« networking the networkers »

16th TF-EMC² Meeting - Wednesday, 22nd September 2010

Copenhagen, Denmark. The meeting was hosted by WAYF.dk.

Table of Contents

1. Welcome and Apologies

Diego Lopez welcomed everyone to the meeting wearing his Spanish jersey and celebrated the outcome of the 2010 World Cup. Attendance and Apologies were recorded on the event registration page: http://www.terena.org/events/details.php?event_id=1652

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/16/

3. Minutes of Last Meeting and Update of Action List

The minutes of the last meeting held on the 16th and 17th of Februray 2010 were approved without corrections and are available at: http://www.terena.org/activities/tf-emc2/meetings/15/minutes.pdf

Reference	Who	Action	Status
20100317-01	Brook	Flag SURFnet's "Operational Excellence Toolkit" to TF-MSP.	*Flagged 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.	*Options are being considered.*
20100317-03	-	TERENA to start working on a TCS FAQ page.	*Kevin Meynell has build the FAQ available at https://www.terena.org/activities/tcs/faq/*
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.	*Will be discussed at this meeting at Agenda point 4d.*
20100317-05	Diego	Diego to put Licia/TERENA in touch with OID software developer.	*Contact on this issue has between made between RedIRIS + TERENA. Work is underway to find a solution.*
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.	*The result of this work is "beer: bucket of end entities registry" https://spaces.internet2.edu/display/BEER/Home Working with WAYF.dk on a JANUS http://code.google.com/p/janus-ssp/ Proof of Concept (PoC).*
20100317-08	Brook	Liaise with Jacob-Steen on logistics for Copenhagen meeting	*This item was renumbered to 08. Complete.*

Discussion on 20100317-07:
Ken explained that BEER is needed, as it is important to exchange metadata about sites. If this PoC is successful a proposal to ISOC.org will be made to fund continued development and likely to be run with a REFEDs hat. This work doesn't halt national federations attempting to do this in the mean time.

Milan questioned the value of metadata exchange without a federation. Ken suggested some instances where this would be valuable in testing interoperability, testbeds, services that don't required unknowing or trusting the user and many more that have yet to be conceived. Nicole asked whether the submitter of the metadata will be known to those consuming metadata from BEER? Ken answered "Yes" and that this point will go into the user stories. If a user story isn't captured it is recommended that it is written up and submit to the REFEDs list to capture these use cases. There are policy issues surrounding BEER and they will be discussed at the REFEDs meeting on October 31st.

4.   Work items updates - All Work items (WI) leaders
4.a Campus Middleware Issues

Torbjörn Wiberg made a verbal presentation on Campus Middleware Issues and how these topic have been integrated into the updated Terms of Reference for TF-EMC2 for its next term under the new title of "Community Outreach" which will take a stronger role in the organisation of EuroCAMP events as well as liaison with the Grid community.

Diego questioned the value of multiple identity providers from a single institution being allowed in a federation, following on from a discussion allowing this within SWAMID. Nicole stated that there were many cases within the UK, including library-walk-in only IdPs at campus' and some faculties needing higher identity vetting requirements. Ken stated that an IdP solely for Alumni is a use-case. It was concluded that currently it is technically easier to segregate on an IdP boundary rather than have mixed Identity vetting values within a single IdP, mostly due to inconsistent policy and implementation by SPs.

Diego flagged an approach by the euroCRIS consortium (http://www.eurocris.org/) with the desire to collaborate in the area of persistent identifiers.

4.b Collaboration with the Grid Community
4.c Community PKI Initiatives

Milan Sova gave a verbal presentation as a combined update on "Collaboration with the Grid Community" and "Community PKI Initiatives" work items. These activities will now be divided between the "Services to the community" and "Community outreach" work items under the proposed Terms of Reference (ToR) for the next iteration of the taskforce.

Milan attended the EUGridPMA, which was held the two days prior to this meeting and has its final day today. The last of the TCS service, the eScience Certificates have now been accepted and will be available from October. The eScience Personal Certificates have been available since March.

On the topic of Levels of Assurance, touched upon in Torbjörn's report, CILogin - this will be the first service to be rated to NIST (800-63) and InCommon Silver. This will allow remote verification of identity vetting. Some changes to the MICS certificate profile is required to make it "compatible". Milan noted that the NIST profile is very much US-centric which poses issues on the applicability of the profile in Europe.

