



**TF-EMC2 Meeting: 3-4 December 2008**

Utrecht, the Netherlands  
Licia Florio

**Table of Contents**

1. Welcome ..... 1

2. TF-ECM2 Work Items presentations ..... 1

    2.1 PKI updates – Licia ..... 1

    2.2 Directory schema – Victoriano Giralt ..... 2

    2.3 Federations – Mikael Linden ..... 2

    2.4 Campus Middleware Issues and LoA - Torbjörn Wiberg ..... 2

    2.5 Diagnostics – Miroslav Milinovic ..... 3

    2.6 Grid - Milan Sova ..... 3

    2.7 Reputation systems - Jaime ..... 3

    2.8 Identity Services beyond Web Single Sign-On – Josh Howlett ..... 4

3. Presentations ..... 4

    3.1 eduGAIN – Deigo Lopez, Josh Howlett ..... 4

    3.2 Clarin - Dieter Van Uytvanck ..... 4

    3.3 InfoCARD – Enrique de la Hoz ..... 4

    3.4 Phosphorus project and OSG-EGEE Authorisation Interoperability WG - Yuri Demchenko ..... 5

    3.5 Pictures - Victoriano Giralt ..... 5

    3.6 Report on IDABC – John Stienen ..... 5

    3.7 Service box proposal- George Thanos ..... 6

4. National updates ..... 6

n. Date of Next Meeting, AOB and Close ..... 7

**1. Welcome**

Diego welcomed the participants and presented the new terms of reference of TF-EMC2. The work item leaders were invited to present their proposals on the work each of the work items would undertake.

**Action:** It was agreed that all work item leaders would send a description of their work item work to the list.

**2 TF-ECM2 Work Items presentations**

**2.1 PKI updates – Licia**

Licia said that this work item will encompass all PKI-related activities, such as TACAR, SCS and any new initiative.

Starting from April 2009, TACAR will also be used to host GN3 CAs.

Due to the expansion of the target community and due to some bugs in the current software, a new version of TACAR should be expected by the end of 2009.

It is expected that TACAR will be enhanced to provide data for the PRQP, the PKI Resource Query Protocol. The PRQP protocol, which is being discussed within the IETF, allows applications to discover and retrieve resources provided by a CA. Because TACAR hosts CAs, it might be rather easy to expand TACAR to also include other CA related information, such as CRLs, OCPS and so on. The PRQP work is carried out by Massimiliano Pala (Dartmouth Univ.).

Ken mentioned that it might be worth monitoring the work of the DomainKeys Identified Mail DKIM, which is also discussed within IETF. There was a discussion on whether DKIM could be a possible use case for TACAR, but there seemed not to be consensus on this.

On the SCS front, Licia reported briefly on the tender process, which started in October 2008. Results are expected at the beginning of 2009.

## 2.2 Directory schema – Victoriano Giralt

This work item will cover mainly SCHAC's developments.

David S. presented his proposal to add SCHACYearOfBirth to store the year of birth of kids, before allowing them on particular websites. Children would login via the WAYF federation. Both Ken and Jens pointed out that the year of birth for children is an issue in US and Canada too.

The SCHAC is considered because the problem is not a Danish problem, but a more international one. SCHAC would be at the moment the quickest way to address this issue.

Because SCHAC provides different object classes, it would be easier to fit the year of birth in one of the classes. It was agreed to add SCHAC yearOf Birth to the experimental branch and to test it until TNC. After that this new attribute will be added to the official SCACH version.

Victoriano also reported that SCHAC experimental branch contains some attributes requested by the GIDP. Victoriano said that unless objections, these attributes have been tested and are ready to be moved to the production branch.

**Action:** Victoriano/Javier and David to work to add SCHAC yearOf Birth to SCHAC experimental branch.

**Action:** Victoriano to move GIDP-related attributes to SCHAC production branch.

## 2.3 Federations – Mikael Linden

Mikael reported on the developments in the Identity federation area. In particular Mikael addressed the organisational issue of federations. Ken said that in US there seems to be consensus in creating a company with limited liability for InCommon.

## 2.4 Campus Middleware Issues and LoA - Torbjörn Wiberg

Torbjörn presented the issues that campuses face in deploying IdMs; most of the issues have

organisational and policy nature.

Torbjörn talked also about LoA, which can be addressed from two different perspectives: from the IdP's perspective which states that eIDs are issued in compliance with a certain LOA and from the system's perspective, which ought to decide the LOA sufficient to trust an eID requesting the service.

The NIST Special Publication 800-63 would be relevant for campuses.

To this regard, Diego suggested looking at possible standards coming from some EU bodies (i.e. ENISA). Mikael said that there also IDABC should be monitored as for instance there are some interesting documents such as the one on authN. IDABC refer to 800-63 normative, but there are some differences.

