

**19th TF-EMC² Meeting – Monday, 7th and Tuesday, 8th November 2011**

Bologna, Italy. The meeting was hosted by GARR.

Table of Contents

1. Welcome and Apologies	1
2. Task Force Chair Renewal	1
3. Approval of Agenda	2
4. Minutes of Last Meeting and Update of Action List	2
5. Work items updates - All Work items (WI) leaders	2
a. Services to the community, Licia Florio	2
b. Identity Services beyond Web Single Sign-On, Josh Howlett	3
c. Academic Data Mobility, Victoriano Giralt.....	3
d. Reputation Systems, Jaime Pérez.....	4
e. Diagnostic-related Activities, Miroslav Milinovic	4
f. Community Outreach, Torbjörn Wiberg.....	4
g. Alternative Forms of Expressing Identity, Diego Lopez	4
h. Service-oriented Collaboration Infrastructures, Niels van Dijk	4
6. National & Community Updates	4
a. Trusted Attribute Aggregation Service (TAAS), George Inman	4
b. Open Source Identity Management for Higher Education, Ken Klingenstein	5
c. GN3 Identity Federations Update, Licia Florio	5
d. Exchanging Group Information with VOOT, Maarten Kremers	5
e. OpenID Connect, Roland Hedberg	5
f. Client Certificates, Ken Klingenstein	5
g. GN3 Innovation, Licia Florio.....	6
h. F-Ticks for Federation Monitoring, Leif Johansson	6
i. VO-support in SURFconext, Maarten Kremers	6
j. Identity Provider Auditing in Croatia, Miroslav Milinovic.....	6
7. Date of Next Meeting.....	6
8. AOB and Close	6
9. Summary of Actions	7

1. Welcome and Apologies

Diego Lopez welcomed everyone to the meeting and announced that this would be his last meeting as TF-EMC2 Chair and that his new career direction will be more heavily focused on Mobility. Attendance and Apologies were recorded on the event registration page:

http://www.terena.org/events/details.php?event_id=2049

2. Task Force Chair Renewal

Diego introduced the proposal that both Victoriano Giralt and Roland Hedberg would be chairs of the task force. The decision was accepted by acclamation and the dual chair arrangement will be effective from the close of this meeting. Roland made a statement on the applicability of the dual chair arrangement. Klaas supported this as Mobility previously had such an arrangement and a natural division of labour formed.

3. Approval of Agenda

The agenda was modified as the meeting progressed with a final version available online:

<http://www.terena.org/activities/tf-emc2/meetings/19/>

4. Minutes of Last Meeting and Update of Action List

The minutes of the last meeting held on the 29th of June 2011 were approved without further corrections and are available at:

<http://www.terena.org/activities/tf-emc2/meetings/18/minutes.pdf>

Reference	Who	Action	Status
20110214-01	Brook	Reserve a slot for personal certificate discussion at the next meeting.	<i>Ken will be prompting the discussion on Day 2 of this meeting.</i>
20110214-02	Ken	Provide information to the mailing list regarding federation diagnostic monitoring work.	<i>This will be covered during Miro's WI update.</i>
20110214-04	Dyonisius Victoriano	TERENA to look at mechanisms to support collaborative editing of SCHAC schema.	<i>Completed. Will be covered by Victoriano during Licia's WI update.</i>
20110214-06	Olivier	Provide details on Nuxeo to the SURFnet labs domestication wiki.	<i>Maarten confirmed that they have received the information from Olivier.</i>
20110215-01	Kristof	Provide details for accessing the metadata signing software.	<i>Ongoing.</i>
20110629-01	Ken	Create an activity on application uses for personal certificates.	
20110629-02	Ken	Circulate the LoA CAMP presentation by the Burton group to the mailing list.	<i>Email posted the mailing list.</i>

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

a. Services to the community, Licia Florio

Licia presented an update on TCS, TACAR, SCHAC and Cloud Storage. Slides available at:

<http://www.terena.org/activities/tf-emc2/meetings/19/emc2-updates.pdf>

There was a call for the happiness of TCS subscribers as a previous call was made prior to the Comodo breach earlier in the year. Ken asked whether the community should be polled again. Diego reversed the question to ask whether Comodo are happy with the RA status of TCS subscribers.

