

TF-EMC2 Meeting

9-10, July

Umeå, Sweden

Introduction

Diego welcomed the participants and bashed the agenda.

SCS

Licia reported on the SCS representatives meeting that took place in Amsterdam in June 2008. Aim of the meeting was to agree on how to continue the service after the current expiration date.

During the meeting, SUNET reported technical problems with Windows Server 2008. The problem is due to the fact that Windows Server 2008 uses the UTF8 format, which is not supported by the GlobalSign system. This issue is still an open issue.

TACAR

Licia reported that TACAR policy was updated in July 2008 to improve the role of the Trusted Introducer (TI). According to the latest version of the policy, the Trusted Introducer is only required to perform the identity vetting for the applying CA and to exchange the PGP keys with the representative of the applying CA. Optionally the TI will also collect the paper documentation.

Grid

Milan reported that the Grid community is working on creating a document to describe authorisation profiles. This work is carried out within the OGF.

For more details see also:

<http://www.eugridpma.org/authz/>

http://www.ogf.org/qf/group_info/view.php?group=ogsa-authz-wg

A discussion on how to link different sets of credentials (Grid/AA) followed. It was agreed that the main issue currently is not the technology (which is ready), but it lies more within policies and relying parties.

REFEDs

Mikael presented an update on REFEDs.

The wiki is available at:

<http://wiki.rediris.es/tf-emc2/index.php/Federations>

From the data available in the wiki it appears that SWITCH, FUNET and NORDUNET federations have the highest coverage in terms of users (respectively 90%, 80% and 80%). The wiki also shows that most of the SPs participating in the various federations belong to the eLearning and content/library areas.

Diego reported on the plan to grant access to the wiki via eduGAIN. At the time the minutes are being written the refeds wiki is eduGAIN protected.

A discussion took place on how to continue REFEDs work in the future.

During the REFEDs meeting in Bruges (May 2008) it was agreed to turn REFEDs into a group independent from TF-EMC2, in order to invest more time and resources

into marketing the work of REFEDs. Since then there were some new developments mainly concerned with the initiative (started by Ken Klingenstein and other people in the task force) to create a special interest group (SIG) within Liberty Alliance. The charter for SIG was sent to Liberty Alliance in July 2008. The SIG would reach out other communities (such as the public sectors) that are also dealing with federating issues. With the SIG being under preparation REFEDs scope appears to be smaller than what envisaged.

Action: Licia to report on the SIG progresses.

Campus Issues

Torbjorn presented the issues in setting up, using and maintaining an Identity Management System in a campus. The primary reason for deploying an Identity Management System is to provide SSO.

Although the need for a proper IdM is acknowledged there are still some issues that are not properly addressed, such as for instance Level of Assurance (LoA), mainly concerning identity provisioning.

Other recurrent issues that arise when deploying IdM relate to the costs for maintaining and updating the systems, on how authorisation of shared resources and de-provisioning of accounts are performed and how ownership of data is handled.

It was agreed to create a knowledge base to increase the collaborations with the campus. It would be useful to create some documents similar to best practises addressing the areas that Törbjorn mentioned.

Ingrid said that there would be a campus activity (proposed by UNINETT) within GN3 and potentially some of these issues could be addressed in this activity.

It was suggested to collect a list of national educational companies.

SCHAC

Victoriano reported about SCHAC, which has proven to be very successful considering the level of adoption. For test purposes there is also a SCHAC experimental branch.

The SCHAC URN name space RFC, which was supposed to be ready by the summer 2008, has been delayed and should be ready by the end of 2008.

Victoriano said that considering the usage of SCHAC it would be good to produce some guidelines on how to use SCHAC attributes.

Victoriano has collaborated with the Australian Federation (which will also use some of the SCHAC attributes) and has started a promising collaboration with the EUNIS group working on Bologna process (RS3wg).

Action: Victoriano to report on the progresses of the RFC.

Diagnostics

Miroslav reported on the status of the diagnostic work that he and his group are carrying out. The aim of a diagnostic system would be to enable end-2-end users report, to allow for a way to offer information about the status of a service in a certain period of time and so on.

Using the data on the REFEDs wiki (where half of the federations do not provide any indication on diagnostics), Miro provided an overview on the diagnostic status across

various federations. Some federations use NAGIONS framework, others use homemade solutions, such as in Croatia and in Norway.