It was said that the EMC2 group should specify what LoA refers to, as it could refer to many different things, such as LoA for attributes, LoA for authN, LoA for services etc.

## **2.5 Diagnostics – Miroslav Milinovic**

Miro reported that he surveyed the federations listed on the REFEDs wiki and only 8 out the 17 available say to be doing something in the monitoring and diagnostic area. It was pointed out that especially in what concerns diagnostics this group should engage with the security community. Maybe having some reports the CSIRT group would help.

## **2.6 Grid - Milan Sova**

Milan said that the Grid work item will report on Grid security related developments.

According to Milan, the most relevant topic for the EMC2 group is currently the work on the Grid authZ profile. The profile will contain recommendations on policy and global trust issues related to grid authorization. The group will eventually agree on a set of minimum requirements to operate a Grid Authorisation Attribute Authority.

The profile is almost finalised, but the document is not public yet.

The document should be available for comment at the time of the next OGF (March 09).

## **2.7 Reputation systems - Jaime**

Jaime presented possible areas to explore about reputation systems.

Josh said that metadata could be used to express reputation information about institutions. Also Internet sites (see ebay) use reputation systems, so it would be worth investigating if there are standard on reputation systems.

For instance in the OpenId's model reputation information is shared among different systems (not in a federation environment).

Mark O'Leary warned to be careful on how to use reputation systems as there might lead to pollute the reputation.

Diego suggested work on this area could start looking at white/black lists and on how to share information about these systems. People interested will have to contact Jaime.

**Action:** All to send information to Jaime on how white/list black lists are implemented.

## 2.8 Identity Services beyond Web Single Sign-On – Josh Howlett

Josh mentioned possible activities for this topic.

Diego invited people to send an email to the emc2 to point out possible applications. Victoriano said he would be interested in accessing Squirrels mail system in a federated way, whereas Mikael suggested exploring provisioning/de-provisioning.

Josh has recently circulated the workplan for this item, see:

[http://www.terena.org/activities/tf-emc2/beyond\\_web/index.html](http://www.terena.org/activities/tf-emc2/beyond_web/index.html)

## 3 Presentations

### 3.1 eduGAIN – Deigo Lopez, Josh Howlett

eduGAIN addresses the problem of confederation, federations of federations. Because there is no native Java implementation for shib-SP, eduGAIN might be used for this purpose as well.

The main entities in eduGAIN are:

1. Metadata service, which publishes the valid metadata of federations
2. PKI, which is multi-rooted
3. Identifier Registry, based on URNs.
4. BE, which are the eduGAIN end-points. Their function is to adapt protocols whenever needed. There are two different types of federations: the real gateway and the endpoint (IFEP).
5. Profiles – A number of profiles have been defined. Diego presented how the various profiles are implemented.

Within GN3, eduGAIN will be moved to service level. The role of the BEs is currently under discussion, mainly in what the concerns their usage when eduGAIN becomes a service.

### 3.2 Clarin - Dieter Van Uytvanck

Clarin (Common Language Resources and Technology Infrastructure) is EC funded project, which aims to create, coordinate and make language resources and technology available and readily useable.

Clarin presented some open issues related to AA. Everybody agreed that Clarin is obviously a very good use case for eduGAIN, for instance Clarin could become a remote BE for eduGAIN. It was agreed to discuss eduGAIN support for Clarin more in detail.

**Action:** Josh, Diego, Mikael, Dieter and anybody interested should be involved in the discussion.

### 3.3 InfoCARD – Enrique de la Hoz

Enrique presented InfoCard principles and how to use it. His talk covered two issues, one concerning attribute release and how to integrate InfoCARD assertions into current Identity Federations and the other one concerning how InfoCARD support could be built into current 1X clients. Because Enrique's tests are performed in Linux environment, Enrique would be interested in integrating InfoCARD with Linux supplicants. However discussion is ongoing with the OpenSEA alliance, which aims to build an open, multi-platform 1X supplicant.

The relation between InfoCard and WAYF was discussed. Enrique said that one of the

advantages of using a card is that WAYF is not needed. To a larger extent an InfoCARD provider would provide the same functionalities as WAYF.

Enrique also added that InfoCard will work in the same way under Geneva.

A demo-site is under developments. Enrique asked participants to provide feedback on his presentation and whether a international pilot might be an option.

### **3.4 Phosphorus project and OSG-EGEE Authorisation Interoperability WG - Yuri Demchenko**

Yuri reported on the effort to support multi-domain authZ being addressed in both Phosphorus project and EGEE interoperability working group. The objective is to make a multi-domain authorisation assertion based on the information received by the previous domain as well as those received by the target domain.

