduction

Diego welcomed the participants and thanked Miroslav Milinovic and CARNet for hosting the meeting.

SCS- Proposal – Licia Florio (TERENA)

Licia gave an update on the status of the project, reporting that after the Call for Proposal was issued (September 2005) TERENA received a number of proposals. Their evaluation led eventually to the appointment of GlobalSign as preferred supplier. The contract between TERENA and GlobalSign was signed on 9 January 2006.

The aim of the proposal was the get pop-up free server certificates for the NRENs (and their community) involved in the proposal.

The contract has been signed for an initial year, with the possibility to extend it in the future and allow more NRENs to join.

More details about the project are on-line at:

<http://www.terena.nl/activities/tf-emc2/scs.html>

AA-RR and HelloSAML – Diego Lopez (RedIRIS)

Diego gave an update about the AA-RR tool and showed how the tool works in the recently started HelloSAML service (<http://hellosaml.rediris.es/>).

Plans for the future include better support for SAML, better log file management and eduGAIN compatibility.

SCHAC – Diego Lopez

Diego gave an update on SCHAC, the schema harmonisation committee established in 2005. The version 1.0 of individual attribute definitions was circulated in the fall 2005 and the following proposal is to have an LDAP schema for SCHAC. The LDAP entry was posted to the list in December 2005.

Diego presented the current version of SCHAC attributes and SCHAC LDAP schema. The final version of SCHAC LDAP Schema is expected to be available in March 2006.

The plans for the future are to standardise SCHAC (applying for an RFC).

A discussion about the URN followed. Currently the MACE URN is being used and the general feeling seemed to be that MACE is perceived more like an American activity and therefore SCHAC would not really fit under MACE.

It was agreed to keep SCHAC name space under MACE for the time being and to explore the possibility of using another name space for the future.

ACTION: Licia and Diego to follow up on the URN for SCHAC.

Application of URNs to AuthZ – Victoriano Giralt (University of Malaga)

Victoriano presented how to use URNs for authorisation. Part of the talk focused on the presentation of some scenarios, whereas the other part of the talks focused on the URNs and the advantages to use them for Authorisation purposes, namely:

- An unique authorization point (the directory) where easily get information on which permissions are granted to a person (or object)
- URNs allow expressing all authorisation assertions in a common form, with application of specific semantics.
- It is possible to use an Agent-Function-Qualifier model, that is: Who can do What on Which object.

The drawback of using URN syntax is that more attributes might be needed (for billing purposes for instance) than what the URN syntax allows for.

The University of Malaga has been using the URNs for authorisation since March 2005.

Shib-enable and HEP – Ken Klingenstein (Internet 2)

Ken reported briefly about HEP, the High Education Person Schema. The purpose of HEP is to be an analysis of the various schemas and not to define a cross schema like SCHAC does.

Ken also talked about Shib-enable, the new initiative which aims to build some consistency and common practices in the use of Shibboleth.

Two mailing lists (one that includes the education institutions that use Shibboleth and the other one that includes the vendors that use Shibboleth) have been set up to foster collaboration.

Croatian AAI – Miroslav Milinovic (SRCE)

Miro presented the AA Infrastructure in Croatia, which is the evolution of the old centralised dialup system, RADIUS-based.

The current AAI project (<http://www.aaiedu.hr/>) started in 2004 and aims to define HrEdu Schema(s) for the Croatian education community, to set up IdPs and finally to set up the AAI for EduHr.

Shibboleth was explored as the technology to use, but it was found too complex. The approach followed was to add the AA features to the existing RADIUS/LDAP infrastructure.

The system does not support SAML at the moment.

e-mail aspects - Serge Aumont (CRU)

Serge presented DKIM (DomainKeys Identified Mail, <http://www.ietf.org/html.charters/dkim-charter.html>) as a way to provide security and reduce spam on mailing lists. DKIM allows to validating the identity that is associated to the message while the message is sent. In this way if the user's identity is trusted all messages coming from the same trusted user would not be considered spam.

DKIM requires the sender of the message to be authenticated before the signature is applied. DKIM uses asymmetric keys, like PGP, but the trust is based on the domain administrative delegation model.

People who plan to use DKIM were asked to send information to the list for everybody to gain experience.

DAME Proposal – Diego Lopez (on behalf of University of Murcia) (Deploying Authorization Mechanisms for Federated Services in the EDUROAM)

Diego presented the proposal prepared by Oscar Cánovas (University of Murcia), who could not attend the meeting.

The project aims to achieve SSO and attribute based network access.

Some concerns about the proposal were raised by Milan, mainly about the use of SAML attributes and they way they are transmitted by the home institution.

It was agreed that more discussion was needed with the people that wrote the proposal to consolidate the concepts and apply for funding via GÉANT2.

At the time these minutes are available, the project is under evaluation by GÉANT2 Executive Committee.

Federation and data protection - Mikael Linden (TUT)

The European directive on privacy specifies how the personal data should be collected and used. The EU working group that deals with these issues is commonly referred as WP29 and Mikael has investigated how the group works and how the directive should be interpreted.

Mikael suggested writing guidelines for policies for national federations. Mikael also suggested TERENA to represent the NRENs in the WP29.

It was agreed to create to appoint a small group of people (Mikael, Diego, Licia, Torbjorn) to carry this task over.

Some people wondered whether this topic relates to the federation work that is being done in REFEDS.

ACTION: Mikael, Torbjorn, Diego and Licia to discuss furthermore about WP29.

1SP – Milan Sova

Milan reported about TACAR discussion during the EUGridPMA meeting which took place in Vienna on 25-27 January.

TACAR is not used as much as expected, due to the way it works. To bootstrap the trust process TACAR requires a face-to-face meeting. The download of certificates from the

TACAR website is not administrator friendly (certificates are stored in a zip file, which has to be downloaded and stored, no possibility to multiple download, etc..)