GN2/GN3

Diego provided an overview on the structure of GN3. Diego said that this group should be mainly concerned with the work carried out by:

1. the Service Activity (SA3) “End User Services in a Federated Environment”, which will include eduroam service, eduGAIN migration to service and a PKI task to use TACAR as a repository for CAs set up or used by GN service (part of the work on this task will also relate to the establishment of a PMA to evaluate CAs policy to match the service requirements).
2. Joint Research Activity (JRA3) “Enabling Communities” which will cover further developments in eduroam (mainly concerning RadSec standardisation work, integration with SSO etc), work on identity federations with the idea of establishing a federation laboratory to operate as a test-bed and will have a third task called “Composable Network” with the aim to define a new framework to enable users to create and request services to compose resources (HD videoconference, physical space to store data for a certain period, etc) on demand in an easy and manageable way.

The proposal was submitted to the EC on September 11.

PKI Resource Query Authority (videoconf)

Massimiliano (connected via videolink) presented the work that he and his team at Dartmouth University are carrying out on interoperability and usability on PKIs. This work focuses on using the PKI Resources Query Protocol (PRQP) to provide a standardised way to query PKI repositories to find URLs for certificates revocations list, certificate policies, OCSP services and others.

The PRQP is undergoing the final call to be accepted as a work item within the PKIX working group in IETF. The protocol allows any client to find out where a PKI resource is. The PRQP responds providing URLs. The server is the Resource Query Authority (RQA), which is certified by a CA to provide PRQP responses.

Because TACAR provides a trusted repository with URLs for CP/CPS, it would be the ideal candidate to run a resource query authority (RQA) that will provide support for CAs in TACAR. Massimiliano proposed to make a test using TACAR with the server (RQA) hosted at Dartmouth University.

What is needed from the CA: whenever the CA wants to provide information for users, PRQP can provide a web interface for the CA to upload such information; it would be useful to know what information the CA wants to provide to their users.

In order to use TACAR, TERENA should create a DNS record "rqa.tacar.org" that would point to some server (hosted at Dartmouth). This server will act as a gateway to recover all the information related to a particular CA.

It was agreed to start the service in a trusted mode (using Dartmouth cert) and for the moment using only two CAs: CESNET and pkiris. . Initially, OCSP and CRL and where users can ask for revocations and new certificates.

It was asked why the protocol uses HTTPs rather than TCP; Massimiliano answered that HTTPs is not blocked by firewall and NAT so it increases the chances to reach resources.

Action: Licia to work with Massimiliano to run a RQA for TACAR.

Future of EMC2

Diego also presented his proposal on how to prolong TF-EMC2. He said that both TF-Mobility and TF-EMC2 focus on middleware even if with some differences; a way forward (also discussed with Klaas Wierenga, chair of TF-Mobility) would be to re-focus both task forces following the protocol stack. In this new perspective all more network-oriented middleware tasks should fall into TF-Mobility, whereas application-oriented middleware tasks should be dealt within TF-EMC2. Diego was propose a chairman of the new group.

A revision of the current EMC2 work items, with the aim of selecting to be included in the new EMC2 charter, took place.

The following was agreed:

1. The AA-RR working item will be dismissed, being obsolete;
2. A discussion on the work to be carried out in the diagnostic area took. Klaas reported that SURFnet detective has been discontinued by SURFnet and that the original creators of the detective (in agreement with SURFnet) will keep working on the tool. There is room for enhancing the former NREN-detective. It was agreed to include the work on the NREN-detective into the new TF-EMC2 charter;
3. REFEDs will still remain an area to work on and will mainly concentrated on the federation in the academic area. The evolution of the proposed SIG will also be monitored. REFEDs work could include also initiative similar to what Leif reported on the SAML2.0 profile for inter-federation that is being prepared by a group of developers (Leif, Scott Cantor, Nate Klingenstein, Andreas Solberg and others). The profile started as a base for Kalmar Union, but it is interesting for other federations as well. REFEDs should also have a new item to look at new models on how IdM could support cloud computers. In the long term the NRENs might decide to procure to acquire cloud computers services for the NRENs in Europe.
4. Two new work items will be added: beyond WebSSO and reputation systems.

Action: Licia and Diego to work on the TF-EMC2 charter.