Ken added that the US Govt is now building out the privacy side of the LoA (when do users need to release attributes to government agencies). uApprove is a product that is being considered. He concluded that there are more issues than identity proofing in LoA.

[**ACTION**] It was agreed to discuss the LoA issue during the next REFEDs meeting in October and report back to the TF-EMC2 mailing list.

Diego asked whether the inclusion of EV Certificates as part of the TERENA Certificate Service would be valuable to the community?

Opinions were mixed with Milan stated that here was "No interest" from the NREN Community. Leif backed up this statement with a survey of SUNET customers not willing to comply with the audit/paperwork side of EV Certificates even if the certificates were available at no cost.

Ken said that there are discussions surrounding EV Certificates and is likely to be a future service of the InCommon incarnation of TCS. Henry from JANET stated that there was quite some interest in EV Certificates particularly in the personal certificate space. Leif added that there are unforseen uses of EV Certificates in the Personal Certificate space worth exploring.

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/16/tf-emc2-copenhagen2010-mm.pdf

4.e Directory Schema

Victoriano gave a presentation on "Directories and Schema". The slides can be found online at:
http://www.terena.org/activities/tf-emc2/meetings/16/schema.pdf

Particularly focusing on updates to the SCHAC schema and the announcement that schacHomeOrganizationType is now multivalued. This allows both :int; and :countryCode: values to be expressed simultaneously. It was reinforced that this attribute expresses the role of the IdP rather than an the alignment of an individual within that organisation.

"official ID numbers" as a subtype within schacPersonalUniqueID was presented. This is a discussion that recently surfaced on the mailing list. One proposal is to use the MRZ (Machine Readable Code) within Passports and National ID Cards. This proposal has limited value in countries without national id cards (many) and without 100% passport issuance.

[**ACTION**] Publish an updated revision of the SCHAC schema (which is currently under review and passed the comment period).

Ken noted that federations seem to define ad-hoc values, to solve specific issues that shouldn't and don't need to be generalised to a wider audience and feels that SCHAC has become the European extension of eduPerson with concerns that the usability of SCHAC outside EU is limited as its schema is not applicable outside the EU community.

The activities of this work item will be moved into "Services to the community". For the new terms of reference Victoriano will be working on a new work item "Academic Data Mobility" which will chart the predominant MIS systems used throughout Europe and their progress toward interoperable mobility.

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/16/refeds-update.pptx

Brook announced that Dyonisius Visser and he had implemented a Discovery Service/Service Provider Proxy within TERENA which supports the REFEDs wiki. It is hoped that all TERENA services will be connected to this service and that all necessary Identity Providers will be connected, either directly or eduGAIN (via SURFfederatie).

Ken asked about the formalities of peering arrangements. Brook responded that we'll directly peer with any IdP or Federation required and don't require a contract or agreement – if the end federation doesn't. To that end TERENA has joined WAYF.dk and WAYF will be sponsoring our promotion to Kalmar Union. It is hoped that eduGAIN and BEER can simplify this process.

The activities of this work item will be moved into "Community outreach" and will become a part of the REFEDs activity which is now independent from the TF-EMC2.

4.g Identity Services beyond Web Single Sign-On

Josh Howlett presented on the progress of Project Moonshot and in particular the meeting held yesterday. The attendee list of yesterday's meeting is available at:
    http://www.terena.org/events/details.php?event_id=1730
and the notes from that meeting are available online:
    http://www.project-moonshot.org/meeting1

This work item will continue on in the updated terms of reference and will be integrated with a sister work item within TF-MNM.

4.h Reputation Systems

Jaime Pereze presented on the current status of the Reputations Systems Work Item which highlighted the work of EQUAL and the proposal by SURFnet and ARNES and a new IETF group domainrep https://www.ietf.org/mailman/listinfo/domainrep

The slide notes are available at:
    http://www.terena.org/activities/tf-emc2/meetings/16/reputation.ppt

5.   Introduction to the new ToR

Diego presented the new Terms of Reference for TF-EMC2, highlighting important changes, and covered the work item that he'll be leading "Alternative Forms of Expressing Identity".
The slide notes are available at:
    http://www.terena.org/activities/tf-emc2/meetings/16/IntroducingToR.ppt

6.   Action proposals under the new ToR
a. Developments on federation-enhanced content-rewriting proxies (EZProxy and others), Diego Lopez

Diego Lopez presented on the issue of content-rewriting proxies which has been discussed on the ECAM list and is an activity that will progress under REFEDs: The slide notes are available at: http://www.terena.org/activities/tf-emc2/meetings/16/ProxySupport.ppt

b. Actions to provide federated group and VO support, Ken Klingenstein & Niels van Dijk

