REFEDs International Meeting
Friday 5 December2008
Utrecht, the Netherlands
Minutes by Licia Florio

Table of Contents

1. Welcome and Apologies

Licia Florio and Ken Klingestein welcomed the attendees to the third REFEDs international gathering. Both Ken and Licia stressed the importance of agreeing on a work plan for REFEDs.

An initial proposal to define REFEDs scope and activities was already circulated in the summer 2008. However at the time, it was thought that Liberty Alliance could become more engaged with the research and education community and that some of the REFEDs envisaged work could be shifted within Liberty. Due to different circumstances, no real progresses have been made and REFEDs work has not progressed.

The agenda was approved and it was agreed to reserve part of the meeting to review and update the initial REFEDs work plan, identifying roles and responsibilities.

2. Federations update and use cases for cross federations

Attendees, who represented the research and education federations in Europe, US, Canada, Australia and Japan, were asked to report about on one major success, one failure and two hot issues they faced developing and deploying their federation.

International Grid Trust Federation (IGTF) – David Group, IGFT chair, reported on IGTF. Dave reminded that IGTF started with the aim to create a trust framework to authenticate end-entities in inter-organisational access to distributed resources. Therefore the inter-federation use case was their starting point.

Furthermore, David also reminded that IGTF does not operate as an Identity Provider, but asserts that the certificates issued by the Accredited Authorities meet or exceed the relevant guidelines.

The main success relates to the number of SPs, which are now in the order of 1000. IGTF is also engaged in cooperation with national federation. Another success also relates to the agreement of the user policy. . Dave will send the policy out.

The possible point of failure concerns scalability, being IGTF a PKI-based federation.

Hot issues:
- Data privacy and persistent identifiers – Grid software uses uPersistent, non-reassignable identifier, which allows to track users.
- AuthZ attributes profile – A dedicated sub-group within IGF has been created with the aim to prepare 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.
- Usage of opaque attributes

RedIRIS Federation (Spain) – Diego Lopez said that the principles of identity federations have been well received in Spain. The drawback is that many federations (scientific foundations, regional federations and so on) are being established.
The important points to address are:

(i) migration to SAML2, in particular in what concerns SPs. A not uncommon scenario is that SPs not always process metadata according to standards, which creates problems;
(ii) level of trust to put into a federation.

Victoriano Giralt reporting about the Andalusian, which should go in production rather soon. The Andalusian federation users will still be member of RedIRIS. Because regional federations are becoming more common, Victoriano suggested this group investigating possible models of cooperation between national research and education federations and regional federations.

AAF (Australian) – Alex reported on the creation of a new attribute called 'sharedToken'. The attribute will give the same TargettedID to all services that a user can access. This attribute was introduced to address the following use cases:

(i) Grid access to resources - Whenever a user needs to access different Grid resources, the user will need to use the same token for all resources. This is meant to ensure that the user's identity has not changed, although has implications on preserving user's privacy – Grid attributes are on purpose persistent not targeted.

(ii) Publication of data in repository – Users need to access publications regardless from the where the users are.

The main issue AAF is currently facing regards the organisational structure of the federation. The first proposal was not very successful. The initial proposal seems to involve charging the institutions, but a body is needed to agree on the parameters to charge on.

CESNET federation Czech Republic – Milan reported that a shib-federation is in the pilot phase in Czech Republic. The main issue seems to have to do with the policy, in what concerns its preparation and the acceptance by the institutions. Milan said this task is taking longer than initially envisaged.

SWAMi (Sweden) – Torbjörn reported that the federation is growing too slowly, due to the campus inability to describe their IdM. Campuses do not seem to know why they issue identities, what for and so on. Other people see this as a common issue for other federation.

As the government is moving forward with the project about eID, the government's activities might push the deployment of federations.

WAYF (Denmark) – David Simonsen reported that the WAYF architecture has been accepted by institutions and SPs (some of which big). WAYF operate a centralised federation. Institutions are re-using federations technology internally. The legal side of the federation has been agreed, so contracts with institutions can be signed.

Because WAYF operated a central sytem, measures had to be taken when the system went down. The problem has been solved adding redundancy (with 3 sites).

The following hot issues have been identified:

(i) operating the federation in a professional way. For instance audit procedures should be introduced to ensure compliancy with the policy.
(ii) Scope of the federation: WAYF include all level of education and the plan is to also include citizens.
(iii) Hiding the WAYF functionalities behind IdPs or SPs. The way to deal with the InfoCard model has not been defined yet.