Open discussion on Stork

Mikael provided an overview on IDABC (<http://ec.europa.eu/idabc/>), a EC funded project initiated few years ago. Some documents (see <http://ec.europa.eu/idabc/en/document/6484/5938>) could be of interest for this group: such as the one that relates to authentication of citizens in Europe, the LoA document and the document proposing an architecture for a pan-EU IdM, which resembles very much eduGAIN, see: <http://ec.europa.eu/idabc/servlets/Doc?id=30989>.

To get involved into this work, it is necessary to approach the national representatives.

EUNIS updates

Victoriano has engaged with the EUNIS group that is involved in the Bologna process. It was agreed that TF-EMC2 group will liaise with this group.

National updates

CARNET – CARNet provides connectivity to primary and secondary schools. Miroslav presented the online tools to provide central support for IdP/SP installations.

PIONIER – Maja reported that PSNC has joined SCS. The moment is ripe for a setting-up a federation. PIONIER has now a range of services (videoconf, eduroam, libraries) and the users realise the benefit of federation.

CESNET – eduID.cz is the newly federation in Czech republic, based on the shib-1.3 pilot.

RedIRIS – SIR is the general country-wise federation in Spain. It's based on PAPI-backend that is able to communicate with OpenId, SAML1.x and SAML2, PAPI and BE (edugain).

Institutions that want to join need to install a connector, validated by RedIRIS. The connector produces assertion in PAPI protocol.

Diego also presented the federated way to access SSH.

Diego presented a new way to use OpenId for instance for a lightweight federation. The idea is to allow the consumer (equivalent of SP) to verify that the IdP is in the list of trusted IdPs and the viceversa. Thomas pointed out that this model might have some issues as it combines a personal identity (OpenId) with a professional identity (which will expire at a certain point).

SWITCH – Thomas provided an overview of the SWITCH-AAI federation and reported that Shib2 deployment is ongoing. In order to improve the metadata signing procedure there is now an offline root CA and an online hardware token keys of the intermediate root CA and the metadata signer. The deployment will start as soon as Shib2.1 is available (this should support CRL).

Thomas was asked why they decided not to use an SCS certificate to sign metadata; he answered that the main pros for going for a CA operated by SWITCH is to have everything in the house, so they are not depending on the CA supplier.

Thomas presented some ideas on the usage of tagging metadata. Tags are extensions to add some additional information to metadata. UK is already using tags in metadata. Tags might be useful for instance on inter-federation cases.

To handle the tags MDSs (Metadata Services) would be established; each federation would register with one of more MDS to register its metadata.

Milan pointed out that:

- Embedding the tag into the metadata is just a way to provide some assertion.
- If we this procedure was used it would take out much of burden to verify the signature of the entities but it requires the cooperation of the federations involved. So if you want two federations to agree and exchange some data it might be quite complicated. Thomas agreed that in bilateral cases there is no need for an MDS.

A discussion followed to better understand benefits and complexity. The conclusion was to further discuss this topic when more experience is gained.

Internet2 – Ken (who joined via videolink) reported that Apple has joined InCommon and Google has showed interest.

A.o.B

Diego said that the de-provisioning issue should be considered for the future.

Summary of the actions

Action code	Description	Status
Action20080710-01	Victoriano to report on the progresses of the SCHAC RFC.	Ongoing
Action20080710-02	Licia to work with Massimiliano to run a RQA for TACAR.	Not Done
Action20080710-03	Licia and Diego to work on the TF-EMC2 charter.	Not done

List of participants

Licia Florio	TERENA
Victoriano Giralt	University of Malaga
Maja Gorecka-Wolniewicz	PIONIER
Roland Hedberg	Umeå University
Leif Johansson	Stockholm university
Thomas Lenggenhager	SWITCH
Mikael Linden	CSC, the Finnish IT Center for Science
Diego Lopez	RedIRIS
Jose-Manuel Macias	RedIRIS
Ingrid Melve	UNINETT
Miroslav Milinovic	Srcce
Sascha Neinert	University of Stuttgart
Anders Nilsson	Umeå univ / SUNET
David Orrell	Eduserv Foundation
Juergen Rauschenbach	DFN-Verein
Panagiotis Saragiotis	ENISA
Hideaki Sone	Tohoku University
Milan Sova	CESNET
Torbjörn Wiberg	Umeå Universitet/SWAMI
Klaas Wierenga	Cisco Systems
Stefan Winter	RESTENA
Tomasz Wolniewicz	PIONIER