Phosphorus has created a XACML Authorisation Interoperability profile for Network Resource, which builds on XACML-Grid profile.

### **3.5 Pictures - Victoriano Giralt**

Victoriano presented the idea elaborated together with Rodney McDuff, to use the RADIUS infrastructure or more in general the federation infrastructure to enhance instant messaging.

The solution proposed is based on XMPP servers and SIP gateways that will use the RADIUS infrastructure to authenticate users.

In what concerns the clients, Victoriano explained that any client that supports the protocols could be used. The idea is not to replace current clients in use, but to create an infrastructure to connect all of them.

The benefit of this approach would be that it is based on open standards (XMPP and SIP) as opposed to proprietary solutions, such as Skype, MSN and similar.

It was pointed out that the proposal would be a typical case of invitation.

**Action:** Victoriano to provide more information on the proposal. All to contact Victoriano if interested in creating a pilot.

### **3.6 Report on IDABC – John Stienen**

IDABC (Interoperable Delivery of European eGovernment Services) aims to provide cross-border public sector services to citizens and enterprises in Europe.

John touched briefly upon the i2010 Action Plan, which aims to:

- create a modern, market-oriented regulatory framework for the digital economy;
- strengthen EU's research and development instruments;
- improve public services and quality of life through the use of ICT.

The EC is engaged in avoiding that member states opt for different and incompatible technologies. To achieve interoperability, the EC plans to promote the implementation of mutually recognised electronic signature (e-signature), which could be used to sign official documents in various sectors, such as electronic tenders, health data, and electronic customs.

An eSignature study was conducted in 2007; one of the main results was that states were

focusing on national implementations only. The conclusions of the study highlighted that there is a trend towards PKI and that a federated validation solution is needed. There are 97 CAs in Europe that are in the Trusted List of Supervised Qualified Certificate service provider.

Work has also been undertaken on eID; a survey was conducted in 30 countries in Europe to assess the impact of multi-level authentication mechanism. The result of the survey led to the definition of four level of assurance. ENISA is working to map the four-authentication level of assurance into SAML profiles.

Concerning the STORK project<sup>1</sup>, two WP are relevant, namely WP2 and WP5.

Attendees agreed that it would be good to establish contact with the STORK representatives, which will have to be done via the member states.

James Farnhill said JISC has contact in UK, whereas Mikael Linden is the representative of Finland in STORK.

US have similar issues and they are trying to move to federations and to get Liberty Alliance involved.

As follow up of this TERENA was invited to join the ePractice.eu, the IDABC initiative the collect and share information on eID Observatory (<http://www.epractice.eu/community/eureid>). People interested in eID issues are invited to join.

### **3.7 Service box proposal- George Thanos**

George presented that GRNET service box, the 1U server that is delivered free of charge to the Greek academic institutes.

GRNet Service Box has a set of pre-installed services which suites the needs of most academic institutes. Services included on the service box include directory service based on Sun DS 5.x, shibboleth IdP 1.3, RADIUS server based on FreeRADIUS, VPN service based on OpenVPN and VoIP Services.

George asked if other NRENs are interested in collaborating on the service.

Diego said that this would be a coordinated effort, for instance the participating could share the load (everybody could take care of something).

Comments: Hungary has a similar service containing eduroam, LDAP, shib IdP; so they will be interested. RedIRIS, and HEAnet are interested.

**Action:** Interested people can contact George (George Thanos [gthanos@admin.grnet.gr](mailto:gthanos@admin.grnet.gr))

## **4 National updates**

**CH** - Thomas presented uApprove, the plug-in for Shib IdP that allows users to see which attributes will be released to a server. Users can then accept or not, or they can reset

---

<sup>1</sup> STORK is a consortium involving 14 countries. STORK aims to implement a EU interoperable system for recognition of eID and authentication.

previously provided information. A demo is available on the SWITCH website for general test. See Thomas's slide online for more information on the demo.

Alex reported about autograph that works with ShARPE, and which works in a similar way as uApprove.

Thomas also reported about the embedded wayf, which allows SPs to customize look & feel, but it still uses the central WAYF transparently. It works integrating two Java scripts: configurator script to change the look and feel and a logic script that is loaded from the central WAYF.

**ES** – SIR is a federation based on the idea to easy entry point for IdPs and SPs. It will support OpenId, eduGAIN, SAML2 and SAML1. SIR can also act as a metadata aggregator. SIR participating institutions can buy Google Apps access and they can login using SIR credentials.

**JP** - Yasuo Okabe reported on the UPKI updates. The Japanese federation is shibboleth based; the federation is operated by NII. Users will be able to authN via Shib and to request Grid certificates that are compliant with IGTF specifications. Users can also use client certificates to authN via shib; in this case the DN of the cert is used to identify the user IdP. Yasuo also reported on eduroam.