HAKA (Finland) – Mikael reported that small institutions do not have resources to operate a shib-Id. For small institutions it would be convenient to buy this as a service, but no providers are available for this.
Current hot issues for HAKA were identified as follows:

(i) audit of federation operations. A model to audit IdPs and SPs has been defined, but the implementation of the audit procedures is still an issue.
(ii) integration with Oracle and Novell IdPs (but this raises lots of issues).

Andrew said generally speaking there are two main ways to conduct audits. In the simpler case the IdPs can prepare a list stating to what procedures they comply; in the more complex scenario audit are conducted against an external standard.

IGTF have a lot of experience about audit. In Asia for instance the Asia PMA members go and audit each other site using government guidelines. In US the government has asked Liberty Alliance to come up with guidelines for federation operators. In the EU PMA, CA operators are requested to do a self-auditing.

Kalmar (Nordic countries) – A memorandum of understanding has been agreed between Finland, Norway and Denmark. Sweden will join later. Full metadata are exchanged. David and Mikael will send the agreement. Most of the discussion was about how binding the agreement is.
Action: metadata to discuss more.

SWITCHAAi (SWITCH) - Thomas reported that the deployment of federation is moving rapidly. New services are coming along and many universities want to move away from LDAP access to applications. SWITCH have set-up a dedicated PKI to sign metadata, with the key stored securely. Shib 2.1 is able to validate keys and CRLS.

The following hot issues were identified:

(i) extending the federation beyond higher education. Especially with the inter-federation use-cases coming along.
(ii) Model to recover costs to operate the federation (approximately 2FTEs are required) especially in the case in which the federation would expand beyond higher education.

DFN-AAi (Germany) – Juergen reported that international scientific publishers have joined the federation and that eLearning SPs are about to join.

The deployment of federation is being slower than planned due to the fact that IdMs at universities are not very good.

The hot issue for DFN concerns DFN-PKI is: short leaved certificates and LoAs.

UKfederation (UK) –
Andrew reported that the penetration of federation is rather high in UK, with 93 service offered and lots of interest from other sectors.

The federation still operates like a pilot, due to the fact that governance issues have not been addressed yet.

The hot issues for UKfederation are related to:

(i) getting people to use the privacy enhancing technology of the federation
(ii) looking for use cases for inter-federations. The obvious one would be allow for shared services for NRENs, such as shared light-paths, shared MCU etc.

Andrew invited this group to prepare a paper to collect these use cases.

Action: The group to define on paper use-cases for cross-federation.

ACONetAAI (Austria) – An ACONet federation exists since recently and it covers 70% of universities.
To date the federations is very much a pilot and no policies have been agreed.

The hot issues for ACONet are:

(i) defining policies to rule participations of institutions that do not belong to the;
(ii) government's federation is non-SAML based and this will create problems when interoperating with.

InCommon I2 (US) – On the positive side, Ken reported that federal applications are becoming available and are part of InCommon.
Ken identified the following issues:

(i) InCommon is not SAML2 at the moment;
(ii) many different federations going to InCommon, which want to join. InCommon does not SAML2 yet.

Ken also reported that NIST 800-63 is undergoing some revisions and that the R&E has emerged as a key community.

EsNet – G: esnet joined Incommon and they are doing also OpenId. Auditing process very thorough according to NESC procedures (??). B: pki federation has scaling problem.

CRU- Push from government to get federations working together. Federations are being used. B: Relying on global metadata for local issues has created problem. HI: migration of federation. Finding an automatic way to get the attributes out of IdPs as most of the IdPs are not providing attributes in the right way.

Hungary – Mostly pilot, using SAML2.

Canada – G: moving from a pilot to production. On the shib side is going well, eduroam is doing v well. F: Dreamspark moved from one team to another and they tested against the CA federation. Verification environment is needed. HI: legal documents, bringing school on, charging institutions (2000 $ to join).

SURFnet – G: more institutions joining and they are dealing with commercial vendors like Sun, Novell. Sharepoint connected to the federation.

Japan – G: trail stage. HI: no key applications, so it is difficult to promote. Intra-university authN is accepted now, but this is not enough for inter-federation cases.

