

**TF-EMC2 Meeting Minutes
Prague 4-5 September, 2007**

Report on REFEDS workshop – Ingrid Melve

The first International confederation meeting organized under the umbrella of TERENA and hosted by CESNET took place on September 3 in Prague.

Attendees coming from Europe, US, Japan, Australia and Brazil, explored the main drivers for creating identity federations in the academic community and discussed a range of policy issues relating to inter-operation of federations.

The participants agreed that collaboration and sharing each other resources to offer users more services than those available at their institutions is the main driver for federations.

The various models according to which federations can interoperate (confederation, peering and leveraging) were also discussed.

A debate on LoA took place, in particular on how to handle LoAs when crossing federation borders. JISC and UKERNA will provide the results on the policy comparison work. Attributes and legal issues were discussed.

There was a discussion on the overlap between the public sector, the business sector and the social sector and how to handle that. Liberty Alliance and OASIS have established working groups to handle these issues. Robin (SUN and Liberty).

The list of actions agreed is reported below:

Action03092007-01: Licia to provide accounts for the wiki

Action03092007-02: All participants agreed to do some ‘homework’, identifying major research projects in their region that need cross-federation connections. This will help to clearly identify use cases. Licia to chase people up to get contributions for the use cases.

Action03092007-03: Licia to collect the links to the policy for the refeds website.

Action03092007-04: Identify which part of eGovernment is interesting for refeds. Olivier to contact the French group and report on the results.

Action03092007-05: Jane and Andrew to circulate the material on the comparisons of federation policies that is being undertaken by JISC and UKERNA.

Action03092007-06: Robin Wilton to report on the developments of the Liberty Alliance eGovernment group.

Action03092007-07: OpenId and CardSpace integration in identity federations: Ken and Ingrid to report on this.

Action03092007-08: Andrew + Eva + Walter to get in touch with the Article 29 Working Party (Art 29 WP) on behalf of TERENA refeds group.

Action03092007-09: Leif, Diego and Andreas to investigate attributes invitation and aggregation issues.

Action03092007-10: Leif to send his proposal to the refeds list describing his ideas for the min requirements.

Action03092007-11: Everybody with experience on the LoA to send info to the refeds list.

Action03092007-12: Leif to provide more inputs on how to proceed to use attributes to ship LoA.

Action03092007-13: Eva to put best practices on-line.

SCS report

NRENs participating in SCS reported to be satisfied to offer SCS certificates to their community. However they reported not to be satisfied with the way GlobalSign (GS) handle the service.

The POST interface and the OCSP are delayed and there is no clear indication on when they will be available.

David Simonsen said some of Danish users reported GS wildcard certs not to work with CAS.

Action: Oliver to look into the usage of wildcard cert with CAS.

Leif, Diego, Milan suggested to approach other vendors and test with other solutions. They will report on the results of the tests.

Alex Reid reminded that the AARNET is establishing a CA, which will be audited by WebTrust. He suggested exploring the possibility to use this CA as possible alternative for GS.

Action: Alex to report more about this.

Grid Report – Milan

Milan reported that the new trend would be to delegate the users authentication to the users home institution, thus to the campuses

A new profile is being discussed by IGFT and is waiting for approval.

REFEDS – Mikael

Mikael presented the REFEDS wiki. Quite a few content on the European federations is available on-line. The wiki will be used to collect material gathered from the REFEDS meeting hold in Prague.

Ken suggested having an area on the wiki to add tools.

Action: Jaap and Jane to work together to set a page on the wiki that contains the list of publishers.

Action: Mikael to add a page on the wiki to add tools and SPs.

Action: All to investigate the following scenario: some universities have campuses abroad, to which federations users are allowed to join? To the federation in place in the state where the campus is or the federation in place in the country where the university belongs to?

Campuses issues

Torbjorn could not attend the meeting; therefore a full report on this topic was not available. Licia announced the next EuroCAMP will take place on 14-15 November in Croatia (Dubrovnik). The programme is under preparation.

Some of the attendees suggested to have a better organized TERENA presence at the next EUNIS conference.

Action: Licia to verify the possibility to organize a slot in the next EUNIS conference to report about TERENA activities.