Niels van Dijk and Ken Klingenstein presented their respective work on federated group and virtual organisation (VO) support. Niel's slide notes are available at:

http://www.terena.org/activities/tf-emc2/meetings/16/TF-EMC2-Copenhagen-22sept2010.pdf

Ken gave a practical demonstration with some background. In meetings to convince people to use federated authentication and group management - changing from managing 200,000 identities to managing an ACL with 200,000 entries wasn't attractive. But with attributes for ACLs and combining attributes from the home IdP with VO supplemented attributes - then they (the community) are excited. Ken showed mockups to give an idea of the service – they don't currently work!

https://spaces.internet2.edu/display/COmanage/

The LIGO mockup available at the COmanage website:

http://co.internet2.edu/mockup/comanage/myco-ligo.html

There is also a Registry of Domesticated Applications available online:

https://spaces.internet2.edu/display/COmanage/Registry+of+Domesticated+Applications

7.   National Updates

No National updates were presented.

8.   Project Updates

a. Automated Testing of SAML 2.0 Behaviour; Compliance Testing (including demo), Andreas Åkre Solberg

Andreas Akre Solberg presented on SAML2 Testing. This is a follow-up on the teaser video that was posted earlier in the year. https://rnd.feide.no/content/federation-lab-automated-saml-20-sp-compliance-testing

The slide notes are available at:

http://www.terena.org/activities/tf-emc2/meetings/16/SAML-Automated-Testing.pdf
http://dl.dropbox.com/u/2381403/Presentations/SAML-Automated-Testing.pdf

The testing has improved a range of products, including simpleSAMLphp, and further work is underway on the range of tests and improvements to various service provider implementations.

Klaas queried whether these issues were specific to the SP, the federation or IdP. The answer was that both were likely. A feature request was made which was spawned during the development of SURFnet detective, on enable a subset of tests to be run.

Milan re-iterated this feature request and asked how this assess profiles such as saml2int.org. Further work on tests to support profiles is required.

Ken believed that the buzz around OpenID has hindered SAML2 Compliance Testing.

Leif said that the B2B market is the target for SAML2 services put together by consultants. Klaas re-interated that B2B market wants to sell to both ends of the equation - so interoperability isn't a driving force. The B2C/C2B market is much more interested in interoperability.

Mikael Linden asked whether are the flaws security issues or just incorrect behaviour. Andreas stated that the focus is currently on creating lots of tests - it hasn't been determined whether tests expose potential security holes.

b. HSM protection for federation metadata signing, Mikael Linden & Janne Lauros

Janne Lauros, from CSC, presented on the Simple Signing Device.
The slide notes are available at: http://www.terena.org/activities/tf-emc2/meetings/16/National%20Update%20on%20SSD,%20tf-emc2-22.09.2010.pdf

c. Logins4Life, David Chadwick (introduced by Diego Lopez)

Diego Lopez presented some work by David Chadwick. He presented linking accounts from the Login4Life service by adding a RedIRIS OpenID provider to show the aggregation of identities. This is a project funded by JISC. If there is any interest you should contact David Chadwick.
The Logins4Life project has its first public demo available at:

http://issrg-testbed-2.cs.kent.ac.uk/Logins4Life/

Other related demos are available at: http://sec.cs.kent.ac.uk/demos/ .
The Logins4Life project website is at http://www.kent.ac.uk/is/projects/loginsforlife/index.html

d. OAuth2 Assertion Profile implementation, Diego Lopez

Diego Lopez presented on the OAuth2lib PHP library that is being developed by RedIRIS.
The slide notes are available at:

http://www.terena.org/activities/tf-emc2/meetings/16/OAuthDevels.ppt

e. eduGAIN Update, Valter Nordh

Valter Nordh presented the current status of the eduGAIN Policy Framework. The slide notes are available at:
http://www.terena.org/activities/tf-emc2/meetings/16/eduGAIN%20TF-EMC2_v2.ppt

A lively discussion of the eduGAIN policy framework and in particular some wording that induces some behavioural changes on participating IdPs. The offending phrase:

> *Home Organisations that expose Identity Providers to eduGAIN MUST have the technical and organisational means to match exposed identities to individual End Users.*