3. Metadata session

Most of the educational federation are preparing to migrate to SAML2. A mix SAML1-SAML2 is to be expected for some time, due to the fact that for instance not all SPs are SAML2-ready yet.
Vic said that simpleSAMLphp helps in bridging SAML1 and SAML2.

A discussion followed concerning the inter-federation scenario and the technology to use. There seems to be consensus on using SAML2 for inter-federations.

Some of the attendees asked whether technical inter-federation issues, such as metadata sharing and SAML2 migrations, should be handled. REFEDs should address, and has been in fact conceived for this, policy and federation operational practises, therefore all technical discussion should take place in EMC2.
It was also stressed that work in this area will be undertaken within GN3 and therefore duplication of work between GN and other groups, such as EMC2 should be avoided.

Attributes - SCHAC seems to have reached a good maturity stage, however need for new attributes might appear at any moment. A discussion followed to agree on the process to follow to discuss new attributes or to review those in the SCHAC schema.
To ease the introduction of new attributes, SCHAC has an experimental branche, where tests can take place. Once the tests are finalised the new attributes are moved to the production branch and their OID are changed.

The work on SCHAC is part of the EMC2 work item called Directory schema, which is led by

Victoriano.

Typically whenever the need for a new attribute or the need for a change to current SCHAC attributes arise, Victoriano, as SCHAC leader, or Licia are approached. A discussion about the specific attribute takes place on the schac list (schac@terena.org).
If there is sufficient consensus on the SCHAC list, then the new attributes are added to the SCHAC experimental branches. Once the test is finalised the attributes are moved to the production branch and their OID is changed.

During the EMC2 meetings, Victoriano normally reports on the progresses related to SCHAC.

Thomas said that if a new attribute is needed then it should be presented both at TF-EMC2 to report about SCHAC technical work and at REFEDs meetings for discussion. The usage of the attribute within a federation concerns policies, and therefore REFEDs would be the appropriate place to address this issue.

It was also suggested that REFEDs could agree on the meaning of key attributes within a federation. An example would be the ePPN attribute. Victoriano said that an URNreg would address this purpose.

Action: Licia to update the websites to make the request process to change/add new attributes to SCHAC more transparent.
Action: Ken to ask MACE to provide with a user-friendly explanation eduPerson attributes.

4. SAML Metadata Signing Policy and Aggregation Practice Statement Framework (SMAPS)

Viviani presented the proposal for a SAML Metadata Aggregation Practice Statement (SMAPS) and for SAML Metadata Signing Policy (SMSP). SMAPS and SMSP would be the equivalent of a CPS and CP for PKI. SMAPS for instance would provide information about how the metadata aggregation is created and on who created the metadata aggregation.

SMSP would provide information on why the metadata aggregation was created and on what the metadata aggregation should be used for.

Especially in the infer-federation scenarios, having these types of documents would help assessing whether two or more federations are compatible and till what extent.

Victoriano and other also pointed out that a standardised contract for joining federations is also needed.

Viviani said that if there were sufficient interest in these topics, it would be good to address the following issues:

(i) Create a SAML equivalent of the RFC 3647;
(ii) Create a SAML metadata aggregation best practices guide;
(iii) Prepare a SAML auditor's framework, if federations decided to assess each other on the IGTF model.

Action: Licia to agree with Viviani on how to proceed about SMAPS and SMSP.

5. Art 29 and legal issues

Andrew provided an overview on Federated Identity and Data Protection Law, under the European Personal Data Directive (95/46/EC).

Andrew also reported on the usage of pseudonymous identifier, such as ePTID (eduPersonTargetedID) and IP addresses. In the case of identifiers like ePTID, they allow a service to recognise a user on a return visit, but they should not disclosure the user's identity. In this case it is therefore unclear whether these type of identifiers are to be considered personal data.

In the case of identifiers like IP addresses things change. According to the Article 29 Working Party's Opinion 4/2007, IP addresses are able to link directly to a user and therefore they should be treated as personal data, at least in the case of ISPs and IdPs.

However Andrew said that the laws in this area are particularly unclear, and national laws might apply, which vary between different European countries. Furthermore the Art 29 Working Party rules cannot be enforced, as they are operate mainly as an advisory committee.

In case of misuse, SPs should notify the IdPs, which should deal with each specific case.

Things might be handled in a different way in the case in which users would be in the position to consent on the type of information the IdPs transfer to the SPs.