Ken stated that the InCommon certificate service is up for renewal and while they are very happy with the service that Comodo is providing he asked "Would using a CA different from TCS cause any problems?". The discussion concluded that this wouldn't be problematic and might be a beneficial exercise.

Licia also detailed a UNINETT Sigma project on federated cloud storage services (similar to the previous discussions on Federated Box.net/Dropbox/S3). Diego reference the [EUDAT project](#) (offering a first version of a Scientific Data Infrastructure).

Leif said that many users, if not all, already use these a combination of these services and questioned whether NRENs want to be in control of all data or just offer secure services? The consensus was NRENs should offer secure and trustworthy services which comply with EU privacy regulations to contrast against "commodity" services which might not fulfill these requirements.

Licia detailed that to further enhance PEER, that Yaco will be contracted for additional features. Ken asked when will a metadata format for OpenID Connect be available and can it be listed in PEER. Leif responded stating "it's just a matter of time".

Ken stated that the frequency of REFEDS meetings is insufficient for maintaining the PEER service instance. It was agreed and Licia should investigate an advisory group within REFEDS to oversee this work.

[ACTION] Licia to create a PEER Service Instance Advisory Group within the framework of REFEDS.

Victoriano presented on the current state of SCHAC (<http://www.terena.org/activities/tf-emc2/meetings/19/schac-urnreg.pdf>). The adoption of 'urn:schac' caused some confusion but the change only applies to attribute values, not attribute names, as all attributes should be named by OID (1.3.6.1.4.1.25178). Attribute values prefixed with the old 'urn:mace:terena.org:schac' will be deprecated following a post by Victoriano to the SCHAC mailing list. From 1 July 2012 it should be a WARNING for use of the old attribute format and it will be an ERROR from 1 January 2013. The URN Registry is available at: <http://urnreg.terena.org/>

A discussion on commonName vs schacSn2 (or schacAdditionalName, schacOptionalName, schacOtherName) concluded that schacSn2 will remain in SCHAC and no other "name parts" will be added to the schema. An update will be made at: <http://www.terena.org/activities/tf-emc2/schacreleases.html>

[ACTION] Victoriano to inform the SCHAC community the phasing out of 'urn:mace:terena.org:schac' attribute values.

b. Identity Services beyond Web Single Sign-On, Josh Howlett

Josh Howlett's presentation (<http://www.terena.org/activities/tf-emc2/meetings/19/19th TF-EMC2 Beyond Web SSO 00.pdf>) described the "Beyond Web SSO" landscape and focused on the progress of Moonshot, highlighting the impressive list of applications that work with Moonshot without modification.

c. Academic Data Mobility, Victoriano Giralt

Victoriano Giralt presented (<http://www.terena.org/activities/tf-emc2/meetings/19/mobility-ssedic.pdf>) on the ADM/RS3G and DSDP projects and that there is a need for funds to continue the project. The future roadmap or amount of funding required is unclear and needs to be decided before a request can be made.

Licia asked whether GN3, GN3+ or GN4 projects are likely to be compatible streams of funding or should other funding options be explored, as a project focused on Campus' doesn't necessarily fit with a project focused around NRENs.

[**ACTION**] Simone and Vic to produce a very short document to describe the state of work completed thus far by the RS3G group, funding needed to finish the development and why GEANT would be a good place to carry out the work.

d. Reputation Systems, Jaime Pérez

Jaime Pérez gave a verbal presentation indicating that work in the DomainRep and other reputation spaces have slowed over the summer period with little to report on at this time.

Ken referred the group to <http://www.ren-isac.net/ses/> which manages white/black lists across distributed environments.

e. Diagnostic-related Activities, Miroslav Milinovic

Miroslav reported (<http://www.terena.org/activities/tf-emc2/meetings/19/tf-emc2-bologna2011.pdf>) on the GN3/JRA3/T1 federation lab work.

