15th TF-EMC² Meeting - Tuesday, 16th and Wednesday, 17th February 2010
Vienna, Austria. The meeting was hosted by ACOnet.

Table of Contents

1. Welcome and Apologies

Diego Lopez welcomed everyone to the meeting. Attendance and Apologies were recorded on the event registration page: http://www.terena.org/events/details.php?event_id=1551

2. Approval of Agenda

The agenda was modified as the day progressed with a final version is available online: http://www.terena.org/activities/tf-emc2/meetings/15/

3. Minutes of Last Meeting and Update of Action List

The minutes of the last meeting held on the 22nd October 2009 were approved without corrections and are available at http://www.terena.org/activities/tf-emc2/meetings/14/tf-emc2-minutes-20091022.pdf

Reference	Who	Action	Status
05052009-01	All	To provide the list of back channels used to connect WebSSO and non- web applications with the aim of collecting use cases.	*This action item has been overridden by the Project Moonshot and SAML/SASL proposals. Done.*
05052009-03	~~All~~ *Miro*	Volunteers needed to the work on diagnostics.	*Within GEMBus there are still some problems with relation to this. Miro has some ideas surrounding this effort. Assign the task to Miro to co-ordinate. Other interested parties should contact Miro.*
05052009-04	DB CLARIN	To better detail their use-cases, particularly the beyond-web use- case.	*This is considered "Done".*
05052009-07	Licia/ ~~Milan~~ Mikael	To prepare a template on the REFEDs wiki for a federation policies matrix.	*Re-assigned to Mikael.*
05052009-08	Licia	To collect URLs on metadata registration systems.	*This action item is unclear. Remove.*
05052009-09	Bob, Serge, Niels	To provide more info on reputation system to Jaime	*This action item is unclear. Remove.*
05052009-10	Licia	To set up a virtual machine containing a similar set-up as the REFEDs wiki	*Some resourcing issues within TERENA have delayed this. Licia/Brook to report back to TF-EMC2 on the Project Plan TERENA has created.*
Following actions are from December 2008 but weren't assigned a number until May 2009			
03122009-01	All work item leaders	To prepare a description of their work item by 1 April. All WI leaders to provide their work plans asap.	*Still required. WI leaders should clarify whether their WI needs an updated description.*
03122009-04	All	To send information to Jaime on how white/list black lists implemented and more in general on reputation systems people are aware of.	*Covered by the results of the EQUAL (Email Quality) meeting. Done.*
03122009-06	VG	To provide more information on PICTURE proposal. All to contact Victoriano if interested in creating a pilot.	*Victoriano to make contact with Rodney McDuff + AAF. Rodney is burried under daily work, even back filling partially a void as UQ HPC manager. He sought funding from NeAT, but was turned down as too wide. He is trying to get QRNO (Queensland Regional NetworkOrganization) interested, no results yet.*
Following actions are correctly dated.			
20091022-01	Brook	Clarify action item with Diego on VM + Cloud systems.	*Relates to **05052009-10**.Not particular to the REFEDs wiki but federated/ confederated services. Brook to take this issue up with Dyonisius Visser in line within TERENAs Federated Services Plan.*
20091022-02	~~?~~ *Diego*	Janus + ITIL explaination	*The increased importance of ITIL within the community is a top down pressure from the Commission in wanting some structure in the deployment of services.*

20091022-03	Licia	Make a requset to the TTC to provide resourcing for REFEDs website.	*REFEDs needs to find its niche in the federation landscape. Further discussion in "Federation Co-ordination."*

[**ACTION**] **Brook** to flag SURFnet's "Operational Excellence Toolkit" to TF-MSP.

4. Work items updates - All Work items (WI) leaders

4.a Campus Middleware Issues

Torbjörn Wiberg made a presentation on Campus Middleware Issues, which is available at: http://www.terena.org/activities/tf-emc2/meetings/15/100216_TW_CampusIssues.pdf

There have been an ever decreasing number of on-campus students and the students are still demanding access to all services. The particular middleware impacts are:

- Student Identification + LoA
- Integration of Applications
- Heavy dependence on middleware infrastructure

The figures of student population turning up on campus was questioned by Lukas. These figures are particular to Umea University. Brook mentioned the cases of USQ and Athabasca as distance education universities that evolved due to "off campus" student populations increasing.

Diego talked about the difficulty in making a public/private collaboration because there is a mix of services that users are demanding and some are now provided by the market.