Diagnostics - Miroslav Milinovic

The refeds wiki has been extended to include the monitoring part, but the list is not complete. Miro reminded the participants to provide information on the monitoring part. In this context it was reported that the monitoring tool suggested within GEANT2, smokping, looks quite promising.

Directories - Victoriano Giralt

Victoriano reported on SCHAC and directories.

News about SCHAC include:

- AAF in Australia has adopted some SCHAC attributes
- Diego has been approached by the Irish group in charge to set up directories for lower education, which is considering SCHAC.
- University of Malaga has put SCHAC under production.

Victoriano submitted a paper for the European R+D conference (The Hague in October), which has been accepted.

A new URNreg attribute should be added to the terena.urn.org.

Action: Vic to liaise with Licia to add the URNreg attribute.

Victoriano also discussed the use of privacy-controlled attributes in DNs, which makes it impossible to hide attributes if the policy requires. The DNs are always returned to queries.

Juergen reported that the geant-urn is almost ready to be used.

Ideas for the coming GN3 – Juergen

Geant2 exec established a small committee to evaluate items for the new proposal.

If there are ideas for topics to include, Diego and Juergen should be approached.

Juergen said that some of the JRA5 work has not been finalized yet and it is likely to be moved into GEANT3.

Diego proposed to include work on the monitoring harmonization in the GEANT3 project.

SAML and WS-* framework – Josh

Josh gave an excellent presentation on WS-* framework.

WS-* framework consists of small number of specifications that can be put together.

The most important of WS-* specifications is WS-security that is a building block to construct security protocols. SAML2 uses WS-Security.

WS-trust is a layer on top of WS-security.

WS-federation shares some similarities with SAML2 in terms of metadata and it also includes a sign-out profiles. WS-federation is not meant for web SSO, but for web services (speaking SOAP).

WS-federation relies on multiple protocols, which makes things more difficult.

WS-* seems to be a good solution for small enterprises but for larger scale, SAML2.0 is much more mature and it is preferred.

A discussion on workflow followed. Ken will meet with Microsoft in the next weeks and will investigate about workflows.
SURFnet is working with Microsoft to make some test to connect ADF with A-Select. UNINETT will have a workshop in October to ask commercial vendors to present integration with Microsoft products and SAML2-based applications.
Ingrid will report more on this.

NRENs Updates

RedIRIS - Diego said that the project to integrate PAPI and SUN IdM has produced the so-called ICGPoA. Some tests have been conducted on the integration of eduroam and SIP.

SCAHC will take over iris-* schemas.

On the grid side RedIRIS is planning to use IGTF MICS profiles (under approval by the IGFT) and pkIRISGrid will become the only active Grid CA for Spain.

Internet2 – Shib2 SP is ready, but Shib2 IdP is not ready yet.

InCommon federation is now operational. Some discussion with the US federal government took place, but hasn't produced the desired results. Microsoft have made contacts to join several federations in US, Norway, Spain and France.

Internet2 has planned a meeting with Google, which has now a task force on AuthN and AuthZ.

iTunes is pretty popular among the universities in US; I2 is also getting in touch with iTunes people.

Ken reported that the new version of ADF allows for the usage of sharepoint in combination with shibboleth (therefore for remote authN).

FUNET - Haka has been operational for two year, with 90% of universities covered. Support has been planned for institutions that do not feel like operating IdPs on their own. The libraries contents are not really introduced into the federations, due to the fact that the libraries seem to prefer the ip-based access.

SCS developed AAIEye monitoring software, which is available for the community.

More info are on-line at:

<http://www.csc.fi/english/institutions/haka/technology/aaieye>

CRU-RENATER – Work is ongoing to shibbolise applications, such as Dokuwiki (authZ based on Sympa), Gforge and WebDav (work in progress) as well on shibbolize SAP.

Work is also ongoing to integrate SCHAC.

Australian Update – CAUDIT coordinates the AuthZ/AuthN work.

AAF is the Australian federation, which will be in production in 2008. AAF will be operated by AusCERT, University of Queensland, MacQuarie University and AARNET.

Alex also reported about on the work to set-up a working certification authority for the academic community. The CA would be submitted to the WebTrust audit.