Will be reviewed for its impact on the library-walk-in use case and an investigation on removing all such encumbrances to an LoA profile will be undertaken.
LoA 0 != LoA 1

f. Secure Management of Information across multiple Stakeholders (SEMIRAMIS), Sascha Neinert

Sascha Neinert presented the work of the SEMIRAMIS project:
http://www.terena.org/activities/tf-emc2/meetings/16/semiramis_at_tfemc2_copenhagen_2010-09-22.pdf

Further information can be found in the flyer: http://www.semiramis-cip.eu/images/stories/Publications/semiramis_flyer_draft_2010%20july%2006.pdf
…or the website: http://www.semiramis-cip.eu/

g. Project COIN, Niels van Dijk

Niels van Dijk presented on the "COllaboration INfrastructure: COIN" project at SURFnet, with more detail than given earlier in the day. The slide notes are available at:
http://www.terena.org/activities/tf-emc2/meetings/16/TF-EMC2-Copenhagen-22sept2010%20COIN%20project.pdf

Andreas asked which API will be preferred for attribute discovery? Niels stated that he'd hope that the vendor will decide between OpenSocial API and SAML/AA and choose which ever is most appropriate for their environment.

Andreas also queried when you'd run into the VO discovery problem. Niels expected that this will be a 0-day problem. What will save the day? As a stop gap Niels stated that initially there will be a small number of IdPs - which will ease the pain. There will also be a promotion of WAYFless URLs. There will be pain - and it is hoped that there will be improvements to the discovery problem progressively.

h. SAML2 IdP Proxy (…to Twitter, Facebook, Google, OpenID, Windows Live ID or whatever), Roland Hedberg & Torbjörn Wiberg

Roland Hedberg presented a demonstration of an IdP Proxy Service which interfaces with various social networking identity provider systems using OAUTH as well as site specific APIs and how to integrate such services into the federation environment. This will be a future service within SWAMID.

Andreas stated that this has the same problem as the discovery problem – as it is difficult to remember which social networking service you used to connect to a service – and there is no way to bond accounts together – leaving you with multiple accounts on services.

i. Discovery Service Geolocation, Jacob Christiansen

Jacob Christiansen provided a demonstration of his IdP Discovery + Geolocation project. This supports the browsers geolocation API to identify the location of the user and display nearby Identity Providers. The slide notes are available at:
http://www.terena.org/activities/tf-emc2/meetings/16/Geo-location%20initial%20PoC.pdf

A site demo'ing this services is available at:
http://jach-map-test2.test.wayf.dk/module.php/core/authenticate.php?as=default-sp

j. Discovery Service Improvements, Brook Schofield

Brook Schofield presented an idea on Discovery Service Improvements based on the XAuth.org Social Networking long tail discovery issue. The slide notes are available at:

http://www.terena.org/activities/tf-emc2/meetings/16/TF-EMC2-Discovery-schofield-20100922.pdf

Brook stated that this concept a) needed work and b) needed a trust point within this system. To be assured that the underlying JavaScript isn't modified and used to collect user traffic patterns. The community believed that this area is worth exploring even though it only covers a small set of cases within the Discovery Problem and that TERENA has the level of trust needed for the R+E Identity Federation community to adopt this if it comes to fruition.

9.   Date of Next Meeting

There has been a request from TF-Storage that TF-EMC2 align with the next TF-Storage meeting (currently unscheduled) in January/February 2011.

The participants expressed their desire for a 2-day TF-EMC2 meeting on the next occasion and would prefer to align its meetings with TF-Mobility and Network Middleware.

A date of the week of February 14th, 2011 was set down. Without a host the TF-* Secretary was asked to find an NREN that would be willing to host the next meeting.

[**ACTION**] Determine an appropriate host + venue for a 3-day combined TF-EMC2 + MNM meeting with sufficient notice for international travellers.

10.   AOB and Close

The meeting closed at 17:30. (Minutes published 27th October 2010)

Summary of Actions

Reference	Who	Action	Status
20100922-01	Licia	Circule notes on the LoA issue from the next REFEDs meeting on TF-EMC2 mailing list.	
20100922-02	Victoriano	Publish an updated revision of the SCHAC schema	
20100922-03	Brook	Determine an appropriate host + venue for a 3-day combined TF-EMC2 + MNM meeting with sufficient notice for international travellers.	

Document History

Date	Comment	Status
22 Sep 2010	Initial text collaboratively written in Google Wave.	Internal
27 Oct 2010	Initial version published for comment.	Published
28 oct 2010	Minor corrections supplied by the Task Force Chair	Published