Niels asked what % of Universities are becoming SPs and providing services? Some organizations are using internal systems to shield their services.

Leif stated that some institutions are using the national federation for an Enterprise SSO. New members of SWAMID have joined only to use some killer applications, such as TCS Personal Certificates (details in the Swedish summary).

4.b Collaboration with the Grid Community

4.c Community PKI Initiatives

Milan Sova presented a combined update on "Collaboration with the Grid Community" and "Community PKI Initiatives" work items, the presentation is available: http://www.terena.org/activities/tf-emc2/meetings/15/TCS-0.1.pdf

The presentation focused on improvements and extensions to the TCS:

- eScience Personal + eScience SSL extended offerings
- Acceptance of the eScience CA by the EUGridPMA
- NRENs can now populate valid domain names so that they don't have to approve each and every certificate request

Diego asked whether this was generic to the TCS or required additional software. Milan clarified that this feature is based on using the djangora portal. Some NRENs already had systems and procedures in place - others have adopted this software.

- Development and use of TCS Shared Portal for Personal + eScience Personal use

Diego asked what support infrastructure was available for end users.

Leif commented that they were investigating getsatisfaction.com for support management. Tomasz stated that his Nokia mobile phone doesn't include the Comodo cert - and pages that host the cert are protected by a cert not included in the phone. Milan suggested checking the fingerprints - but Tomasz stated where would the fingerprints be hosted.

Comodo certs are not properly handled by Nokia and Symbian OS in general.

Milan noted that due that Microsoft does not push all the accepted certificates roots to the users anymore. This means that in the moment in which a user connects to a site protected with a cert issued by a trusted CA, Microsoft update is launched to install the cert chain on the user's machine. However some institutions block Microsoft update. It was agreed that an alternative way to obtain Comodo's roots should be found. Currently TACAR cannot be used for this purpose as it uses a Comodo's cert.

[**ACTION**] **Milan** to discuss this problem with the TCS PMA and report on any solution.

It was also noted that it would be good if TERENA TCS pages contained an FAQ section.

[**ACTION**] **TERENA** to start working on a TCS FAQ page.

François mentioned that installing certificates on Nokia S40s is possible using Bluetooth connection to the phone: http://nokicert.googlecode.com/

Ajourn for Lunch

The "Brown Bag Lunch" experiment was moderately successful. It resulted in a 90-minute lunch rather than 60 minutes. The experience of a "schnitty" was enjoyed by many.

4.d Diagnostic-related Activities

Miroslav Milinovic gave a presentation on Diagnostic-related Activities, and further clarified and focused the presentation to look at "Monitoring and Measurement of Federation Activity", which is available at: http://www.terena.org/activities/tf-emc2/meetings/15/tf-emc2-vienna2010-miro.pdf

Ken Klingenstein discussed the success of the NIH and their use of federated services. NIH are happy with federated access and federated users use their services 10x more than those without federated services. They have had a user request their old NIH access back - because a local institution IdP was down and the user couldn't publish a paper. Their local helpdesk wasn't aware that they were federated and couldn't help the user. There is an operational need for helpdesks to know about these services and that the system is accurately monitored. Ken believed that uApprove will exacerbate this problem because some users will restrict their attributes and won't have access to the service.

Lukas clarified the workflow when using uApprove - the access issue is generated by the users own actions.

Thomas noted that we should distinguish between active monitoring and passive monitoring to get a better sense of whether the services are operational. This requires having trend data on use (access allowed/denied) and an understanding of the dependencies of the service.

[**ACTION**] Miro to document the monitoring (both active and passive) that are available and mechanisms to determine whether the service is working or not.

Miro asked for input on the proposed work. Thomas wanted to know the urgency of this document vs the importance. Ken commented on the SWITCHaai document and wanted clarification on response time vs time zones.

Niels stated that you'll only receive support during Dutch office hours for SURFfederatie.

In summary:

- Current practices document could wait. A report on currency of information in the REFEDs wiki would suffice.
- Development of the dependencies required for accurate monitoring.

Tomasz questioned whether a dynamic implementation of eduroam will not allow monitoring in this manner.

Diego stated that the current monitoring system doesn't work down to the resolution necessary to identify whether services are working and that a push of data to a central monitoring point is required to make monitoring accurate, this gives you the added flexibility of choosing what data to send in order to comply with local privacy regulations and organizational policy.

Mark O'Leary discussed a dynamic eduroam pilot on JANET and the use of IFmap to instrument the activity of individual servers. This will be presented in TF-Mobility on Thursday.