UNINETT – Work is ongoing to integrate FEIDE and eduroam. UNINETT has since recently started work on storage facilities. The OpenID/FEIDE bridge has been developed.

UKERNA/JISC – Some work is ongoing on how to set-up Shib IdP in Windows environment and on how to use other federation access management products (SAML2-based).

NIIF – NIIF is in the process of deploying a Shibboleth-based federation.

GEANT2

Juergen reported on GEANT2/JRA5 progresses. Lots of deliverables produced and available on-line at:

www.geant2.net/jra5/deliverables

UPKI Project in Japan - Yasuo Okabe (Kyoto University)

UPKI is the name for the Authentication and Authorisation platform sponsored by NII and the information infrastructure centers in seven universities in Japan. The UPKI project encompass SSO for Digital Library Service and other universities via Shibboleth/SAML, S/MIME and wireless LAN roaming.

Access to UPKI via the portal: <https://upki-portal.nii.ac.jp/>

eID Project – Olivier

The eID project aims to implement a EU wide interoperable system for recognition of eID and authentication to allow for the use of national electronic identities in any Member State. CRU was contacted by the French government involved in eID.

Earnest report – Licia

Licia reported on the results of EARNEST technical sub-study. EARNEST is foresight study funded via GEANT2 in order to consider the direction of research and education networking in the coming few years. The study comprises seven areas of investigation, one of which looking at technical issues.

The technical report has been finalized. The report covers the following areas:

- transmission technologies
- controlplane and routing technologies
- network virtualisation
- operation and performances
- middleware
-

The report has been circulated on the EMC2 list.

Implementation of an URN registry – Candido/Victoriano

Candido and Victoriano presented an interface that makes the management of URN registries easier. Milan pointed out that in order to allow other people to use the interface not only the code is needed but also the specifications.

The protocol needs still some work and Victoriano asked for volunteers.

Action: Victoriano and Candido to circulate more information about the tool.

Joint session with TF-ECS

Jan presented the authentication issues that TF-VVS are looking at.

Authentication in SIP is mostly done using digest authentication, even if this approach does not allow authenticating the server.

Leif pointed out that NTLM is not a vendor-specific product anymore.

There was consensus on the fact that the academic community should push SAML profiles (the PBX should be able to handle SAML profiles) and this could be done via the SIP open-source community.

Leif suggested attending the SIP interoperability event, as a way to influence the vendors. Vendors are very likely to implement SIP identity, but there is no certainty they will implement some SAML profiles (to exchange attributes).

During the presentation there was a discussion about the usage of signed headers in SIP, which are supposed to work as saml tokens, but there is no possibility to add attributes. The headers that are going to be signed are defined via an RFC so it is quite fixed.

Shintau project - George Inman University of Kent

Shintau is a project to aggregate attributes. For authorization purposes the attributes are generally provided by a single entity known as an Identity Provider, which can prove sometimes not to be sufficient.

Shintau is working to provide an internationally recognised standard for attribute aggregation.

CoManage – Mike Gettes (remotely) and Ken

Ken presented CoManage tool on behalf of Mikael. CoManage is quite interesting as it uses directories to manage groups and privileges. The project started from the need to integrate Internet2 Middleware (Signet/Grouper, etc.) products and to allow for daily usage.

Next Meeting

Next TF-EMC2 will take place on 4-5 February, in Marseilles (France).

Summary of the actions

Action: Oliver to look into the usage of SCS wildcard cert with CAS.

Action: Alex to report on the possibility to use the Australian CA (under implementation) also for academic community in EU.

Action: Victoriano to liaise with Licia to add the URNreg attribute.

Action: Victoriano and Candido to circulate more information on the tool to manage URN registries

Action: Licia to verify the possibility to organize a slot in the next EUNIS conference to report about TERENA activities.

Action: Jaap and Jane to work together to set a page on the wiki that contains the list of publishers.

Action: Mikael to add a page on the wiki to add tools and SPs.

Action: All to investigate the following scenario: some universities have campuses abroad, to which federations users are allowed to join? To the federation in place in the state where the campus is or the federation in place in the country where the university belongs to?