The proposed changes are the following:

- easier joining rules for EuGridPMA members (the policy needs to be amended)
- enable end user access. This would be possible using a ServerSign EDU cert.
- provide for selection/pre-selected sets of certificates

The changes require a change of the policy, which was approved.

ACTION: Licia to make sure that the policy is changed accordingly.

ACTION: Milan, Licia, Christos and Diego to prepare a more detailed proposal for the updates needed for TACAR.

Milan also suggested TERENA to expand TACAR in order to run an OCSP, in a sort of TERENA Academic Certificate Validation Service.

NREN Updates

EuGridPMA Updates

Christos reported about the EUGridPMA meeting that took place in Vienna on 25-27 January. IrisGridKI, the PKI run by RedIRIS, has been accredited.

Certificate Validation Service was also discussed. So far EuGridPMA has used a flat PKI model which makes the CRLs distribution quite simple. In the future this model might change; therefore it is important to discuss the Certificate Validation Service.

The CAOPS WG active under GGF is working to define a federation guideline based on the grid experiences.

CRU/Renater

Olivier provided an update about the middleware activities in France.

France has joined eduroam, although at the time of the meeting they were not fully operational yet, due to some ongoing work to define the national policy.

France is also working to establish a federation (federation.cru.fr), which is shibboleth-based. The project, started in April 2005, will provide access to digital contents and should be compliant with the liberty alliance specifications.

CRU developed Sympa mailing list manager, which includes advanced middleware features, like LDAP, SSO, S/MIME, SOAP.

RedIRIS Updates

RedIRIS is working on improving PAPI, which in the future will be compliant with Shibboleth and EduGAIN.

SWITCH Updates

SwitchAAI, which has been operational since autumn 2005 has integrated the CA registration procedure with the Shibboleth infrastructure, allowing for the users verification via Shibboleth. This brings campuses Identity Providers in the loop.

Internet2 Updates

Ken provided an update on I2 activities. A meeting would take place during the next GGF (Global Grid Forum) to foster interoperability among the different Grid projects. To date there is no management consol for the NRENs to provide support for the VOs.

Incommon has got rid of liability, which will allow them to inter-operate with the EU federations.

OpenSSL has been certified by the US federal government.

Ken also reported about the progresses of Shibboleth2.0, which will be SAML2.0 based. Shibboleth2.0 will have extended functionality for the AuthN requests and will converge towards the standards in use by Liberty Alliance.

UK

In UK will set-up in the coming months a Shibboleth-based federation that on the long term will replace Athens.

DFN

DFN is working to set up an AAI in Germany, which will be Shibboleth based. The main driver for choosing Shibboleth was the need to access digital library.

UNI-C

At the beginning of 2006 UNI-C started a project to establish an AA infrastructure in Denmark.

Discussion

In UK there is some discussion going on to set-up a federation and John Paschoud asked whether it makes sense to set up one federation for everything or whether it would be better to create more federations. The answer was that it depends on the purpose the federation is needed for.

SWITCH federation for example is only meant for high education (these were originally SWITCH customers) and therefore one federation is sufficient.

In Spain the secondary schools are not really tackled by the NREN, therefore there are no real plans to include them in the HE federation.

The Netherlands will probably also have a global federation which will include secondary schools.

Next Meeting

The next meeting will take place during the TERENA Conference on Sunday 14 May.

The following meeting was agreed to take place in Malaga in the week starting on Monday 16 October and hosted by the local University.

The final dates and logistics will be announced at a later moment.

Summary of the Actions

ACTION	Description	Status
ACTION01-01	Licia and Diego to follow up on the URN for SCHAC	Ongoing. Meanwhile TERENA got an OID (http://www.terena.nl/activities/tf-emc2/oid.html)
ACTION01-02	Mikael, Torbjorn, Diego and Licia to discuss furthermore about WP29.	Ongoing
ACTION01-03	Milan, Licia, Christos and Diego to prepare a more detailed proposal for the updates needed for TACAR.	Proposal sent to the list on 13 March 2006. The implementation phase has started.
ACTION01-04	Licia to make sure that TACAR policy is changed accordingly.	The work on the policy is ongoing.

List of Attendees

Avgust	Jauk	ARNES
Brian	Gilmore	The University of Edinburgh
Christos	Kanellopoulos	GRNET/AUTH
David	Simonsen	UNI-C
Denis	Stancer	SRCE
Dubravko	Penezic	Srce
Ede	Feher	NIIF/Hungarnet
Hansruedi	Born	SWITCH
John	Paschoud	London School of Economics
John	Dyer	TERENA
José A.	Montenegro	University of Málaga
Jürgen	Rauschenbach	DFN-Verein
Ken	Klingenstein	Internet2
Klaas	Wierenga	SURFnet
Kolbjørn	Barmen	UNINETT
Ksenija	Furman Jug	ARNES
Kurt	Baumann	SWITCH
Licia	Florio	TERENA
Luis	Guido	FCCN
Maja	Gorecka-Wolniewicz	PIONIER
Mark	Tysom	UKERNA
Maurizio	Molina	DANTE
Mika	Suvanto	CSC, the Finnish IT Center for Science
Mikael	Linden	CSC, the Finnish IT Center for Science
Milan	Sova	CESNET
Miroslav	Mllinović	Srce
Olivier	salaun	CRU
Rok	Papež	ARNES
Roland	Hedberg	Umeå University
Serge	Aumont	CRU
Thomas	Lenggenhager	SWITCH
Tomasz	Wolniewicz	PIONIER
Torbjörn	Wiberg	Umeå Universitet
Victoriano	Giralt	University of Malaga