[**ACTION**] Miro to explore opportunities with TF-CSIRT and TF-NOC on monitoring/measurement.

f. Community Outreach, Torbjörn Wiberg

Torbjörn Wiberg wasn't present at the meeting and no update was provided.

g. Alternative Forms of Expressing Identity, Diego Lopez

Diego presented (<http://www.terena.org/activities/tf-emc2/meetings/19/OFEIupdate-20111107.pdf>) on the integration of STORK with R&E Identity Federations, GemSTS and the standardisation of JSON. The two proxy proposals, previously presented to REFEDS, have been reformulated to converge on a common goal.

h. Service-oriented Collaboration Infrastructures, Niels van Dijk

Maarten Kremers gave a verbal update on behalf of Niels van Dijk, summarising the current work in SURFconext, OpenConext and VOOT integration (which will be covered in more depth tomorrow).

Ken asked which verbs does VOOT support? As READ is certainly important but what about JOIN & LEAVE. Leif said there is a need for bidirectional publish/subscribe of group information.

Ken stated that he and Niels were still planning a VAMP (Virtual Organisation Architecture and Middleware Planning) event to target three audiences: us, VO operators, VO architects.

Discussion on how to bring the appropriate people to a REFEDS/TERENA event and whether EGI.eu or the CERN lead workshop series are useful. Licia reported that a result of the November meeting in RAL, UK is for a roadmap to be presented at REFEDS on what is covered in their own territory (Grid), what will be covered by identity federations and what areas remain for development/definition as a collaboration of the two groups.

6. National & Community Updates

a. Trusted Attribute Aggregation Service (TAAS), George Inman

George Inman from the University of Kent presented on Trusted Attribute Aggregation Service (TAAS) (<http://www.terena.org/activities/tf-emc2/meetings/19/TAAS-Bologna-2.pdf>). More information is available on the website <http://sec.cs.kent.ac.uk/demos/taas.html>

b. Open Source Identity Management for Higher Education, Ken Klingenstein

Ken lead the discussion Open Source Identity Management for Higher Education (OSIdM4HE) project (<https://spaces.internet2.edu/display/OSIdM4HE/OSIdM4HE+Initiative>) and referred people to the wiki for further information.

Kuali Rice was originally an API specification. The community didn't like an API spec and wanted running code which led to the creation of this project.

c. GN3 Identity Federations Update, Licia Florio

Licia presented an update from Andreas Solberg on the GN3 Identity Federations research task (<http://www.terena.org/activities/tf-emc2/meetings/19/Andreas-updates.pdf>) covering DiscoJuice 2.0 (<http://discojuice.org/>), Fed-Lab (<https://fed-lab.org/>), SAMLmetaJS (<http://samlmetajs.simplesamlphp.org/>) and SAMLtracer (<https://fed-lab.org/software/firefox-saml-tracer/>).

Discussion of the "trust" model of a centrally hosted service as provided by DiscoJuice 2.0 highlighted concerns with devolving responsibility for metadata trust to a 3rd party. It was concluded that DiscoJuice hosted is ideal for rapid development and pilot deployments and implementers should be aware of the implications of blindly trusting metadata.

d. Exchanging Group Information with VOOT, Maarten Kremers

Maarten Kremers covered Exchanging Group Information with VOOT (<http://www.terena.org/activities/tf-emc2/meetings/19/VOOT-tfemc2-nov2011.pdf>). More information is available on the wiki <https://github.com/andreassolberg/voot/wiki> and <http://openvoot.org/voot-2.0.html>.

Ken asked about non-web applications and how do they integrate. Maartin stated that the REST API is used. Licia asked how this could support the eScience community. This will be taken up on the list.