4.e Directory Schema

Victoriano gave a concise presentation with the limited time. The slides can be found online at: http://www.terena.org/activities/tf-emc2/meetings/15/schema.pdf

The presentation discussed liaising with RS3G (Rome Students Systems and Standards Group). This group has developed an implementation of the Bologna process. There is potential for extension of schac and further adoption.

On the RFC for urn:schac prefix front (The most significant change will be the use of urn:schac:... prefix rather than urn:mace.org:terena.org:schac:...) Comments from IETF to the RFC supplied by Victoriano were made available on the Wave and via the mailing list.

At the conclusion of Victoriano's talk Diego urged people from NRENs or Campus' that are implementing any of the Bologna process that they should attend the event the joint TF-EMC2 and RS3G Meeting http://www.terena.org/events/details.php?event_id=1630

4.f Federation Coordination

Mikael Linden presented an update of the REFEDs wiki and the progress of federations reported on this site. The presentation is available at: http://www.terena.org/activities/tf-emc2/meetings/15/refeds-update-emc2-vienna2010.ppt

Mikael noted that he does not have much time for REFEDs and it would be good to get more support from TERENA. Ken asked to recruit a dedicated person to carry out some specific work for independent federation advocacy.

Mikael talked about "federations.org" (domain taken) and the need for information to be collected and presented in a better form.

Significant discussion occurred on the Wave and within the room regarding the naming of a service and the content and focus of the site/service.

A summary of the discussion follows:

- Need for a dedicated resource to do this.
- Funding is available from the community - if someone (some organization) is willing to commit to this site/service.

The federations.org domain was suggested. It is currently taken but is available for purchase for $2,888. Federated.org is available $1,760. More info http://www.buydomains.com/premium_domain_purchasing

4.g Identity Services beyond Web Single Sign-On

No work on this item was presented. Presentation on Project Moonshot and SAML/SASL at the joint TF-EMC2 and Mobility session on Wednesday afternoon.

4.h Reputation Systems

Diego Lopez presented some preliminary work by Jaime who was unable to attend the meeting. A document including three use cases is available at the wiki. Diego asked those running or planning to run services related to these use cases (like the CoUniverse in Masaryk University, or the fedrated BitTorrent in Sweden) to get in contact with Jaime. The slide notes are available at: http://www.terena.org/activities/tf-emc2/meetings/15/reputation.ppt

5. National Updates

TERENA: OID registry and service federation

Licia requested from the community information on software available to maintain the TERENA OID registry - currently available at http://www.terena.org/activities/tf-emc2/oid.html

[**ACTION**] Diego to put Licia/TERENA in touch with OID software developer.

SURFnet: Demos of Federation-in-a-box and Mobile PKI

Joost van Dijk introduced the session and gave a background of the Mobile PKI initiative within SURFnet. http://www.terena.org/activities/tf-emc2/meetings/15/IdentityProviderInABox.pdf

François Kooman presented the Mobile PKI solution and the issue with GSM SIM cards that either do/don't support mobile pki. The issues is dependent on your mobile phone operator and the SIM cards they supply.
Futher information is available in the presentation slides and from a report on Mobile PKI:
http://www.terena.org/activities/tf-emc2/meetings/15/MobilePKI.pdf
http://www.terena.org/news/community/download.php?news_id=2528

Vienna University: VICAJOP

Lara Spendier presented on the work of VIrtual CAmpus for JOint Programmes (VICAJOP) the slides are available at: http://www.terena.org/activities/tf-emc2/meetings/15/pres_vicajop.pdf

The presentation highlighted two points:

- How to get institutions connected to their local federation
- How to get federations to talk to each other (or create a virtual federation aggregated from multiple federations)

Peter S. requested a Hands on EuroCAMP or a not so hands on EuroCAMP in the east.

Ken stated that EuroCAMP is focused (or being refocused) toward the Campus level so maybe there is a need for a REFEDs CAMP. There is a line where something needs to transfer between the campus' level and the federation level.

To make up time the session will commence at 8:45 tomorrow.