**HR** – Their federation is now supporting RADIUS, SOAP/SAML whereas before it supported, RADIUS, LDAP, SOAP. There is one centralised IdP in the all country.

Srcce has developed their own monitoring system, which is also used for statistic purposes.

**DK** – WAYF is very much engaged in preserving users' privacy.

**AAF** – AAF has done lots of work on LoA, due to the work on PKI and the need to access some government resources. They identified four LoA and they are mapping them into the federation.

**UK** – James reported on the UK access federation and on some project that use the federation to access other service. Concerning attribute release policies there is not any real uApprove-like implementation yet.

**CRU** - CRU federation will be migrated to RENATER by the end of 2008. CRU is setting up a national anti-spam service. Victoriano said that for the university it would be important to be able to access logs. SURFnet is implementing a similar solution for their customs.

**I2** – Ken reported that COmanage is ready to be released as beta version. Geneva will support SAML and could function as Shib IdP and SP. On the federation side, it was said that InCommon is growing and in the future its governance, pricing and packaging principles, will be addressed. The silver profile has been approved; this is based on the Federal eAuth level of assurance program, which will include four levels of trust. Silver is roughly equivalent to the eAuth level 2.

#### **n. Date of Next Meeting, AOB and Close**

The next EMC2 meeting will take place in UK on 5-6 May 2009. The meeting will be hosted by the University of Loughborough.

#### **Action List**

Reference	Who	Action	Status
<b>03122009-01</b>	All work item leaders	To prepare a description of their work item work item by 1 April.	Outstanding
<b>03122009-02</b>	Victoriano/Javier/David	To add SCHAC yearOf Birth to SCHAC experimental branch.	Outstanding
<b>03122009-03</b>	Victoriano	To move GIdP-related attributes to SCHAC production branch.	Outstanding
<b>03122009-04</b>	All	To send information to Jaime on how white/list black lists are implemented and more in general on reputation systems they are aware of.	Outstanding
<b>03122009-05</b>	Josh, Diego, Mikael, Dieter	To discuss how eduGAIN can be used for Clarin.	Outstanding
<b>03122009-06</b>	Victoriano	To provide more information on PICTURE proposal. All to contact Victoriano if interested in creating a pilot.	Outstanding
<b>03122009-07</b>	Milan	To report on the Grid AuthZ profile.	Outstanding
<b>03122009-08</b>	All	To contact George for a possible international service box pilot. (George Thanos <a href="mailto:gthanos@admin.grnet.gr">gthanos@admin.grnet.gr</a> )	Outstanding

### **List of Participants**

First Name	Last Name	Affiliation
Kristof	Bajnok	NIIF / Hungarnet
Enrique	de la Hoz de la Hoz	University of Alcala
Paul	Dekkers	SURFnet
Yuri	Demchenko	UvA
James	Farnhill	JISC
Licia	Florio	TERENA
Abraham	Gebrehiwot	CNR - IIT
Victoriano	Giralt	University of Malaga
David	Groep	Nikhef (IGTF)
Jens	Haeusser	University of British Columbia / Canadian Access Federation
Nicole	Harris	JISC
Roland	Hedberg	Umeå University
Michael	Helm	ESnet
Andrew	Hindle	Ping Identity.
Jasmina	Hodzic	University of Oslo
Josh	Howlett	JANET(UK)
David	Kelsey	STFC-RAL

Kenneth	Klingenstein	Internet2
Jaap	Kuipers	SURFnet
Thomas	Lenggenhager	SWITCH
Mikael	Linden	CSC, the Finnish IT Center for Science
Diego	Lopez	RedIRIS
Jose-Manuel	Macias	RedIRIS
Patricia	McMillan	The University of Queensland (AAF)
Miroslav	Milinovic	Srce
Anders	Nilsson	Umeå university SUNET
Mark	O'Leary	JANET(UK)
Yasuo	Okabe	Kyoto University
Dubravko	Penezic	Srce
Remco	Poortinga - van Wijnen	SURFnet
Jaime	Pérez	RedIRIS
Juergen	Rauschenbach	DFN-Verein
Alex	Reid	AARNet
Peter	Schober	University of Vienna / ACOnet
David	Simonsen	WAYF - Where Are You From
Noboru	Sonehara	National Institute of Informatics
Milan	Sova	CESNET
John	Stienen	European Commission
George	Thanos	GRNET
Joost	van Dijk	SURFnet
Niels	van Dijk	SURFnet
Mark	Viens	Ping Identity
Glenn	Wearen	HEAnet Ltd
Torbjörn	Wiberg	Umeå universitet/SWAMI
Klaas	Wierenga	Cisco Systems
Stefan	Winter	RESTENA