Lukas asked how much of a departure is VOOT from the OpenSocial standard. Maarten stated that OpenSocial Lite/Light specification is very similar to VOOT.

e. OpenID Connect, Roland Hedberg

Roland presented on OpenID Connect (http://www.terena.org/activities/tf-emc2/meetings/19/oic_tf-emc2.pdf) and have a thorough walk through of OpenID Connect and how it relates to OpeniD and OAuth2. The eventual result will be a testing service with workload divided between Andreas Solberg (Front-end) and Roland (Back-end).

f. Client Certificates, Ken Klingenstein

Ken prompted the discussion on the Use, Installation and How to Drive Adoption of Client Certificates. Currently 15 of 22 TCS countries subscribe to TCS Personal. Of particular note are the MIT/Virginia installers for personal certificates that are used for Email Signing, File Access, eduroam, and some other services.

Discussion on whether certificates make a device that connects to eduroam a personal device that relates to a user or not concluded that additional access control to the certificate needs to be enforced. Ken referenced security policy enforcement, which is available on iOS and can be used to required a password on the device to protect the certificate.

Current progress is documented at

<https://spaces.internet2.edu/display/InCollaborate/InCommon+Personal+Certificate+Provisioning+and+Application+Setup+Tool>

g. GN3 Innovation, Licia Florio

Licia announced that GN3+ was calling for ideas that could move from the national or taskforce level to being projects supported within the framework of GN3 and referred to an ECAM call (<https://www.terena.org/activities/ecam/calls/201110.html>) that proposed four areas for consideration by GN3+.

h. F-Ticks for Federation Monitoring, Leif Johansson

Leif presented on the creation of an F-Ticks logger for Shibboleth IdP

(<http://www.terena.org/activities/tf-emc2/meetings/19/f-ticks-saml-tf-emc2-bologna-2011.pdf>). The code is available from <https://github.com/leifj/ndn-shib-fticks>

[**ACTION**] Miro to provide an update on his F-Ticks for Federations pilot to the mailing list or the group.

i. VO-support in SURFconext, Maarten Kremers

Maarten presented on the VO and Virtual IdP components of SURFconext

(http://www.terena.org/activities/tf-emc2/meetings/19/VO_Support_SURFconext-tfemc2-nov2011.pdf).

j. Identity Provider Auditing in Croatia, Miroslav Milinovic

Miroslav presented the Identity Provider Auditing work completed by Srce

(<http://www.terena.org/activities/tf-emc2/meetings/19/tf-emc2-bologna2011-aaieduhr-auditing.pdf>) which checked a range of mandatory and optional compliance requirements in the areas of organization policy/procedure, data quality and technical correctness. A website for the audit is available <http://www.aaiedu.hr/certificiranje/> (in Croatian).

Ken asked whether there is a charge for the auditing? Miro stated that it has been decided that auditing will be an integral component of the service of the federation.

Ken added that there is a need for some adjectives before the word "audit" so we know exactly what we are talking about. Internet2/InCommon audits are focused on LoA 2 (InCommon Silver) which is defined and campus audits are the next stage. The initial idea was to have the university internal auditor perform the work at no cost. University auditors weren't interested in this this and as a result InCommon will come and perform an audit at low cost - and for institutions that don't want to wait for the InCommon audit process can take advantage of Kantara auditors.

Leif encouraged people to continue this conversation in the Kantara WGs because there is already effort in these forums.

7. Date of Next Meeting

The next two meetings will be virtual meetings to be held in February and May with a physical meeting combined with TF-EMC2 in June/July.

8. AOB and Close

The meeting closed at 17:30.

9. Summary of Actions

Reference	Who	Action	Status
20110215-01	Kristof	Provide details for accessing the metadata signing software.	
20110629-01	Ken	Create an activity on application uses for personal certificates.	
20111107-01	Licia	Create a PEER Service Instance Advisory Group within the framework of REFEDS.	
20111107-02	Victoriano	Inform the SCHAC community the phasing out of 'urn:mace:terena.org:schac' attribute values.	
20111107-03	Victoriano Simone	Produce a very short document to describe the state of work completed thus far by the RS3G group, funding needed to finish the development and why GEANT would be a good place to carry out the work.	
20111107-04	Miro	Explore opportunities with TF-CSIRT and TF-NOC on monitoring/measurement.	
20111107-05	Miro	Provide an update on F-Ticks for Federations pilot to the mailing list or the group.	