GN3: Federation Activities

Andreas Solberg provided a succinct presentation on the research activities underway within GN3 project. The slides are available at:

http://www.terena.org/activities/tf-emc2/meetings/15/identityFederations.pdf

6. Recent results

SAML2 profiles for a federation

Andreas Solberg followed on with saml2int profile work. The slides are available at: http://www.terena.org/activities/tf-emc2/meetings/15/saml2int.pdf

HAKA SAML profile

Mikael Linden then presented on the profile work in Finland which has built on the work of saml2int. The slides are available at: http://www.terena.org/activities/tf-emc2/meetings/15/saml2-haka.ppt

The Haka profile has some modifications to saml2int including:

- Mandating HTTP**S** endpoints
- Additions requiring single logout to use redirect binding and signing (though single logout is still optional)
- Optional Discovery Service
- Mandating the use of a known Certificate Authority.

Lukas asked if there were any examples of applications requiring this [known use of CA].

[**ACTION**] Mikael Linden to distribute list of Applications/Provider that require a known CA rather than self signed certificates.

Josh asked why the decision for validUntil rather than cachedDuration. Leif clarified that they don't have overlapping semantics and both can be both used. Some profiles make them either or.

Discussion on whether making additions to saml2int means that you are no longer a saml2int participant/compliant. Andreas clarified that there will be the SAML profile, then SAML2int and then national profiles. For interoperability in Kalmar Union they drop those national requirements and revert to SAML2int.

PKNG

Leif Johansson presented on "PKI: The Next Generation", the slides are available at: http://www.terena.org/activities/tf-emc2/meetings/15/pkng.pdf

Leif claimed that he spent more time looking for the fonts than working on the presentation. This is work being conducted within the IRTF (Internet Research Task Force). Progress is slower and it is less active than the work of the IETF. BGP is used for network management, but is also a trust management protocol because it expresses business relationships. Traditional PKI trust is top-down from CAs that you don't have a natural relationship with. While there is a lot of trust and relationships naturally in a bottom-up model.

IRTF page on PKNG: http://www.irtf.org/charter?gtype=rg&group=pkng

Andreas noted that this topic might be interesting to address the problem to sign metadata.

UIs for Discovery Services

Lukas Hämmerle presented on improvements to metadata to improve the Discover Service experience. The slides are available at: http://www.terena.org/activities/tf-emc2/meetings/15/LH-TF-EMC2-Vienna.pdf

Lukas presented the improvements made to discovery service since the Classic WAYF had been created:

- simpleSAMLphp discovery improvements
- SWITCHaai embedded WAYF improvements

The current work is available on the Internet2 Wiki at: https://spaces.internet2.edu/display/~lajoie@idp.protectnetwork.org/DSUI

Lukas posed the question "Should we separate the metadata info from the UI info and store these two things into different files?"

Milan noted adding extra information reminds attribute certificates; in this view it would be sufficient to provide an URL to the extra information. A solution would be that an SP would (dynamically) provide any further information in a well-known location.

This would have the plus that if updates on specific SP-info, there would be no need to update the all metadata and to re-distribute them. Leif suggested looking at XRD protocol used in OpenID to associate resources to an identifier. There seems to be consensus to split the metadata info from other info related to entities.

[**NOTE**] Lukas provided an update on the mailing list to questions not answered during the presentation http://www.terena.org/mail-archives/tf-emc2/msg01392.html

Single Log-Out

Kristof Bajnok presented on Single Log-Out and the NIIF developed extension to Shibboleth. Slides available at: http://www.terena.org/activities/tf-emc2/meetings/15/emc2_2010_slo.pdf

The issue raised about Single Logout is that it isn't universally or consistently implemented and the use of Single Logout could give users the false feeling that they have been logged out when they may not have been logged out.

One of the main problems is the session management among the three parties involved. Niels noted that some federations have more parties, for instance in SURFfederaties there would be already 5 parties involved.

eduGAIN Policy Feedback Session

Josh Howlett presented an update on eduGAIN. The slides are available at:
http://www.terena.org/activities/tf-emc2/meetings/15/eduGAIN%20update.ppt

This was a summary of the current and expected progress of eduGAIN. There are 3 main stages:

- PoC
- Pilot
- Production

Mikael Linden presented on the 3 policies that constitute eduGAIN. The slides are available at:
http://www.terena.org/activities/tf-emc2/meetings/15/worm-report.ppt

There was some discussion on who are the natural members of eduGAIN and what limits (if any) exist for people joining.

Diego wants to ensure that a limit of one federation per country isn't acceptable for SIR/Confia/Spain and shouldn't be imposed.

Much discussion on CERN and whether they are a SWITCHaai member (which is currently not the case) and whether they could join directly. This option has been left open and allows groups to make a proposal to the NREN PC.