Andrew's talk raised lots of interest from the attendees. Because Andrew mainly assessed the European scenario, Ken agreed to collect use cases from the US perspective.

For more information about this please refer to:
http://www.terena.org/activities/refeds/data-protection.html

Action: Ken to develop use cases from the US perspective.
Action: Mikael reported on the Finnish law to require strong authN.

6. REFEDs Roadmap

A discussion followed to agree on a REFEDs roadmap.

Ken presented a list of topics, which ought to be addressed in inter-federation scenarios. The aim was to agreeing on which group (REFEDs, Liberty Alliance, others) would be the most suitable to work on each of the topics.
The discussion led to the following agreements:

- Learning the business of federations (business models, governance structures, membership models, etc) and sharing that knowledge - **REFEDs**

- Coordination of interfederation basic technical approaches (from InfoCard and attribute management strategies to metadata tagging and services to, gasp, monitoring and diagnostics) **TF-EMC2**
- Coordination of interfederation basic policy issues (from overlapping or competing members to common policy frameworks to legal structures between federations, orphanages) - **REFEDs**
- Application enablement, from DKIM to video - **TF-EMC2**
- Federated operator standards, best practices, audits, etc. - **REFEDs**
- Support of virtual organizations in science, humanities, etc.- **REFEDs**
- eGov Interactions - **Liberty Alliance (LA)**
- LOA profiles - **REFEDs +LA**
- Common membership agreement formats - **REFEDs**
- Standardized member POP - **REFEDs**
- Outreach of model to other vertical sectors (eg. Medical, Telecomm and ISP's) - **LA**
- Outreach of R&E feds to other emerging national feds - **REFEDs** mainly in what concerns national liaisons
- Short-term multi-fed metadata - **REFEDs + Internet2**
- Long-term solutions to dynamic metadata, etc. – **TF-EMC2**
- Effective attribute standards/mapping processes - **REFEDs for the policy implications+ TF-EMCs for the technical implementation**
- Coordination of attributes ->English in uApprove, Autograph, InfoCard, etc. - **REFEDs for the policy implications+ TF-EMCs for the technical implementation**
- Convening and hosting REfeds - TERENA

Action: Licia to circulate a roadmap to the list.

7. REFEDs Next Meeting

The next REFEDs meeting will take place on Sunday 7 June in Malaga, during the TERENA Networking Conference.

Action List

Reference	**Who**	**Action**	**Status**
05122008-01	All	To define on paper use-cases for cross-federation.	
05122008-02	Licia	To update the websites to make the request process to change/add new attributes to SCHAC more transparent.	Done
05122008-03	Ken	To ask MACE for eduPerson attributes user-friendly explanation.	
05122008-04	Licia Viviani	To on how to proceed about SMAPS and SMSP.	Ongoing
05122008-05	Ken	Ken to develop use cases from the US perspective on data protection.	
05122008-06	Andrew	To prepare documents on data protections	Done
05122008-06	Mikael	To reported on the Finnish law to require strong authN.	
05122008-07	Licia	To circulate a roadmap to the list. Draft document on-line at: http://www.terena.org/activities/refeds/activities.html	Done

List of Participants

First Name	**Last Name**	**Affiliation**
Kristof	Bajnok	NIIF / Hungarnet
Andrew	Cormack	JANET(UK)
Licia	Florio	TERENA
Victoriano	Giralt	University of Malaga
David	Groep	Nikhef (IGTF)
Mehdi	Hached	Renater
Jens	Haeusser	University of British Columbia / Canadian Access Federation
Nicole	Harris	JISC
Michael	Helm	ESnet
Bob	Hulsebosch	Telematica Instituut
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
Patricia	McMillan	The University of Queensland (AAF)
Yasuo	Okabe	Kyoto University
Viviani	Paz	AusCERT
Remco	Poortinga van Wijnen	SURFnet
Juergen	Rauschenbach	DFN-Verein
Alex	Reid	AARNet
Olivier	Salaün	CRU
Peter	Schober	University of Vienna / ACOnet
Matthew	Shears	Internet Society
David	Simonsen	WAYF - Where Are You From
Milan	Sova	CESNET
Eefje	van der Harst	SURFnet BV
Joost	van Dijk	SURFnet
Karel	Vietsch	TERENA
Torbjörn	Wiberg	Umeå universitet/SWAMI
Klaas	Wierenga	Cisco Systems