Much discussion surrounded the recommended attributes and the use of SHOULD:

- Leif recommends that there should be a guide on how you write defensively for federated applications: "Good coding practices for federated identity".
- Nicole highlighted that there are recommendations that are in conflict between UK Federation and eduGAIN policy.

7. Beyond Web Single Sign On

This section of the programme is a joint TF-EMC2 and TF-Mobility session:

SAML/SASL

First, Klaas Wierenga, presented on an IETF draft on "A SASL Mechanism for SAML"
http://tools.ietf.org/id/draft-wierenga-ietf-sasl-saml-00.txt

Klaas provided some background to SASL (RFC4422) and the fact that it is simple for everything except channel binding - and there are a number of applications that already support SASL.

Project Moonshot

Josh Howlett presented on the history of Project Moonshot and the current proposal. Some preparatory reading was provided on the mailing list so people would have time to digest the information presented in this session.

- Introductory Email: http://www.terena.org/mail-archives/mobility/msg03451.html
- Briefing Paper: http://www.terena.org/mail-archives/mobility/pdfEKnl2kkFsw.pdf
- Feasibility Analysis: http://www.terena.org/mail-archives/mobility/pdfYmAUrcXImJ.pdf

The presentation slides are available at: http://www.terena.org/activities/tf-emc2/meetings/15/Moonshot%20-%20TF%20Vienna%20Presentation%2001.pdf

There are significant components of this proposal that don't exist - though it is built on top of existing mechanisms that need to be extended.

In the outlined of proposed work - Josh has made a call to build a team of GSS ninjas that will modify an array of applications ordered by user demand and use-case priority.

8. National Updates

USA Update

Ken Klingenstein presented on:

- The federation now helps sell the network w/InCommon having 6M+ users.
- Moving people to SAML2.0.
- eduroam expansion.
- LoA is the new discussion topic "InCommon Silver and Bronze" rather than talking about Shibboleth.
- eduroam - Alumni + K-12 + InCommon relationship
- What to do if you can't wait for interfederation?

Discussion on the need for a metadata aggregator or some mechanism to "trust" or "sponsor" the integration of

[**ACTION**] Ken to clarify the exceptions that people "want" to be connected to a federation and distribute on the REFEDs list.
Klaas asked whether there were any general comments regarding the TF-EMC2 National Updates, they are available as part of the meeting agenda online as posted to the mailing list.

Niels wanted to have a further explanation of the P2P system detailed in Leif's updated and how it differs from LionShare. Leif details the individual and group mechanisms to limit the distribution of P2P sharing. They are looking at sensor networks for the transfer of data between peers. The only group that has a solution are the grid community. Other members are predominately using FTP and Email.

A question was posed to Ken regarding GENI with reference to FEDERICA in Europe. GENI is a collection of projects (PlanetLab, Orca, two other subprojects) and Ken can't speak of the funding of the project. GENI has created a security architecture paper than the subprojects will need to align to in the future.

Cees de Laat has been involved in reviews of GENI and he is also involved with FEDERICA. Since there will be a FEDERICA II project proposed at the end of the year there is some benefits in cross-pollination between the two groups.

9. Date of Next Meeting

The week of 20th of September, 2010 with a tentative location of Copenhagen.
[**ACTION**] Brook to liaise with Jacob-Steen on logistics for Copenhagen meeting.

10. AOB and Close

The meeting closed at 17:30. (Minutes published 10th March 2010)

Summary of Actions

Reference	Who	Action	Status
20100317-01	Brook	Flag SURFnet's "Operational Excellence Toolkit" to TF-MSP.	
20100317-02	Milan	To discuss this problem [of gaining access to the Comodo root certs without the dependency of Comodo certs] with the TCS PMA and report on any solution.	
20100317-03	-	TERENA to start working on a TCS FAQ page.	
20100317-04	Miro	Document the monitoring [requirements] (both active and passive) that are available and mechanisms to determine whether the service is working or not.	
20100317-05	Diego	Diego to put Licia/TERENA in touch with OID software developer.	
20100317-06	Mikael	Distribute list of Applications/Provider that require a known CA rather than self signed certificates.	
20100317-07	Ken	Clarify the exceptions that people "want" to be connected to a federation and distribute on the REFEDs list.	
20100317-07	Brook	Liaise with Jacob-Steen on logistics for Copenhagen meeting	

Document History

Date	Comment	Status
17 Feb 2010	Initial text collaboratively written in Google Wave.	Internal
10 Mar 2010	Initial version published for comment.	Published